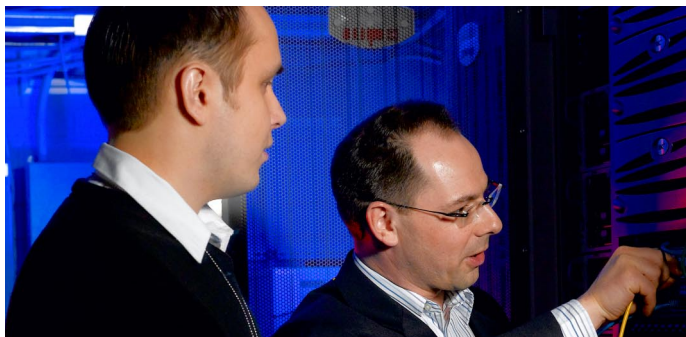


**STONESOFT**



**Appliance Installation Guide**

---

# **StoneGate SSL-400**

---

# 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](http://www.stonesoft.com/en/support/eula.html)

## 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/](http://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/](http://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/](http://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, 1259028, 1271283, 1289183, 1289202, 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 and 7,302,480 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 © 2008 Stonesoft Corporation. All rights reserved. All specifications are subject to change.

Revision: SGAIG\_SSL-400\_20080516

# Introduction

Thank you for choosing Stonesoft's StoneGate appliance. This guide provides instructions for the initial hardware installation and the maintenance of the SSL-400 appliance.

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

Your SSL VPN appliance is a self-contained unit with all necessary management features built in. The system architecture is explained on the next page.

The purpose of this appliance installation guide is to help you get started with your StoneGate appliance. See [Product Documentation](#), on page 4 for information on other available documentation.

## Contents

<a href="#">Getting Started</a> .....	4
<a href="#">Safety Precautions</a> .....	5
<a href="#">Front Panel</a> .....	7
<a href="#">Connecting the Cables</a> .....	8
<a href="#">Configuring the Appliance</a> .....	9
<a href="#">Managing the Appliance</a> .....	24
<a href="#">Maintenance Operations</a> .....	28
<a href="#">Appendix: Front Panel Indicators</a> ...	30
<a href="#">Disposal Instructions</a> .....	30



**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](#), on page 5 before you conduct any installation or maintenance operations on the appliance.

---

# Getting Started

The StoneGate SSL VPN appliance runs independently with the necessary services for end-users and administration in one appliance.

There are three points of access to services offered by the appliance:

- The *Web Console* is used for interface configuration and other such basic operating-system-level settings.
- The *StoneGate SSL VPN Administrator* is used for setting up and managing the SSL VPN features.
- The *Application Portal* is a Web user interface you can set up for end-users. The portal offers one-click access to services you offer through the SSL VPN access point. You can also configure the two administration services mentioned above to be accessible through this portal.

This guide walks you through the interface configuration and outlines the basic setup required to get the system up and running. For more information on setting up the SSL VPN system, consult the *StoneGate SSL VPN Administrator's Guide*.

## Installation Procedure

The appliance installation involves the following mandatory steps:

1. Connect the cables.
2. Configure the basic system settings (time, interfaces, routing).
3. Import the license.
4. Import a certificate.
5. Configure the SSL VPN user accounts, access rules, and services.

## 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/](http://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 locations of the power on/off switch 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.
- 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.



**Caution** – Never open the appliance covers! There are no user serviceable parts inside. Opening the covers may lead to serious injury and will void the warranty.

---

## General Safety Precautions

Follow these rules to ensure general safety:

- Keep the area around the appliance clean and free of clutter.
- 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.

## 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.

---

## Operating Precautions

Care must be taken to assure that the appliance's 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.

## Operating and Storage Temperatures

The allowed operating temperature of the appliance is +10...+35°C. The allowed storage temperature is -40...+70°C. Do not operate or store the appliance in temperatures outside these limits.

