

StoneGate™



StoneGate™
SSL-3200 Series

Appliance Installation Guide

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) No 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.

SSL VPN Powered by PortWise.

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.

Revision: SGAIG_SSL-3200_Series_20110502

Introduction

Thank you for choosing Stonesoft's StoneGate™ appliance. This guide provides instructions for the initial hardware installation and the maintenance of the SSL-3200 Series appliances. See *Product Documentation* (page 4) for information on other available documentation.

The use of the appliance is subject to the acceptance of the End User License Agreement, which can be found at the Stonesoft website.

Contents

Installation Procedure	4
Product Documentation	4
Safety Precautions	5
Unpacking the Appliance	8
Front Panel	9
Back Panel	12
Installing the Solid State Disk	13
Installing Express Modules	14
Rack-Mounting	15
Connecting the Cables	21
Configuring the Appliance	24
Managing the Appliance	43
Maintenance Operations.....	45
Disposal Instructions	52

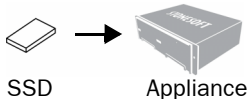


Caution – Never open the covers of the appliance! There are no user serviceable parts inside. Opening the covers may lead to serious injury and will void the warranty. Read the *Safety Precautions* (page 5) before you conduct any installation or maintenance operations on the appliance.

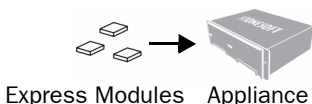
Installation Procedure

▼ To install the appliance

1. If the Solid State Disk (SSD) is not pre-installed in the appliance, install the SSD. See *Installing the Solid State Disk* (page 13).



2. Install an express module in each slot on the appliance. See *Installing Express Modules* (page 14).



3. Install the appliance into a rack and connect the cables. See *Rack-Mounting* (page 15) and *Connecting the Cables* (page 21).
4. Configure the basic system settings (time, interfaces, and routing), and import the license and a certificate. See *Configuring the Appliance* (page 24).

Product Documentation

The available PDF documentation can be accessed through the StoneGate SSL VPN Administrator's front page. The StoneGate SSL VPN Administrator also has embedded instructions that you can open by clicking the **Help** link or question mark icon on the various pages. Install the free Adobe Reader program to view the PDF documents (available at www.adobe.com/reader/).

Safety Precautions

The following safety information and procedures must be followed whenever working with the StoneGate Appliance. However, be advised that StoneGate Appliances are not end-user serviceable, and you must never open the appliance covers for any reason. Doing so may lead to serious injury and will void any hardware warranty that may be associated with your appliance.

Electrical Safety Precautions

Basic electrical safety precautions should be followed to protect yourself from harm and the appliance from damage:

- Be aware of the location of the power button as well as the room's emergency power-off switch, disconnection switch, or electrical outlet. If an electrical accident occurs, you can then quickly cut power to the system.
- Do not work alone when working with high-voltage components.
- Before removing or installing main system components, be sure to disconnect the power first. Turn off the system before you disconnect the power cord.
- Use only one hand when working with powered-on electrical equipment. This is to avoid making a complete circuit, which will cause electrical shock. Use extreme caution when using metal tools, which can easily damage any electrical components or circuit boards they come into contact with.
- Do not use mats designed to decrease electrostatic discharge as protection from electrical shock. Instead, use rubber mats that have been specifically designed as electrical insulators.
- The power supply cord must include a grounding plug and must be plugged into a grounded electrical outlet. Use only the cord supplied with the appliance.
- The power cord plug cap that plugs into the AC receptacle on the power supply must be an IEC 320, sheet C13, type female connector.
- If you have to replace the motherboard battery, install it the same way as the original battery. Make sure that the positive side faces up on the motherboard. This battery must be replaced only with the same or an equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.
- Do not open the enclosures of power supplies or SSD Drive to avoid injury.

General Safety Precautions

Follow these rules to ensure general safety:

- Keep the area around the appliance clean and free of clutter.
- The appliance weighs approximately 13 kg (29 lbs.) when fully loaded. When lifting the appliance, two people at either end should lift slowly with their feet spread out to distribute the weight. Always keep your back straight and lift with your legs.
- We recommend using a regulating uninterruptible power supply (UPS) to protect the appliance from power surges, voltage spikes and to keep your system operating in case of a power failure.

Power Supplies

Appliances with DC Power Supply

- The appliance must be used in a Restricted Access Location and the users must be well-trained to operate it.
- The socket-outlet for pluggable equipment must be installed near the equipment and must be easily accessible.
- Appliance inlet must have SPS approval or have min. 15 AWG wire provided for the power supply.
- The Mains Supply plug on the power supply cord is the disconnect device of the appliance. To disconnect the appliance, you must first disconnect the mains and then disconnect the ground.

Appliances with AC Power Supply

- The appliance inlet is the disconnect device.

ESD Precautions

Electrostatic discharge (ESD) is generated by two objects with different electrical charges coming into contact with each other. An electrical discharge is created to neutralize this difference, which can damage electronic components and printed circuit boards. Use a grounded wrist strap designed to prevent static discharge.

Note – Use a UPS (Uninterruptible Power Supply) in critical environments with your StoneGate appliance. If after a brief power outage your StoneGate appliance only partially starts up (for example, the power light is on, but the NIC LEDs are off and the appliance does not connect) turn the appliance off for five seconds and then back on.

Laser Precautions

Class 1 Laser Product



Caution – Invisible laser radiation is emitted from the end of fiber cable and from aperture of the port when no fiber cable is connected. Do not stare into the beam and avoid direct exposure to the beam.

Operating Precautions

Care must be taken to assure that the appliance cover is in place when the appliance is operating to ensure proper cooling. If this rule is not strictly followed, the warranty may become void. Do not open the power supply casing. Power supplies can only be accessed and serviced by a qualified technician of the manufacturer.

Operating and Storage Temperatures

The allowed operating temperature of the appliance is +5...+35°C. The allowed storage temperature is -20...+65°C. Do not operate or store the appliance in temperatures outside these limits. If the appliance or the express modules have been stored in temperatures below 0°C or above +40°C, allow for 2 hours to bring the appliance and the express modules to normal operating temperature before turning on the appliance. Otherwise, the appliance or the express modules may be damaged.

Lithium Battery Precautions



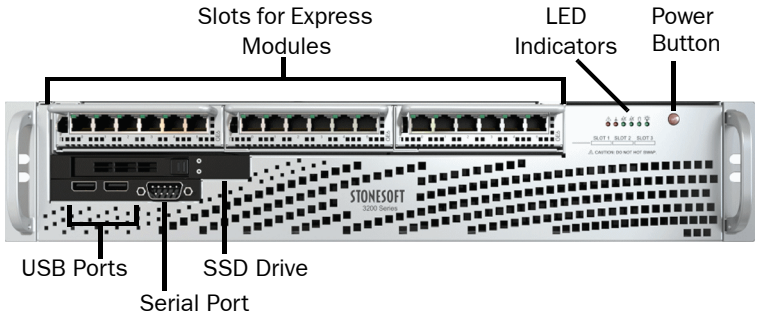
Caution – The battery must be replaced by authorized service personnel only. Danger of explosion if battery is incorrectly replaced. Replacement battery must be same or equivalent type recommended by the manufacturer. Used batteries must be discarded according to the manufacturer's instructions. Short-circuiting the battery may heat the battery and cause severe injuries.

Unpacking the Appliance

Inspect the box the appliance was shipped in and any other boxes included in the delivery. If the Solid State Disk (SSD) is not pre-installed in the appliance, the SSD is delivered in a separate box. The express modules are always delivered in separate boxes. Note if any of the boxes are damaged in any way. If the appliance itself or any components delivered with the appliance show any damage, file a damage claim with the carrier who delivered the appliance or the components.

Do not remove the anti-tamper tapes on any part of the appliance.

Front Panel



On the front panel, there are slots for the StoneGate express modules, a Solid State Disk (SSD) Drive, two USB ports, and a serial port. There are two more USB ports on the back of the appliance. See *Back Panel* (page 12).

