



StoneGate SSL VPN Technical Note #5386

Virtual Appliance Installation and Configuration on VMware ESX/ESXi

Created: January 28, 2010

STONESOFT

Secure Information Flow

Table of Contents

Introduction to Installing an SSL VPN Virtual Appliance.....	3
What Is a StoneGate SSL VPN Virtual Appliance?.....	3
Prerequisites.....	3
Importing the Virtual Appliance	4
Setting Up the Virtual Appliance	7
Logging In to the Web Console	7
Changing the Web Console Password.....	8
Setting System Time	9
Configuring Interfaces	9
Configuring Routing.....	12
Configuring DNS Settings	13
Generating a Certificate	13
Logging In to the StoneGate SSL VPN Administrator.....	15
Importing a License	16
Importing Certificate Keys and Certificates	17
Moving On	19
Managing the Virtual Appliance	20
Logging in to the Command Line	20
To Enable SSH Access to the Appliance	20
To Access the Appliance Using SSH	21
Checking System Information	21
Restarting Services	21

Introduction to Installing an SSL VPN Virtual Appliance

What Is a StoneGate SSL VPN Virtual Appliance?

Virtualization technologies like VMware Virtual Infrastructure 3.x and vSphere allow implementation of virtual datacenters where servers are consolidated over a hypervisor distributed across multiple physical servers. This maximizes resilience to hardware failures, optimizes scalability and minimizes operating and maintenance costs.

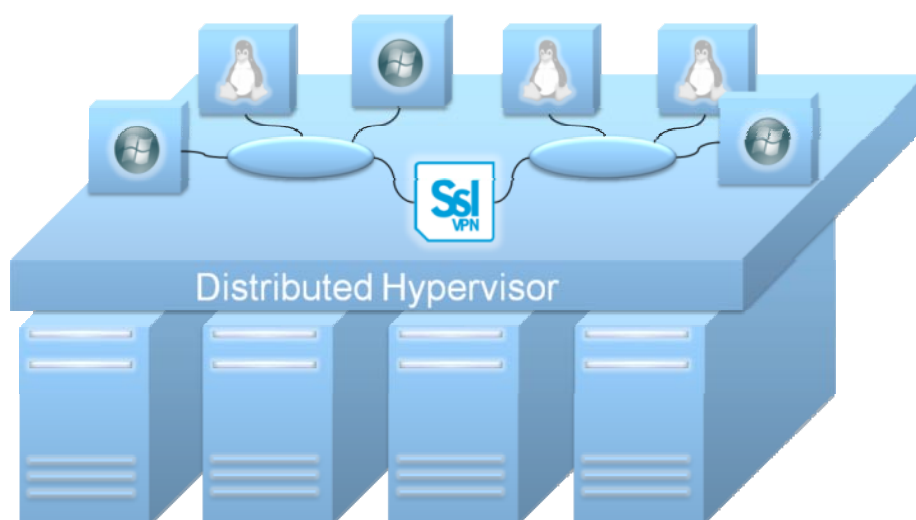


Figure 1. Virtual Datacenter

The StoneGate SSL VPN Virtual Appliance builds an application portal, which is dynamically populated depending on multiple criteria, with an emphasis on strong authentication, end-point security, and assessment and abolishment techniques.

This document presents the guidelines for deploying StoneGate SSL VPN Virtual Appliance within a VMware-based virtual infrastructure in ESX and ESXi systems.

Prerequisites

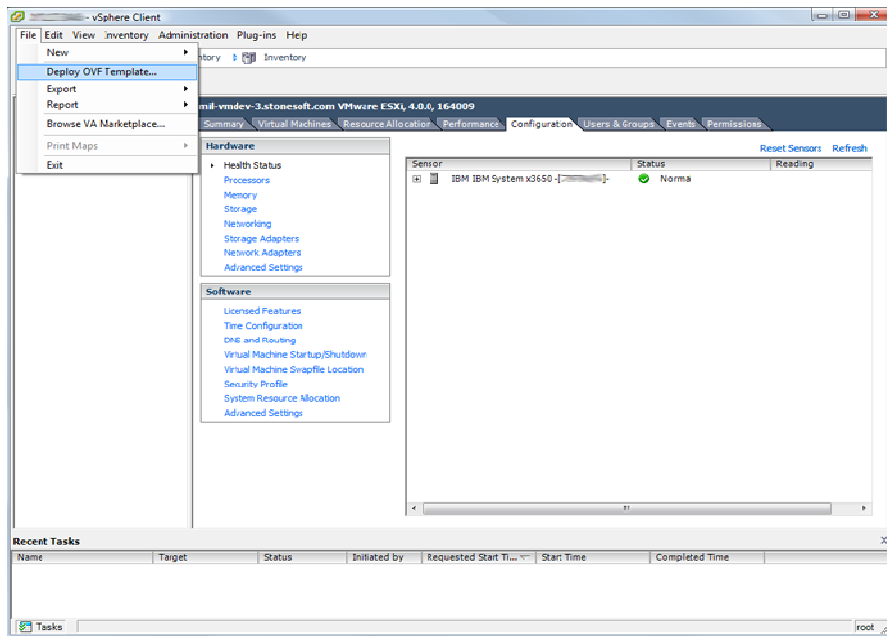
To successfully implement a StoneGate SSL VPN Virtual Appliance, you need to have the following components installed and configured:

- VMware Virtual Infrastructure
- StoneGate Management Center, if you plan to manage StoneGate SSL VPN centrally.

