

StoneGate™



StoneGate™
FW-315 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 Stonesoft 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.

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 © 2012 Stonesoft Corporation. All rights reserved. All specifications are subject to change.

Revision: SGAIG_FW-315_20120404

Introduction

Thank you for choosing a Stonesoft™ appliance. This guide provides instructions for the initial hardware installation and the maintenance of the FW-315 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	7
Front Panel	8
Back Panel	9
Connecting the Cables	11
Initial Configuration	13
Maintenance Operations.....	23
Default Port Settings	25
Conformity Marks.....	26
Compliance Information.....	26
Disposal Instructions	29



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

Note – You must have a working Management Center on a separate server to bring the appliance(s) operational. See the *Stonesoft Management Center Installation Guide*.

▼ To install the appliance

1. Configure the Firewall element in the Management Client, and save or upload the initial configuration. See the *Firewall/VPN Installation Guide*.
 - You can upload the initial configuration to the Stonesoft Installation Server in preparation for plug-and-play configuration.
 - Alternatively, you can save the initial configuration on a USB stick.
2. If the initial configuration is on a USB stick, insert the USB stick in a USB port on the appliance.
3. (*Models with wireless support*) Connect the antennas to the appliance as described in *Connecting the Antennas* (page 11).
4. Connect the cables to the appliance (see *Connecting the Cables* (page 11)). The appliance starts up and the initial configuration is transferred to the appliance.
 - If the initial configuration has been uploaded to the Stonesoft Installation Server, the appliance automatically connects to the Installation Server, and the initial configuration is transferred from the Installation Server to the appliance.
 - If the initial configuration is on a USB stick, the initial configuration is automatically imported from the USB stick to the appliance.

See *Initial Configuration* (page 13) for more information on the configuration methods.

Product Documentation

Press **F1** in any Management Client window to view the *Online Help*.

All PDF guides are available:

- On the Management Center CD-ROM (in the *Documentation* folder)
- At the Stonesoft website at http://www.stonesoft.com/en/support/technical_support_and_documents/manuals/

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 electronic equipment. However, please be advised that Stonesoft 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.

WLAN Precautions

- Data traffic by a wireless connection may allow unauthorized third parties to receive data. Take the necessary steps to secure your radio network. See www.wi-fi.org for information on securing your WLAN.
- National restrictions and requirements for authorization may apply to wireless devices. Check the latest status of national regulations with the local authorities.

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 Stonesoft appliance. If after a brief power outage your Stonesoft appliance only partially starts up (for example, the power light is on, but 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 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...+40°C. The allowed storage temperature is -20...+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.

For California:

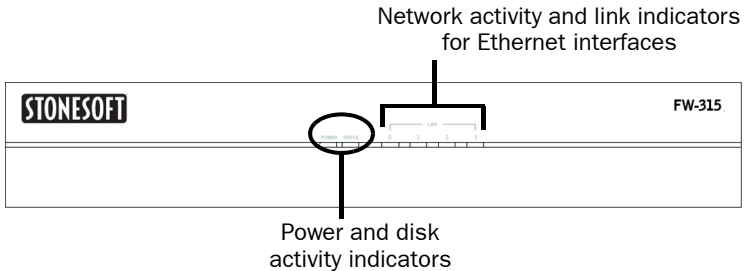
Perchlorate Material - special handling may apply. See www.dtsc.ca.gov/hazardouswaste/perchlorate.

This notice is required by California Code of Regulations, Title 22, Division 4.5, Chapter 33: Best Management Practices for Perchlorate Materials. This product/part includes a battery that contains Perchlorate material.

Unpacking the Appliance

Inspect the box the appliance was shipped in and note if it was damaged in any way. If the appliance itself shows damage, file a damage claim with the carrier who delivered it. Confirm that the Stonesoft anti-tamper tape on the appliance is intact.

Front Panel



Note – Standby power is supplied to the system even when the appliance is turned off.

The indicators in the front panel provide you with critical information related to different parts of the system. The front panel indicator lights are explained below.