## Lithium Battery Precautions

---



**Caution** – Do not change the battery; 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.

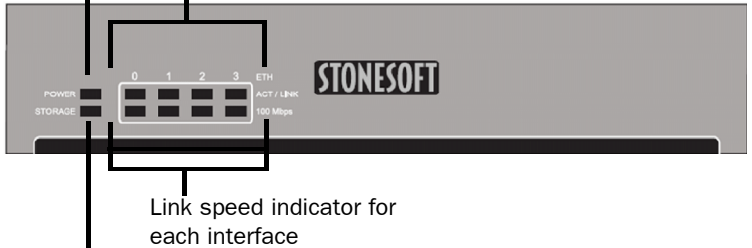
---

# Front Panel

Illustration 1 Front Panel

Power indicator

Network activity/link indicator for each interface



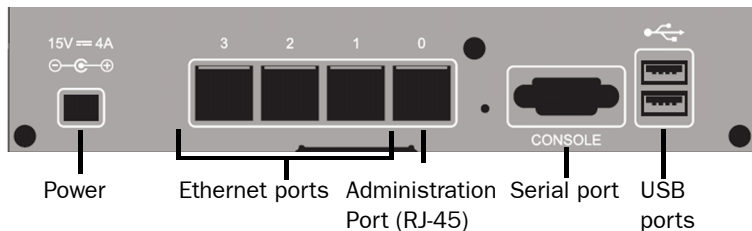
Disk activity indicator

Link speed indicator for each interface

For more information on the indicator lights and their states, see [Appendix: Front Panel Indicators](#), on page 30.

# Connecting the Cables

Illustration 2 Back Panel



## ▼ To connect the cables

1. Connect the network cables to the LAN ports.
2. Connect the supplied network cable to the administration port eth0 and to the network port of a computer that you will use to configure the appliance.
  - The administration port has a fixed IP address (192.168.100.1) that you cannot change. 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 the next page for more information on how to connect to and configure the appliance.
  - The administration port's IP address is active only when a network cable is plugged into the port.
  - If you want to manage the appliance remotely, we recommend that you set up access through the Application Portal in the same way as other services that the appliance offers to users.
3. Connect the power cable to the appliance and into a grounded electrical outlet. We recommend that you connect the appliance to a UPS (uninterruptible power supply) device to ensure continued and reliable operation during blackouts or other disturbances in the power grid.

---

**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. If you wait less than five seconds, the appliance may not have time to clear properly and may fail to start.

---

# 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.

The only interface that is defined when you receive the appliance is the management interface (eth 0). You must define basic settings for other interfaces to prepare the appliance for your network.

To configure the appliance for the first time, complete the sections below in order. Start by [Logging In to the Web Console](#).

## Logging In to the Web Console

### ▼ To log in to the Web Console

1. Attach the network cable supplied with the appliance to the management port (eth 0) and to any computer that has the necessary display, mouse, keyboard, and a graphical user interface with a Web browser.
2. Open the Web browser on the attached computer and connect to address **https://192.168.100.1:10000**. The login for the appliance Web Console opens ([Illustration 3](#)).

Illustration 3 Web Console Login

STONESOFT

**Login to StoneGate SSL VPN Web Console**

You must enter a username and password to login to the StoneGate Web Console server on 127.0.0.1.

Username

Password

Remember login permanently?

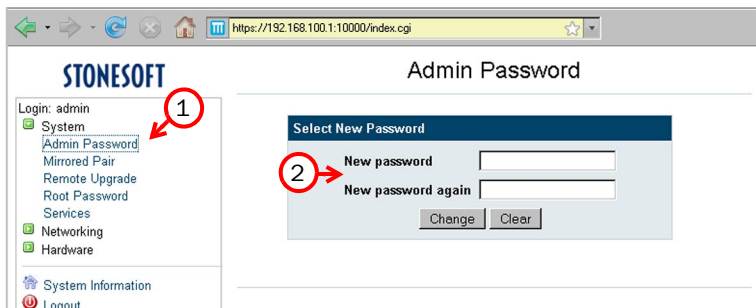
3. Log in. By default, the username is **admin** and password is **Pass1234**; we strongly advise you to change the password after logging in according to the instructions below.