The front panel also has six LED indicators and the Power button. The status of the Power button and all the indicators on the front panel (including the indicators for the SSD Drive) are explained below. See the separate *Express Module Guide* delivered with the appliance for information on the port indicators for the express modules.

Power Button







Table 1 Power Status

Status	Explanation
Green	Indicates power is being supplied to the system's power supply unit. This LED is illuminated when the system is operating normally.

LED Indicators

The front panel has six LED indicators in the upper right corner. The LEDs provide you with critical information related to different parts of the system.

Table 2 Front Panel LEDs

	Indicates a power failure in the power supply when flashing.
	When flashing, indicates a fan failure. When continuously on, indicates an overheat condition, which may be caused by cables obstructing the airflow in the system or the ambient room temperature being too warm.
	Indicates network activity on the onboard Ethernet interface 1 when flashing (the interface is on the back panel of the appliance).
	Indicates network activity on the onboard Ethernet interface 0 when flashing (the interface is on the back panel of the appliance).
	Indicates hard drive activity when flashing.
	Indicates power is being supplied to the system's power supply units. This LED is illuminated when the system is operating normally.

SSD Drive Indicators

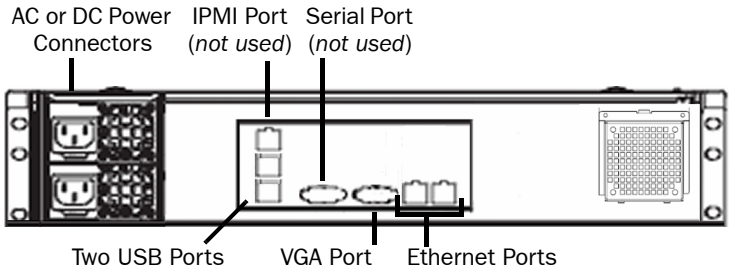
The indicators for the Solid State Disk (SSD) Drive are explained below.



Table 3 SSD Drive Indicators

Indicator	Status	Explanation
Power	Blue	A Solid State Disk is in the drive.
Disk	Unlit	This indicator is not currently used.

Back Panel



The LED indicators for the two fixed Ethernet ports are explained below.

Fixed Ports



Table 4 Indicators for Fixed Ports

Indicator	Color	Explanation
Activity	Yellow	Link ok, blinks on activity.
Link	Unlit	No link or the speed is 10 Mbps.
	Green	Speed is 100 Mbps.
	Amber	Speed is 1 Gbps.

Installing the Solid State Disk

If the Solid State Disk (SSD) is not pre-installed in the appliance, you must first install the SSD.



Caution – We recommend using a grounding strap when handling an SSD. Uninstalled SSDs are sensitive to ESD damage.

▼ To install the Solid State Disk

1. Locate the Solid State Disk included in the delivery package.
2. Locate the Solid State Disk Drive on the appliance's back panel (see the illustration in *Back Panel* (page 12)).
3. Press the release button on the Solid State Disk to release the lever on the disk.



4. Insert the disk into the drive.
5. Press the lever down to lock the disk into position.

Proceed to *Installing Express Modules* (page 14).

Installing Express Modules

This section provides information on installing StoneGate express modules into the appliance. You must install an express module in each slot before you can make the appliance operational. The process of installing an express module is the same for all express module types. Read the *Safety Precautions* (page 5) before proceeding.



Caution – Do not install or remove express modules if the appliance is powered on to avoid damaging the express modules and the modular appliance.

▼ To install an express module

1. Make sure that the appliance is turned off and that no cables are connected to the appliance or to wall outlets.
2. (*Recommended*) Fasten a grounding strap to your wrist so that it contacts your bare skin and attach the other end of the strap to the appliance.
3. Select the slot where you want to install the express module.
4. Push the module into the slot the sticker side up until the front panel of the module is even with the front panel of the appliance.



Caution – Do not insert the express module upside down. Inserting the express module incorrectly may damage the appliance and the express module and will void the warranty.

5. Repeat steps 3 and 4 until you have installed an express module in each slot.
 - You must install an express module in each slot before you can configure the appliance.

Proceed to *Rack-Mounting* (page 15).

Rack-Mounting

This section provides information on installing the StoneGate appliance into a rack unit. You can install the appliance into a two-post or a four-post rack unit.



Caution – Read the *Safety Precautions* (page 5) before proceeding.

Preparing for Rack-Mounting

The appliance delivery includes the rail assemblies and the mounting screws you need to install the system into the rack.

Read the sections below before you begin the installation.

Choosing a Setup Location

Decide on a suitable location for the rack unit that will hold the appliance:

- The appliance must be situated in a clean, dust-free area that is well ventilated.
- Avoid areas where heat, electrical noise and electromagnetic fields are generated.
- Leave enough clearance in front of the rack to enable you to open the front door completely (~63 cm/25 inches).
- Leave enough clearance in the back of the rack to allow for sufficient airflow and ease in servicing (~76 cm/30 inches).

Rack Precautions

- Ensure that the leveling jacks on the bottom of the rack are fully extended to the floor with the full weight of the rack resting on them.
- In single rack installation, stabilizers should be attached to the rack.
- In multiple rack installations, the racks should be coupled together.
- Always make sure the rack is stable before extending a component from the rack.
- Extend only one component at a time—extending two or more simultaneously may cause the rack to become unstable.

Appliance Precautions

- Determine the placement of each component in the rack before you install the rails.
- Install the heaviest components on the bottom of the rack first, and then work up.

- The appliance must be connected to grounded power outlets.
- Use a regulating uninterruptible power supply (UPS) to protect the appliance from power surges, voltage spikes and to keep your system operating in case of a power failure.
- Always keep the rack's front door and all panels and components on the appliances closed when not servicing to maintain proper cooling.

Before Installing the Appliance Into a Rack

- Make sure that the rack is securely anchored onto an unmovable surface or structure before installing the appliance into the rack.
- Unplug the power cord(s) of the rack before installing the appliance into the rack.
- Make sure that the system is adequately supported. Make sure that all the components are securely fastened to the appliance to prevent components falling off from the appliance.
- Be sure to install an AC power disconnect for the entire rack assembly. This power disconnect must be clearly marked.
- The rack assembly shall be properly grounded to avoid electric shock.
- The rack assembly must provide sufficient airflow to the appliance for proper cooling.

Installing the Appliance into a Rack

Note – Do not install the appliance upside down.

This section provides information on installing the appliance into a rack unit. There are a variety of rack units on the market, so the assembly procedure may differ slightly from what is instructed. If necessary, refer to the instructions that came with the rack unit you are using.

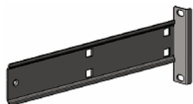
If you are installing the appliance into a Telco-type rack, follow the general directions below. The main difference in the installation procedure is whether you are installing the appliance into a two-post rack or a four-post rack. Proceed to one of the following:

- *Installing the Appliance Into a Two-Post Rack* (page 17)
- *Installing the Appliance Into a Four-Post Rack* (page 18)

Installing the Appliance Into a Two-Post Rack

▼ To install the appliance into a two-post rack

1. Locate the two rack-mounting brackets that are meant for the two-post rack installation.



2. Locate the three pairs of supports on the side of the appliance and the corresponding holes on the brackets.
3. Align the holes against the two supports towards the rear of the appliance and push the bracket under the supports.
 - The brackets are marked with L for “left” and “R” for right.



4. Secure the bracket to the appliance by inserting a screw through the hole at the end of the bracket (see the illustration above).
5. Repeat steps 3 and 4 on the other side of the appliance.
6. Attach each bracket to the rack with two screws through the holes in the front of the bracket.

