



STONEGATE 5.3

SMC INSTALLATION GUIDE

STONEGATE MANAGEMENT CENTER

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 3

Using StoneGate Documentation	7
How to Use This Guide	8
Typographical Conventions	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

CHAPTER 4

Planning the Management Center Installation . .	11
StoneGate System Architecture	12
Overview to the Installation Procedure	13
Important to Know Before Installation	13
Supported Platforms	13
Date and Time Settings	13
Hosts File	13
Obtaining Installation Files	14
Downloading the Installation Files	14
Checking File Integrity	14
Creating the Installation CD-ROM	14
Obtaining License Files	15

INSTALLING THE MANAGEMENT CENTER

CHAPTER 5

Installing the Management Center	19
Getting Started with Management Center Installation	20
Installing on Linux	20
Configuration Overview	20
Installing Management Center Components . . .	21
Installing a Management Server	23
Installing a Log Server	24
Installing a Web Portal Server	25
Installing an Authentication Server	26

Installing in Demo Mode	27
Finishing the Installation	28
Starting the Management Center After Installation	29
Starting the Management Server	29
Starting the Management Client	29
Logging in to the Management Center	30
Accepting the Management Server Certificate	30
Installing Licenses	31
Binding POL-Based Licenses to Servers	32
Starting the Log Server and Web Portal Server	33
Starting Servers Manually	33
If the Log Server or Web Portal Server Fails to Start	34
Generating Server Certificates	34
After the Management Center is Installed	36
Configuring Secondary Management Servers . .	37
Overview	37
Installing a License for a Secondary Management Server	37
Installing a Secondary Management Server . .	37
Configuring Log Servers for Backup Management Servers	40
Applying the Authentication Server Configuration	40
Non-Graphical Installation	41

CHAPTER 6

Distributing Management Clients through Web Start	43
Getting Started with Web Start Distribution . . .	44
Distributing Clients from the SMC Servers	44
Distributing Clients from a Separate Server . . .	45
Accessing the Web Start Clients	46

CHAPTER 7

Configuring NAT Addresses for StoneGate Components	47
Configuration Overview	48
Configuration Overview	49
Defining Locations	49
Adding SMC Server Contact Addresses	51
Setting the Management Client's Location	53

MAINTENANCE

CHAPTER 8
Upgrading 57

Getting Started with Upgrading the Management Center 58
Configuration Overview 58
Upgrading Licenses 59
Upgrading Licenses Under One Proof Code 59
Upgrading Licenses Under Multiple Proof Codes 60
Installing Licenses 61
Upgrading the Management Center 62

CHAPTER 9
Uninstalling the Management Center 67

Overview to Uninstalling the Management Center 68
Uninstalling in Windows 68
Uninstalling in Linux 69

APPENDICES

APPENDIX A
Command Line Tools 73

Management Center Commands 74
Engine Commands 83
Server Pool Monitoring Agent Commands 89

APPENDIX B
Default Communication Ports. 91

Management Center Ports 92
Firewall/VPN Engine Ports 94
IPS Engine Ports 98

Index. 101

INTRODUCTION

In this section:

[Using StoneGate Documentation](#) - 7

[Planning the Management Center Installation](#) - 11

CHAPTER 3

USING STONEGATE DOCUMENTATION

Welcome to Stonesoft's StoneGate™ Management Center. This chapter describes how to use the *StoneGate Management Center 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

The *Management Center Installation Guide* is intended for the administrators who install the StoneGate Management Center. It describes the 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 3.1 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 3.2 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 system requirements for running the StoneGate Management Center can be found in the Management Center [Release Notes](#) available at the Stonesoft 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.

CHAPTER 4

PLANNING THE MANAGEMENT CENTER INSTALLATION

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

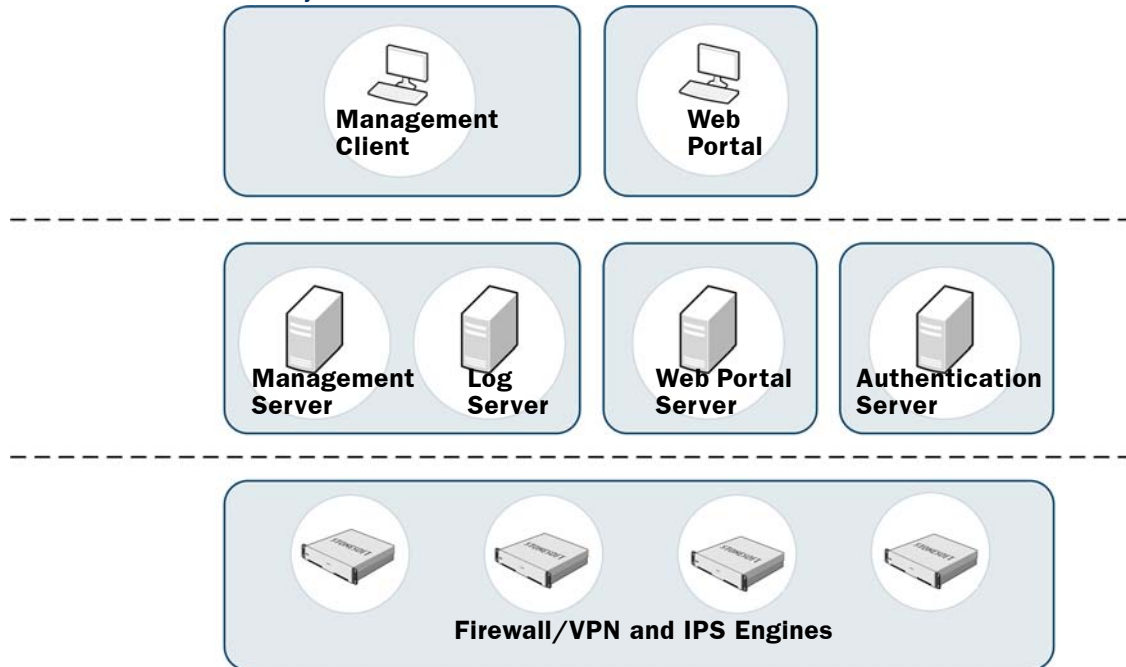
The following sections are included:

- ▶ [StoneGate System Architecture](#) (page 12)
- ▶ [Overview to the Installation Procedure](#) (page 13)
- ▶ [Important to Know Before Installation](#) (page 13)
- ▶ [Obtaining Installation Files](#) (page 14)
- ▶ [Obtaining License Files](#) (page 15)

StoneGate System Architecture

A StoneGate system consists of one or more firewall/VPN or IPS engines, the Management Center, and Management Client(s). The Management Server, Log Server, and one or more Management Clients are always included in the installation. The type and number of optional components and engines varies according to environment and depends on your licenses.

Illustration 4.1 StoneGate System Architecture



The Management Center consists of the following standard components:

- The Management Server.
- One or more Log Servers.

The Management Client is a single unified tool that is used for all configuration and monitoring tasks related to the whole StoneGate system. You can install an unlimited number of Management Clients.

Optionally, and for a separate license fee, you can also have:

- One or more backup Management Servers.
- One or more Web Portal Servers for Web Portal users.
- One Authentication Server with up to two nodes for end-user authentication.

The Management Center components can be installed separately on different machines or on the same machine, depending on your requirements.

The Management Center can manage several StoneGate firewalls and IPS Sensors and Analyzers. See the *Management Center Reference Guide*, *Firewall/VPN Reference Guide*, and the *IPS Reference Guide* for general information on the Management Center, firewalls, and IPS engines.

Overview to the Installation Procedure

1. Install and configure the Management Center and a Management Client. This is explained in [Installing the Management Center](#) (page 19).
2. (Optional) Set up Management Client distribution through Java Web Start for automatic installation and upgrade. This is explained in [Distributing Management Clients through Web Start](#) (page 43).
3. If network address translation (NAT) is applied to communications between system components, define Contact Addresses. This is explained in [Configuring NAT Addresses for StoneGate Components](#) (page 47).

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

Once you have installed the Management Center components and the Management Client, and configured the communications between the system components, you can proceed to configuring and installing the firewall/VPN and IPS engines. See the *Firewall/VPN Installation Guide*, and the *IPS Installation Guide* for information on installing the engines.

Important to Know Before Installation

Consult the *Management Center Reference Guide*, the *Firewall/VPN Reference Guide*, or the *IPS Reference Guide* if you need more detailed background information on the operation of StoneGate than what is offered in this chapter.

Supported Platforms

The *Release Notes* list the basic requirements for installation. For information on supported and certified hardware, search for the version-specific *Hardware Requirements* in the technical documentation search at <http://www.stonesoft.com/en/support/>.

Date and Time Settings

Make sure that the Date, Time, and Time zone settings are correct on any computer you will use as a platform for any Management Center component, including the workstations used for the Management Client. 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. StoneGate always uses UTC internally.

Hosts File

Due to a restriction of the Java platform, the Management Server and Log Server hostnames must be resolvable on the computer running the Management Client (even if running on the same computer as the servers) to ensure good performance.

To ensure that the hostnames can be resolved, you can add the IP address-hostname pairs into the local hosts file on the client computer:

- In Linux: `/etc/hosts`
- In Windows: `\WINNT\system32\drivers\etc\hosts`

Obtaining Installation Files

Depending on your order, you may have received ready-made installation CD-ROMs for the Management Center. Otherwise, download the installation files from the Stonesoft website.

Downloading the Installation Files

▼ To download the installation files

1. Go to the Stonesoft Downloads page at <https://my.stonesoft.com/download>.
2. Enter your license code or log in using an existing user account.
3. Download the `.iso` image files or the installation `.zip` file.

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.

What's Next?

- ▶ If you downloaded the installation files as a `.zip` file, unzip the contents to the installation location and proceed to creating [Obtaining License Files](#) (page 15).
- ▶ Otherwise, continue by [Creating the Installation CD-ROM](#).

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.

Obtaining License Files

You must generate license files and install them after the installation to bring your system fully operational. Each Management Server, Log Server, Web Portal Server, and Authentication Server must have its own license. However, a Management Server license that includes the high availability features is a combined license for all Management Servers and must list the IP addresses of all the Management Servers. The Authentication Server license allows a maximum of 5 RADIUS clients (excluding other StoneGate components) to use the authentication methods provided by the Authentication Server, and a maximum of 50 named users for user linking in the Authentication Server's user database.

You must also generate and install licenses for any firewall, IPS and SSL VPN engines to be able to make them operational.

For more information on licenses, see the *Administrator's Guide*.

▼ To generate a new license

1. Go to the License Center at www.stonesoft.com/license/.
2. Enter the required code (proof-of-license or proof-of-serial number) in the correct field and click **Submit**. The license page opens.
3. Click **Register**. The license generation page opens.
4. Enter the IP addresses of the Management Center components you want to use.
5. Enter the Management Server's proof-of-license code 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. Later, this information is shown in the Management Client for all licenses imported into the system.
6. Click **Submit Request**. The license file is sent to you in a moment. It will also become available for download at the license page.

All licenses include a maximum version on which they are valid. Automatic upgrade and installation of licenses is enabled by default. If you have disabled automatic license upgrades, you need to upgrade the licenses when you upgrade to a new major release of the software.

INSTALLING THE MANAGEMENT CENTER

In this section:

[Installing the Management Center](#) - 19

[Distributing Management Clients through Web Start](#) - 43

[Configuring NAT Addresses for StoneGate Components](#) - 47

CHAPTER 5

INSTALLING THE MANAGEMENT CENTER

This chapter instructs how to install the StoneGate Management Center on Windows and Linux platforms.

The following sections are included:

- ▶ [Getting Started with Management Center Installation](#) (page 20)
- ▶ [Installing Management Center Components](#) (page 21)
- ▶ [Starting the Management Center After Installation](#) (page 29)
- ▶ [After the Management Center is Installed](#) (page 36)
- ▶ [Configuring Secondary Management Servers](#) (page 37)
- ▶ [Non-Graphical Installation](#) (page 41)

Getting Started with Management Center Installation

You are ready to start the Management Center installation when you have obtained and verified the installation files. See [Obtaining Installation Files](#) (page 14) for more information on these tasks.



Caution – Make sure that the operating system version you plan to install on is supported. The supported platforms for running the Management Center are listed in the Release Notes of the Management Center.

Log in to the system where you are installing the Management Center with the correct administrative rights. In Windows, you must log in with administrator rights. In Linux you must log in as root.

During the installation, certificates can be generated for the server components. The certificates are needed for authentication in establishing the secure encrypted communication channel between system components.

We recommend installing a Management Client on the system on which you install the Management Server. After this, further Management Clients can be installed locally by running the Management Center installer or be made available through Java Web Start (see [Distributing Management Clients through Web Start](#) (page 43)), which eliminates the need to update all Management Clients individually at each version upgrade. The Management Client has no configurable parameters.

Installing on Linux

The installation creates sgadmin user and group accounts. If there is a pre-existing sgadmin account, the installation fails. All the shell scripts are owned by sgadmin and can be executed either by root or the sgadmin user. The shell scripts are executed with sgadmin privileges. After the installation, the sgadmin account is disabled. The sgadmin account is deleted at uninstallation.

Configuration Overview

1. Install the Management Center. See [Installing Management Center Components](#) (page 21). If you are installing on separate servers, install the Management Server as the first component.
2. Start the Management Center. See [Starting the Management Center After Installation](#) (page 29).
3. (*Optional*) Install the secondary Management Server(s). See [Configuring Secondary Management Servers](#) (page 37).



Caution – Do not install the Management Center on a StoneGate appliance.

Installing Management Center Components

For obtaining, verifying, and preparing the installation files, see [Obtaining Installation Files](#) (page 14).

This section guides you through a Management Center installation in a graphical user interface. For command line installation in Linux, see [Non-Graphical Installation](#) (page 41).

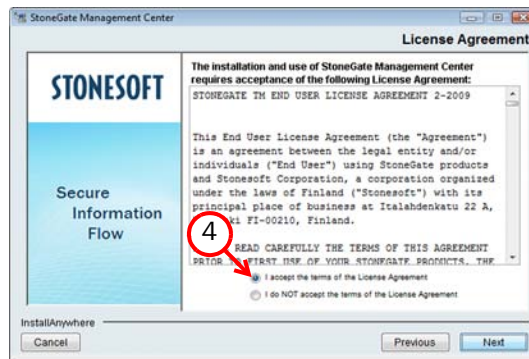
▼ To start the Installation

1. If you are installing from a .zip file, unzip the file.
2. Start the installation:
 - On Windows, run the file `\StoneGate_SW_Installer\Windows\setup.exe`
 - On Linux, run the file `/StoneGate_SW_Installer/Linux/setup.sh`

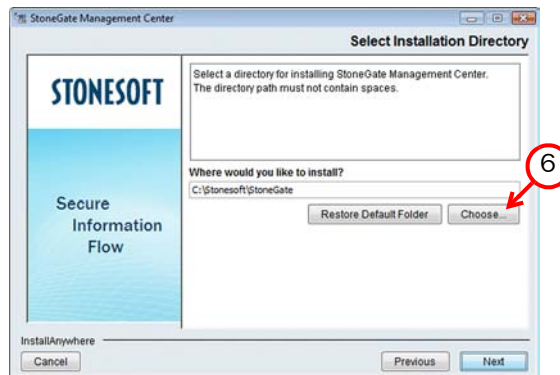


Note – If you are installing from CD-ROM in Linux, and the CD-ROM is not automatically mounted, mount the CD-ROM with “`mount /dev/cdrom /mnt/cdrom`”.