## 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** (Illustration 4).

Illustration 4 Changing the Web Console password



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

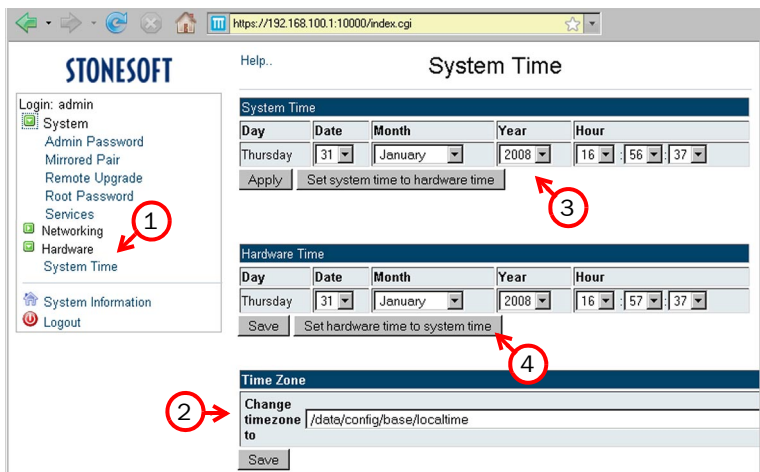
## Setting System Time

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** (Illustration 5).

Illustration 5 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 (depending on software version):
  - **Set hardware time to system time** (on SSL VPN 1.1.0.0) or
  - **Copy from system time** (on subsequent releases).

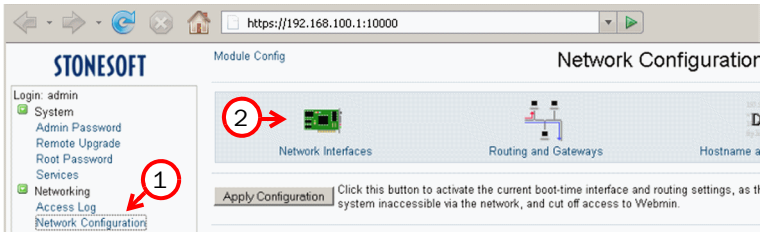
## Configuring Interfaces

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, note that in a mirrored setup, the port eth1 must be dedicated 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

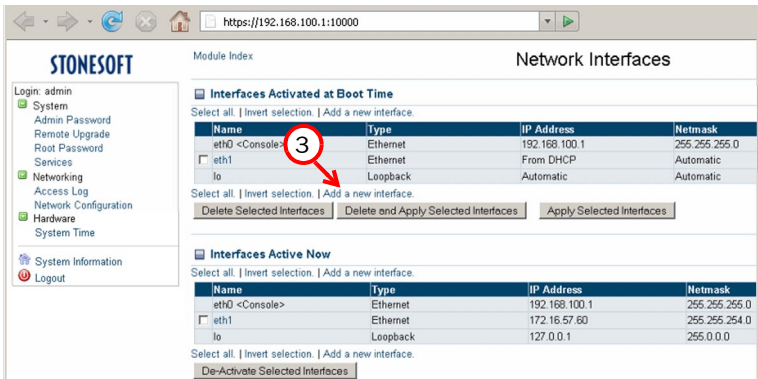
1. In the Web Console, under the **Networking** category in the menu on the left, and select **Network Configuration** (Illustration 6).

Illustration 6 Web Console - Network Configuration



2. On the right, click **Network Interfaces**.
3. Under Interfaces **Activated at Boot Time**, click **Add a new interface** just below the interface table (Illustration 7).

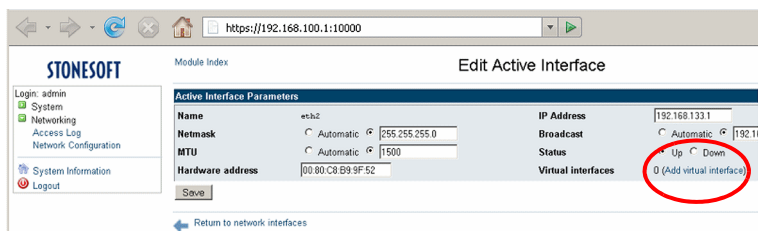
Illustration 7 Adding a New Interface



4. 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.
- (Optional) To add IP addresses to the physical interface, click the interface name in the **Activated at Boot Time** table and click **0 (Add Virtual Interface)** for the **Virtual Interfaces** setting (Illustration 8).

Illustration 8 Adding a virtual interface



- 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**.

- Add all necessary interfaces as explained above.