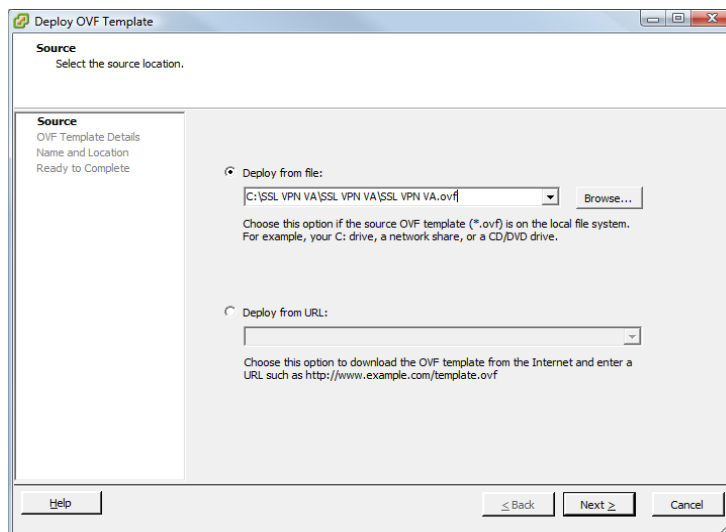
Importing the Virtual Appliance

To deploy the Virtual Appliance

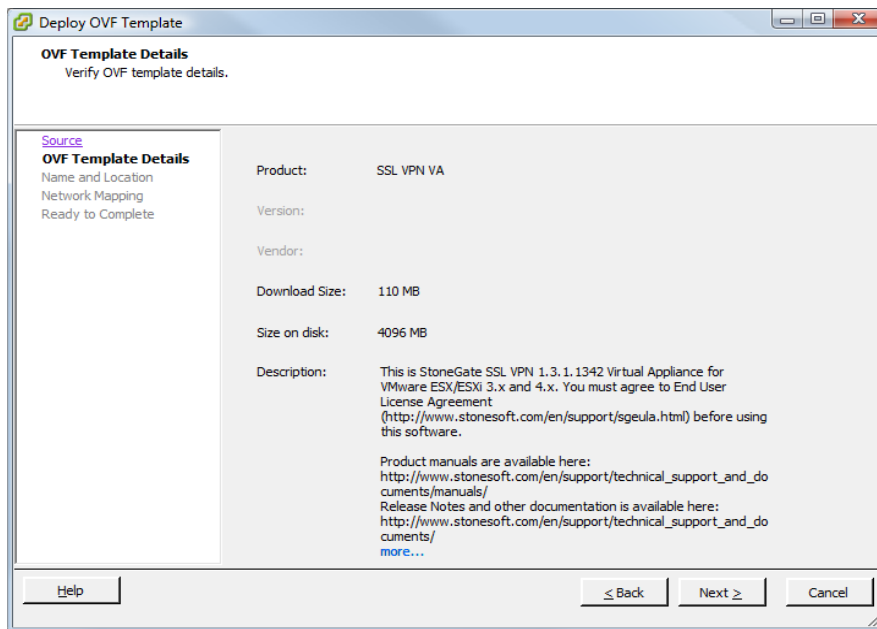
1. Connect to VMware Virtual Center or ESX/ESXi system using vSphere Client.
2. In the **File**, menu, select either
 - **Deploy OVF Template** in VMWare Virtual Infrastructure 4.0, or
 - **Virtual Appliance**→**Import...** in VMware Virtual Infrastructure 3.5The Deploy OVF Template wizard opens.



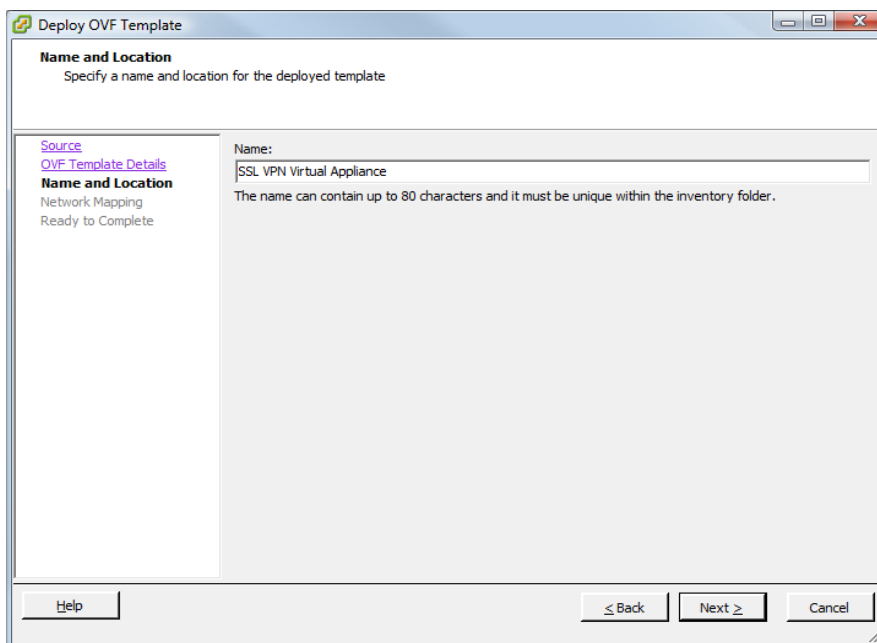
3. **Browse** to locate the **.ovf** (Open Virtual Format) file of the StoneGate SSL VPN Virtual Appliance.