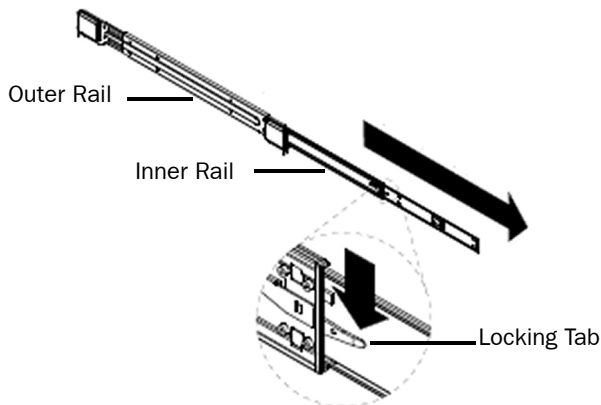
Proceed to *Connecting the Cables* (page 21).

Installing the Appliance Into a Four-Post Rack

There are two sets of rails that you can use for installing the appliance into a four-post rack. The only difference is the length of the rails. This section explains the installation for both types of rails.

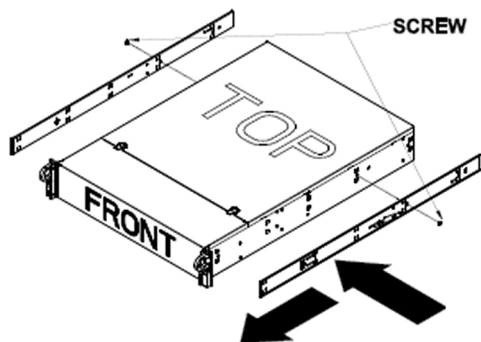
▼ To install the appliance into a four-post rack

1. Locate the two pairs of brackets in the delivery package: two inner rails that attach to the appliance and two outer rails that attach to the rack.

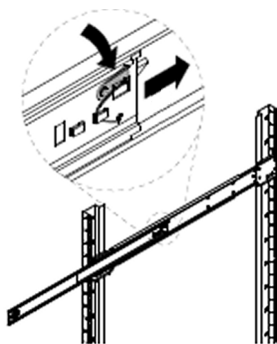


2. Detach the inner rails from the outer rails (press the locking tab to release the inner rails as shown in the illustration above).
 - The rails are marked with L for “left” and “R” for right.
3. Locate the rail buttons on the side of the appliance and the corresponding holes on an inner rail.

4. Align the holes against its corresponding button. Once all are aligned, push the holes toward their corresponding buttons.

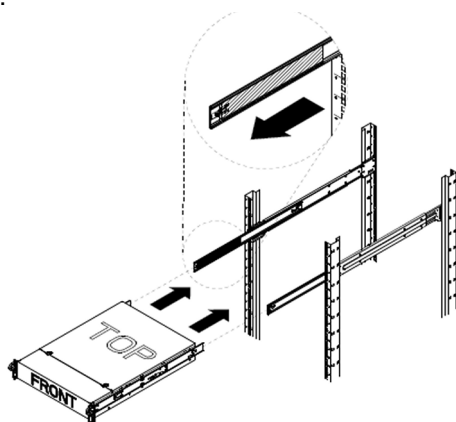


5. Secure the rail to the appliance with a screw.
6. Repeat steps 3-5 on the other side of the appliance.
7. Insert the outer rails to the rack. If necessary, push the locking tab on the rail to retreat the outer rails.



8. Attach the outer rails to the rack with two screws through the holes at the ends of the rails.

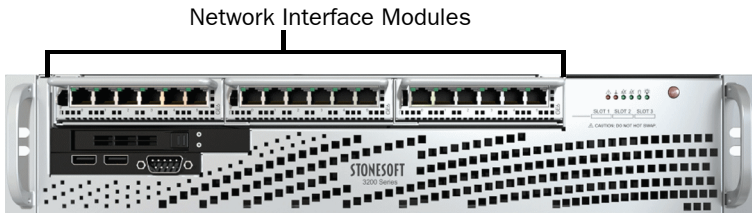
- 9.** Line up the rear of the inner rails with the front of the extended outer rails.



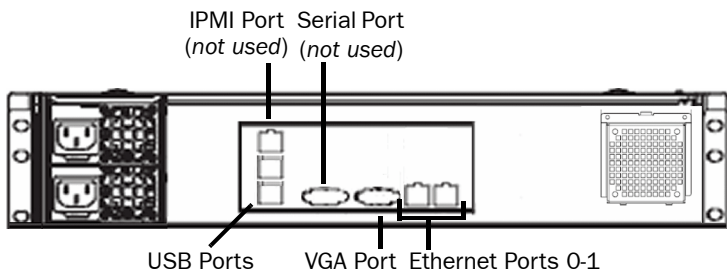
- 10.** Slide the inner rails into the outer rails, keeping the pressure even on both sides (you may have to press the locking tabs when inserting). When the appliance has been pushed completely into the rack, you should hear the locking tabs “click” as the rails lock. Proceed to *Connecting the Cables* (page 21).

Connecting the Cables

Front Panel



Back Panel



Connecting Network Cables

1. Connect the supplied network cable to the management port eth0 on the appliance's back panel and to the network port of a computer that you will use to configure the appliance.
 - The default IP address of the management port is 192.168.100.1. You can change the default IP address when you configure the appliance. Configure the computer you use for connecting to the appliance to use an IP address in the same network (192.168.100.0/24). See *Configuring the Appliance* (page 24) for information on how to connect to and configure the appliance.
 - The management port's IP address is active only when a network cable is plugged into the port.
2. Connect network cables to the Ethernet ports.
 - The two Ethernet ports 0-1 on the back panel belong to slot 0. The slot numbers for the express modules on the front panel

start from 1. The port numbers on the modules start from 0. Both slot and port numbers increase from left to right.

- You are free to choose which Ethernet ports you connect to which network. The Ethernet ports are mapped to Interface IDs during the initial configuration. See the next section for information on connecting network cables to the SFP ports on SFP express modules.

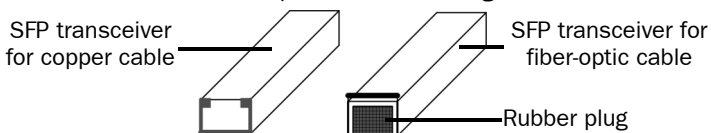
Note – When the appliance is powered and you need to unplug it, always wait at least five (5) seconds before plugging in the appliance again. Otherwise, the appliance may not have time to clear properly and fails to start.

Connecting Cables to SFP Ports

If you have installed an SFP express module on the appliance, you can use the ports on the module as either copper or fiber ports by inserting a small form-factor pluggable (SFP) transceiver for copper or fiber-optic cable into the ports.

▼ To connect cables to SFP ports

1. Insert the SFP transceiver in the port slot until you feel the connector on the transceiver snap into place. The illustration below shows the correct position of inserting the SFP transceiver.



Note – Make sure that the latch on the SFP transceiver is up (see the illustration above) when you insert the SFP transceiver in the port slot.

2. If the SFP transceiver has a rubber plug, remove the plug after inserting the transceiver into the slot.
3. Connect the copper or fiber-optic cable to the SFP transceiver.

Note – Each SFP port must match the wavelength specifications at the other end of the cable. The cable must not exceed the stipulated cable length for reliable communications.

Cable Types

Make sure that the copper cables you use are correctly rated (CAT 5e or CAT 6 in gigabit networks).

Speed/Duplex Settings

Network cards at both ends of each cable must have identical speed/duplex settings. This also applies to the automatic negotiation setting: if one end of the cable is set to autonegotiate, the other end must also be set to autonegotiate. Gigabit standards require interfaces to use autonegotiation—fixed settings are not allowed at gigabit speeds.

Connecting Management Cables

▼ To connect management cables

- Choose one of the following:
 - Connect a monitor to the VGA port on the appliance's back panel and a keyboard to a USB port.
 - Or connect the supplied null-modem cable to the serial port on the appliance's front panel and to a computer that you will use for a terminal connection.