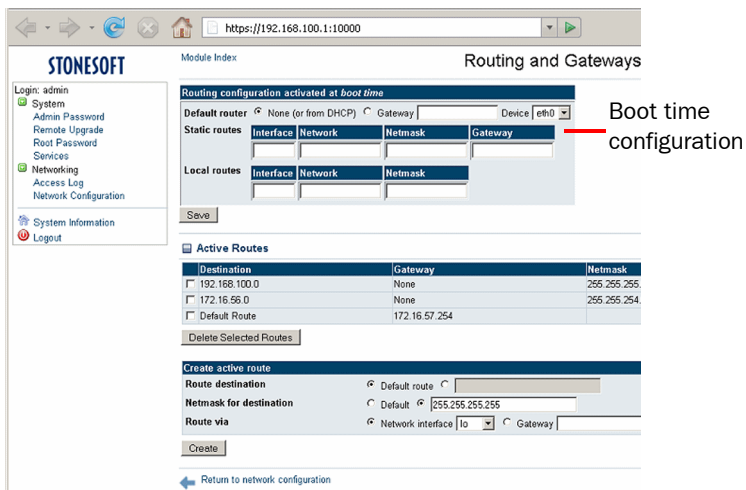
The interfaces are activated when you reboot the appliance or through the **Apply Selected Interfaces** action on the main Network Interfaces page.

## Configuring Routing

### ▼ To configure routing

- In the Web console, under **Networking** category in the menu on the left, select **Network Configuration**.
- On the right, click the **Routing and Gateways** icon. The routing view opens (Illustration 9).

Illustration 9 Routing and Gateways view



3. In the **Route 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 **Route 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.



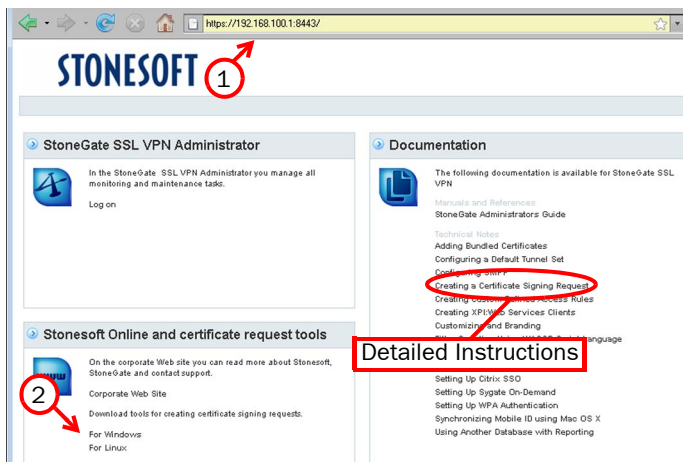
**Caution** – Never use the factory-installed standard keys and certificates for anything other than testing in a closed environment! If you do not generate new keys and certificates, the security of the system is severely compromised.

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 *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://192.168.100.1:8443` as the address in your Web browser.

Illustration 10 Launching SSL VPN Administrator Interface



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.

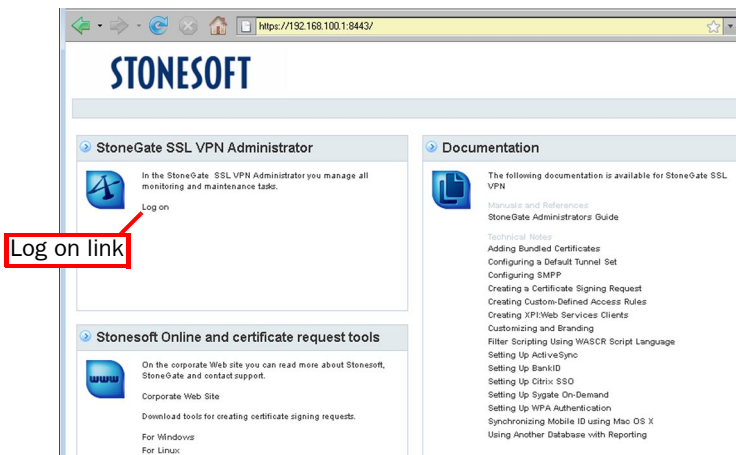
When you have the signed certificate, import it to the StoneGate SSL VPN Administrator and activate it for the Administration Service and Access Point (see [Logging In to the Web Console](#), on page 9 and [Importing Certificate Keys and Certificates](#), on page 21).