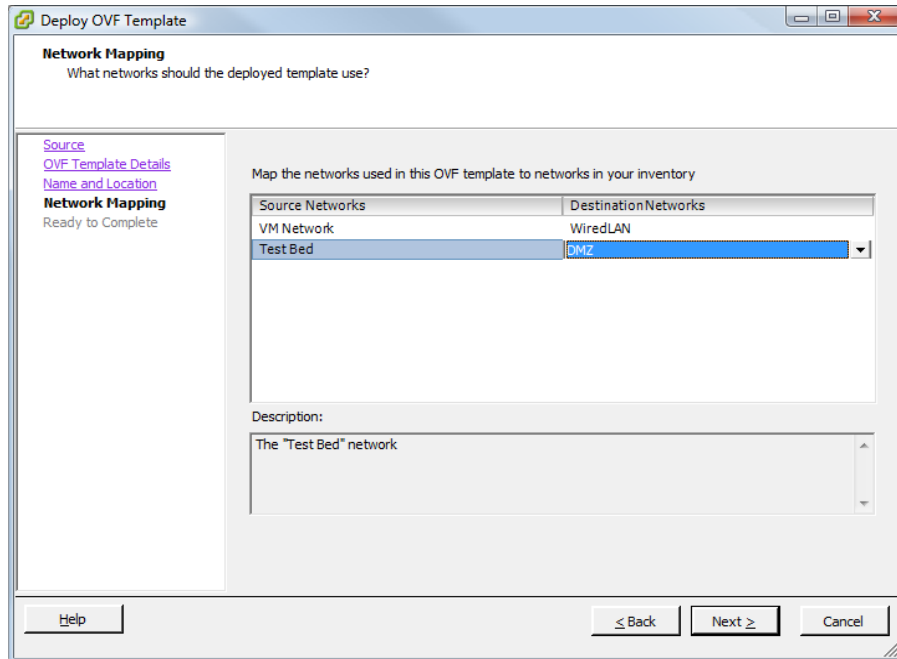
4. Click **Next**. A summary of the Virtual Appliance details is displayed.



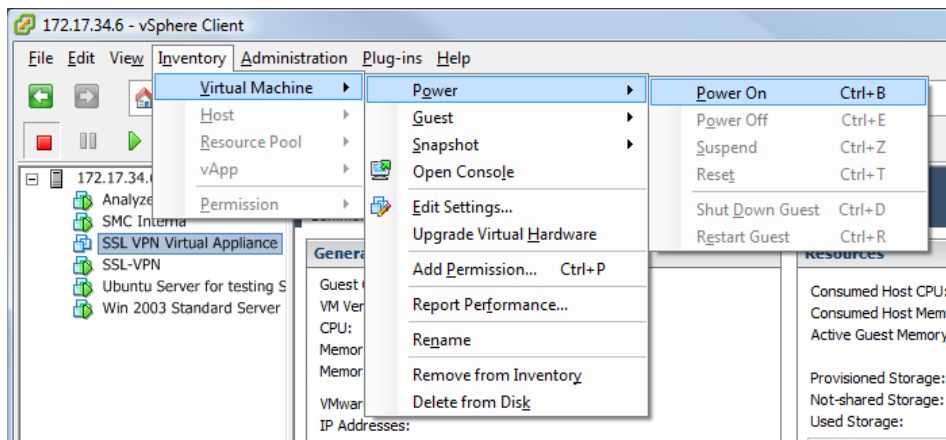
5. Click **Next**.
6. Define a name for the Virtual Appliance, and click **Next**.



7. Map the network segments and click **Next**.

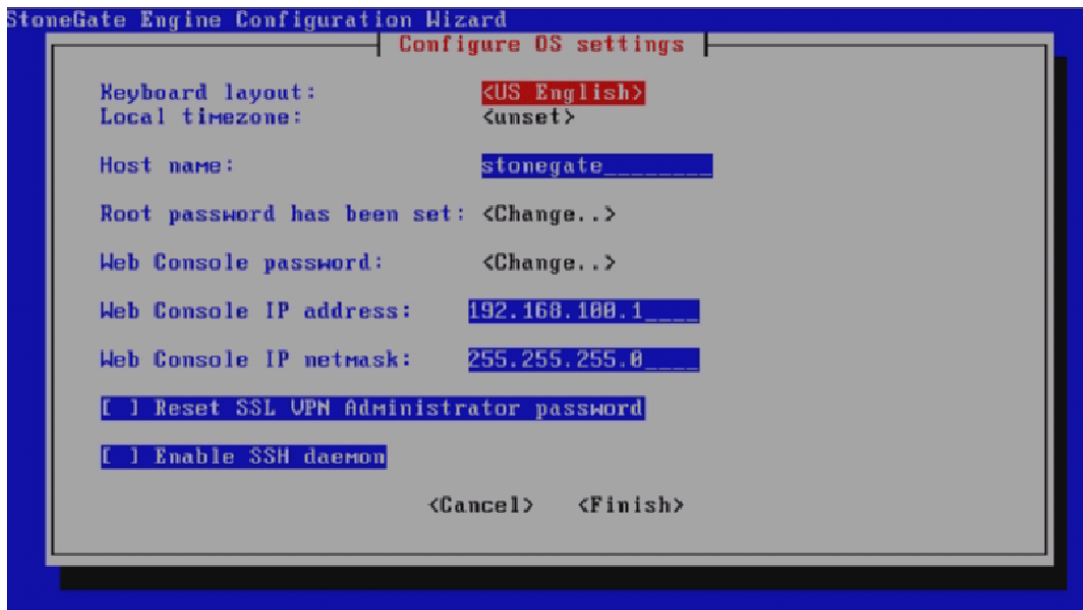


8. Click **Finish** to complete the Virtual Appliance import process. The Virtual Appliance is imported and appears in the Inventory on the left side of the vSphere Client.
9. Select the StoneGate SSL VPN Virtual Appliance and select **Inventory**→**Virtual Machine**→**Power** →**Power On** from the Inventory menu.



10. Select **Inventory** →**Virtual Machine** →**Open Console**.

11. Configure the basic settings in the StoneGate Engine Configuration Wizard.



In the Configuration Wizard, you can change the following parameters:

- Keyboard layout
- Local timezone
- Host name
- Root password
- Web Console password
- Web Console IP address
- Web Console IP netmask

12. Select **Finish** to finalize the SSL VPN Virtual Appliance configuration. If you click **Finish** without making any changes, the SSL VPN default settings apply.