3. When the Installation Wizard shows the Introduction screen, click **Next** to start the installation. The License Agreement appears.
 - You can click **Cancel** at any time to exit the installer.
 - You can click **Previous** at any time to go back.



4. Indicate that you agree to the license agreement.
5. Click **Next**.



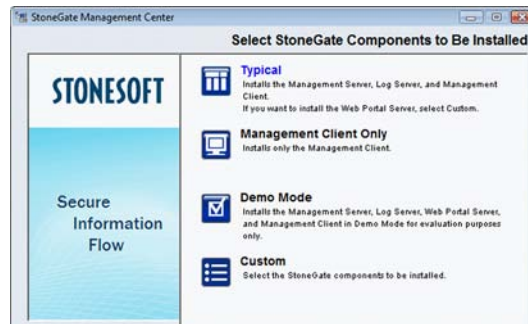
6. (Optional) Click **Choose** to browse for a different installation folder. This folder is for the application, and a Log Server can have a separate data storage location.

7. Click **Next**.



8. Select the settings for creating shortcuts. These shortcuts can be used to manually start components and to run some maintenance tasks.

9. Click **Next**.



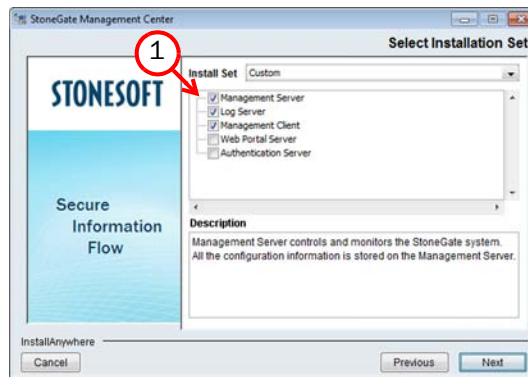
10. Click one of the icons to select the installation type:

- **Typical** installs all Management Center components except the Web Portal Server.
- **Management Client Only** installation is meant for administrators' workstations.
- **Demo Mode** installation is meant for evaluating StoneGate in a simulated environment.
- **Custom** installation allows you to select components one by one.

11. Click **Next**.

▼ To select components for the Custom installation

1. Select the components that you want to install.



2. Click **Next**.



Note – Make sure you have a license for any separately licensed components before installing them. The Web Portal Server and Authentication Server are not included in standard Management Center licenses.

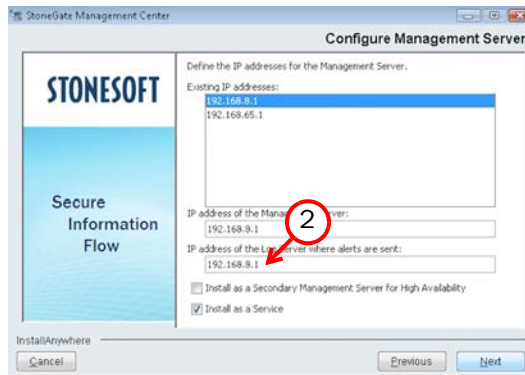
What's Next?

- ▶ For Demo Mode installations, proceed to [Installing in Demo Mode](#) (page 27).
- ▶ Otherwise, proceed to the next applicable section according to the components you are installing:
 - [Installing a Management Server](#).
 - [Installing a Log Server](#) (page 24).
 - [Installing a Web Portal Server](#) (page 25).
 - [Installing an Authentication Server](#) (page 26).

Installing a Management Server

▼ To configure the Management Server installation

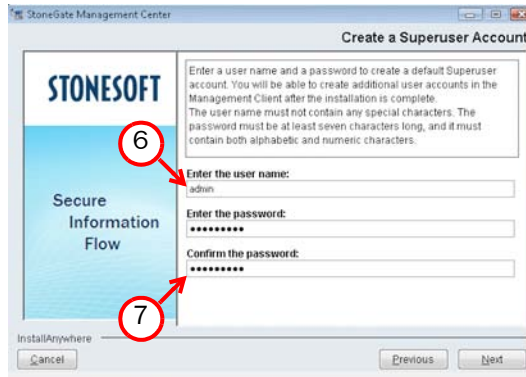
1. Enter or select the Management Server's IP address. The Management Server's license must be generated with this IP address as the binding.



2. Enter the IP address of the Log Server to which this Management Server sends its alerts.
3. (Optional) To install a backup server, select **Install as a Secondary Management Server for High Availability** and see [Installing a Secondary Management Server](#) (page 37).
4. Leave **Install as a Service** selected to make the Management Server start automatically.
5. Click **Next**. You are prompted to create a superuser account.



Note – This is the only account that can log in after the installation.



6. Type in a **User Name**.
7. Enter and confirm the **Password**.
8. Click **Next**.

What's Next?

- ▶ Proceed to the next applicable section according to the components you are installing:
 - [Installing a Log Server](#).
 - [Installing a Web Portal Server](#) (page 25).
 - [Installing an Authentication Server](#) (page 26).
 - [Finishing the Installation](#) (page 28).

Installing a Log Server

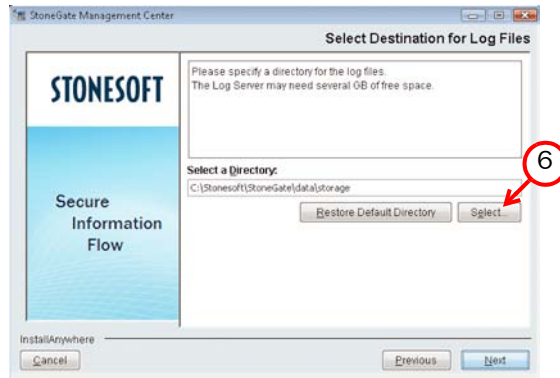
▼ To configure the Log Server installation

1. Enter or select the Log Server's IP address. If IP address binding is used, the Log Server's license must be generated with this IP address as the binding.



2. Enter the IP address of the Management Server that controls this Log Server.
3. If the components are installed on different machines and the Management Server is not reachable at the moment, deselect **Certify the Log Server during the Installation** to avoid connection attempts after installation. Certifying is mandatory for running the Log Server.

4. Leave **Install as a Service** selected to make the Log Server start automatically.
5. Click **Next**.



6. (Optional) Click **Select** to browse for a different storage folder for log data. Remote locations are not suitable for active storage, since quick and reliable access is required.
7. Click **Next**.

What's Next?

- ▶ Proceed to the next applicable section according to the components you are installing:
 - [Installing a Web Portal Server](#).
 - [Installing an Authentication Server](#) (page 26).
 - [Finishing the Installation](#) (page 28).

Installing a Web Portal Server



Note – Make sure you have a license for the Web Portal Server before installing it. The Web Portal Server is an optional component and is not included in standard Management Center licenses. You can use the Previous button to return to component selection.

▼ To configure the Web Portal Server installation

1. Enter or select the Web Portal Server's IP address. If IP address binding is used, the Web Portal Server's license must be generated with this IP address as the binding.



2. Type in the IP address for the Management Server that controls this Web Portal Server.

3. If the components are installed on different machines and the Web Portal Server is not reachable at the moment, deselect **Certify the Web Portal Server during the Installation** to avoid connection attempts after installation. Certifying is mandatory for running the Web Portal Server.
4. Leave **Install as a Service** selected to make the Web Portal Server start automatically.
5. Click **Next**.

What's Next?

- ▶ Proceed to the next applicable section according to the components you are installing:
 - [Installing an Authentication Server](#).
 - [Finishing the Installation](#) (page 28).

Installing an Authentication Server



Note – Make sure you have a license for the Authentication Server before installing it. The Authentication Server is an optional component and is not included in standard Management Center licenses. You can use the Previous button to return to component selection.

▼ To configure the Authentication Server installation

1. Enter or select the Authentication Server's IP address.



2. Enter or select the IP address of the Management Server that controls this Authentication Server.
3. If you are installing the components are installed on different machines and the Management Server is not reachable at the moment, deselect **Certify the Authentication Server during the Installation** to avoid connection attempts after installation. Certifying is mandatory for running the Authentication Server and for installing the second node of a cluster.
4. Leave **Install as a Service** selected to make the Authentication Server start automatically.
5. Click **Next**.

What's Next?

- ▶ Proceed to [Finishing the Installation](#) (page 28).

Installing in Demo Mode

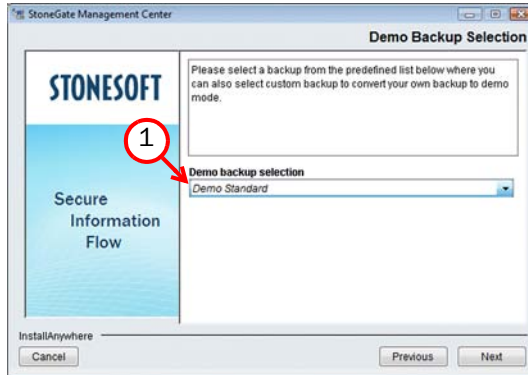
The Demo mode installation creates a simulated network environment for evaluation.



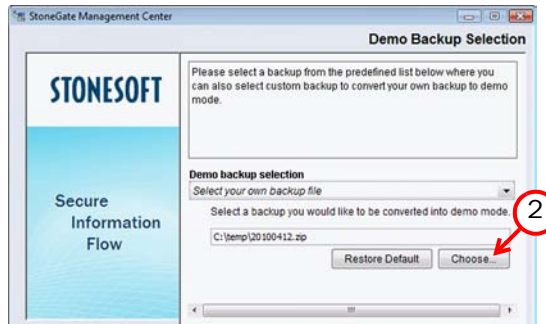
Note – Demo mode installation is for evaluation only. A Management Center in Demo mode cannot be used with any traffic inspection engines and cannot be upgraded.

▼ To install in Demo Mode

1. Select the type of demo to install:
 - Use a standard backup to simulate a preconfigured environment.
 - Select your own backup file to create the simulation based on your own backup.



2. (Custom backup file only) Click **Choose** and browse to the location of the backup file.



3. Click **Next**. The installation starts.
4. When the installation finishes, click **Next**.



- Click **Done** to close the installer. The Management Center starts up automatically in the background.

What's Next?

- ▶ The simulated environment is now ready for your testing. Proceed to [Logging in to the Management Center](#) (page 30).

Finishing the Installation



Caution – If you are installing any server components as a service on a Windows system, make sure the Services window is closed before you proceed.

▼ To finish the installation

- (64-bit architecture only) Select the running mode for the installation and click **Next**.
 - If the computer has less than 6000 MB of physical memory available, 32-bit mode is recommended.



- Check the displayed information.



- Click **Install** to install the selected components. This is the last chance to **Cancel** or make changes by clicking **Previous**.
- Depending on the options you selected, you may be prompted to generate certificates in the course of the installation. If this happens, see the section [To generate a certificate for a StoneGate server](#) (page 35).

5. Click **Done** to close the installer.



Note – If any Log Server, Web Portal Server, or Authentication Server certificate was not retrieved during the installation, a certificate must be retrieved manually before the server can be started. See [To manually certify a Server](#) (page 34).

Starting the Management Center After Installation

Proceed through the listed sections in order to start the Management Center for the first time:

1. [Starting the Management Server](#).
2. [Starting the Management Client](#).
3. [Logging in to the Management Center](#) (page 30).
4. [Installing Licenses](#) (page 31).
5. [Binding POL-Based Licenses to Servers](#) (page 32).
6. [Starting the Log Server and Web Portal Server](#) (page 33).

Starting the Management Server

If the Management Server has been installed as a service, it should start automatically both after the installation and during the operating system boot process. In Windows, the **StoneGate Management Server** service is controlled in the Services window, which can be found in the Windows Control Panel under the Administrative Tools category.

If the Management Server is installed as a service and has successfully started, proceed to [Starting the Management Client](#). Otherwise, start the Management Server manually as explained below.

▼ To start a Management Server that is not installed as a service

- In Windows, use the shortcut icon in the location you selected during installation or run the script `<installation directory>/bin/sgStartMgtSrv.bat`.
- In Linux, run the script `<installation directory>/bin/sgStartMgtSrv.sh`.

Starting the Management Client

▼ To start a locally-installed Management Client

- In Windows, use the shortcut icon in the location you selected during installation or run the script `<installation directory>/bin/sgClient.bat`.
- In Linux, run the script `<installation directory>/bin/sgClient.sh`. A graphical environment is needed for the Management Client.

What's Next?

- ▶ [Logging in to the Management Center](#) (page 30).

Logging in to the Management Center

The Management Client connects to the Management Server and to Log Servers. See [Default Communication Ports](#) (page 91) for a list of the ports used.

In **Demo Mode**, use the following credentials to log in to one of the default scenarios:

- **User Name:** demo
- **Password:** demo
- **Server Address:** 127.0.0.1

▼ To log in to the Management Center

1. Type in the user name and password for the Administrator you defined during the Management Server installation.
2. Type in the Management Server's IP address or DNS name.
3. Leave **Remember Server Address** selected if you want the Management Client to add the address permanently in the Server Address list.



4. Click **Login**.

If you connect to the Management Server from an external network, the Management Server's IP address may be translated using NAT.

Tip – You can access the *Online Help* system in the Login window or any other window in the Management Client by pressing the **F1** key.

Accepting the Management Server Certificate

A certificate dialog is displayed when the Management Client contacts any Management Server for the first time. As a precaution, you can ensure that the communication really is with your Management Server by checking the Certificate Authority fingerprint as explained below.

▼ To check the Certificate Authority fingerprint

1. View the Management Server fingerprint on the Management Server:
 - In Windows, use the shortcut icon in the location you selected during installation (default: **Start**→**Programs**→**StoneGate**→**Show Fingerprint**) or run the script `<installation directory>/bin/sgShowFingerprint.bat`.
 - In Linux, run the script `<installation directory>/bin/sgShowFingerprint.sh`.
2. If the fingerprint matches, click **Accept**. The Management Client loads and opens.

Installing Licenses

The Management Center servers require licenses to become operational. To obtain licenses, see [Obtaining License Files](#) (page 15). You can install licenses even before the components are installed.

With no valid Management Server license, a notification is shown when you log in. If the message appears after licensing, make sure the licensed IP address is correct and active on the server when the Management Server service starts up.

▼ To install licenses through the License Information message

- Click **Continue** and select the license file(s) in the dialog that opens.



What's Next?

- ▶ If the message is not shown, install the licenses as explained below.
- ▶ Otherwise, proceed to the section [To check that the licenses were installed correctly](#).

▼ To install licenses

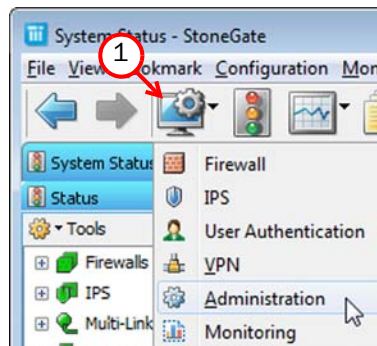
1. Select **File**→**System Tools**→**Install Licenses**.