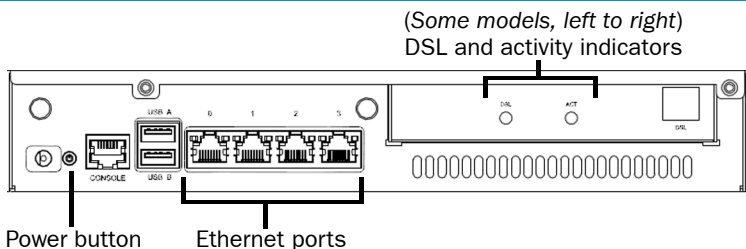
Table 1 Power and Disk Activity Indicators

Indicator	Status	Explanation
POWER	Unlit	The power is off or the appliance is in standby mode. Check the Power button light in the back panel. If the light is off, no power is supplied. If the light is red, the appliance is in standby mode.
POWER	Blue	Indicates power is being supplied to the system's power supply unit. This indicator is illuminated when the system is operating normally.
STATUS	Magenta	Indicates hard disk activity.

Table 2 Network Activity and Link Indicators for Ethernet Interfaces

Indicator	Status	Explanation
0 to 3	Unlit	No link.
0 to 3	Green	Link ok.

Back Panel



The back panel indicator lights and the colors of the Power button light are explained below.

The connectors on the back panel are explained in detail in *Connecting the Cables* (page 11).

Power Button

The color of the Power button light shows the status of the appliance. The light is red when the appliance is in standby mode and blue when the appliance is operating normally. When you first connect the appliance to a power source the Power button light is red. You must push the Power button to change the status of the appliance from standby to active.

Note – If you need to turn off the appliance, always wait at least ten (10) seconds before turning it on again. Otherwise, the appliance may not have time to clear properly and fails to start.

Ethernet Port Indicators

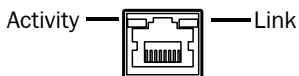


Table 3 Port Indicators

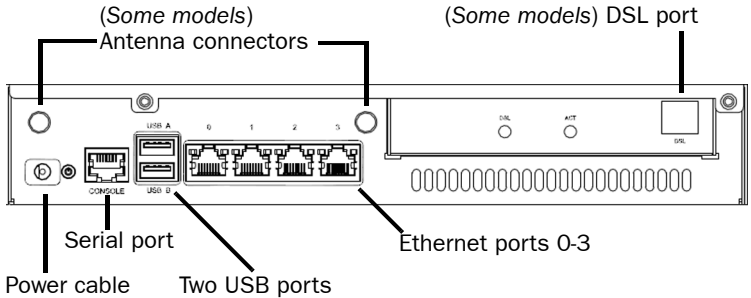
Status	Explanation
Both indicators are unlit	No link.
Both indicators are lit	Link ok. Activity indicator blinks on activity.

DSL Port Indicators

Table 4 DSL and Activity and Indicators for DSL Port

Indicator	Status	Explanation
ACT	Green	A modem connection is up.
DSL	Green	A cable is plugged in to the DSL port.

Connecting the Cables



Only some FW-315 Series appliances support wireless connections. If your appliance does not have WLAN support, proceed to *Connecting the Cables* below.

Connecting the Antennas

▼ To connect the antennas

1. Locate the two antennas included in the delivery.
2. Install the antennas to the two connectors on the appliance's back panel (see *Back Panel* (page 9)) and tighten the knurled nuts at the base of the antennas to secure them firmly to the appliance.
3. Orient the antennas.

Connecting the Cables

▼ To connect network cables

- Connect network cables to the Ethernet ports.
 - The ports are numbered 0-3. The 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.
 - If you intend to use the plug-and-play configuration method, connect a cable at least to Ethernet port 0 that is used for contacting the Stonesoft Installation Server.
- 4. Connect the cable to the DSL port.
 - The DSL port number is 5.

5. (Optional) Connect a 3G modem to one of the USB ports.
 - The port number of the 3G modem is 0.

In appliances that have WLAN support, the port number of the integrated wireless network card is 4.

Note – The ports and port numbers of the physical appliance must match the interface definitions and Interface IDs that you have defined for the firewall engine in the Stonesoft Management Client.

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 the Appliance to the Power Supply

▼ To connect the appliance to the power supply

1. Connect the power cable to the power connector on the back of the appliance.
2. Plug the power cord into a grounded, high-quality power strip that offers 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 a sudden loss of power.