# Logging in to the StoneGate SSL VPN Administrator

## ▼ To log in to the StoneGate SSL VPN Administrator

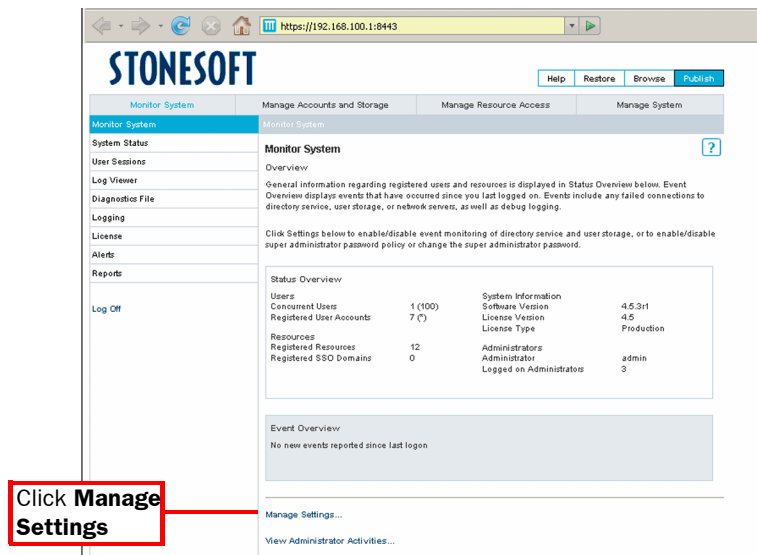
1. Click **Log on** in the topmost area on the left under the title **StoneGate SSL VPN Administrator** (Illustration 11).

Illustration 11 Launching SSL VPN Administrator Interface



2. Log in. By default the username is **admin** and the password is **Pass1234**.
3. When the StoneGate SSL VPN Administrator opens, click **Manage Settings** in the bottom part of the right panel (Illustration 12).

Illustration 12 Opening the Manage Settings view



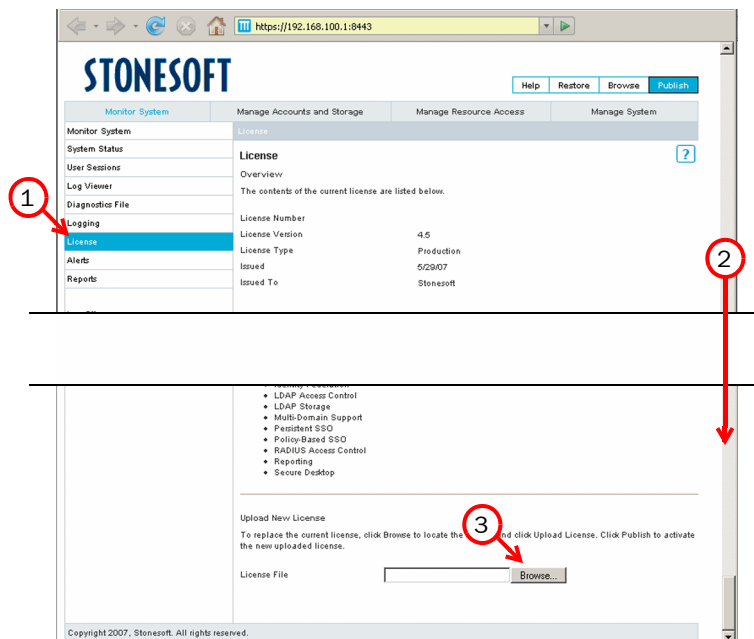
4. Change to a secure password in the **Super Administrator Password** section on the page that opens. After changing the default password, import your license and the working certificate.