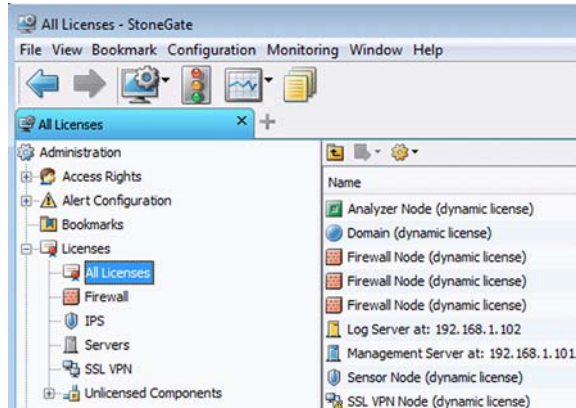
2. Import one or more license files in the dialog that opens.

▼ To check that the licenses were installed correctly

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



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



3. Check that all licenses you imported are listed here.

What's Next?

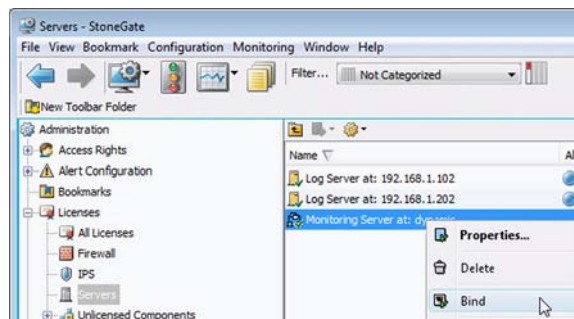
- ▶ If you have Log Server or Web Portal Server licenses that are bound to the Management Server's POL code, proceed to [Binding POL-Based Licenses to Servers](#).
- ▶ Otherwise, continue by [Starting the Log Server and Web Portal Server](#) (page 33).

Binding POL-Based Licenses to Servers

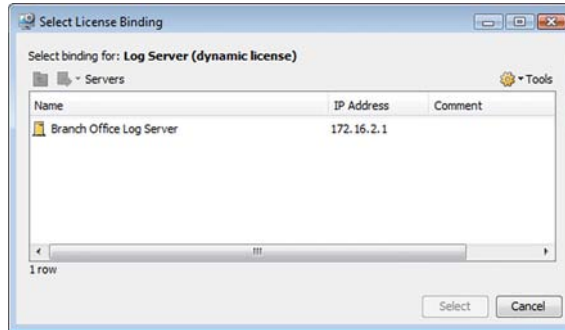
You must bind management-bound Log Server and Web Portal Server licenses to specific Log or Web Portal Servers. The licenses contain no IP address information to automatically bind them.

▼ To bind a management-bound license to a Log or Web Portal Server

1. Browse to **Administration**→**Licenses**→**Servers**. Installed licenses appear in the right panel.



2. Right-click a management-bound license (a license that states **Dynamic** in place of an IP address) and select **Bind**. The Select License Binding dialog opens.



3. Select the correct server from the list.
4. Click **Select**. The license is now bound to the selected Log or Web Portal Server element.

If you made a mistake, you can still right-click the license and select **Unbind**.



Note – The license is permanently bound to the Log or Web Portal Server when the server is started for the first time. Such licenses cannot be re-bound to some other Log or Web Portal Server without re-licensing or deleting the Log or Web Portal Server element it is bound to. Until you do that, the unbound license is shown as Retained.

Starting the Log Server and Web Portal Server

If the Log Server and the Web Portal Server have been installed as a service, the servers are started automatically during the operating system boot process. However, if the operating system is rebooted and the servers do not yet have a license, you may need to start them as explained here.

- If you installed the Log Server or Web Portal Server as a service, you can start or stop the server manually in Windows through the Services window.
- In other cases, you can start the Log Server or Web Portal Server manually as explained in [Starting Servers Manually](#).

Starting Servers Manually

To start the Log Server or Web Portal Server manually, run the scripts in a console window. Read the console messages for information on the progress. Closing the console stops the service.

▼ To start the Log Server and Web Portal Server manually

1. Start the Log Server:
 - In Windows, use the shortcut icon in the location you selected during installation (default: **Start**→**Programs**→**StoneGate**→**Log Server**) or run the script `<installation directory>/bin/sgStartLogSrv.bat`.
 - In Linux, run the script `<installation directory>/bin/sgStartLogSrv.sh`.

2. If you have a Web Portal Server, start it in the same way:
 - In Windows, use the shortcut icon in the location you selected during installation (default: **Start**→**Programs**→**StoneGate**→**Web Portal Server**) or run the script `<installation directory>/bin/sgStartWebPortalServer.bat`.
 - In Linux, run the script `<installation directory>/bin/sgStartWebPortalServer.sh`.

What's Next?

- ▶ If you have started all servers successfully, proceed to [After the Management Center is Installed](#) (page 36).
- ▶ If you have trouble starting the server, see [If the Log Server or Web Portal Server Fails to Start](#).

If the Log Server or Web Portal Server Fails to Start

If the Log Server or Web Portal Server does not start automatically as a service.

1. Try starting the server manually as explained in the previous section to see if there is some error displayed on the console.
2. Check licenses are correctly bound to components as explained in [To check that the licenses were installed correctly](#) (page 31) and [To bind a management-bound license to a Log or Web Portal Server](#) (page 32).
3. Ensure that the server has a valid *certificate* for secure system communications. If there are certificate-related problems or problems you are not able to identify, try (re)generating the certificate as explained below.

Generating Server Certificates



Note – If the Management Server is not running, see [Starting the Management Server](#) (page 29).

▼ To manually certify a Server

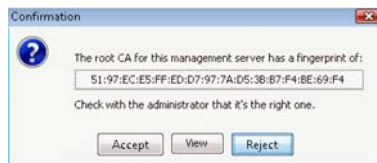
- In Windows, run the `<installation directory>/bin/sgCertifyLogSrv.bat` or the `<installation directory>/bin/sgCertifyWebPortalServer.bat` script depending on server type.
- In Linux, run the `<installation directory>/bin/sgCertifyLogSrv.sh` or the `<installation directory>/bin/sgCertifyWebPortalServer.sh` script depending on server type.

▼ To generate a certificate for a StoneGate server

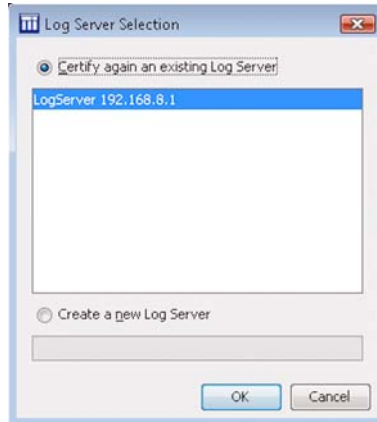
1. Enter the user name and password for the account you created during the Management Server installation (other accounts with unrestricted permissions can also be used).



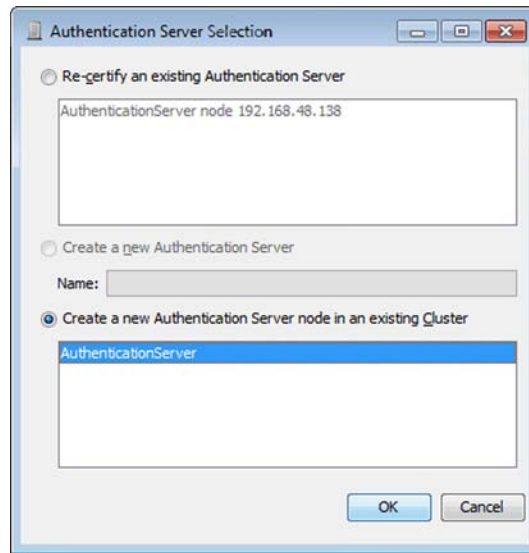
2. Click **Accept** to accept the certificate fingerprint of the Management Server's Certificate Authority. As a precaution, you can ensure that the communication really is with your Management Server as explained in [To check the Certificate Authority fingerprint](#) (page 30). The Log Server Selection or Web Portal Server Selection dialog opens.



3. (Log Server or Web Portal Server only) Identify the component:
 - If the correct server is listed, select it.
 - If the correct server is not listed, select **Create a New Log Server** or **Create a ne Web Portal Server** and enter a **Name**. This name is shown in the Management Client.



4. (Authentication Server only) Identify the component:
- If the correct server is listed, select it.
 - If the correct server is not listed, select **Create a New Authentication Server** and enter a **Name**. This name is shown in the Management Client.
 - If you are installing the second node of an existing Authentication Server, select **Create a new Authentication Server node in an existing cluster** and select the Authentication Server where you want to add the node.



5. Click **OK**.

What's Next?

- ▶ Start the Log Server or Web Portal Server as described in [Starting the Log Server and Web Portal Server](#) (page 33), then proceed to [After the Management Center is Installed](#).
- ▶ The Authentication Server installation is complete. Proceed to [After the Management Center is Installed](#).

After the Management Center is Installed

- If you want to install a secondary Management Server, proceed to [Configuring Secondary Management Servers](#) (page 37).
- If you want to allow administrators to install Management Clients through Web Start, continue to [Distributing Management Clients through Web Start](#) (page 43).
- If NAT is applied to communications between any system components, proceed to [Configuring NAT Addresses for StoneGate Components](#) (page 47).
- If you installed an Authentication Server, continue by [Applying the Authentication Server Configuration](#) (page 40).
- Otherwise, you are ready to configure the firewall and IPS element(s) in the Management Client. The elements must be configured before installing the physical engines. See the *Firewall/VPN Installation Guide* and the *IPS Installation Guide* for more information.

Configuring Secondary Management Servers

This section guides you through a secondary Management Center installation in a graphical user interface. For command line installation, see [Non-Graphical Installation](#) (page 41).



Caution – You must install and configure the Management Server that you want to use as the primary Management Server before installing secondary Management Server(s). See [Installing a Management Server](#) (page 23).

Only one Management Server at a time can be used for configuring and managing StoneGate. A secondary Management Server is only used as a backup for the primary Management Server. You can use one to four secondary Management Servers with one primary Management Server. The configuration data stored on the primary Management Server is automatically replicated to the secondary Management Servers.

Overview

1. If you have not yet installed a license for the secondary Management Server, install the license. See [Installing a License for a Secondary Management Server](#).
2. Install the secondary Management Server using the Installation Wizard. See [Installing a Secondary Management Server](#).
3. Add the IP addresses of all your Management Servers to the Log Server's configuration. See [Configuring Log Servers for Backup Management Servers](#) (page 40).

Installing a License for a Secondary Management Server

To use secondary Management Servers, you must have a special Management Server license that lists the IP addresses of all the Management Servers within the same SMC. You must install the license in the Management Client before installing the secondary Management Server(s).

If you do not yet have the license, generate the license at the Stonesoft website after receiving the Proof-of-License (see [Obtaining License Files](#) (page 15)), and then install the license as described in [Installing Licenses](#) (page 31).

Installing a Secondary Management Server

▼ To install a secondary Management Server

1. If you are installing from a .zip file, unzip the file and run **install.exe** on Windows or **setup.sh** on Linux. Alternatively, insert the StoneGate installation CD-ROM and run the setup executable:
 - On Windows, run `CD-ROM\StoneGate_SW_Installer\Windows\install.exe`
 - On Linux, run `CD-ROM/StoneGate_SW_Installer/Linux/setup.sh`



Note – If the CD-ROM is not automatically mounted in Linux, mount the CD-ROM with `mount /dev/cdrom /mnt/cdrom`.

2. Proceed according to the instructions in the Installation Wizard until you are prompted to select which components you want to install.

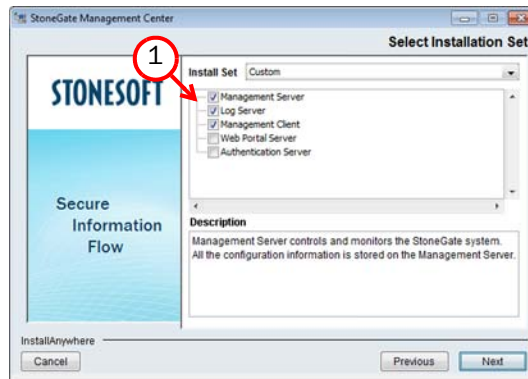
- If you also want to install a Log Server and a local Management Client on this computer, you can leave **Typical** selected. Otherwise, you must select **Custom**.



- Click **Next**.

▼ To select components for the Custom installation

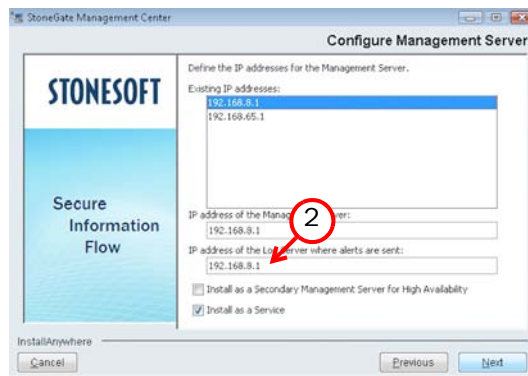
- Select the components that you want to install (select at least **Management Server**).



- Click **Next**.

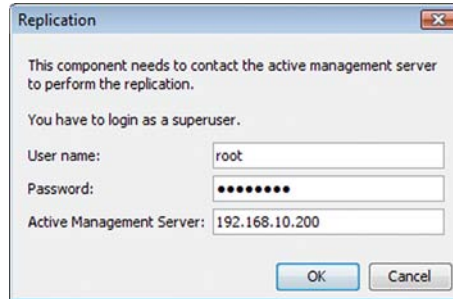
▼ To configure the secondary Management Server

- Enter or select the Management Server's IP address. The Management Server's license must be generated with this IP address as the binding.

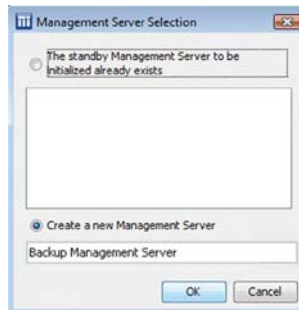


- Enter the IP address of the Log Server to which this Management Server sends its alerts.

3. Select **Install as a Secondary Management Server for High Availability**.
4. Leave **Install as a Service** selected to make the Management Server start automatically.
5. Click **Next**. After a while, a login prompt for Replication opens.



6. Enter the user name and the password for an unrestricted administrator account (such as the account you created during the installation of the primary Management Server).
7. Click **OK**. The Management Server Selection dialog opens.



8. Identify the component:
 - If the correct server is listed, select it.
 - If the correct server is not listed, select **Create a New Management Server** and type in a name. This name is shown in the Management Client.
9. Click **OK**. The databases are synchronized.

After successful database synchronization between the secondary Management Server and primary Management Server, the installation is complete. If the synchronization fails for some reason (such as a network connection problem), the secondary Management Server is not installed properly. Rerun the Installation Wizard as above.

Repeat the steps above as necessary to install other secondary Management Servers.

Configuring Log Servers for Backup Management Servers

For Log Servers to recognize secondary Management Servers, you must add the IP addresses of all the secondary Management Servers to the Log Servers' local configuration.

▼ To configure Management Server IP addresses on Log Servers

1. Open a command line on the Log Server computer.
2. Run the script `<installation_directory>/bin/sgChangeMgtIPOnLogSrv` and give the IP addresses of all Management Servers (including all previously installed Management Servers) separated with spaces.

Example `sgChangeMgtIPOnLogSrv 192.168.10.200 192.168.10.220`

The secondary Management Server configuration is now complete. If there is a firewall between the primary Management Server and the secondary Management Server(s), you must add rules that allow the communications between the servers when you define your firewall policy.