Proceed to *Setting Up the Virtual Appliance*.

Setting Up the Virtual Appliance

Logging In to the Web Console

To log in to the Web Console

1. Make sure your client is connected to the same network segment as the StoneGate SSL VPN Virtual Appliance management port (Network Adapter 1). The client must have a display, mouse, keyboard, and a graphical user interface with a Web browser.



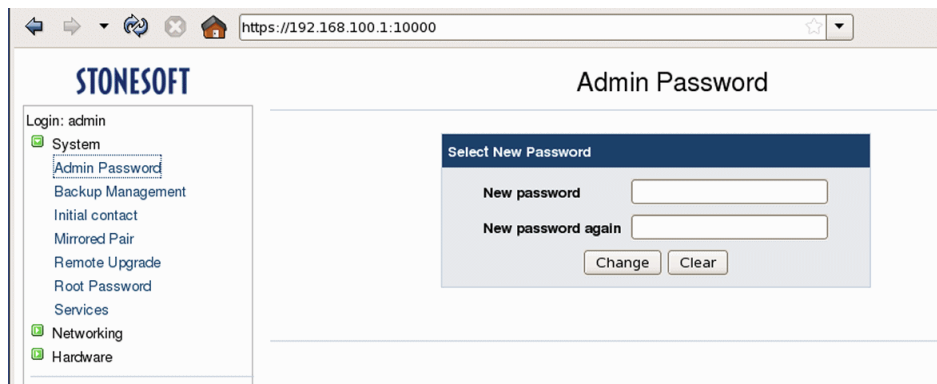
2. Open the Web browser on the attached client and connect to the address <https://<SSL VPN IP Address>:10000>. The login for the appliance Web Console opens.
3. Log in to the Web Console. By default, the username is **admin** and password is **Pass1234**, but we strongly advise you to change the password after logging in according to the instructions below, if you have not done it during the installation.

Continue to *Changing the Web Console Password*.

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**.

Continue to *Setting System Time*.

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 click **System Time**.

The screenshot shows the STONESOFT System Time configuration page. The browser address bar shows <https://192.168.100.1:10000>. The page title is "System Time". On the left, there is a navigation menu with "System Time" selected under the "Hardware" category. The main content area has three sections:

- System Time**: A table with columns Day, Date, Month, Year, and Hour. The values are Monday, 23, February, 2009, and 13:49:20. There are "Apply" and "Copy from hardware time" buttons below.
- Hardware Time**: A table with columns Day, Date, Month, Year, and Hour. The values are Monday, 23, February, 2009, and 13:49:11. There are "Save" and "Copy from system time" buttons below.
- Time Zone**: A section with a "Change" dropdown menu set to "UTC" and a "Save" button below.

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** and click **Save**.

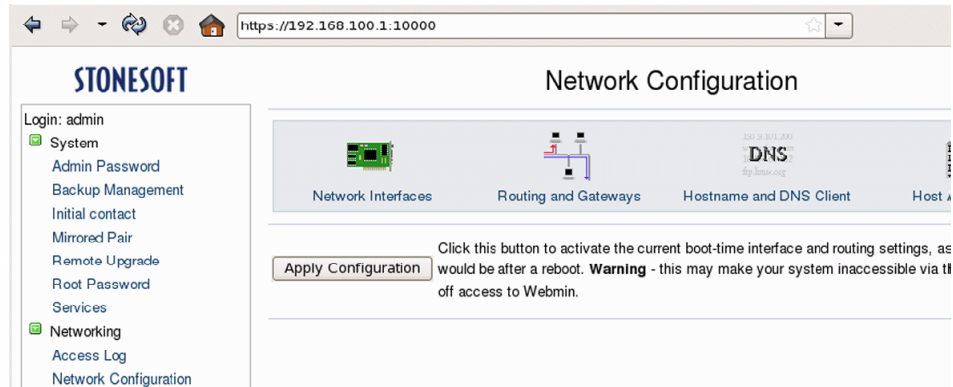
Continue to *Configuring Interfaces*.

Configuring Interfaces

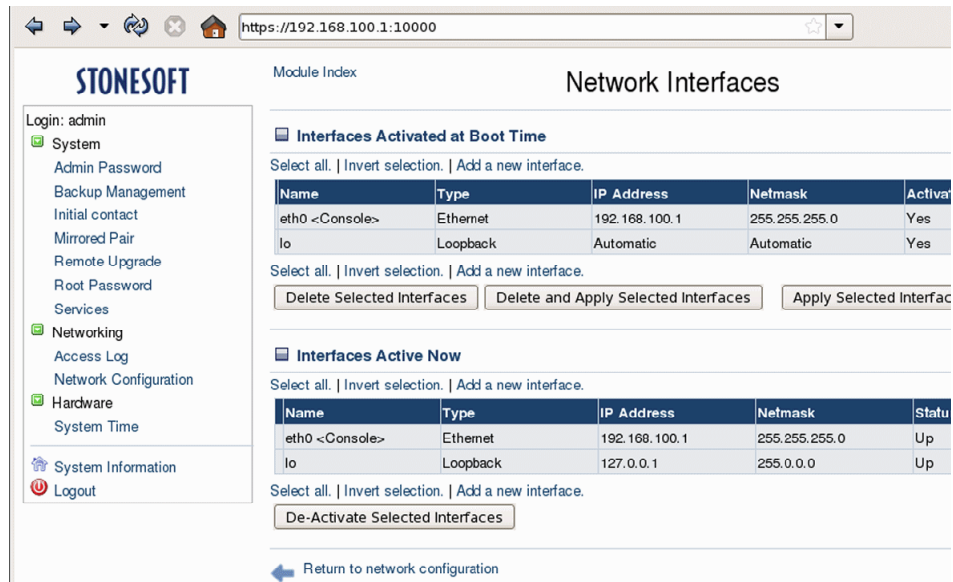
You must add at least one interface in addition to the management port to offer services to your users (a typical configuration requires two or more additional interfaces). If you plan to create a pair of mirrored Virtual Appliances, note that in a mirrored setup, the eth1 port must be dedicated for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

To configure a network interface

1. In the Web Console, under the **Networking** category in the menu on the left, select **Network Configuration**. The Network Configuration view opens.