# Importing a License

## ▼ To import a license

1. After you log in and change your password, select **License** in the menu on the left (Illustration 13).

Illustration 13 StoneGate SSL VPN Administrator - Monitor System



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

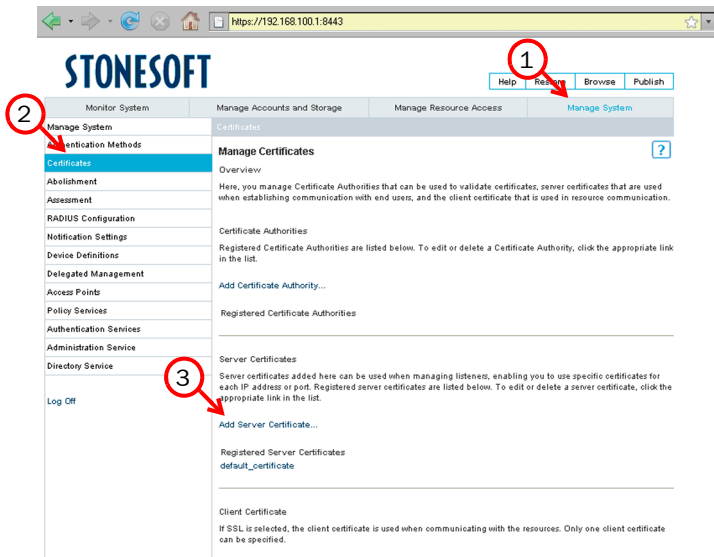
**Note** – If your certificate is a bundled certificate, which may contain intermediate certificates, you must split the certificate before adding it to the StoneGate SSL VPN Administrator. See [TN2068 Adding Bundled Certificates](#) for information on how to do this.

See [Generating a Certificate](#), on page 16 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.

Illustration 14 StoneGate SSL VPN Administrator - Manage System

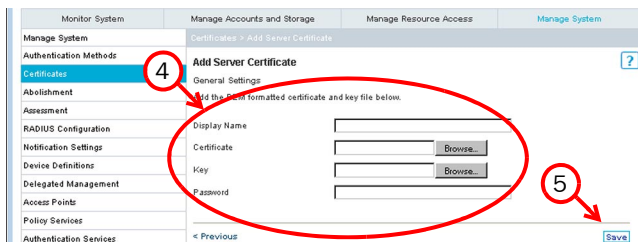


2. Select **Certificates** in the menu on the left. The Manage Certificates page is displayed
3. Click **Add Server Certificate**.

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.

Illustration 15 StoneGate SSL VPN Administrator - Add Server Certificate

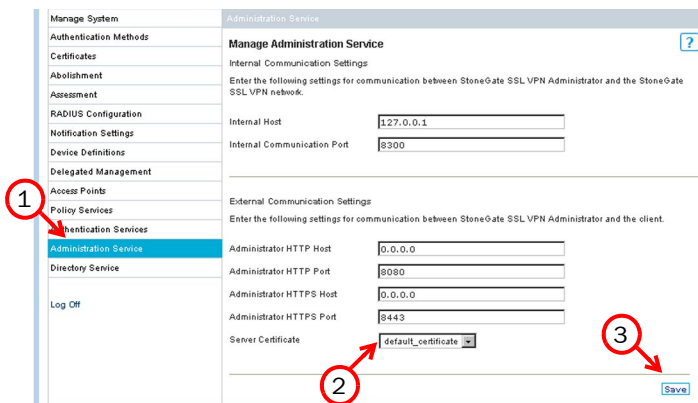


5. Click **Save**. This imports the certificate, but it is not activated yet.

▼ **To activate the certificate**

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

Illustration 16 StoneGate SSL VPN Administrator - Administration Service



2. Select the correct Server Certificate from the list.
3. Click **Save**.
4. Select **Access Points** in the menu on the left.

Illustration 17 StoneGate SSL VPN Administrator - Access Points

The screenshot shows the StoneGate SSL VPN Administrator interface. On the left, a sidebar menu has 'Access Points' highlighted in blue, with a red circle containing the number '4' and an arrow pointing to it. The main content area is titled 'Manage Access Points' and includes an 'Overview' section with instructions. Below this is a table titled 'Registered Access Points' with the following data:

Service ID	Display Name	Internal Host
2	Access Point	127.0.0.1

A red circle containing the number '5' and an arrow points to the 'Access Point' header in the table.

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

Illustration 18 StoneGate SSL VPN Administrator - Access Point

The screenshot shows the 'Edit Access Point "Access Point"' configuration page. The 'Server Certificate' field is a dropdown menu currently set to 'default\_certificate', with a red circle containing the number '6' and an arrow pointing to it. 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' (checked), 'Distribute key files automatically' (unchecked), and 'Support crypto cards' (unchecked).

6. Select the correct Server Certificate from the list.
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 *Administrator's Guide*.

Your next steps with the software will include:

1. 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.
2. Defining access rules for allowing access to the services on the appliance.
3. 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.

## Managing the Appliance

### Logging in to the Command Line

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.

If the command line has not been used before, you must first set the command line password and enable SSH access as explained below.