What's Next?

- ▶ If you want to allow administrators to install Management Clients through Web Start, continue to [Distributing Management Clients through Web Start](#) (page 43).
- ▶ If NAT is applied to communications between any system components, proceed to [Configuring NAT Addresses for StoneGate Components](#) (page 47).
- ▶ Otherwise, you are ready to configure the firewall and IPS element(s) in the Management Client. The elements must be configured before installing the physical engines. See the *Firewall/VPN Installation Guide* and the *IPS Installation Guide* for more information.

Applying the Authentication Server Configuration

To make the Authentication Server operational, you must apply the configuration.

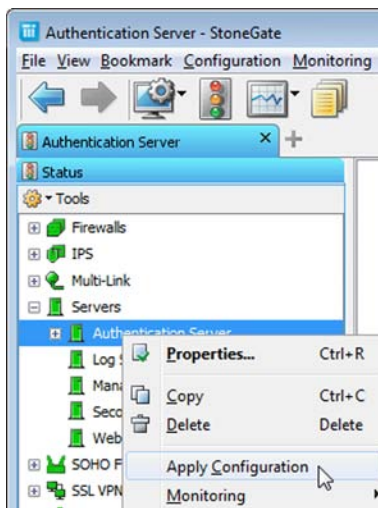


Note – If you are installing a cluster of Authentication Server nodes, apply the configuration only after creating and installing both nodes. Once the configuration has been applied to a single Authentication Server, the server cannot be converted into a cluster.

▼ To apply the Authentication Server configuration

1. Expand **Servers** in the System Status view.

2. Right-click **Authentication Server** and select **Apply Configuration**. A progress dialog opens.



3. Click **Close** when the operation finishes.

What's Next?

- ▶ Continue the configuration of the Authentication Server in the Management Client. See the *Administrator's Guide* or the *Management Client Online Help*.

Non-Graphical Installation

In Linux, the Management Center can also be installed on the command line. Before installing, check the installation package integrity using the MD5 or SHA-1 file checksums as explained in [Checking File Integrity](#) (page 14).



Note – You need a graphical environment to use the Management Client. It cannot be run on the command line. Only the server components can be run in a command line-only environment.

▼ To begin the non-graphical installation

1. Open the shell and change to the directory where the installer is stored.
 - If installing from a CD-ROM, the installer is in:
`CD-ROM/StoneGate_SW_Installer/Linux/`
 - If the CD-ROM is not automatically mounted, mount the CD-ROM with command:
`mount /dev/cdrom /mnt/cdrom`
2. Run the command `./setup.sh -nodisplay` (the `-nodisplay` switch can be omitted if there is no graphical environment running). The installer starts. You can use the following general commands at any point where the installer asks for your input:
 - Type `back` to return to the previous step.
 - Type `quit` to cancel the installation.
3. When prompted, press **Enter** to continue. The license agreement is displayed.

4. Press **Enter** to scroll through the license agreement and accept by typing “**y**”. You are prompted to select the installation directory.
5. Press **Enter** to install to the default installation directory, or specify a different directory. If you specify a different directory, you are prompted to confirm it.
6. You are prompted to select the link location for shortcuts to the most commonly used command line tools.
7. Press **Enter** to create the StoneGate links in the default directory or select one of the other options. A reminder to verify the hosts file appears.
8. Press **Enter** to continue.
9. Select the StoneGate components you want to install:
 - Press **Enter** to install all Management Center components except the Web Portal Server.
 - Press **2** to install only the Management Client.
 - Press **3** to install a simulated network environment for evaluation in Demo Mode.
 - Press **4** to install a different selection of components.
10. (*Customized installation only*) Enter the numbers of the components you want to select/deselect, separated by commas.
 - Entering the number of a selected component deselects it.
 - Entering the number of a component that is not selected selects it.
 - By default, the Management Server, Log Server, and Management Client are selected.
 - You can verify your selection by typing **back** in the next stage.

Example To install only the Web Portal Server, type 1,2,3,4 and press Enter.

The other installation options for the Management Center components are the same as in the graphical installation.

CHAPTER 6

DISTRIBUTING MANAGEMENT CLIENTS THROUGH WEB START

The Management Client can be distributed through Java Web Start. This eliminates the need for each administrator to upgrade their client when the SMC is upgraded to a new version (the version of the client must always match the version of the respective server).

The following sections are included:

- ▶ [Getting Started with Web Start Distribution](#) (page 44)
- ▶ [Distributing Clients from the SMC Servers](#) (page 44)
- ▶ [Distributing Clients from a Separate Server](#) (page 45)
- ▶ [Accessing the Web Start Clients](#) (page 46)

Getting Started with Web Start Distribution

In addition to installing Management Clients through the Installation Wizard, you can also distribute them through Java Web Start. Management Clients distributed with Web Start have the same set of features as clients installed with the installation wizard, but when you upgrade, Web Start automatically downloads the new version when the user logs.

There are two ways to configure Web Start access:

- you can activate an internal Web server on the Management Server (the server distributes only Web Start clients). There is no need for manual installation or upgrade.
- you can use a separate web server or network drive for distributing the clients. You must install these files manually and perform a fresh installation at each SMC version upgrade.

What's Next?

- ▶ [Distributing Clients from the SMC Servers.](#)
- ▶ [Distributing Clients from a Separate Server](#) (page 45).

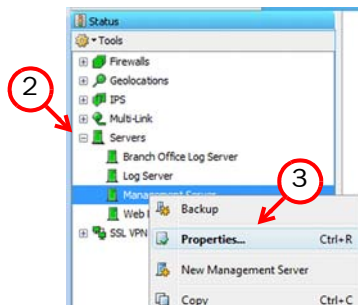
Distributing Clients from the SMC Servers

▼ To enable a Web Start server

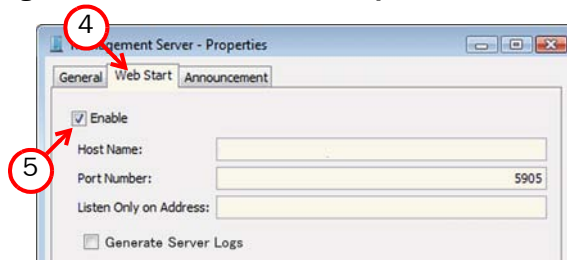
1. Click the System Status icon in the toolbar. The System Status view opens.



2. Expand **Servers**.



3. Right-click a Management Server and select **Properties**. The Properties dialog opens.



4. Switch to the **Web Start** tab.
5. Select **Enable**. The Web Start server options are enabled.

6. (Optional) Change the (TCP) **Port Number** that the Web Start Server uses. By default, the standard HTTP port 80 is used on Windows and 8080 on Linux (which does not allow the use of reserved ports for this type of service).



Note – Make sure that the port is not used by other listening services on the server. For ports reserved for StoneGate services, see [Default Communication Ports](#) (page 91).

7. Click **OK**.

With these settings, the users can access the Web Start files at any addresses that the Management Server may have.

What's Next?

- ▶ Test the client as explained in [Accessing the Web Start Clients](#) (page 46).

Distributing Clients from a Separate Server

If you do not want to use the Management Server as a Web Start server, you can place the Web Start package on a Web server.

The Web Start package can also be placed on a shared network drive. The path to the files, including the drive letter, must be the same for all administrators who use that particular version of the installation package. If the network drive paths vary, consider placing the package on a Web server instead.



Note – You must delete the existing files and install a new Web Start package according to these instructions each time you upgrade the Management Center. Otherwise, any administrators who use Web Start-installed Management Clients are not able to log in.

▼ To install the Web Start package

1. Browse to **StoneGate_SW_Installer**→**Webstart** on the installation CD-ROM.



Caution – The Web Start installation creates an `index.html` file in the installation directory. Any existing `index.html` file will be overwritten.

2. Copy all files and all directories from the `webstart` directory on the installation CD-ROM to the directory where you want the Web Start files to be served.
3. On the command line, change to the directory where the Web Start files are located on your server.

4. Run the Web Start setup script and give the URL or the path of the directory where the Web Start files are located on your server as the parameter:
 - Windows: `cscript webstart_setup.vbs <web start directory>`
 - Linux: run `webstart_setup.sh <web start directory>`

Table 6.1 Examples

Installation on	Example Web Start Directory
Web server	<code>http://www.example.com/webstart/</code>
Network drive	<code>file://localhost/c:/webstart/</code>

5. If necessary, modify the configuration of the Web server to return the appropriate MIME type for .jnlp files (`application/x-java-jnlp-file`). Consult the manual of your Web server for instructions on how to configure the MIME type.
6. Delete the `webstart_setup.vbs` and `webstart_setup.sh` files from the directory.

Accessing the Web Start Clients

After configuration, the administrators can access the Management Client using the Web Start package. To be able to use the Web Start Management Client, there must be a current version of the Java Runtime Environment (JRE) installed (the version required is shown on the login page).

▼ To access the Web Start Clients

1. Enter the Web Start download page address in your Web browser
`http://<server address>:<port>`
 - `<port>` is only needed if the server is configured to run on a different port from the HTTP standard port 80.
2. Click the link for the Web Start client.
 - Web Start automatically checks if the version on the server is already installed on your local computer. If not, the new client is automatically installed on your computer. This is done each time the client is started this way, automatically upgrading your client installation whenever needed without any action from you.
 - The client starts and displays the login dialog.
3. Log in with your account credentials.

What's Next?

- ▶ If NAT is applied to communications between any system components, proceed to [Configuring NAT Addresses for StoneGate Components](#) (page 47).
- ▶ Otherwise, you are ready to configure the firewall and IPS element(s) in the Management Client. You must configure the elements before installing the physical engines. See the *Firewall/VPN Installation Guide* and the *IPS Installation Guide* for more information.

CHAPTER 7

CONFIGURING NAT ADDRESSES FOR STONEGATE COMPONENTS

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 any of the system components.

The following sections are included:

- ▶ [Configuration Overview](#) (page 48)
- ▶ [Defining Locations](#) (page 49)
- ▶ [Adding SMC Server Contact Addresses](#) (page 51)
- ▶ [Setting the Management Client's Location](#) (page 53)

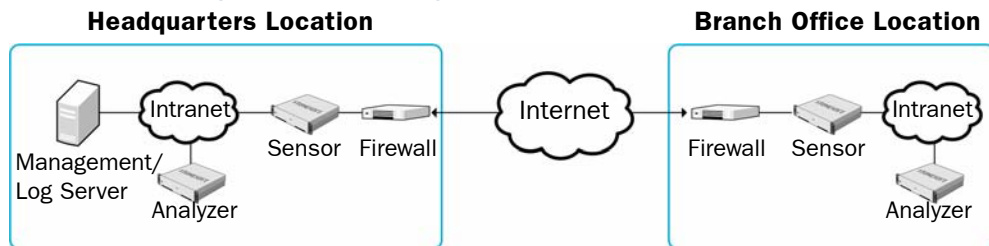
Configuration Overview

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 91).

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 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 main 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 7.1 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 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 if they also need to connect to the SMC servers at the headquarters and NAT is applied to the communications.

To be able to view logs, the administrators at the branch office must select the "Branch Office" Location in the Management Client.

Configuration Overview

1. Define Location element(s). See [Defining Locations](#).
2. Define contact addresses for the Management Server, and Log Server(s). See [Adding SMC Server Contact Addresses](#) (page 51).
3. Select the correct Location for your Management Client. See [Setting the Management Client's Location](#) (page 53).
4. Select the correct Location for firewalls and IPS engines when you create the Firewall or IPS elements. See the *Firewall/VPN Installation Guide* and *IPS Installation Guide*.

Defining Locations

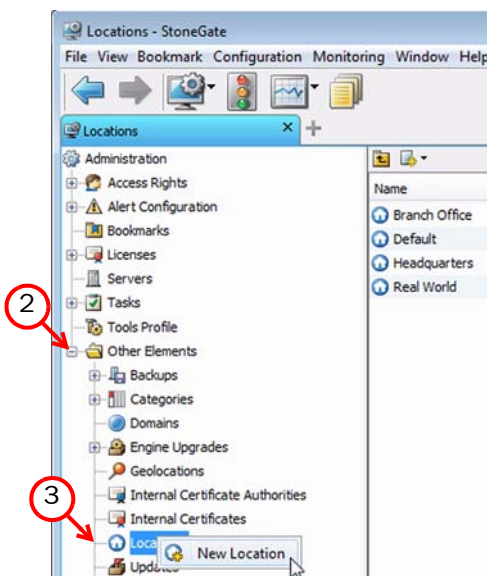
The first task is to group the system components into Location elements based on which components are on the same side of a NAT device. The elements that belong to the same Location element always use the primary IP address (defined in the main Properties dialog of the element) when contacting each other.

▼ To create a new Location element

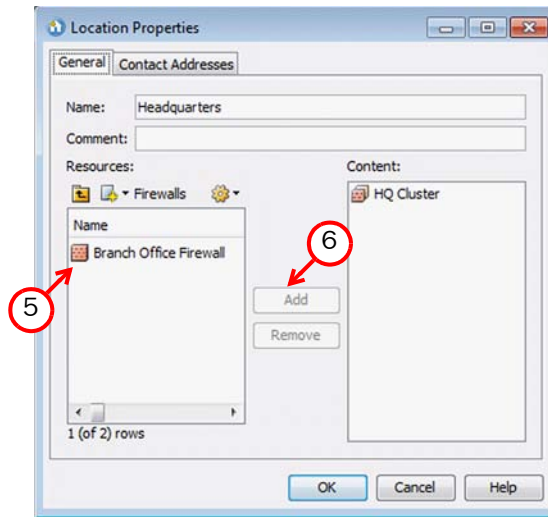
1. Click the Configuration icon in the toolbar, and select **Administration**. The Administration Configuration view opens.



2. Expand **Other Elements**.



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 create other Locations as necessary.

What's Next?

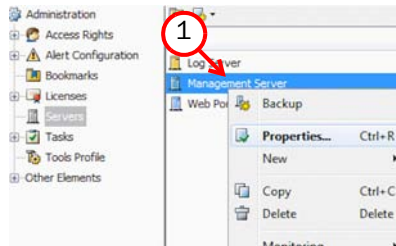
- ▶ If your Management Server or Log Server needs a contact address, proceed to [Adding SMC Server Contact Addresses](#) (page 51).
- ▶ Otherwise, you are ready to configure the firewall and IPS element(s) in the Management Client. You must configure the elements before installing the physical engines. See the *Firewall/VPN Installation Guide* and the *IPS Installation Guide* for more information.

Adding SMC Server Contact Addresses

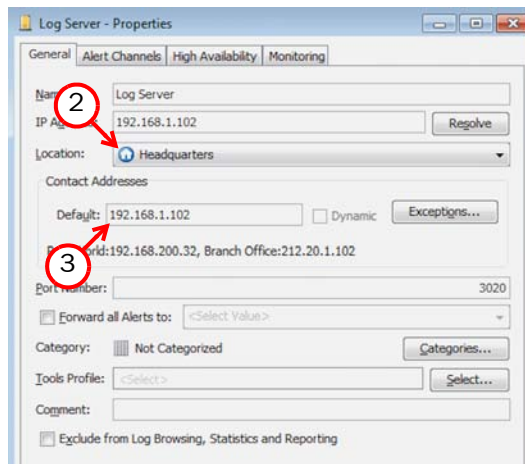
The Management Server, Log Server, and Authentication Server can have more than one contact address for each Location. You must define two or more contact addresses per Location if you have secondary Management Servers or Log Servers. Multiple contact addresses are required so that remote components can connect to a Management Server or a Log Server even if the primary Management Server or Log Server fails. You must also define two or more contact addresses per Location if you have configured Multi-Link, so that remote components can connect to the server(s) even if a NetLink goes down.