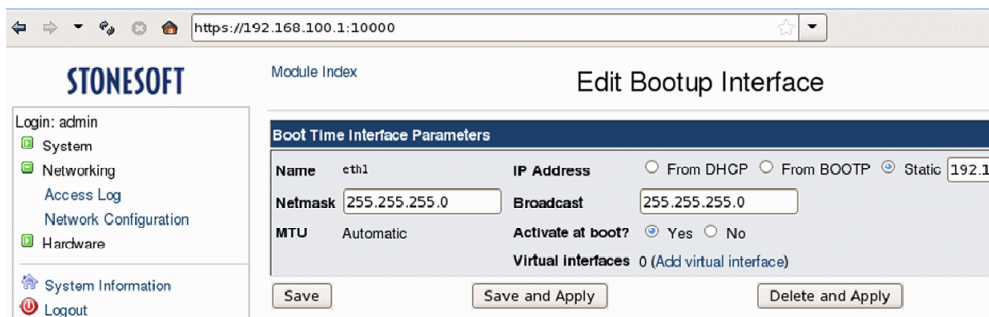


2. On the right, click the **Network Interfaces** icon. The Network Interfaces view opens.



3. Under Interfaces Activated at Boot Time, click **Add a new interface** just below the interface table. The Create Bootup Interface view opens.

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.
5. Click **Create** to save your changes or **Create and Apply** to save your changes and activate the new interface.
6. (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 Interface** setting.



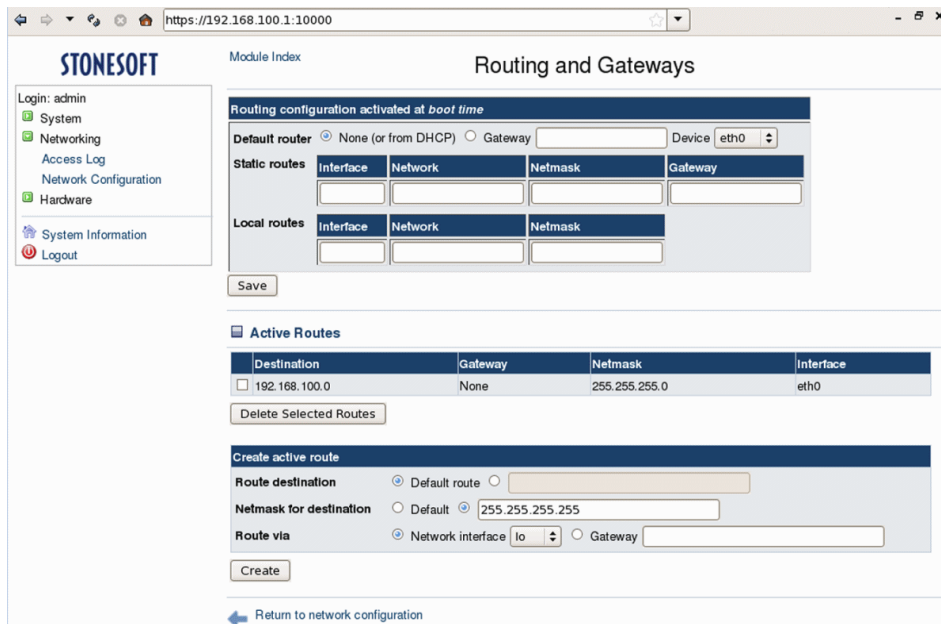
- Fill in the details of the virtual interface and click **Create** to save your changes or **Create and Apply** to save your changes and activate the new interface.
 - You can add more virtual interfaces to the same physical interface. The number of virtual interfaces is shown in front of the Add Virtual Interface action in **Virtual Interfaces**.
7. 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.

Continue to *Configuring Routing*.

Configuring Routing

To configure routing

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



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 as **None (or from DHCP)**, select the correct network interface in the **Device** drop-down menu, and click **Save**.
 - If you want to define the default gateway manually, select **Gateway**, add the IP address into the **Gateway** field, select **Device** from the drop-down menu, 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 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 IP address 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.

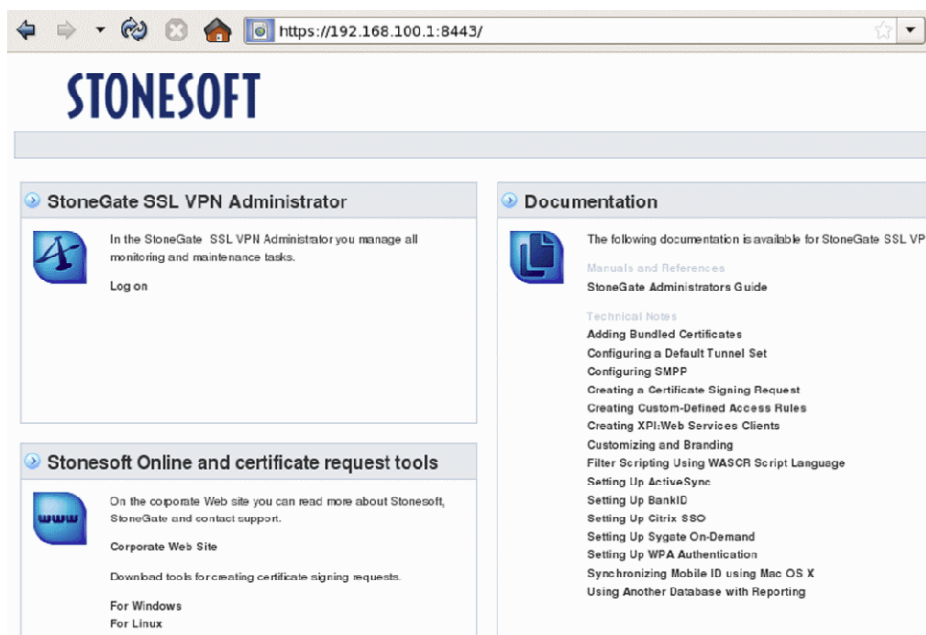
The appliance contains a factory-installed certificate that allows testing in a closed network without the need to install an actual working certificate on the appliance. When installing the appliance for other use, you must always generate a working certificate.