Connecting the Appliance to the Power Supply

▼ To connect the appliance to the power supply

1. Connect the power cables to the AC or DC power connectors on the back of the appliance.
 - We recommend connecting both power connectors to a power source to guarantee that the appliance can function even if one of the power connectors fails.
2. Plug the power cords into grounded, high-quality power strips that offer protection from electrical noise and power surges.
 - We highly recommend using an uninterruptible power supply (UPS) to ensure continuous operation and minimize the risk of damage to the appliance in case of sudden loss of power.
 - For a truly redundant power supply, connect each power connector on the appliance to a different UPS, so that the failure of one UPS will not cut off the power to both power supplies.

See *Safety Precautions* (page 5) for more information on the AC and DC power supplies.

Proceed to *Configuring the Appliance* (page 24).

Configuring the Appliance

Before the appliance can offer any services to the users, you must configure the networking settings for all interfaces you intend to use. Start by *Defining the Basic Settings*.

Defining the Basic Settings


The only interface that is defined when you receive the appliance is the management port eth 0 on the appliance's back panel. The default IP address of the management port is 192.168.100.1. You can change the default IP address and other default settings for the appliance in the engine configuration wizard.

▼ To start the engine configuration wizard

1. Connect the supplied null-modem cable to the serial port on the appliance's front panel and to a computer that you will use for a terminal connection.
2. On the computer, open a terminal with settings 9600bps, 8 databits, 1 stopbit, no parity.
3. Turn on the appliance using the power button. The engine bootup process is shown in the console and, after some time, the engine configuration wizard starts.

▼ To set the keyboard layout

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



```
Configure OS settings
Keyboard layout:      <US English>
Local timezone:      <unset>
Host name:           stonegate
Root password has been set: <Change...>
```

2. Highlight the correct layout and press ENTER.

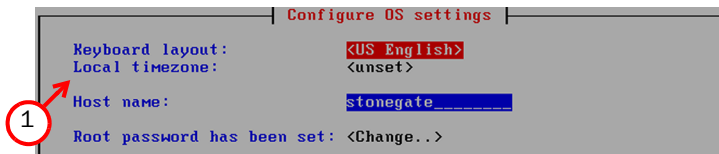
Tip: Type in the first letter to move forward more quickly in the list of keyboard layouts.



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

▼ To set the engine's timezone

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



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

Note – The timezone setting affects only the way the time is displayed on the engine command line. The actual operation always uses UTC time.

▼ To set the rest of the OS settings

1. Type in the name of the SSL VPN engine.

```
Configure OS settings
Keyboard layout: <US English>
Local timezone: <unset>
Host name: stonegate
Root password has been set: <Change..>
Web Console password: <Change..>
Web Console IP address: 192.168.100.1
Web Console IP netmask: 255.255.255.0
[ ] Reset SSL VPN Administrator password
[ ] Enable SSH daemon
<Cancel> <Finish>
```

2. Highlight the entry field for **Web Console Password** using the arrow keys and press ENTER to change the password that the user **admin** uses to access the SSL VPN Web Console.
 - By default, the password is **Pass1234**. We strongly advise you to change the password either in this dialog or after logging in to the Web Console for the first time.
3. Enter the IP address and the netmask for the Web Console.
 - The default IP address of the Web Console is 192.168.100.1. If you want to use the default IP address, configure the computer you use for connecting to the Web Console to use an IP address in the same network (192.168.100.0/24).
4. (Optional) Highlight Enable SSH Daemon and press the spacebar on your keyboard to select the option and allow remote access to engine command line using SSH.

Note – It is not necessary to enable the SSH daemon now for ongoing management, as you can also set this option through the SSL VPN Web console. We recommend that you enable the SSH access in the Web Console when needed and then disable the access again when you are done.

5. Highlight **Finish** and press ENTER. The engine configuration wizard closes.

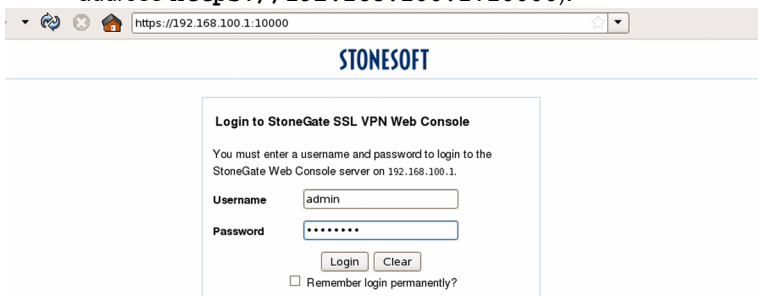
Continue by *Logging in to the Web Console* (page 27).

Logging in to the Web Console

The *Web Console* is used for interface configuration and other such basic operating-system-level settings.

▼ To log in to the Web Console

1. Open the Web browser on the computer attached to the appliance and connect to the Web Console at the address **https://<Web Console IP Address>:10000**. The login for the appliance Web Console opens.
 - If you did not change the Web Console IP address in the engine configuration wizard, the address is the default Web Console address **https://192.168.100.1:10000**.

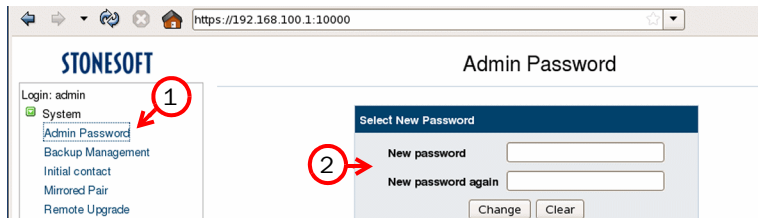


2. Log in. By default, the username is **admin** and password is **Pass1234**.
 - If you changed the Web Console password in the engine configuration wizard, log in using the new password, and continue by *Setting System Time* (page 28).
 - If you did not change the password in the engine configuration wizard, we strongly advise you to change the password according to the instructions below.

Changing the Web Console Password

▼ To change the password for the basic settings console

1. In the Web console, expand **System** in the menu on the left and select **Admin Password**.



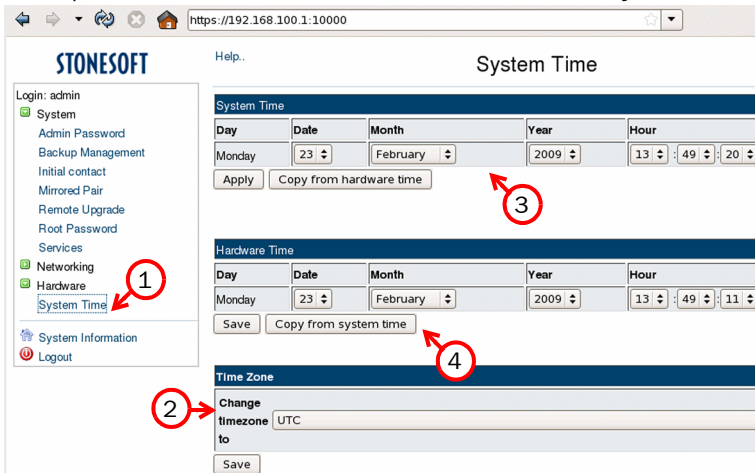
2. Type a new password in both fields on the right and click **Change**.

Setting System Time

System time must be set correctly for proper operation (used for example, in access rules, certificate validity checking, and log entries).

▼ To set the system time

1. Expand **Hardware** in the menu on the left and select **System Time**.



2. Select the correct **Time Zone** and click **Save**.
3. Change the time in the **System Time** section and click **Apply**.

4. Synchronize the times by clicking **Copy from system time**.

Configuring Interfaces

You must add at least one interface in addition to the management port to offer services to your users (a typical configuration requires two or more additional interfaces). If you plan to create a pair of mirrored appliances, we recommend using the port eth1 on the appliances' back panel for communications between the pair of mirrored appliances (instructions on how to set up a mirrored pair can be found in the *StoneGate SSL VPN Administrator's Guide*).