Note – When the appliance is powered and you need to unplug it, always wait at least ten (10) seconds before plugging in the appliance again. Otherwise, the appliance may not have time to initialize itself properly and fails to start.

Initial Configuration

To start using the appliance, you must activate the network interfaces and establish a secure connection to the Management Server as outlined in the sections below.

There are three ways to configure the engine software.

- *Plug-and-play configuration:* Connect the antennas (some models only) and the cables to the appliance. The appliance automatically connects to the Stonesoft Installation Server, downloads the initial configuration, and connects to the Management Server.

Note – If the appliance does not have a DSL port and no 3G modem is plugged in to the appliance, Ethernet port 0 is the only port that can be used for connecting to the Installation Server.

- *Automatic configuration:* You can configure the engine automatically with a USB stick that contains the initial configuration.
- *Engine configuration wizard:* If plug-and-play configuration or automatic configuration is not possible or desired, you can use the engine configuration wizard.

To successfully complete the initial configuration, the following steps are required before you can configure the appliance:

1. The Firewall element must be defined in the Management Center.
2. Engine-specific configuration information must be available from the Management Server. The required information depends on the configuration method:
 - *Plug-and-play configuration:* The engine's initial configuration has been uploaded to the Stonesoft Installation Server.
 - *Automatic configuration:* You have the initial configuration file on a USB stick.
 - *Engine configuration wizard:* You have a one-time password for the engine.

See the *Firewall/VPN Installation Guide* for details.

Note – The appliance must contact the Management Server before it can be operational.

Continue according to the selected configuration method:

- *Configuring the Engine with Plug-and-Play Method* (page 14)
- *Configuring the Engine Automatically* (page 15)
- *Using the Engine Configuration Wizard* (page 16)

Configuring the Engine with Plug-and-Play Method

Plug-and-play configuration is possible only if the engine's initial configuration has been uploaded to the Stonesoft Installation Server. See the *Firewall/VPN Installation Guide* or the *Online Help* of the Management Client for details.

▼ To configure the engine with the plug-and-play method

1. (Optional) If you want to view the progress of the plug-and-play configuration, connect the appliance to a computer using the serial cable supplied with the appliance, and open on the computer a terminal with settings 9600bps, 8 databits, 1 stopbit, no parity.
2. (Optional) Plug in an empty USB stick in one of the USB ports on the appliance if you want to save information on the progress of the plug-and-play configuration on a USB stick.
 - Saving the progress information on a USB stick may be useful, for example, for troubleshooting purposes.
3. Connect the antennas (*only models with wireless support*) and the cables to the appliance (see *Connecting the Cables* (page 11)).
 - The appliance automatically tries to contact the Stonesoft Installation Server. If the contact succeeds, the appliance downloads the initial configuration from the Installation Server, and contacts the Management Server.
 - The appliance uses specific ports in a specific order when it tries to connect to the Installation Server. If a 3G modem has been plugged in to the appliance, the appliance first tries the connection through the 3G modem. If the connection attempts fail and a cable is plugged in to the DSL port, the appliance next tries the connection through the DSL port. If connecting to the Installation Server still fails, the appliance finally tries to connect to the Installation Server through Ethernet port 0.

Note – The wireless port cannot be used for connecting to the Installation Server. If the appliance does not have a DSL port and no 3G modem is plugged in to the appliance, Ethernet port 0 is the only port that can be used for connecting to the Installation Server.

See *Default Port Settings* (page 25) for detailed information on the ports, their default settings, and the order in which the ports are used in connecting to the Installation Server.

The firewall engine installation is complete when the appliance has contacted the Installation Server, downloaded the initial configuration,

and contacted the Management Server. The appliance automatically reboots itself after initial contact with the Management Server. See *After Successful Management Server Contact* (page 22) for more details.

If the Plug-and-Play Configuration Fails

- If the plug-and-play configuration fails and you had plugged in a USB stick to the appliance, you can check for the reason in the log (`sg_autoconfig.log`) written on the USB stick.
- If you see a “connection refused” error message, ensure that the Management Server IP address is reachable from the engine and check the settings that you have defined for the firewall engine’s interfaces in the Management Client. See *Connecting the Cables* (page 11) for information on port numbers and *Default Port Settings* (page 25) for the correct port settings. The port numbers and settings must match the interface IDs and other interface settings in the Management Client.