CAUTION – Never use the factory-installed standard keys and certificates for anything else 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, enter <https://<SSL VPN IP Address>:8443> as the address in your Web browser.

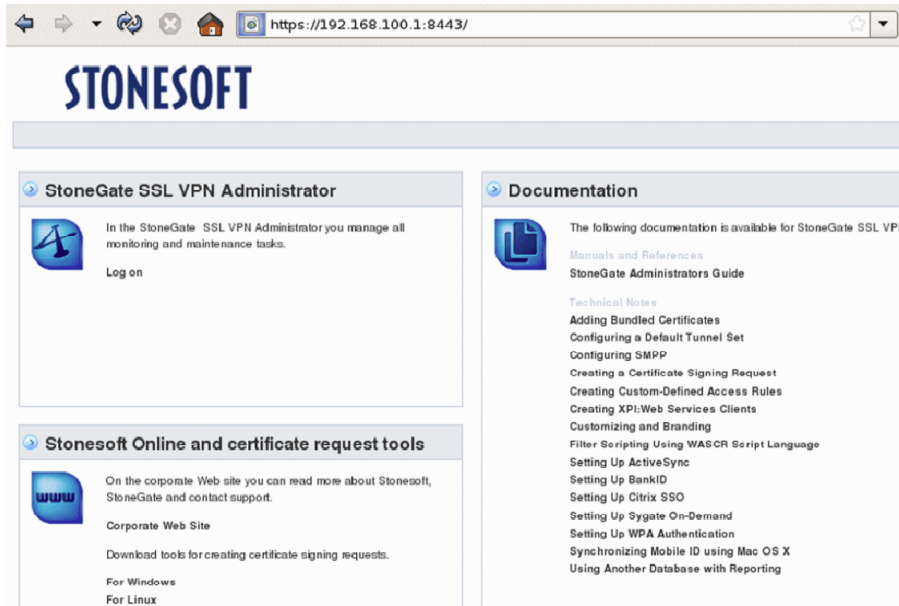


2. Click either the **For Windows** or **For Linux** link according to your operating system to download certificate-related tools to your workstation.
3. Extract all the files in the *.zip* archive to the same location.
4. Open a command line and run the *makescr* script that was just extracted from 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.
 - In Web browsers, by default, many commercial certificate authorities are configured as trusted.
8. 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 *StoneGate SSL VPN Administrator's Guide*, and in this document chapters *Logging In to the Web Console*, and *Importing Certificate Keys and Certificates*).

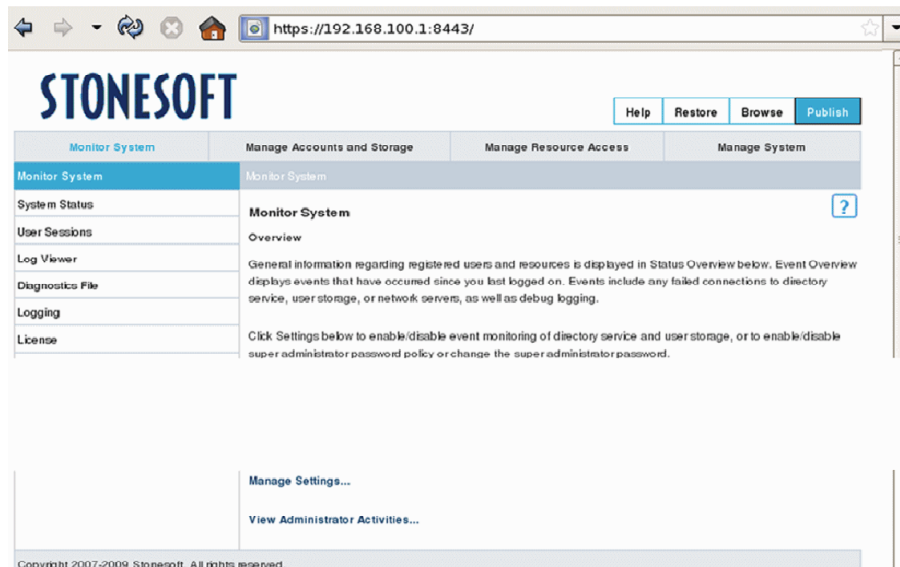
Logging In to the StoneGate SSL VPN Administrator

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**.



2. Log in. By default the username is **admin** and the password is **Pass1234**.
3. When the StoneGate SSL VPN Administrator opens, scroll down to the end of the page.



4. Click **Manage Settings** in the bottom part of the right panel.
5. 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.