▼ Configuring a network interface

1. In the Web Console, expand **Networking** in the menu on the left, and select **Network Configuration**.



2. On the right, click **Network Interfaces**.

- Under **Interfaces Activated at Boot Time**, click **Add a new interface** just below the interface table.

STONESOFT

Module Index

Network Interfaces

Login: admin

- System
 - Admin Password
 - Backup Management
 - Initial contact
 - Mirrored Pair
 - Remote Upgrade
 - Root Password
 - Services
- Networking
 - Access Log
 - Network Configuration
- Hardware
 - System Time
- System Information
- Logout

Interfaces Activated at Boot Time

Select all. | Invert selection. | Add a new interface.

Name	Type	IP Address	Netmask	Active
eth0 <Console>	Ethernet	192.168.100.1	255.255.255.0	Yes
lo	Loopback	Automatic	Automatic	Yes

Select all. | Invert selection. | Add a new interface.

Delete Selected Interfaces Delete and Apply Selected Interfaces Apply Selected Interfaces

Interfaces Active Now

Select all. | Invert selection. | Add a new interface.

Name	Type	IP Address	Netmask	Status
eth0 <Console>	Ethernet	192.168.100.1	255.255.255.0	Up
lo	Loopback	127.0.0.1	255.0.0.0	Up

Select all. | Invert selection. | Add a new interface.

De-Activate Selected Interfaces

Return to network configuration

- Fill in the interface details according to your network setup:
 - The typical setting for **Activate at boot** is **Yes**. If you set this option to **No**, the interface is disabled until you change this setting and then reboot or manually apply the boot-time configuration on the main Network Interfaces page.
- Click **Create** to save your changes or **Create and Apply** to also activate the new interface.

6. (Optional) To add IP addresses to the physical interface, click the interface name in the **Interfaces Activated at Boot Time** table and click **(Add Virtual Interface)** for the **Virtual Interfaces** setting.
- Fill in the details of the virtual interface and click **Create** to save your changes or **Create and Apply** to also activate the new interface.
 - You can add more virtual interfaces to the same physical interface. The number of virtual interfaces is shown in front of the Add Virtual Interface action in **Virtual Interfaces**.

The screenshot shows the STONESOFT web interface. On the left is a navigation menu with categories like System, Networking, and Hardware. The main content area is titled 'Edit Bootup Interface'. It contains a form for 'Boot Time Interface Parameters' for interface 'eth1'. The form includes fields for Name, IP Address (set to 192.168.100.1), Netmask (255.255.255.0), Broadcast (255.255.255.0), MTU (Automatic), and Activate at boot? (Yes). The 'Virtual Interfaces' field is circled in red and displays '0 (Add virtual interface)'. At the bottom of the form are three buttons: 'Save', 'Save and Apply', and 'Delete and Apply'.

7. Add all necessary interfaces as explained above.
8. Click **Save and Apply** to activate the interfaces.
- You can alternatively activate the interfaces by selecting the **Apply Selected Interfaces** action on the main Network Interfaces page.
 - If you have not activated the interfaces by selecting either of these actions, the interfaces that you have configured are automatically activated when you reboot the appliance.

Configuring Routing

▼ To configure routing

1. In the Web console, under **Networking** category in the menu on the left, select **Network Configuration**.
2. On the right, click the **Routing and Gateways** icon. The routing view opens.

STONESOFT

Module Index

Routing and Gateways

Login: admin

- System
- Networking
 - Access Log
 - Network Configuration
- Hardware
- System Information
- Logout

Routing configuration activated at boot time

Default router: None (or from DHCP) Gateway Device: eth0

Interface	Network	Netmask	Gateway

Local routes

Interface	Network	Netmask

Save

Active Routes

Destination	Gateway	Netmask
<input type="checkbox"/> 192.168.100.0	None	255.255.255.0

Delete Selected Routes

Create active route

Route destination: Default route

Netmask for destination: Default 255.255.255.255

Route via: Network interface to Gateway

Create

Boot time configuration

3. In the **Routing configuration activated at boot time** section at the top, fill in the details for the default route:
 - If the default gateway is assigned by a DHCP server, leave the selection to **None (or from DHCP)**, select the correct network interface in the **Device** list, and click **Save**.
 - If you want to define the default gateway manually, select **Gateway**, fill in the IP address and **Device** information, and click **Save**.

4. Still in the **Routing configuration activated at boot time** section at the top, fill in the details for other routes:
 - For a network that is routed through a next-hop gateway (such as a router), fill all fields on the **Static Routes** line and click **Save** without changing any of the other settings.
 - For routes to devices that are connected directly (such as through a hub or directly through a crossover cable), fill in all fields on the **Local Routes** line and click **Save** without changing any of the other settings.
5. If you want to add temporary routes that are not preserved when the device reboots, fill in the details in the **Create Active Route** section at the bottom:
 - **Route Destination:** either **Default route** (where all traffic without any more specific routing definition is sent) or a specific network or IP address.
 - **Netmask for destination:** either **Default** or the netmask you type in.
 - **Route via:** either a **Network interface** (for directly connected networks) or the IP address of a **Gateway** (for a next-hop gateway to which the traffic is forwarded).
 - Click **Create** to add the new route after filling in the details. The route is activated immediately.

The routes added in the **Route configuration activated at boot time** section are activated when you reboot the appliance.

Configuring DNS Settings

If you want services to be available by domain names as well as IP addresses, you must configure the DNS settings as below.

▼ To Configure the DNS Settings

1. In the Web console, under **Networking** category in the menu on the left, select **Network Configuration**.
2. On the right, click the **Hostname and DNS client** icon.
3. Type the **Hostname** of the appliance in the reserved field.
4. In **DNS Servers**, type in the IP addresses of your DNS servers (1 per field).
5. (*Optional*) In **Resolution order**, you can select the order in which the addresses are queried from different sources (from left to right) to override the standard order.
6. (*Optional*) In **Search domains**, select **Listed** and type in your domain (for example: example.com).

Generating a Certificate

Authentication in SSL is based on certificates as the proof of identity. The appliance contains a factory-installed certificate that allows testing in a closed network without the need to install an actual working certificate on the appliance. When installing the appliance for other use, you must always generate a working certificate.



Caution – Never use the factory-installed standard keys and certificates for anything other than testing in a closed environment! If you do not generate new keys and certificates, the security of the system is severely compromised.

The procedure below explains how to generate a certificate request using the tools included with the appliance. Other tools may be used, if you prefer (the certificate must be in the .pem format). See the *SSL VPN Administrator's Guide* for more information on certificates.

▼ To generate a certificate request

1. While still connected to the appliance with a network cable, enter **https://<Web Console IP Address>:8443** as the address in your Web browser.

2. Click either the For Windows or For Linux link according to your operating system to download certificate-related tools to your workstation.

3. Extract all files in the .zip archive to the same location.
4. Open a command line and run the `makescr` script that was just extracted from the archive.
5. Fill in the required details. See TN2073 Creating a Certificate Signing Request for more detailed information.
6. After this, the following files are generated:
 - `server.csr`: the certificate request file that is used to generate the actual certificate.
 - `private.pk8`: the private certificate key that you must import to StoneGate SSL VPN.
 - `private.key`: the private certificate key in an alternative format. You can delete this file.
7. Send the `server.csr` certificate request for signing to the certificate authority or sign it using an internal certificate authority (CA) that you maintain.
 - If the CA is not configured as trusted in the Web browser the end-users connect with, the users see a certificate warning that they need to accept to access resources.
 - Many commercial certificate authorities are configured as trusted in Web browsers by default.