#### ▼ To enable SSH access to the appliance

1. Log in to the basic Web console remotely through the Access Point or locally through the management port (eth0) at the address `https://192.168.100.1:10000`.
  - For detailed instructions for establishing the local connection, see [Logging In to the Web Console](#), on page 9.

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. In the menu on the left, select **Services**.
5. On the right, under Access Control, select the **Enable SSH daemon** option.

## ▼ To Access the Appliance Using SSH

1. 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 basic Web console remotely through the Access Point or locally through the management port (eth0) at the address **https://192.168.100.1:10000**.
  - For detailed instructions for establishing the local connection, see [Logging In to the Web Console](#), on page 9.
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 basic Web console remotely through the Access Point or locally through the management port (eth0) at the address `https://192.168.100.1:10000`.
  - For detailed instructions for establishing the local connection, see [Logging In to the Web Console](#), on page 9.
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.

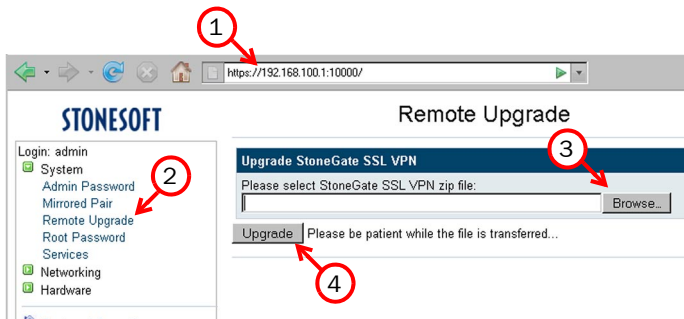
## Upgrading

The upgrade requires a .zip file for the new software version. You can download the file from the Stonesoft website. Transfer the file to the computer you use to connect to the StoneGate SSL VPN Administrator on the appliance.

### ▼ To upgrade the Software

1. Check the Release Notes for the version you are about to install for any version-specific exceptions, issues, and procedures that you may need to follow.
  - The release notes are available in the StoneGate technical knowledge base at <http://www.stonesoft.com/en/support/>
2. Log in to the basic Web console remotely through the Access Point or locally through the management port (eth0) at the address `https://192.168.100.1:10000`.
  - For detailed instructions for establishing the local connection, see [Logging In to the Web Console](#), on page 9.
3. Expand **System** in the menu on the left and select **Remote Upgrade** ([Illustration 19](#)).

Illustration 19 Upgrading the Software



4. Click the **Browse** button on the right and select the .zip file for the new software version for the upgrade.
5. Back in the main upgrading view, click the **Upgrade** button and wait for the upgrade to finish.
6. In the **System** menu on the left, select **Services** and click the **Reboot** button. The upgrade is finished.

# Maintenance Operations

## 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 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 and accessible, press `Enter`, log in and issue command `reboot`.
  - Otherwise, cycle the power off and on as appropriate.

---

**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 is shown.
5. Select **Switch to previously installed software version**. Note the indicated partition (A or B). 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 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 and accessible, press `Enter`, log in and issue command `reboot`.
    - Otherwise, cycle the power off and on as appropriate.
- 

**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 is shown.
  5. Select **System Restore Options** from the boot menu.
  6. Type `1` and press `Enter` to clear the settings. A confirmation prompt is shown.
  7. 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](#), on page 9.

## Appendix: Front Panel Indicators

The front panel indicator lights are explained below.

TABLE 14.1 POWER and STORAGE Indicators

Indicator	Color	Explanation
POWER	Green	Indicates power is being supplied to the system's power supply unit. Illuminated when the system is operating normally.
STORAGE	Red	Indicates hard drive activity.

TABLE 14.2 Network Connection Indicators

Indicator	Color	Explanation
ACT/LINK	Unlit	No link.
ACT/LINK	Green	Link ok, blinks on activity.
100 Mbps	Unlit	Link speed is 10 Mbps.
100 Mbps	Green	Link speed is 100 Mbps.

## Disposal Instructions

Dispose of the appliance separately from normal domestic 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](http://www.stonesoft.com/support).

---

**STONESOFT**

**Stonesoft Corporation**  
Itälahdenkatu 22 A  
00210 Helsinki  
Finland

**Stonesoft Inc.**  
1050 Crown Pointe Parkway  
Suite 900  
Atlanta, GA 30338 USA