The screenshot shows the StoneSoft web interface. At the top left is the 'STONEISOFT' logo. To the right are buttons for 'Help', 'Browse', 'Restore', and 'Publish'. Below these are four tabs: 'Monitor System', 'Manage Accounts and Storage', 'Manage Resource Access', and 'Manage System'. The 'Monitor System' tab is active, and within it, the 'License' option is selected and highlighted in blue. The main content area is titled 'License' and contains an 'Overview' section. It states: 'The contents of the current license are listed below.' Below this is a table of license details:

License Number	
License Version	4.8
License Type	Production
Issued	12/7/09
Issued To	Installation Default License Installation Default License Installation Default License
Issued By	Stonesoft Stonesoft support@stonesoft.com
Validity StoneGate SSL VPN	12/7/09 -- *
Max Concurrent Users	10 (currently 0 concurrent users)
Max Named Users	10000 (currently 0 users registered)
Validity Authentication Service	12/7/09 -- *
Max StoneGate Authentication Users	10000 (currently 0 users registered)
Max RADIUS clients	1
Max Resources	*(currently 1 resources registered)
Max Authentication Methods	2147483647

Below the table is a section titled 'Licensed DNS Names' with the text: 'The license includes the following DNS Names:' followed by a bulleted list:

- 127.0.0.1
- localhost

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

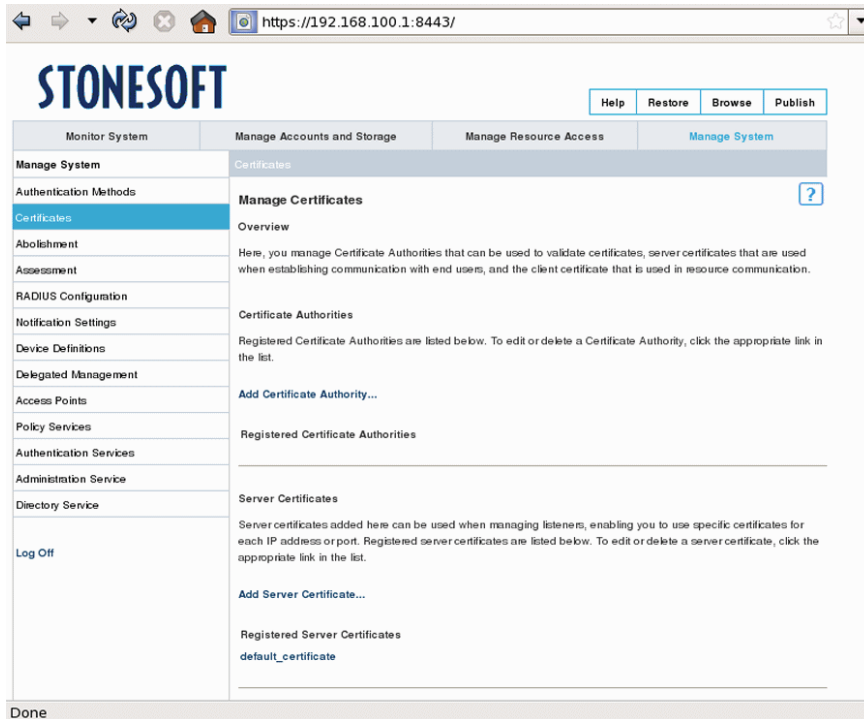
NOTE – If your certificate is a bundled certificate, which may contain intermediate certificates, you must split the certificate before adding it to the StoneGate SSL VPN Administrator.

See *TN2068 Adding Bundled Certificates* for information on how to do this. See section *Generating a Certificate* 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	Manage Accounts and Storage	Manage Resource Access	Manage System
Manage System	Certificates > Add Server Certificate		
Authentication Methods	Add Server Certificate ?		
Certificates	General Settings		
Abolishment	Add the PEM formatted certificate and key file below.		
Assessment	Display Name	<input type="text"/>	
RADIUS Configuration	Certificate	<input type="text"/>	<input type="button" value="Browse..."/>
Notification Settings	Key	<input type="text"/>	<input type="button" value="Browse..."/>
Device Definitions	Password	<input type="text"/>	
Delegated Management	<input type="checkbox"/> Using Hardware Security Module		
Access Points	< Previous		<input type="button" value="Save"/>
Policy Services			
Authentication Services			
Administration Service			

5. Click **Save**. This imports the certificate, but it is not activated yet. For activating the certificate, proceed to *To activate the certificate*.