▼ To define 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. If necessary, enter additional **Default** contact address(es).
 - A default contact address is automatically entered based on the element properties.
 - If the server has multiple Default contact addresses, separate the addresses with commas.
 - If necessary, the **Exceptions** button allows you to define other contact addresses for specific Locations



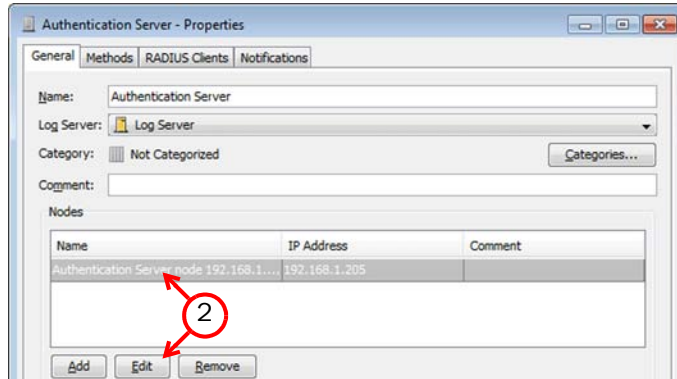
Note – Elements that belong to the same Location element always use the primary IP address when contacting each other instead of any Contact Addresses. All elements not specifically put in a certain Location are treated as an additional Location.

4. Click **OK**.

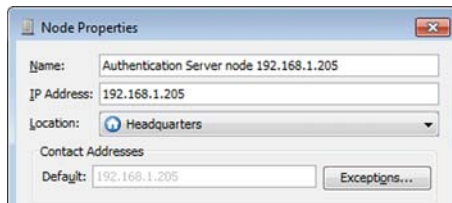
Define the contact addresses for other servers as necessary in the same way.

▼ To define Authentication Server contact addresses

1. Right-click the Authentication Server and select **Properties**. The Authentication Server properties open.



2. Select the node for which you want to define contact addresses and click **Edit**. The Node Properties dialog opens.



3. Select the **Location** of this server.
4. If necessary, enter additional **Default** contact address(es).
 - A default contact address is automatically entered based on the element properties.
 - If the server has multiple Default contact addresses, separate the addresses with commas.
 - If necessary, the **Exceptions** button allows you to define other contact addresses for specific Locations.
5. Click **OK**.



Note – Elements that belong to the same Location element always use the primary IP address when contacting each other instead of any Contact Addresses. All elements not specifically put in a certain Location are treated as an additional Location.

What's Next?

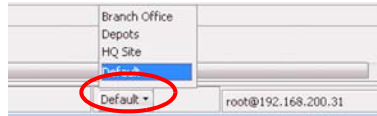
- ▶ If NAT is performed between your Management Client and a Log Server, proceed to [Setting the Management Client's Location](#) (page 53).
- ▶ Otherwise, you are ready to configure the firewall and IPS element(s) in the Management Client. You must configure the elements before installing the physical engines. See the *Firewall/VPN Installation Guide* and the *IPS Installation Guide* for more information.

Setting the Management Client's Location

When NAT is performed between the Management Client and a Log Server, you must select the correct Location for your Management Client in the status bar at the bottom of the Management Client window to be able to view logs.

▼ To select the Management Client's Location

- ➔ Click the **Default** Location name in the status bar at the bottom of the window and select the correct Location.



What's Next?

- ▶ You are ready to configure firewall and IPS element(s). See the *Firewall/VPN Installation Guide* and the *IPS Installation Guide* for more information.

MAINTENANCE

In this section:

Upgrading - 57

Uninstalling the Management Center - 67

CHAPTER 8

UPGRADING

This chapter explains how you can upgrade the StoneGate Management Center.

The following sections are included:

- ▶ [Getting Started with Upgrading the Management Center](#) (page 58)
- ▶ [Upgrading Licenses](#) (page 59)
- ▶ [Upgrading the Management Center](#) (page 62)

Getting Started with Upgrading the Management Center

You can upgrade Management Center components without uninstalling the previous version. It is important to upgrade the Management Center components before upgrading the engines, because the old Management Center version may not be able to recognize the new version engines and generate a valid configuration for them. Many older versions of engines can be controlled by newer Management Center versions. See the *Release Notes* for possible version-specific restrictions.



Caution – All the Management Center components (Management Server, Management Client, Log Server, the optional Web Portal Server, and the optional Authentication Server) must use the same software version to be able to work together. Plan ahead to perform all necessary upgrades.

The security engines do not require a continuous connection to the Management Center and they continue to operate normally during the Management Center upgrade. The engines temporarily store their logs locally if the Log Server is unavailable and then send them to the Log Server as it becomes available again.

For more detailed instructions, see the *Online Help* of the Management Client or the *Administrator's Guide* PDF.

Before upgrading, read the *Release Notes* for the new version at http://www.stonesoft.com/en/support/technical_support_and_documents.

Configuration Overview

1. Obtain the installation files and check the installation file integrity as explained in [Downloading the Installation Files](#) (page 14).
2. (If automatic license updates have been disabled) Update the licenses as explained in [Upgrading Licenses](#) (page 59).
3. Upgrade all Management Servers, Log Servers, and Web Portal Servers as explained in [Upgrading the Management Center](#) (page 62).
4. Upgrade any locally installed the Management Clients by running the Management Center installer and any Web Start distributions that are located on an external servers as explained in [Distributing Clients from a Separate Server](#) (page 45).

What's Next?

- ▶ If the current licenses are valid for the new version, proceed to [Upgrading the Management Center](#) (page 62).
- ▶ Otherwise, continue by [Upgrading Licenses](#) (page 59).

Upgrading 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). Automatic regeneration and installation of licenses is enabled by default. You can also upgrade the licenses at the Stonesoft website.

If you do not need to upgrade licenses, proceed to [Upgrading the Management Center](#) (page 62).

What's Next?

- ▶ Proceed to [Upgrading Licenses Under One Proof Code](#) to upgrade the licenses one by one.
- ▶ Proceed to [Upgrading Licenses Under Multiple Proof Codes](#) (page 60) to upgrade several licenses at once.

Upgrading Licenses Under One Proof Code

▼ To upgrade a license

1. Take your Web browser to 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 to upgrade the license.

Repeat for other licenses.

What's Next?

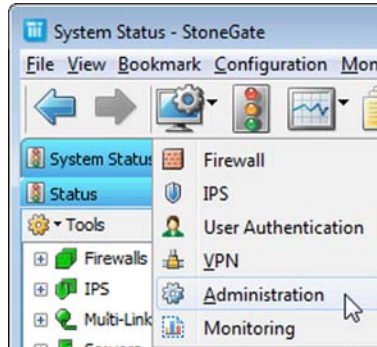
- ▶ Proceed to [Installing Licenses](#) (page 61).

Upgrading Licenses Under Multiple Proof Codes

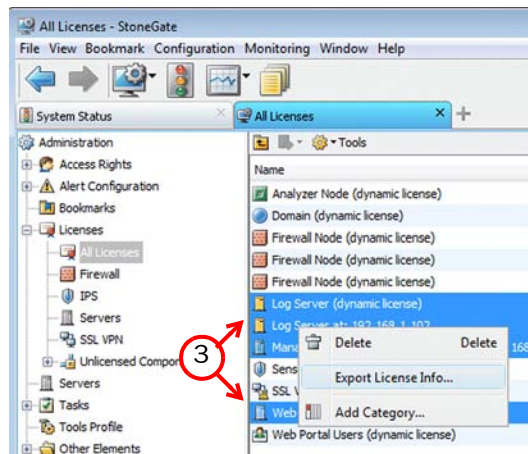
If you have several existing licenses with different POL (proof-of-license) codes that you need to upgrade, you can make the work easier by generating the new licenses all at once.

▼ To upgrade multiple licenses

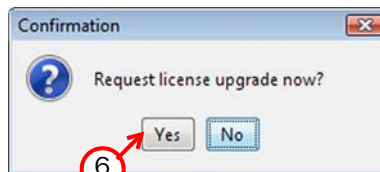
1. Click the Configuration icon and select **Administration**. The Administration Configuration view opens.



2. Browse to **Licenses**→**All Licenses**. All the licenses appear in the right panel.



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**. The StoneGate License Request Browser dialog opens.
5. Save the license information file. A confirmation dialog opens.



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

7. Upload the license upgrade request file to the Stonesoft License Center website using the multi-upgrade form.

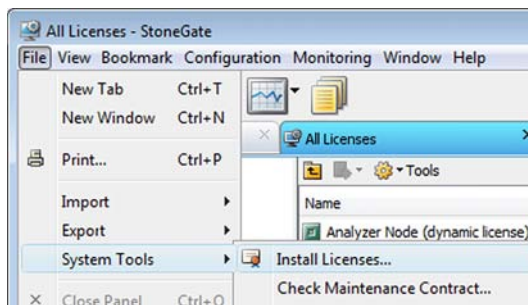
You can view and download your current licenses at the license website (log in by entering the proof-of-license or proof-of-serial number code at the License Center main page).

Installing Licenses

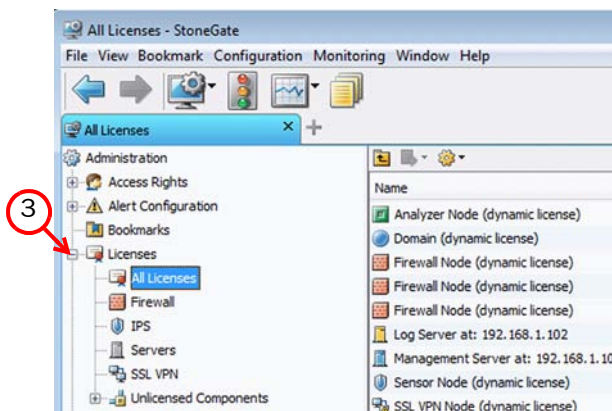
After you have upgraded the licenses as described above, you install the license file in the Management Client.

▼ To install licenses

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



2. Select one or more license files in the standard dialog that opens.
3. Browse to **Licenses**→**All Licenses** in the Administration Configuration view.



4. Check that the licenses are now correctly upgraded to the new version. When you only upgrade the software version in the license, old licenses are automatically replaced.

Upgrading the Management Center

There is no need to uninstall the previous version. Upgrading from all older versions may not be possible without an intermediate upgrade. See the *Release Notes* for more information.

It is possible to revert automatically to the previous installation if the Management Center upgrade fails for some reason. The installer can also back up of the Management Server configuration. For more information on backups (such as the steps for restoring), refer to the *Online Help* of the Management Client or the *Administrator's Guide* PDF.

The same installer works with all Management Center components, including locally Installed Management Clients.

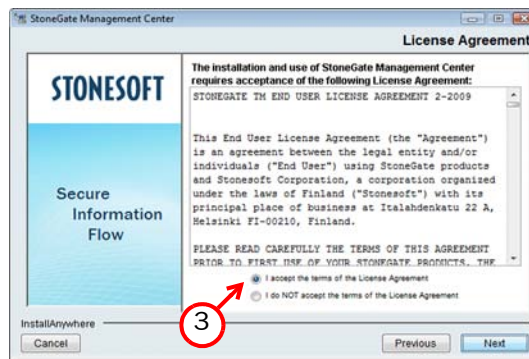
▼ To upgrade Management Center components

1. Start the installation (from the unzipped installer files or from the CD-ROM):
 - In Windows, run `\StoneGate_SW_Installer\Windows\setup.exe`
 - In Linux, run `/StoneGate_SW_Installer/Linux/setup.sh`

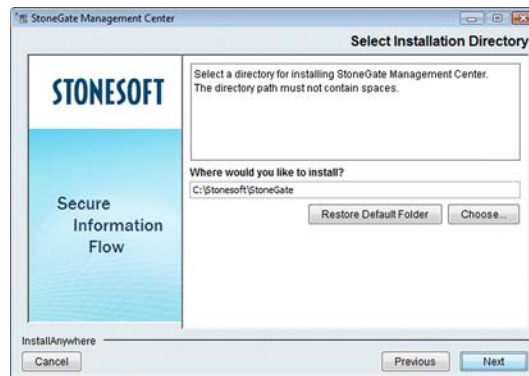


Note - If the CD-ROM is not automatically mounted in Linux, mount it with command `"mount /dev/cdrom /mnt/cdrom"`.

2. When the Installation Wizard shows the Introduction screen, click **Next** to start the upgrade. The License Agreement appears.



3. Indicate that you accept the License Agreement and click **Next** to continue the installation.



4. Make sure the installation directory is correct for your installation and click **Next**.
 - All installed components must be upgraded at the same time. You can install additional components if you wish (see [Installing the Management Center](#) (page 19) for installation instructions).



5. (Management Server only, optional) Select **Save Current Installation** to save a copy of the current installation that you can revert to at any time after the upgrade.
6. Click **Next**.



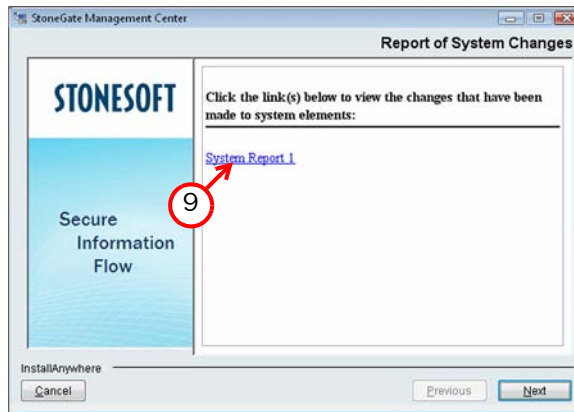
7. (Management Server only) Select the configuration data backup option and click **Next**:
 - Select **Yes** to create a backup that can be used and viewed without a password.
 - Select **Yes, encrypt the backup** to create a password-protected backup. You are prompted for the password as you confirm the selection.
 - Select **No** if you already have a recent backup of the Management Server.



Caution – If you are working on a Windows system and you are upgrading any StoneGate component that runs as a service, make sure the Services window is closed before you complete the next step. Otherwise, the service may not be installed correctly.



8. Check the displayed information and click **Install**. The upgrade begins.



9. (Optional) When the upgrade is finished, follow the link(s) in the notification to launch the report(s) of system changes in your Web browser before you exit the installer.
10. (Secondary Management Servers only) If you have more than one Management Server for high availability, synchronize the Management database between the primary Management Server and the secondary Management Server(s) after you have upgraded the secondary Management Server(s).
- 10a. Right-click the secondary Management Server in the Management Client and select **Control Management Servers**. The Control Management Servers dialog opens.
- 10b. Right-click the active Management Server and select **Synchronize** to synchronize the database on all the secondary Management Servers or right-click a single secondary Management Server and select **Synchronize** to synchronize the database only on the selected secondary Management Server.

10c. Confirm the synchronization by clicking **Yes**.

What's Next?