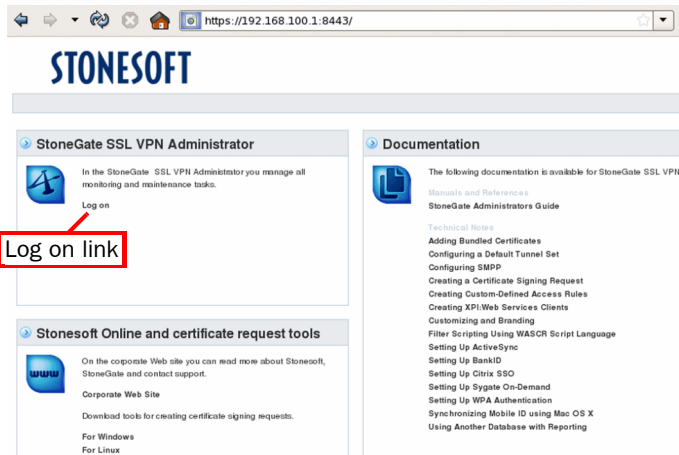
When you have the signed certificate, import it to the StoneGate SSL VPN Administrator and activate it for the Administration Service and Access Point. See *Logging in to the Web Console* (page 27) and *Importing Certificate Keys and Certificates* (page 39).

Logging in to the StoneGate SSL VPN Administrator

The *StoneGate SSL VPN Administrator* is used for setting up and managing the SSL VPN features.

▼ To log in to the StoneGate SSL VPN Administrator

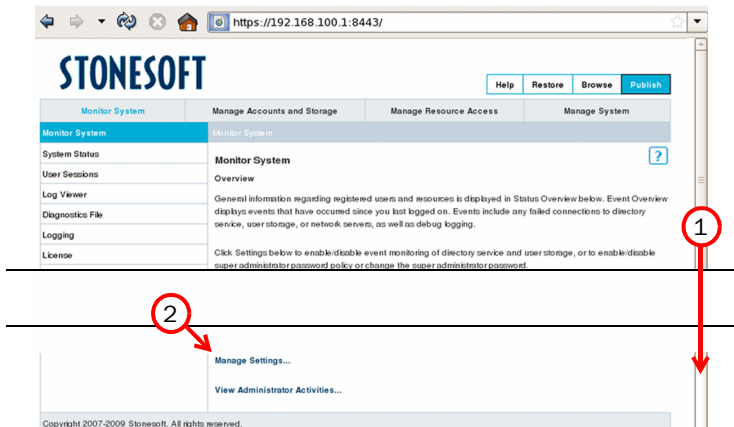
1. Click **Log on** in the topmost area on the left under the title **StoneGate SSL VPN Administrator**.



2. Log in. By default the username is **admin** and the password is **Pass1234**. We strongly advise you to change the password after logging in according to the instructions below.

Changing the SSL VPN Administrator Password

1. When the StoneGate SSL VPN Administrator opens, scroll down to the end of the page.
2. Click **Manage Settings** in the bottom part of the right panel.



3. Change to a secure password in the **Super Administrator Password** section on the page that opens.

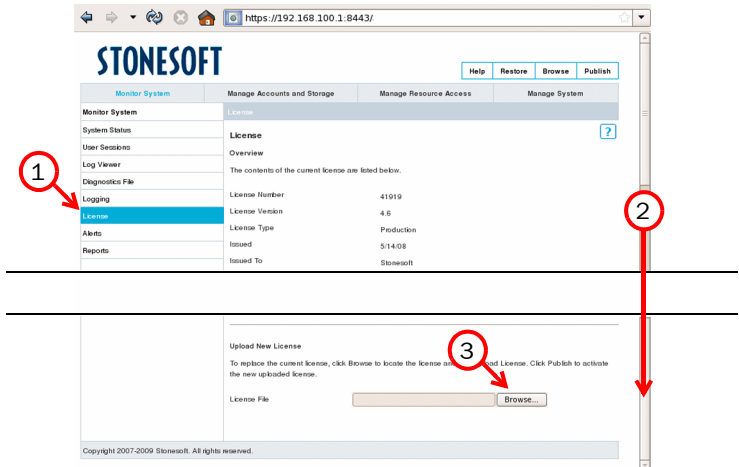
After changing the default password, import your license and the working certificate.

Importing a License

For the initial configuration of the appliance, you must import the SSL VPN license through the StoneGate SSL VPN Administrator. If you later connect the appliance to the StoneGate Management Center, you can optionally manage the licenses also through the StoneGate Management Client. See the *StoneGate Administrator's Guide* or the *Online Help* of the Management Client for more information.

▼ To import a license

1. After you log in and change your password, select **License** in the menu on the left.



2. On the right, scroll down to the end of the license information page displaying details of the temporary factory-installed license.
3. Click the **Browse** button next to the **License File** field at the bottom of the page and select and import your license file using the dialog that opens.

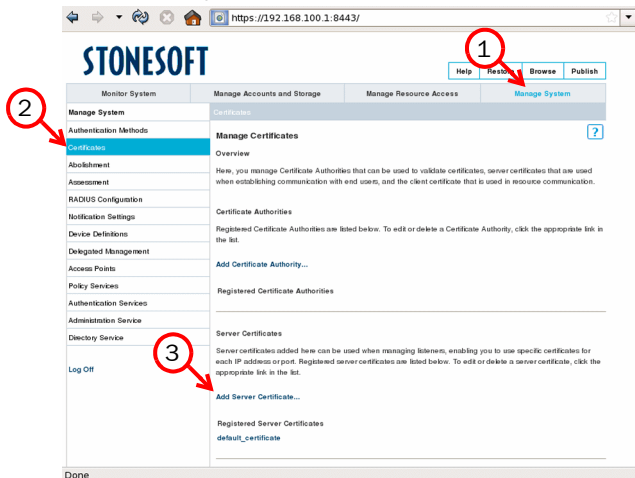
Importing Certificate Keys and Certificates

Note – If your certificate is a bundled certificate, which may contain intermediate certificates, you must split the certificate before adding it to the StoneGate SSL VPN Administrator. See TN2068 Adding Bundled Certificates for information on how to do this.

See *Generating a Certificate* (page 34) for information on how to generate a working certificate. When you have the signed certificate, you must import the certificate and the associated private key in the StoneGate SSL VPN Administrator.

▼ To import a certificate key and certificate

1. In the SSL VPN Administrator, switch to the **Manage System** section at the top menu.



2. Select **Certificates** in the menu on the left. The Manage Certificates page is displayed
3. Click **Add Server Certificate**.

4. Fill in the details:

- **Display Name:** the name you want to give to the certificate for display in the StoneGate SSL VPN Administrator interface.
- **Certificate:** Browse and select the signed certificate file.
- **Key:** Browse and select the private certificate key file (`private.pk8`).
- **Password:** If you protected the certificate key with a password when you generated it, type in the same password here.

Monitor System **4** Manage Accounts and Storage Manage Resource Access Manage System

Management System Certificates > Add Server Certificate

Authentication Methods **Add Server Certificate** ?

Certificates

Abolishment

Assessment

RADIUS Configuration

Notification Settings

Device Definitions

Delegated Management

Access Points

Policy Services

Authentication Services

Administration Service

General Settings

Add the PEM formatted certificate and key file below.

Display Name

Certificate Browse...

Key Browse...

Password

Using Hardware Security Module

Previous Save **5**

5. Click **Save**. This imports the certificate, but it is not activated yet.

▼ To activate the certificate

1. Select **Administration Service** in the menu on the left.

Monitor System Manage Accounts and Storage Manage Resource Access Manage System

Management System Administration Service

Authentication Methods **Manage Administration Service** ?

Abolishment

Assessment

RADIUS Configuration

Notification Settings

Device Definitions

Delegated Management

Access Points

Policy Services

Authentication Services

Administration Service

Directory Service

Log Off

Internal Communication Settings

Enter the following settings for communication between StoneGate SSL VPN Administrator and the StoneGate SSL VPN network.

Internal Host

Internal Communication Port

External Communication Settings

Enter the following settings for communication between StoneGate SSL VPN Administrator and the client.