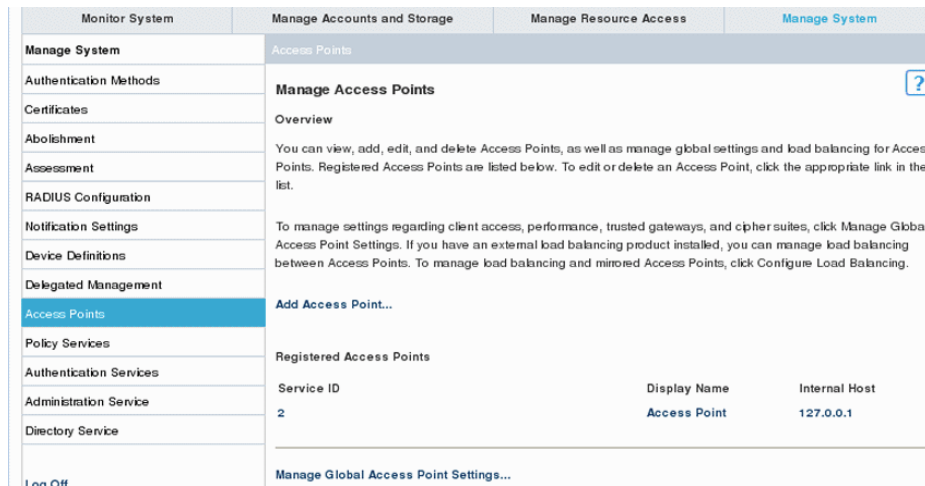
To activate the certificate

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

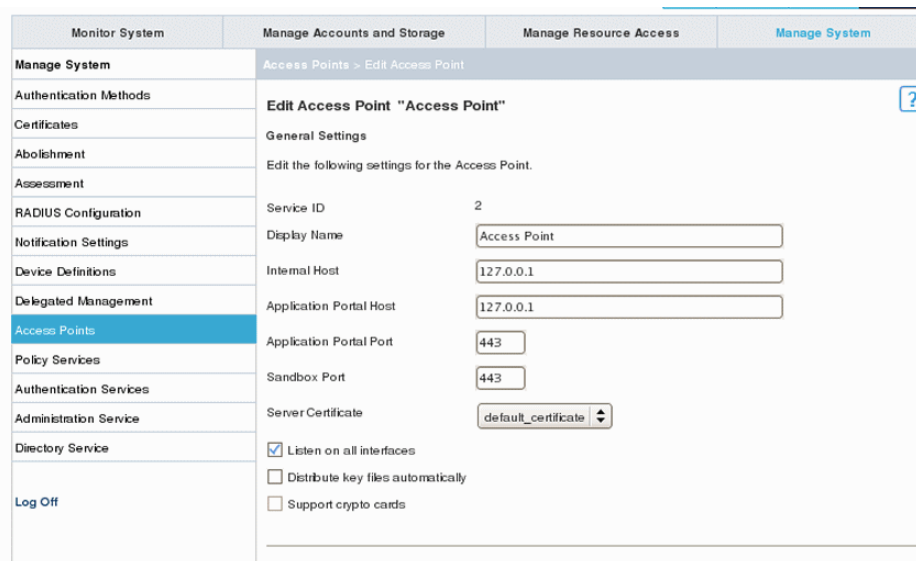
Monitor System	Manage Accounts and Storage	Manage Resource Access	Manage System
Manage System	Administration Service		
Authentication Methods	Manage Administration Service ?		
Certificates	Internal Communication Settings		
Abolishment	Enter the following settings for communication between StoneGate SSL VPN Administrator and the StoneGate SSL VPN network.		
Assessment	Internal Host	<input type="text" value="127.0.0.1"/>	
RADIUS Configuration	Internal Communication Port	<input type="text" value="8300"/>	
Notification Settings			
Device Definitions	External Communication Settings		
Delegated Management	Enter the following settings for communication between StoneGate SSL VPN Administrator and the client.		
Access Points	Administrator HTTP Host	<input type="text" value="0.0.0.0"/>	
Policy Services	Administrator HTTP Port	<input type="text" value="8080"/>	
Authentication Services	Administrator HTTPS Host	<input type="text" value="0.0.0.0"/>	
Administration Service	Administrator HTTPS Port	<input type="text" value="8443"/>	
Directory Service	Server Certificate	<input type="text" value="default_certificate"/>	
Log Off	< Previous		<input type="button" value="Save"/>
Done			

2. Select the correct **Server Certificate** from the list and click **Save**.

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



4. Click **Access Point** under the title Registered Access Points. The information of the selected Access Point is shown.
5. Select the correct Server Certificate from the drop-down list.



6. 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 on the Online Help of the StoneGate SSL VPN Administrator.

For step-by-step instructions for the 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:

1. Create an external user storage.
2. Create 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. Define access rules for allowing access to the services on the Virtual Appliance.
4. Define the services you want to offer.
 - 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 Virtual 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 and you have not activated SSH, 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://<SSL VPN IP Address>:10000>.
2. For detailed instructions for establishing the local connection, see *Logging In to the Web Console* previously in this document.
3. In the Web Console, expand **System** in the menu on the left and select Root Password.
4. 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.
5. In the menu on the left, select **Services**.
6. 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.
3. 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://<SSL VPN IP Address>:10000>.
 - For detailed instructions for establishing the local connection, see *Logging In to the Web Console*.
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) at the address <https://<SSL VPN IP Address>:10000>.
 - For detailed instructions for establishing the local connection, see *Logging In to the Web Console*.
2. Expand **System** in the menu on the left and select **Services**.
3. On the right, select the services that you want to restart.
4. Click **Restart** to restart the services selected above.

Copyright and Disclaimer

© 2000—2010 Stonesoft Corporation. All rights reserved.

These materials, Stonesoft products, and related documentation are protected by copyright and other laws, international treaties and conventions. All rights, title and interest in the materials, Stonesoft products and related documentation shall remain with Stonesoft and its licensors. All registered or unregistered trademarks in these materials are the sole property of their respective owners. No part of this document or related Stonesoft products may be reproduced in any form, or by any means without written authorization of Stonesoft Corporation.

Stonesoft provides these materials for informational purposes only. They are subject to change without notice and do not represent a commitment on the part of Stonesoft. Stonesoft assumes no liability for any errors or inaccuracies that may appear in these materials or for incompatibility between different hardware components, required BIOS settings, NIC drivers, or any NIC configuration issues. Use these materials at your own risk. Stonesoft does not warrant or endorse any third party products described herein.

THESE MATERIALS ARE PROVIDED "AS-IS." STONESOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO, THE INFORMATION CONTAINED HEREIN. IN ADDITION, STONESOFT MAKES NO EXPRESS OR IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE WITH RESPECT THE INFORMATION CONTAINED IN THESE MATERIALS. IN NO EVENT SHALL STONESOFT BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL OR INCIDENTAL DAMAGES, INCLUDING, BUT NOT LIMITED TO, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING FROM THE USE OF THESE MATERIALS, EVEN IF ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH DAMAGES.

Trademarks and Patents

Stonesoft, the Stonesoft logo and StoneGate are all trademarks or registered trademarks of Stonesoft Corporation. Multi-Link technology, Multi-Link VPN, and the StoneGate clustering technology-as well as other technologies included in StoneGate-are protected by patents or pending patent applications in the U.S. and other countries. All other trademarks or registered trademarks are property of their respective owners.

Stonesoft Corporation

Itälahdenkatu 22A
FI-00210 Helsinki
Finland

Tel. +358 9 476 711
Fax +358 9 4767 1234

STONESOFT

Secure Information Flow

Stonesoft Inc.

1050 Crown Pointe Parkway
Suite 900
Atlanta, GA 30338
USA

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