- ▶ If administrators have Management Clients installed locally, upgrade the Management Clients by running the same Management Center installer on those hosts.
- ▶ If you are distributing Web Start Management Clients from an external server, install a new Web Start package in the same way as the original installation was made. See [Distributing Management Clients through Web Start](#) (page 43).
- ▶ Otherwise, the Management Center upgrade is now complete. See the *Firewall/VPN Installation Guide* and *IPS Installation Guide* if you are upgrading engines as well.

CHAPTER 9

UNINSTALLING THE MANAGEMENT CENTER

This chapter instructs how to uninstall the Management Center components.

The following sections are included:

- ▶ [Overview to Uninstalling the Management Center](#) (page 68)
- ▶ [Uninstalling in Windows](#) (page 68)
- ▶ [Uninstalling in Linux](#) (page 69)

Overview to Uninstalling the Management Center

It is not possible to uninstall the Management Center components one by one. If you have several Management Center components installed on the same computer, all components are uninstalled. The `sgadmin` account is deleted during the uninstallation of the Management Center.

By default, the Management Center is installed in the following directories:

- **Windows:** `C:\stonesoft\stonegate`
- **Linux:** `usr/local/stonegate`

There is a `.stonegate` directory in each user's home directory in the operating system, which contains the Management Client configuration files. These files are not automatically deleted but can be removed manually after the uninstallation.



Note – Backup the Management Server and the Log Server before uninstalling the Management Center if you want to preserve the stored data.

Uninstalling in Windows

▼ To uninstall in Windows

1. Launch the uninstaller in one of the following ways:
 - Open the list of installed programs through the Windows Control Panel, right-click StoneGate Management Center, and select **Uninstall/Change**.
 - Alternatively, run the script `<installation directory>\uninstall\ uninstall.bat`



2. When the uninstaller starts, click **Uninstall**. All Management Center components are uninstalled.

Uninstalling in Linux

▼ To uninstall in graphical mode

1. Stop the Management Center components on the machine.
2. Run the script `<installation directory>/uninstall/uninstall.sh`
3. When the uninstaller starts, click **Uninstall**. All Management Center components are uninstalled.

▼ To uninstall in non-graphical mode

1. Stop the Management Center components on the machine.
2. Run the script `<installation directory>/uninstall/uninstall.sh -nodisplay`

APPENDICES

In this section:

Command Line Tools - 73

Default Communication Ports - 91

Index - 101

APPENDIX A

COMMAND LINE TOOLS

This appendix describes the command line tools for StoneGate Management Center and the engines.

The following sections are included:

- ▶ [Management Center Commands](#) (page 74)
- ▶ [Engine Commands](#) (page 83)
- ▶ [Server Pool Monitoring Agent Commands](#) (page 89)

Management Center Commands

Management Center commands include commands for the Management Server, Log Server, Web Portal Server, and Authentication Server. Most of the commands are found in the `<installation directory>/bin/` directory. In Windows, the command line tools are *.bat script files. In Linux, the files are *.sh scripts.



Note – Using the Management Client is the recommended configuration method, as most of the same tasks can be done through it.

Commands that require parameters must be run through the command line (cmd.exe in Windows). Commands that do not require parameters can alternatively be run through a graphical user interface, and may be added as shortcuts during installation.

Table A.1 Management Center Command Line Tools

Command	Description
<pre>sgArchiveExport [host=<address>] [login=<login name>] pass=<password> [format=CSV/XML/CEF] i=<input file> [o=<output file>] [f=<filter file>] [e=<filter expression>] [-h -help] [-v]</pre>	<p>Displays or exports logs from archive. This command is only available on the Log Server. The operation checks privileges for the supplied administrator account from the Management Server to prevent unauthorized access to the logs.</p> <p>Enclose details in double quotes if they contain spaces.</p> <p>Host specifies the address of the Management Server. If the parameter is not defined, the loopback address is used.</p> <p>login defines the username for the account that is used for this operation. If this parameter is not defined, the username root is used.</p> <p>pass defines the password for the user account.</p> <p>format defines the file format for the output file. If this parameter is not defined, the XML format is used.</p> <p>i defines the source from which the logs will be exported. Can be a folder or a file. The processing recurses into subfolders.</p> <p>o defines the destination file where the logs will be exported. If this parameter is not defined, the output is displayed on screen.</p> <p>f defines a file that contains the filtering criteria you want to use for filtering the log data. You can export log filters individually in the Management Client through Tools→Save for Command Line Tools in the filter's right-click menu.</p> <p>e allows you to type in a filter expression manually (using the same syntax as exported filter files).</p> <p>-h or -help displays information on using the script.</p> <p>-v displays verbose output on the command execution.</p> <p>Example (exports logs from one full day to a file using a filter): sgArchiveExport login=admin pass=abc123 i=c:/stonesoft/stonegate/data/archive/firewall/ year2009/month12/day01/ f=c:/stonesoft/ stonegate/export/MyExportedFilter.flp format=CSV o=MyExportedLogs.csv</p>

Table A.1 Management Center Command Line Tools (Continued)

Command	Description
sgBackupAuthSrv	Creates a backup of Authentication Server user information. The backup file is stored in the <i><installation directory>/backups/</i> directory. Backing up the Authentication only backs up Users, not the configuration of the Authentication Server. The Authentication Server configuration is included in the Management Server backup. Also see sgRestoreAuthBackup .
sgBackupLogSrv	Creates a backup of Log Server configuration data. The backup file is stored in the <i><installation directory>/backups/</i> directory. Twice the size of log database is required on the destination drive. Otherwise, the operation fails. Also see sgRestoreLogBackup .
sgBackupMgtSrv	Creates a complete backup of the Management Server (including both the local configuration and the stored information in the configuration database). The backup file is stored in the <i><installation directory>/backups/</i> directory. Twice the size of the Management Server database is required on the destination drive. Otherwise, the operation fails. Also see sgRestoreMgtBackup and sgRecoverMgtDatabase .
sgCertifyAuthSrv	Contacts the Management Server and creates a new certificate for the Authentication Server to allow secure communications with other system components. Renewing an existing certificate does not require changing the configuration of any other system components.
sgCertifyLogSrv [host =<Management Server Address [\ <i>Domain</i> >]]	Contacts the Management Server and creates a new certificate for the Log Server to allow secure communications with other system components. Renewing an existing certificate does not require changing the configuration of any other system components. Host specifies the address of the Management Server. If the parameter is not defined, the loopback address is used. Domain specifies the administrative Domain the Log Server belongs to if the system is divided in administrative Domains. If the Domain is not specified, the Shared Domain is used.
sgCertifyMgtSrv	Creates a new certificate for the Management Server to allow secure communications between the StoneGate system components. Renewing an existing certificate does not require changes on any other system components.

Table A.1 Management Center Command Line Tools (Continued)

Command	Description
<p>sgCertifyWebPortalSrv [host=<Management Server Address [\Domain]>]</p>	<p>Contacts the Management Server and creates a new certificate for the Web Portal Server to allow secure communications with other system components. Renewing an existing certificate does not require changing the configuration of any other system components.</p> <p>Host specifies the address of the Management Server. If the parameter is not defined, the loopback address is used.</p> <p>Domain specifies the administrative Domain the Web Portal Server belongs to if the system is divided in administrative Domains. If the Domain is not specified, the Shared Domain is used.</p>
<p>sgChangeMgtIPOnAuthSrv <IP address></p>	<p>Changes the Management Server's IP address in the Authentication Server's local configuration to the IP address you give as a parameter. Use this command if you change the Management Server's IP address. Restart the Authentication Server service after this command.</p>
<p>sgChangeMgtIPOnLogSrv <IP address></p>	<p>Changes the Management Server's IP address in the Log Server's local configuration to the IP address you give as a parameter. Use this command if you change the Management Server's IP address. Restart the Log Server service after this command.</p>
<p>sgChangeMgtIPOnMgtSrv <IP address></p>	<p>Changes the Management Server's IP address in the local configuration to the IP address you give as a parameter. Use this command if you change the Management Server's IP address. Restart the Management Server service after this command.</p>
<p>sgClient</p>	<p>Starts a locally installed StoneGate Management Client.</p>
<p>sgCreateAdmin</p>	<p>Creates an unrestricted (superuser) administrator account. The Management Server needs to be stopped before running this command.</p>

Table A.1 Management Center Command Line Tools (Continued)

Command	Description
<pre> sgExport [host=<Management Server Address [\Domain]>] [login=<login name>] pass=<password> file=<file path and name> type=<all nw ips sv rb al> [-recursion] [-system] [name= <element name 1, element name 2, ...>] </pre>	<p>Exports elements stored on the Management Server to an XML file.</p> <p>Enclose details in double quotes if they contain spaces.</p> <p>Host specifies the address of the Management Server. If the parameter is not defined, the loopback address is used.</p> <p>Domain specifies the administrative Domain for this operation if the system is divided in administrative Domains. If the Domain is not specified, the Shared Domain is used.</p> <p>login defines the username for the account that is used for this operation. If this parameter is not defined, the username root is used.</p> <p>pass defines the password for the user account.</p> <p>type specifies which types of elements are included in the export file: all for all exportable elements, nw for network elements, ips for IPS elements, sv for services, rb for security policies, or al for alerts.</p> <p>recursion includes referenced elements in the export, for example, the network elements used in a policy that you export.</p> <p>system includes any system elements that are referenced by the other elements in the export.</p> <p>name allows you to specify by name the element(s) that you want to export.</p>

Table A.1 Management Center Command Line Tools (Continued)

Command	Description
<pre> sgHA [host=<Management Server Address [\Domain]>] [login=<login name>] pass=<password> [-h -help] [-set-active] [-set-standby] [-force-active] [-sync] </pre>	<p>Controls highly available (active and standby) Management Servers.</p> <p>Host specifies the address of the Management Server. If the parameter is not defined, the loopback address is used.</p> <p>Domain specifies the administrative Domain for this operation if the system is divided in administrative Domains. If the Domain is not specified, the Shared Domain is used.</p> <p>Login defines the username for the account that is used for this operation. If this parameter is not defined, the username <code>root</code> is used.</p> <p>pass defines the password for the user account.</p> <p>-h or -help displays information on using the script.</p> <p>-set-active sets a standby Management Server as the active Management Server, sets the formerly active Management Server as a standby Management Server, and synchronizes the database between them.</p> <p>-set-standby sets the active Management Server as a standby Management Server.</p> <p>-force-active sets a standby Management Server as the active Management Server without synchronizing the database with the formerly active Management Server.</p> <p>-sync functions differently on a standby Management Server and an active Management Server. If you run it on an active Management Server, it replicates the active database to every standby Management Server that has the Include in Database Replication option selected in its properties. If you run it on a standby Management Server, it replicates the active database from the active Management Server only to this standby Management Server (regardless of whether the Include in Database Replication option is selected in the standby Management Server's properties).</p>
<pre> sgImport host=<Management Server Address [\Domain]> [login=<login name>] pass=<password> file=<file path and name> </pre>	<p>Imports StoneGate Management Server database elements from a StoneGate XML file. When importing, existing (non-default) elements are overwritten if both the name and type match.</p> <p>Host specifies the address of the Management Server. If the parameter is not defined, the loopback address is used.</p> <p>Domain specifies the administrative Domain for this operation if the system is divided in administrative Domains. If the Domain is not specified, the Shared Domain is used.</p> <p>Login defines the username for the account that is used for this operation. If this parameter is not defined, the username <code>root</code> is used.</p> <p>pass defines the password for the user account.</p> <p>file defines the file whose contents you want to import.</p>

Table A.1 Management Center Command Line Tools (Continued)

Command	Description
<pre> sgImportExportUser host=<Management Server Address [\Domain]> [login=<login name>] pass=<password> action=[import export] file=<file path and name> </pre>	<p>Imports and exports a list of Users and User Groups in an LDIF file from/to a StoneGate Management Server's internal LDAP database. To import User Groups, all User Groups in the LDIF file must be directly under the stonegate top-level group (dc=stonegate).</p> <p>The user information in the export file is stored as plaintext. Handle the file securely.</p> <p>Host specifies the address of the Management Server. If the parameter is not defined, the loopback address is used.</p> <p>Domain specifies the administrative Domain for this operation if the system is divided in administrative Domains. If the Domain is not specified, the Shared Domain is used.</p> <p>login defines the username for the account that is used for this operation. If this parameter is not defined, the username root is used.</p> <p>pass defines the password for the user account.</p> <p>action defines whether users are imported or exported.</p> <p>file defines the file that is used for the operation.</p> <p>Example: sgImportExportUser login=admin pass=abc123 action=export file=c:\temp\exportedusers.ldif</p>
<pre> sgImportWebClientLanguage host=<Management Server Address [\Domain]> [login=<login name>] pass=<password> file=<file path and name> </pre>	<p>Imports an additional language to the Web Portal end-user interface. You can run the command when the Web Portal Server service is running, but the imported language does not become available until the service is restarted.</p> <p>Host specifies the address of the Management Server. If the parameter is not defined, the loopback address is used.</p> <p>Domain specifies the administrative Domain for this operation if the system is divided in administrative Domains. If the Domain is not specified, the Shared Domain is used.</p> <p>login defines the username for the account that is used for this operation. If this parameter is not defined, the username root is used.</p> <p>pass defines the password for the user account.</p> <p>file defines the file that is used for the operation. The imported file must use the UTF-8 or UTF-16 text encoding. The file name must follow the format messages_XX[_YY[_ZZ]].txt where XX is the two-character ISO language code, YY the ISO country code and ZZ the ISO language variant code. The country code and language variant code are optional.</p> <p>Example: sgImportWebClientLanguage host=192.168.1.101/Helsinki login=ricky pass=abc123 file=messages_sv_fi.txt</p>

Table A.1 Management Center Command Line Tools (Continued)

Command	Description
<p>sgInfo</p>	<p>Creates a ZIP file that contains copies of configuration files and the system trace files. The resulting ZIP file is stored in the logged in user's home directory. The file location is displayed on the last line of screen output. Provide the generated file to Stonesoft support for troubleshooting purposes.</p>
<p>sgOnlineReplication [-h --help] [login=<login name>] pass=<password> active-server= <name of active Management Server> standby-server= <name of standby Management Server> standby-server-address= <IP address of standby Management Server></p>	<p>Replicates the Management Server's database from the active Management Server to the standby Management Server.</p> <p>Note! Use this script only if the secondary Management Server's configuration has been corrupted, the secondary Management Server's certificate has expired, or in new SMC installations if the automatic database replication between the Management Servers has not succeeded. Otherwise, synchronize the database through the Management Client (see Synchronizing Management Databases Manually (page 293) or use the sgHA command.</p> <p>-h --help options display the help message</p> <p>pass defines the password for the user account.</p> <p>active-server option specifies the IP address of the active Management Server from which the Management database is replicated.</p> <p>standby-server option specifies the name of the standby Management Server to which the Management database is replicated.</p> <p>standby-server-address option specifies the IP address of the standby Management Server to which the Management database is replicated.</p>
<p>sgReinitializeLogServer</p>	<p>Located in <installation directory>/bin/install. Creates a new Log Server configuration if the configuration file has been lost.</p>
<p>sgRestoreArchive ARCHIVE_DIR</p>	<p>Restores logs from archive files to the Log Server. This command is available only on the Log Server.</p> <p>ARCHIVE_DIR is the number of the archive directory (0 – 31) from where the logs will be restored. By default, only archive directory 0 is defined. The archive directories can be defined in the <installation directory>/data/LogServerConfiguration.txt file:</p> <p>ARCHIVE_DIR_xx=PATH.</p>
<p>sgRestoreAuthBackup</p>	<p>Restores the Authentication Server user information from a backup file in the <installation directory>/backups/ directory.</p> <p>Apply the Authentication Server's configuration after this command.</p>

Table A.1 Management Center Command Line Tools (Continued)

Command	Description
sgRestoreCertificate	Restores the Certificate Authority (CA) or the Management Server certificate from a backup file in the <i><installation directory>/backups/</i> directory.
sgRestoreLogBackup	Restores the Log Server (logs and/or configuration files) from a backup file in the <i><installation directory>/backups/</i> directory.
sgRestoreMgtBackup	Restores the Management Server (database and/or configuration files) from a backup file in the <i><installation directory>/backups/</i> directory.
sgRevert	Note! This script is located in the <i><installation directory>/uninstall/</i> directory. Reverts to the previous installation saved during the upgrade process. The previous installation can be restored at any time, even after a successful upgrade.
sgShowFingerPrint	Displays the CA certificate's fingerprint on the Management Server.
sgStartAuthSrv	Starts the Authentication Server.
sgStartLogDatabase	Starts the Log Server's database. (The Log Server's database is started and stopped automatically when starting/stopping the Log Server service.)
sgStartLogSrv	Starts the Log Server and its database.
sgStartMgtDatabase	Starts the Management Server's database. There is usually no need to use this script.
sgStartMgtSrv	Starts the Management Server and its database.
sgStartWebPortalSrv	Starts the Web Portal Server.
sgStopLogSrv	Stops the Log Server.
sgStopMgtSrv	Stops the Management Server and its database.
sgStopMgtDatabase	Stops the Management Server's database. There is usually no need to use this script.
sgStopWebPortalSrv	Stops the Web Portal Server.
sgStopRemoteMgtSrv [host =<Management Server Host Name>] [port =<port number>] [login =<login name>] [pass =<password>]	Stops the Management Server service when run without arguments. To stop a remote Management Server service, provide the arguments to connect to the Management Server. host is the Management Server's host name if not localhost. port is the Management Server's Management Client port number (by default, 8902). login is a StoneGate administrator account for the login. pass is the password for the administrator account.