Administrator HTTP Host

Administrator HTTP Port

Administrator HTTPS Host

Administrator HTTPS Port

Server Certificate **2**

Save **3**

Done

2. Select the correct Server Certificate from the list.
3. Click **Save**.

4. Select **Access Points** in the menu on the left.

The screenshot shows the 'Manage System' interface. On the left sidebar, the 'Access Points' menu item is highlighted and circled with a red '4'. The main content area shows the 'Access Points' overview page. Under the 'Registered Access Points' section, there is a table with one entry: 'Access Point' with Service ID '2' and Internal Host '127.0.0.1'. This table is circled with a red '5'.

Service ID	Display Name	Internal Host
2	Access Point	127.0.0.1

5. Click **Access Point** under the title Registered Access Points.

6. Select the correct Server Certificate from the list.

The screenshot shows the 'Edit Access Point' configuration page for 'Access Point'. The 'Server Certificate' dropdown menu is circled with a red '6' and is currently set to 'default_certificate'. Other fields include Service ID (2), Display Name (Access Point), Internal Host (127.0.0.1), Application Portal Host (127.0.0.1), Application Portal Port (443), and Sandbox Port (443). There are also checkboxes for 'Listen on all interfaces', 'Distribute key files automatically', and 'Support crypto costs'.

7. Scroll to the bottom of the page and click **Save**.

Moving on

After importing the license and the working certificate, your SSL VPN system is ready to be configured with additional administrator accounts and the user accounts and services that you want the appliance to provide in your network. This configuration is explained in the *StoneGate SSL VPN Administrator's Guide* and in the help pages that you can access at the StoneGate SSL VPN Administrator pages.

For step-by-step instructions for tasks outlined below, consult the help system (click the **Help** link at the top menu of the StoneGate SSL VPN Administrator pages once logged in) or the *SSL VPN Administrator's Guide*.

Your next steps with the software will include:

1. Creating an external user storage.
2. Creating user groups and users. Accounts for both administrator users and your end-users are created in the same way. Administrator access can be controlled with access rules based on user groups.
3. Defining access rules for allowing access to the services on the appliance.
4. Defining the services you want to offer.
 - Note that in addition to other services, you can also configure the Web console and the StoneGate SSL VPN Administrator to be accessible remotely through the Application Portal.

After configuring the administrator accounts, user accounts, and services, you can optionally connect the SSL VPN appliance to the StoneGate Management Center. This allows you to monitor the appliance status through the StoneGate Management Client. You can optionally also manage the SSL VPN licenses through the Management Client. In addition, you can configure that SSL VPN logs are sent to the StoneGate Management Center and can be viewed through the Management Client. See the *StoneGate Administrator's Guide* or the *Online Help* of the Management Client for more information.

Managing the Appliance

Enabling Command Line Access

You can enable SSH on the appliance to remotely connect to the operating system command line (Linux) to use standard networking tools (like Ping) or to transfer files through SSH. You can alternatively connect to the engine through serial console.

If the command line has not been used before, you must first set the command line password.

▼ To enable command line access to the appliance

1. Log in to the Web Console remotely through the Access Point or locally through the management port eth0 on the appliance's back panel at the address **https://<Web Console IP Address>:10000**.
 - For detailed instructions for establishing the local connection, see *Logging in to the Web Console* (page 27).
2. In the Web Console, expand **System** in the menu on the left and select **Root Password**.
3. On the right, type in and confirm the command line password for the account "root". The "root" account is always the only account for command line access.
4. (Optional) To enable SSH on the appliance, first select **Services** in the menu on the left, and then select the **Enable SSH daemon** option under Access Control on the right.

Connecting to Engine Command Line

Once you have enabled command line access (see *Enabling Command Line Access* above), you can connect to the engine command line.

▼ To connect to engine command line

1. Do one of the following:
 - Connect the serial cable supplied with the appliance to the serial port on the appliance's front panel and to a computer, and then open a terminal on the computer using the settings 9600bps, 8 databits, 1 stopbit, no parity.
 - Connect to the appliance's IP address on any interface using an SSH client (for example, PuTTY) on the standard port (TCP/22).
2. Log in with username **root** and the password you set through the Web console.

- The default key map is set to US English. If you want to change the key map, run the command **sg-reconfigure --no-shutdown**.
- The dash character is located to the left of the backspace key in the US English keyboard layout.

Checking System Information

This section explains how you can check basic system operating status and the software version that the access point is running. The actual SSL VPN services are monitored through the StoneGate SSL VPN Administrator in the Monitor System pages (see the *StoneGate SSL VPN Administrator's Guide* for details on the SSL VPN services monitoring).

▼ To check the system status and installed software version

1. Log in to the Web Console remotely through the Access Point or locally through the management port eth0 on the appliance's back panel at the address **https://<Web Console IP Address>:10000**.
 - For detailed instructions for establishing the local connection, see *Logging in to the Web Console* (page 27).
2. Information on the software version and system status is displayed on the right. If you navigate away from this view, you can return by selecting **System Information** in the menu on the left.

Restarting Services

▼ To restart services

1. Log in to the Web Console remotely through the Access Point or locally through the management port eth0 on the appliance's back panel at the address **https://<Web Console IP Address>:10000**.
 - For detailed instructions for establishing the local connection, see *Logging in to the Web Console* (page 27).
2. Expand **System** in the menu on the left and select **Services**.
3. On the right, select the services that you wish to restart.
4. Click **Restart** to restart the services that are selected above.

Maintenance Operations

Changing the Password for Command Line Access

The account for the user `root` is the only account for engine command line access. You can change the password for the `root` account through the engine configuration wizard following the instructions below or through the SSL VPN Web Console as described in *Enabling Command Line Access* (page 43).

▼ To change the root password in configuration wizard

1. Connect to the engine command line as described in *Connecting to Engine Command Line* (page 43).
2. Issue the command `sg-reconfigure`. The engine configuration wizard starts.



Configure OS settings

Keyboard layout:	<US English>
Local timezone:	<unset>
Host name:	stonegate
Root password has been set:	<Change..>
Web Console password:	<Change..>
Web Console IP address:	192.168.100.1
Web Console IP netmask:	255.255.255.0
<input type="checkbox"/> Reset SSL VPN Administrator password	
<input type="checkbox"/> Enable SSH daemon	
<Cancel> <Finish>	

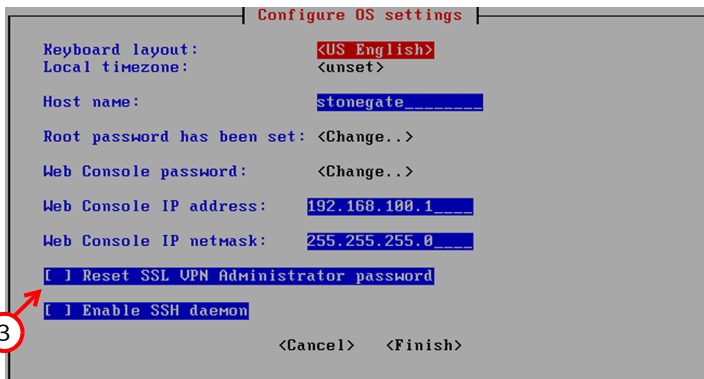
3. Highlight the entry field for **Root Password Has Been Set** using the arrow keys and press ENTER.
4. Enter and confirm the new password in the dialog that opens.
5. Highlight **Finish** and press ENTER.

Resetting the SSL VPN Administrator Password

If you have forgotten the password that the user **admin** uses to access the SSL VPN Administrator, you can reset the password back to the default password **Pass1234**.

▼ To reset the SSL VPN Administrator password

1. Connect to the engine command line as described in *Connecting to Engine Command Line* (page 43).
2. Issue the command `sg-reconfigure`. The engine configuration wizard starts.



3. Highlight **Reset SSL VPN Administrator Password** using the arrow keys and press the spacebar on your keyboard.
4. Highlight **Finish** and press ENTER.

After resetting the password to the default **Pass1234**, we strongly recommend that you log in to the SSL VPN Administrator and change the default password to a secure password. See *Logging in to the StoneGate SSL VPN Administrator* (page 36).

Reverting to Previously Installed Software Version

This procedure allows you to undo a software upgrade.