Table A.1 Management Center Command Line Tools (Continued)

Command	Description
<pre>sgTextBrowser pass=<password> [e=<filter expression>] [f=<filter file>] [format=CSV/XML/CEF] [host=<Management Server address [\Domain]>] [login=<login name>] [o=<output file>] [m=current/stored] [-v] [-h]</pre>	<p>Displays or exports current or stored logs. This command is available on the Log Server.</p> <p>Enclose the file and filter names in double quotes if they contain spaces.</p> <p>The pass parameter defines the password for the user account used for this operation.</p> <p>The e parameter defines the filter that you want to use for filtering the log data. Type the name as shown in the Management Client. The f parameter defines the StoneGate exported filter file that you want to use for filtering the log data.</p> <p>The format parameter defines the file format for the output file. If this parameter is not defined, the XML format is used.</p> <p>The host parameter defines the address of the Management Server used for checking the login information. If this parameter is not defined, Management Server is expected to be on the same host where the script is run. If Domains are in use, you can specify the Domain the Log Server belongs to. If <code>domain</code> is not specified, the Shared Domain is used.</p> <p>The login parameter defines the username for the account that is used for this export. If this parameter is not defined, the username <code>root</code> is used.</p> <p>The o parameter defines the destination output file where the logs will be exported. If this parameter is not defined, the output is displayed on screen.</p> <p>The m parameter defines whether you want to view or export logs as they arrive on the Log Server (<code>current</code>) or logs stored in the active storage directory (<code>stored</code>). If this option is not defined, the current logs are used.</p> <p>The -h option displays information on using the script.</p> <p>The -v option displays verbose output on command execution.</p>

Engine Commands

The commands in the following two tables can be run on the command line on the analyzer, firewall, and/or sensor engines.

Table A.2 StoneGate-Specific Command Line Tools on Engines

Command	Engine Type	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>firewall, sensor</p>	<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 <code>show</code> 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.2 StoneGate-Specific Command Line Tools on Engines (Continued)

Command	Engine Type	Description
<pre>sg-bootconfig [--primary-console=ttty0 tttyS PORT,SPEED] [--secondary-console=ttty0 tttyS PORT,SPEED] [--flavor=up smp] [--initrd=yes no] [--crashdump=yes no Y@X] [--append=kernel options] [--help] apply</pre>	<p>analyzer, firewall, sensor</p>	<p>Can be used to edit boot command parameters for future bootups.</p> <p>--primary-console=ttty0 tttyS PORT,SPEED parameter defines the terminal settings for the primary console.</p> <p>--secondary-console=ttty0 tttyS PORT,SPEED parameter defines the terminal settings for the secondary console.</p> <p>--flavor=up smp [-kdb] parameter defines whether the kernel is uniprocessor or multiprocessor.</p> <p>--initrd=yes no parameter defines whether Ramdisk is enabled or disabled.</p> <p>--crashdump=yes no Y@X 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=kernel options 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>analyzer, firewall, sensor</p>	<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 local console connection to the engine to use this command.</p>
<pre>sg-cluster [status [-c SECONDS]] [online] [lock-online] [offline] [lock-offline] [standby] [safe-offline]</pre>	<p>firewall</p>	<p>Used to display or change the status of the node.</p> <p>status [-c SECONDS] command displays cluster status. When -c SECONDS is used, status is shown continuously with the specified number of seconds between updates.</p> <p>online command sends the node online.</p> <p>lock-online command sends the node online and keeps it online even if another process tries to change its state.</p> <p>offline command sends the node offline.</p> <p>lock-offline command sends the node offline and keeps it offline even if another process tries to change its state.</p> <p>standby command sets an active node to standby.</p> <p>safe-offline command sets the node to offline only if there is another online node.</p>
<pre>sg-contact-mgmt</pre>	<p>analyzer, firewall, sensor</p>	<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>

Table A.2 StoneGate-Specific Command Line Tools on Engines (Continued)

Command	Engine Type	Description
<pre>sg-dynamic-routing -start -stop -restart -force-reload -backup <file> -restore <file> -sample-config -route-table</pre>	firewall	<p>-start starts the Quagga routing suite.</p> <p>-stop stops the Quagga routing suite and flushes all routes made by zebra.</p> <p>-restart restarts the Quagga routing suite.</p> <p>-force-reload forces reload of the saved configuration.</p> <p>-backup <file> backs up the current configuration to a compressed file.</p> <p>-restore <file> restores the configuration from the specified file.</p> <p>-sample-config creates a basic configuration for Quagga.</p> <p>-route-table prints the current routing table.</p>
<pre>sg-ipsec -d [-u <username[@domain]> -si <session id> -ck <ike cookie> -tri <transform id> -ri <remote ip> -ci <connection id>]</pre>	firewall	<p>Deletes VPN-related information (use <code>vpninfo</code> command to view the information). Option <code>-d</code> (for delete) is mandatory.</p> <p><code>-u</code> deletes the VPN session of the named VPN client user. You can enter the user account in the form <code><username@domain></code> if there are several user storage locations (LDAP domains).</p> <p><code>-si</code> deletes the VPN session of a VPN client user based on session identifier.</p> <p><code>-ck</code> deletes the IKE SA (Phase one security association) based on IKE cookie.</p> <p><code>-tri</code> deletes the IPSEC SAs (Phase two security associations) for both communication directions based on transform identifier.</p> <p><code>-ri</code> deletes all SAs related to a remote IP address in gateway-to-gateway VPNs.</p> <p><code>-ci</code> deletes all SAs related to a connection identifier in gateway-to-gateway VPNs.</p>
<pre>sg-logger -f FACILITY_NUMBER -t TYPE_NUMBER [-e EVENT_NUMBER] [-i "INFO_STRING"] [-s] [-h]</pre>	analyzer, firewall, sensor	<p>Can be used in scripts to create log messages with the specified properties.</p> <p><code>-f FACILITY_NUMBER</code> parameter defines the facility for the log message.</p> <p><code>-t TYPE_NUMBER</code> parameter defines the type for the log message.</p> <p><code>-e EVENT_NUMBER</code> parameter defines the log event for the log message. The default is 0 (H2A_LOG_EVENT_UNDEFINED).</p> <p><code>-i "INFO_STRING"</code> parameter defines the information string for the log message.</p> <p><code>-s</code> parameter dumps information on option numbers to stdout</p> <p><code>-h</code> parameter displays usage information.</p>

Table A.2 StoneGate-Specific Command Line Tools on Engines (Continued)

Command	Engine Type	Description
sg-raid [-status] [-add] [-re-add] [-force] [-help]	analyzer, firewall, sensor	Configures a new hard drive. This command is only for StoneGate appliances that support RAID (Redundant Array of Independent Disks) and have two hard drives. -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.
sg-reconfigure [--boot] [--maybe-contact] [--no-shutdown]	analyzer, firewall, sensor	Used for reconfiguring the node manually. --boot option applies bootup behavior. Do not use this option unless you have a specific need to do so. --maybe-contact option contacts the Management Server if requested. This option is only available on firewall engines. --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.
sg-selftest [-d] [-h]	firewall	Runs cryptography tests on the engine. -d option runs the tests in debug mode. -h option displays usage information.
sg-status [-l] [-h]	analyzer, firewall, sensor	Displays information on the engine's status. -l option displays all available information on engine status. -h option displays usage information.

Table A.2 StoneGate-Specific Command Line Tools on Engines (Continued)

Command	Engine Type	Description
<code>sg-toggle-active SHA1 SIZE --force [--debug]</code>	analyzer, firewall, sensor	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>). 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. <code>--debug</code> option reboots the engine with the debug kernel. <code>--force</code> option switches the active configuration without first verifying the signature of the inactive partition.
<code>sg-upgrade</code>	firewall	Upgrades the node by rebooting from the installation CD-ROM. Alternatively, the node can be upgraded remotely using the Management Client.
<code>sg-version</code>	analyzer, firewall, sensor	Displays the software version and build number for the node.
<code>sginfo</code> <code>[-f] [-d] [-s] [-p] [--] [--help]</code>	analyzer, firewall, sensor	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. <code>-f</code> option forces <code>sgInfo</code> even if the configuration is encrypted. <code>-d</code> option includes core dumps in the <code>sgInfo</code> file. <code>-s</code> option includes slapcat output in the <code>sgInfo</code> file. <code>-p</code> option includes passwords in the <code>sgInfo</code> file (by default passwords are erased from the output). <code>--</code> option creates the <code>sgInfo</code> file without displaying the progress <code>--help</code> option displays usage information.

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.3 General Command Line Tools on Engines

Command	Description
<code>dmesg</code>	Shows system logs and other information. Use the <code>-h</code> option to see usage.

Table A.3 General Command Line Tools on Engines (Continued)

Command	Description
halt	Shuts down the system.
ip	Displays IP address information. Type the command without options to see usage. Example: type ip addr for basic information on all interfaces.
ping	Tests connectivity with ICMP echo requests. Type the command without options to see usage.
ps	Reports the status of running processes.
reboot	Reboots the system.
scp	Secure copy. Type the command without options to see usage.
sftp	Secure FTP. 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.
traceroute	Traces the route packets take to the specified destination. Type the command without options to see usage.
vpninfo	Displays VPN information and allows you to issue some basic commands. Type the command without options to see usage.

Server Pool Monitoring Agent Commands

You can test and monitor the Server Pool Monitoring Agents on the command line with the commands described in the table below.

Table A.4 Server Pool Monitoring Agent Commands

Command	Description
<code>sgagentd [-d]</code> <code>[-v level]</code> <code>[-c path]</code> <code>[test [files]]</code> <code>[syntax [files]]</code>	<p>Allows you to test different configurations before activating them.</p> <ul style="list-style-type: none"><code>-d</code> Don't Fork as a daemon. All log messages are printed to stdout or stderr only.<code>-v level</code> Set the verbosity level. The default level is 5. Levels 6-8 are for debugging where available.<code>-c path</code> Use the specified path as the first search directory for the configuration. <p><code>test [files]</code> Run in the test mode - status queries do not receive a response. If you specify the files, they are used for reading the configuration instead of the default files. The output is directed to syslog or eventlog instead of the console where the command was run unless you use the <code>-d</code> option.</p> <p><code>syntax [files]</code> Check the syntax in the configuration file. If no files are specified, the default configuration files are checked. The output is directed to syslog or eventlog instead of the console where the command was run unless you use the <code>-d</code> option.</p>

Table A.4 Server Pool Monitoring Agent Commands (Continued)

Command	Description
<p>sgmon <code>[status/info/proto]</code> <code>[-p port]</code> <code>[-t timeout]</code> <code>[-a id]</code> <code>host</code></p>	<p>Sends a UDP query to the specified host and waits for a response until received, or until the timeout limit is reached.</p> <p>The request type can be defined as a parameter. If no parameter is given, <code>status</code> is requested. The commands are:</p> <p><code>status</code> - query the status.</p> <p><code>info</code> - query the agent version.</p> <p><code>proto</code> - query the highest supported protocol version.</p> <p><code>-p port</code> Connect to the specified port instead of the default port.</p> <p><code>-t timeout</code> Set the timeout (in seconds) to wait for a response.</p> <p><code>-a id</code> Acknowledge the received log messages up to the specified <code>id</code>. Each response message has an <code>id</code>, and you may acknowledge more than one message at a given time by using the <code>id</code> parameter. Note that messages acknowledged by <code>sgmon</code> will no longer appear in the firewall logs.</p> <p><code>host</code></p> <p>The IP address of the host to connect to. To get the status locally, you may give <code>localhost</code> as the host argument. This parameter is mandatory.</p> <p>Return value:</p> <p>0 if the response was received</p> <p>1 if the query timed out</p> <p>-1 in case of an error</p>

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 92)
- ▶ [Firewall/VPN Engine Ports](#) (page 94)
- ▶ [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