The appliance has two working partitions. One is designated as active and the other as inactive. The inactive partition is used for upgrades and the status is switched between the partitions when the upgrade is ready to be activated. If the appliance does not start up with the new version, it automatically switches to the previous configuration at the next reboot. You can also switch back to the previously installed software version manually as instructed here whenever necessary.

▼ To switch back to the previously active version

1. Connect the serial cable supplied with the appliance to the serial port on the appliance's front panel and to a computer.
2. On the computer, open a terminal with settings 9600bps, 8 databits, 1 stopbit, no parity.
3. (Re)start the appliance:
 - If the appliance is powered on, press `Enter`, log in with username `root` and the password you set through the Web console (see *Enabling Command Line Access* (page 43), and issue command `reboot`.

Note – When the appliance is powered and you need to unplug it, always wait at least five (5) seconds before plugging in the appliance again. Otherwise, the appliance may not have time to clear properly and fails to start.

4. Wait until a boot menu or a list of partitions is shown. Proceed to Step 6 if the boot menu is shown.
5. (If a list of partitions is shown) The currently active partition is highlighted in the list of partitions. Select the inactive partition and press `Enter`. A list of available commands opens.
6. Select **Switch to previously installed software version** or **Boot SG SSL-VPN** <name of partition> and press `Enter`. The appliance switches partitions and boots up.

If you want to undo this operation, repeat the steps exactly as above.

Resetting the Appliance to Factory Settings

Note – Perform a factory reset only if you have a specific need to do so. Consult Stonesoft Support before performing this operation if you are unsure of whether this operation is necessary or not.

▼ To reset to factory settings

1. Connect the serial cable supplied with the appliance to the serial port on the appliance's front panel and to a computer.
2. On the computer, open a terminal with settings 9600bps, 8 databits, 1 stopbit, no parity.
3. (Re)start the appliance:
 - If the appliance is powered on, press `Enter`, log in with username `root` and the password you set through the Web console (see *Enabling Command Line Access* (page 43), and issue command `reboot`.

Note – When the appliance is powered and you need to unplug it, always wait at least five (5) seconds before plugging in the appliance again. Otherwise, the appliance may not have time to clear properly and fails to start.

4. Wait until a boot menu or a list of partitions is shown. Proceed to Step 6 if the boot menu is shown.
5. (If a list of partitions is shown) The currently active partition is highlighted. Press `Enter`. A list of available commands opens.
6. Select **System Restore Options** and press `Enter`.
7. Type `1` and press `Enter` to clear the settings. A confirmation prompt is shown.
8. Type **YES** and press `Enter` to perform the reset. If you decide to cancel the operation, type **NO** and press `Enter`.



Caution – Do not unplug the power from the appliance or interrupt the reset in any way. If the reset is interrupted, the appliance may become unusable until serviced.

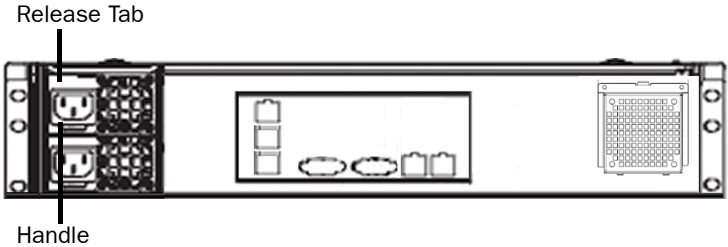
To use the appliance after a factory reset, you must configure it as explained in *Configuring the Appliance* (page 24).

Replacing Power Supply Modules

You can use both AC and DC power supply modules on the appliance. If necessary, you can replace a power supply module with a new one.

▼ To replace a power supply module

1. Unplug the power cord from the DC power supply module or disconnect the wires from the AC power supply module.
2. Locate the release tab on the left side of the power supply.



3. Push the release tab to the right to release the power supply from its locking position.
4. Pull out the power supply using the handle provided.
5. Replace the power supply with a new one.
6. Push the power supply into the power bay until you hear a click.



Caution – Do not open the casing of a power supply. Power supplies can only be accessed and serviced by a qualified technician from the manufacturer.

Replacing the Solid State Disk



Caution – We recommend using a grounding strap when handling a Solid State Disk (SSD). Uninstalled SSDs are sensitive to ESD damage.

If necessary, you can replace the Solid State Disk in the appliance with another one of the same model.

▼ To replace the Solid State Disk

1. Connect to the engine command line as described in *Connecting to Engine Command Line* (page 43).
2. Shut down the engine:
 - If the appliance is powered on, press `Enter`, log in as the user `root` with the password you set through the Web console (see *Enabling Command Line Access* (page 43), and issue the command `halt`.
3. Unplug all power cords from the system or the wall outlets.
4. Locate the Solid State Disk drive on the appliance's back panel (see *Back Panel* (page 12)).
5. Press the release button to release the lever that locks the disk into position.



6. Pull the lever carefully to remove the disk from the drive.
7. Press the release button on the new disk to release the lever.
8. Insert the disk into the drive.
9. Press the lever down to lock the disk into position.

Replacing Express Modules



Caution – Do not install or remove express modules if the appliance is powered on to avoid damaging the express modules and the appliance.

▼ To replace an express module

1. Connect to the engine command line as described in *Connecting to Engine Command Line* (page 43).
2. Shut down the engine:
 - If the appliance is powered on, press `Enter`, log in as the user `root` with the password you set through the Web console (see *Enabling Command Line Access* (page 43), and issue the command `halt`.
3. Unplug all power cords from the system or the wall outlets.
4. Disconnect all the cables from the appliance.
5. (*Recommended*) Fasten a grounding strap to your wrist so that it contacts your bare skin and attach the other end of the strap to the appliance.
6. Locate the express module's release lever on the left of the module's front panel.
7. Release the module from its locking position by pressing the lever right, hold the lever down, and pull the module carefully out of the slot using the handle on the module's front panel.
8. Replace the module with a new one. See *Installing Express Modules* (page 14).



Caution – Do not power on the appliance if you have not installed an express module in each slot.

Removing SFP Transceivers

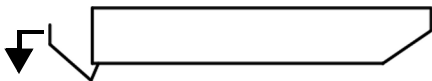
If necessary, you can remove the SFP transceivers from the SFP ports.



Caution – Invisible laser radiation is emitted from the end of fiber-optic cable and from fiber port. Do not stare into the beam and avoid direct exposure to the beam.

▼ To remove an SFP transceiver

1. Connect to the engine command line as described in *Connecting to Engine Command Line* (page 43).
2. Shut down the engine:
 - If the appliance is powered on, press `Enter`, log in as the user `root` with the password you set through the Web console (see *Enabling Command Line Access* (page 43), and issue the command `halt`.
3. Unplug all power cords from the system or the wall outlets.
4. Disconnect the cable from the SFP transceiver.
5. Pull down the latch on the SFP transceiver.



6. Pull the SFP transceiver carefully out of the port slot.

If you want to replace the SFP transceiver you have removed, follow the instructions in *Connecting Cables to SFP Ports* (page 22).

Disposal Instructions



Dispose of the appliance separately from household waste at an appropriate waste disposal facility at the end of its useful service life.

StoneGate Appliance Installation Guide

This booklet covers the initial installation and configuration tasks specific to your StoneGate Appliance.

For information on how to prepare the Management Center for a new engine installation, see the other available documentation. See inside for further details.

All documentation and our technical knowledge base is available at: www.stonesoft.com/support.

STONESOFT

Secure Information Flow

**Stonesoft Corporation
International Headquarters**

Itälahdenkatu 22 A
FI-00210 Helsinki, Finland
tel. +358 9 4767 11
fax. +358 9 4767 1349
www.stonesoft.com

**Stonesoft Inc.
Americas Headquarters**

1050 Crown Pointe Parkway
Suite 900
Atlanta, GA 30338, USA
tel. +1 866 869 4075
fax. +1 770 668 1131