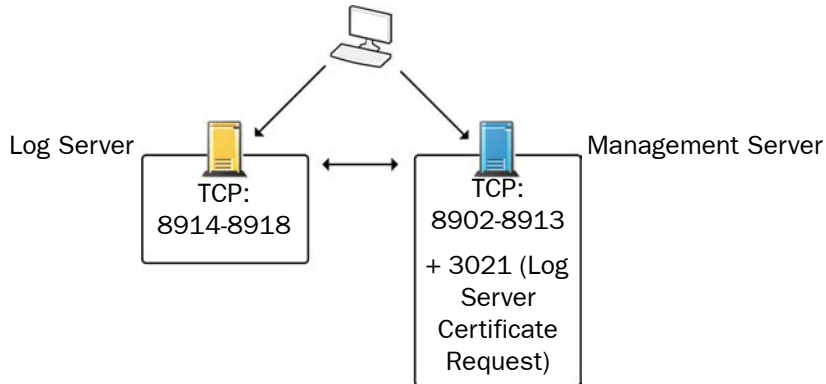
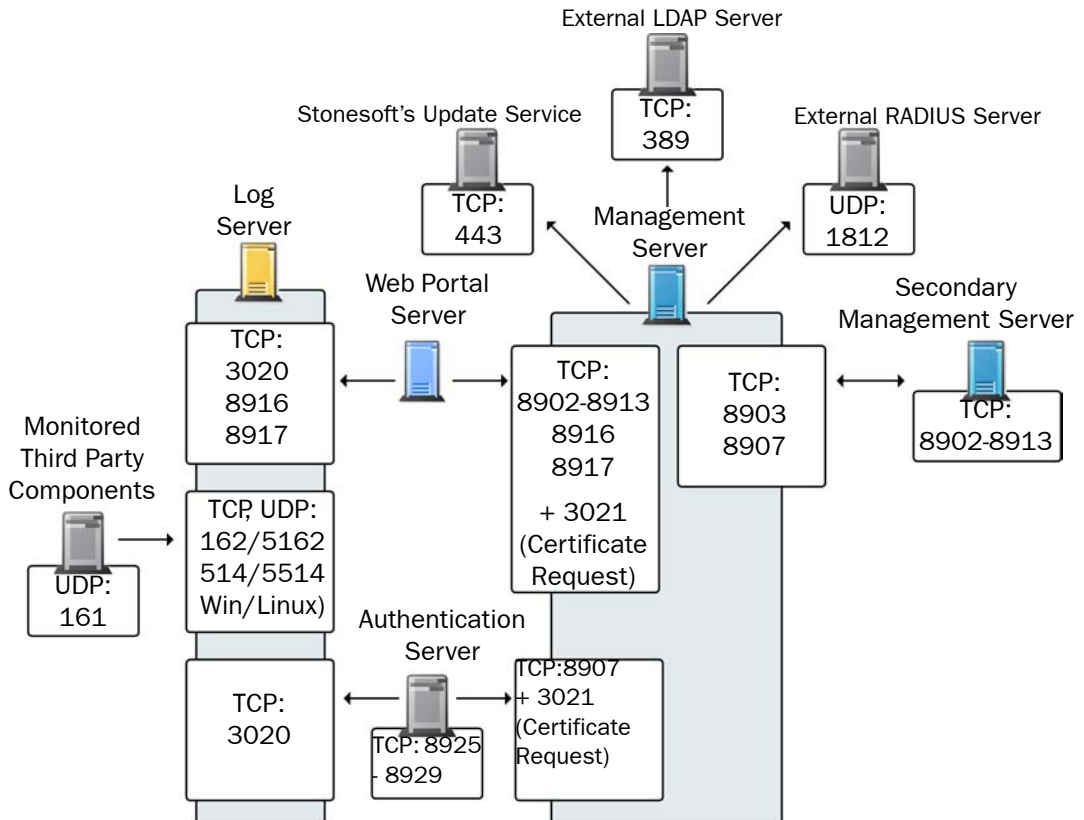


Illustration B.2 Default Destination Ports for Optional SMC Components and Features



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]

Firewall/VPN Engine Ports

The illustrations below present an overview to the most important default ports used in communications between firewall/VPN engines and the SMC and between clustered firewall engines. See the table below for a complete list of default ports for the fully-featured firewall/VPN engines.

Illustration B.3 Destination Ports for Basic Firewall/VPN Engine Communications

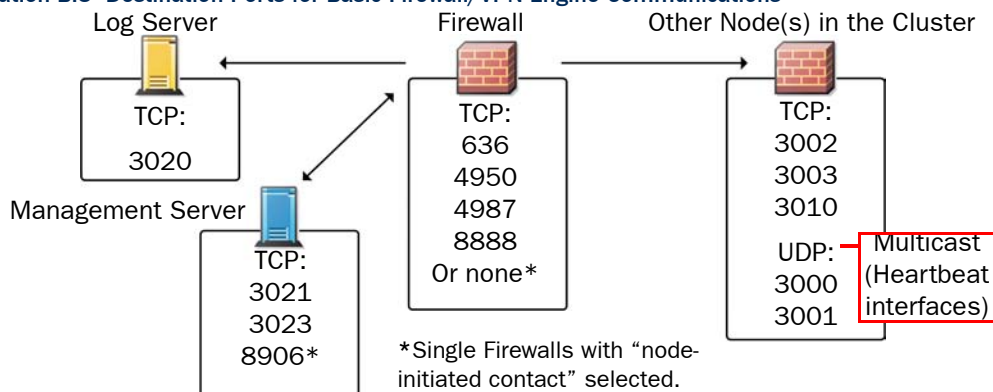
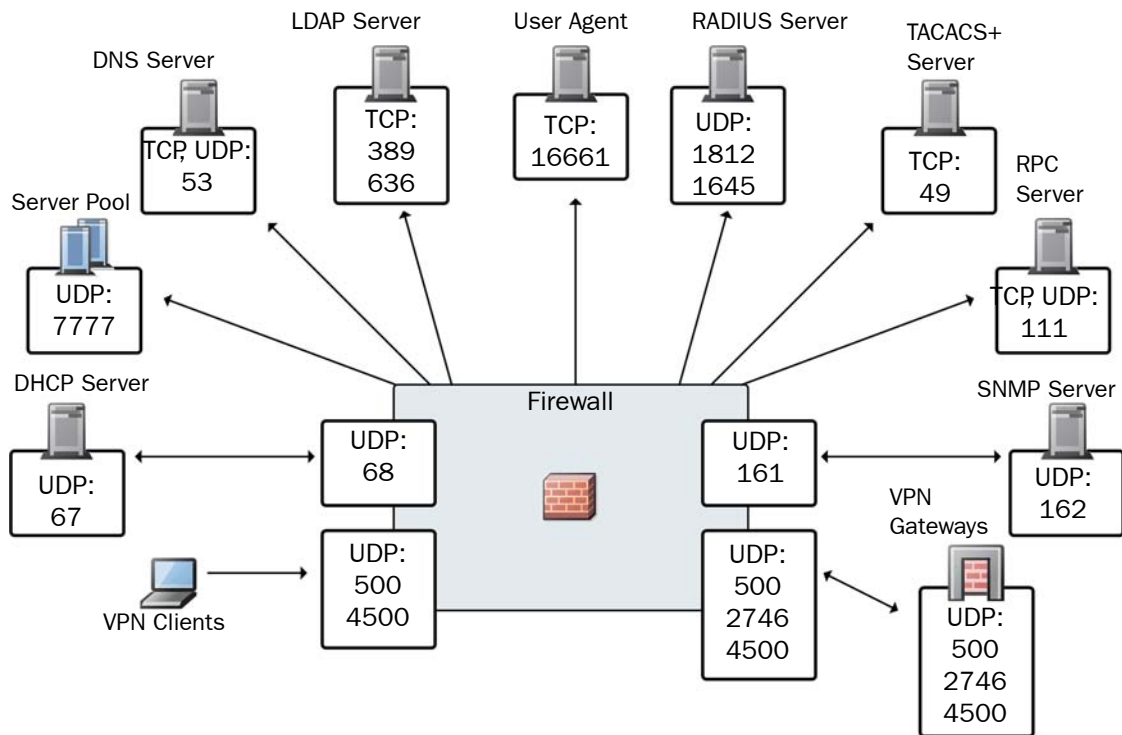


Illustration B.4 Default Destination Ports for Firewall/VPN Engine Service Communications



The table below lists all default ports StoneGate Firewall/VPN 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 Firewall/VPN Default Ports

Listening Host	Port/Protocol	Contacting Hosts	Service Description	Service Element Name
Anti-virus signature server	80/TCP	Firewall	Anti-virus signature update service.	HTTP
Authentication Server	8925-8929/TCP	Firewall	User directory and authentication services.	LDAP (TCP), RADIUS (Authentication)
BrightCloud Server	2316/TCP	Firewall	BrightCloud web filtering update service.	BrightCloud update
DHCP server	67/UDP	Firewall	Relayed DHCP requests and requests from a firewall that uses dynamic IP address.	BOOTPS (UDP)
DNS server	53/UDP, 53/TCP	Firewall	Dynamic DNS updates.	DNS (TCP)
Firewall	67/UDP	Any	DHCP relay on firewall engine.	BOOTPS (UDP)

Table B.2 Firewall/VPN Default Ports (Continued)

Listening Host	Port/Protocol	Contacting Hosts	Service Description	Service Element Name
Firewall	68/UDP	DHCP server	Replies to DHCP requests.	BOOTPC (UDP)
Firewall	161/UDP	SNMP server	SNMP monitoring.	SNMP (UDP)
Firewall	500/UDP	VPN clients, VPN gateways	VPN negotiations, VPN traffic.	ISAKMP (UDP)
Firewall	636/TCP	Management Server	Internal user database replication.	LDAPS (TCP)
Firewall	2543/TCP	Any	User authentication (Telnet) for Access rules.	SG User Authentication
Firewall	2746/UDP	StoneGate VPN gateways	UDP encapsulated VPN traffic.	SG UDP Encapsulation
Firewall	3000-3001/ UDP 3002-3003, 3010/TCP	FW/VPN engine	Heartbeat and state synchronization between clustered firewalls.	SG State Sync (Multicast), SG State Sync (Unicast), SG Data Sync
Firewall	4500/UDP	VPN client, VPN gateways	VPN traffic using NAT-traversal.	NAT-T
Firewall	4950/TCP	Management Server	Remote upgrade.	SG Remote Upgrade
Firewall	4987/TCP	Management Server	Management Server commands and policy upload.	SG Commands
Firewall	8888/TCP	Management Server	Connectivity monitoring; monitoring of blacklists, connections, and status for old engine versions.	SG Monitoring
Firewall	15000/TCP	Management Server, analyzer	Blacklist entries.	SG Blacklisting
LDAP server	389/TCP	Firewall	External LDAP queries, including StartTLS connections.	LDAP (TCP)
Log Server	3020/TCP	Firewall	Log and alert messages; monitoring of blacklists, connections, status, and statistics.	SG Log
Management Server	3021/TCP	Firewall	System communications certificate request/renewal (initial contact).	SG Initial Contact
Management Server	3023/TCP	Firewall	Monitoring (status) connection.	SG Reverse Monitoring

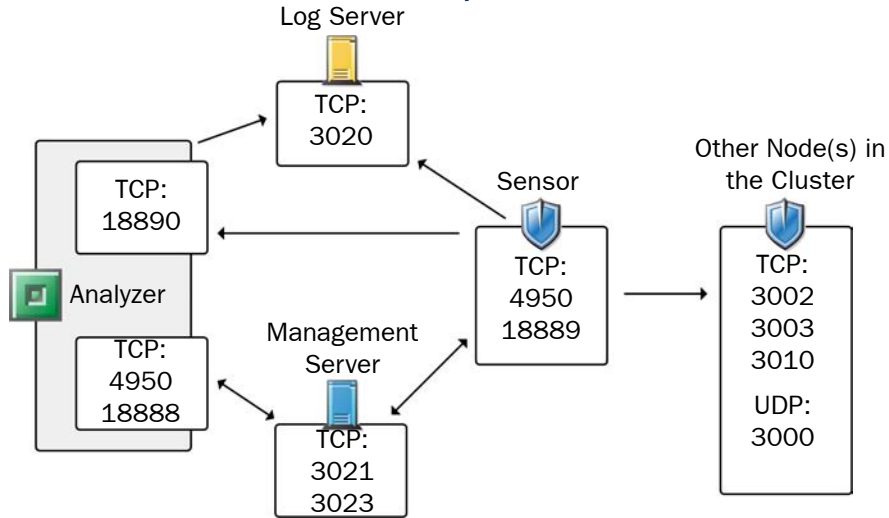
Table B.2 Firewall/VPN Default Ports (Continued)

Listening Host	Port/Protocol	Contacting Hosts	Service Description	Service Element Name
Management Server	8906/TCP	Firewall	Management connection for Single Firewalls with “node-initiated contact” selected.	SG Dynamic Control
RADIUS server	1812, 1645/UDP	Firewall	RADIUS authentication requests.	RADIUS (Authentication), RADIUS (Old)
RPC server	111/UDP, 111/TCP	Firewall	RPC number resolve.	SUNRPC (UDP), Sun RPC (TCP)
Server Pool Monitoring Agents	7777/UDP	Firewall	Polls to the servers’ Server Pool Monitoring Agents for availability and load information.	SG Server Pool Monitoring
SNMP server	162/UDP	Firewall	SNMP traps from the engine.	SNMP Trap (UDP)
TACACS+ server	49/TCP	Firewall	TACACS+ authentication requests.	TACACS (TCP)
User Agent	16661/TCP	Firewall	Queries for matching Users and User Groups with IP addresses.	SG Engine to User Agent
VPN gateways	500/UDP, 2746/UDP (StoneGate gateways only), or 4500 UDP	Firewall	VPN traffic. Ports 2746 and 4500 may be used depending on encapsulation options.	ISAKMP (UDP)

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.5 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.3 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

Table B.3 IPS-Specific Ports (Continued)

Listening Hosts	Port/Protocol	Contacting Hosts	Service Description	Service Element Name
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
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

INDEX

A

administration client, see management client
authentication server
 installing, 26

B

binding licenses, 32

C

certificate authority
 checking fingerprint, 30
checksums, 14
command line installation
 see non-graphical installation
command line tools, 73
commands
 engine, 83
 log server, 74
 management server, 74
compatibility with different platforms, 13
contact addresses, 47–53
 exceptions, 51, 52
contact information, 10
customer support, 10

D

database user account, 23
date and time settings, 13
demo mode, 27
documentation available, 9

E

exceptions to contact addresses, 51, 52

F

file integrity, 14
fingerprint of certificate authority, 30
fingerprint of certificates, 81

G

generating server certificates, 34
GUI client, see management client

H

hardware requirements, 10
hosts file, 13

I

installation files, 14

 creating CD-ROMs, 14
integrity of files, 14

J

java web start, 43–46

L

licenses, 15
 binding, 32
 checking, 31, 61
 installing, 31, 61
 retained, 33
 upgrading, 15, 59–61
linux for management center, 20
locations, 47–53
log server
 contact addresses, 51–53
 installing, 24–25
 starting, 33

M

management bound licenses, 32
management center
 components, 12
 installing, 19–42
 upgrading, 62
management client
 configuration files, 68
 installing, 20, 43–46
 installing using web start, 44–46
 logging in, 30
 setting location, 53
 starting, 29
 web start, 46
management server
 contact addresses, 51–53
 database user account, 23
 installing, 23–24
 starting, 29
MD5 checksum, 14
monitoring server, see web portal server

N

NAT (network address translation), 47–53
 locations, 47–53
non-graphical installation, 41–42

O

overview to the installation, 13

P

- planning installation, 11–15
- platforms supported, 13

R

- requirements for hardware, 10
- retained licenses, 33

S

- secondary management servers, installing, 37–40
- servers
 - authentication server, 26
 - certifying, 34
 - log server, 24–25
 - management server, 23–24
 - secondary management servers, 37–40
 - starting manually, 33
 - web portal server, 25
- sgadmin user account, 20
- SHA-1 checksum, 14
- starting
 - log server, 33
 - management client, 29
 - management server, 29
 - servers manually, 33
 - web portal server, 33
- stonegate architecture, 12
- support services, 10
- supported platforms, 13
- system architecture, 12
- system requirements, 10

T

- technical support, 10
- typographical conventions, 8

U

- uninstalling, 67–69
- upgrading, 57–65
 - licenses, 59–61
 - management center, 62

W

- web portal server
 - installing, 25
 - starting, 33
- web start, 43–46
 - enabling web start server, 44–45
- web start files
 - creating manually, 45–46

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