If attempts to connect to the Installation Server through the 3G modem, DSL port, and Ethernet 0 port have failed, the appliance starts the connecting process again and retries the ports in the same order (3G modem, DSL port, and finally Ethernet 0 port). If necessary, you can run the command `sg-reconfigure --stop-autocontact` on the engine command line to stop this process. See *Connecting to the Engine Command Line* (page 23) for information on using the engine command line.

If plug-and-play configuration continues to fail, you can save the initial configuration on a USB stick and configure the engine using the automatic configuration method. See *Configuring the Engine Automatically* below.

Configuring the Engine Automatically

The automatic configuration requires that you have a suitable configuration saved on a USB memory stick. See the *Firewall/VPN Installation Guide* or the *Online Help* of the Management Client for details.

▼ To configure the engine from a USB memory stick

1. Insert the USB stick that contains the configuration saved in your Management Client in one of the USB ports on the appliance.
2. Connect the antennas (*only models with wireless support*) and the cables to the appliance (see *Connecting the Cables* (page 11)). The appliance automatically imports the configuration from the

USB stick and then tries to make the initial contact to the Management Server.

- If the connection is successful, the appliance automatically reboots itself and the engine configuration is finished.

If you configure the engine with a USB stick, you must set a password for the **root** account in the Management Client to enable command line access to the engine. If you want to allow remote access to the engine using SSH, enable the SSH daemon for the engine in the Management Client. See the *Online Help* for more information.

Proceed to *After Successful Management Server Contact* (page 22).

If the Automatic Configuration Fails

- If the automatic configuration fails, you can check for the reason in the log (`sg_autoconfig.log`) written on the USB stick.
- If you see a “connection refused” error message, ensure that the Management Server IP address is reachable from the engine and check the IP addresses you have defined in the Management Client.
- If the configuration with the USB stick still does not succeed, remove the USB stick from the USB port, and follow the instructions for the manual configuration. See *Using the Engine Configuration Wizard* below.

Using the Engine Configuration Wizard

You can use the engine configuration wizard with all Management Center and Firewall versions. If you have saved the initial configuration on a USB stick, you can import it in the configuration wizard to reduce typing.

▼ To start the configuration wizard

1. Connect appliance to a computer using the serial cable supplied with the appliance.
2. On the computer, open a terminal with settings 9600bps, 8 databits, 1 stopbit, no parity.
3. Turn on the appliance using the power on/off switch. The engine bootup process is shown in the console and, after some time, the engine configuration wizard starts.

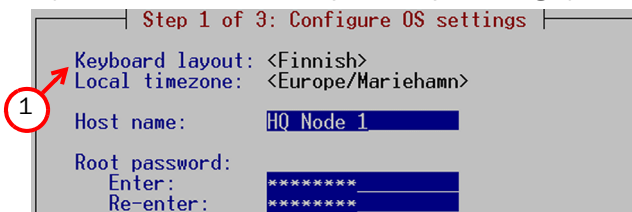
Note – You can (re)start the engine configuration wizard at any time using the `sg-reconfigure` command on the engine command line.

▼ To select the configuration method

1. Do one of the following:
 - To import a saved configuration, highlight **Import** using the arrow keys and press ENTER.
 - To skip the import, highlight **Next** and press ENTER.
2. If you selected the Import option, select the configuration file.

▼ To set the keyboard layout

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



2. Highlight the correct layout and press ENTER.

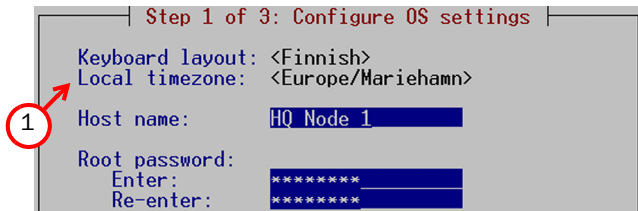
Tip: Type in the first letter to move forward more quickly in the list of keyboard layouts.



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.

Note – The appliance's clock is automatically synchronized with the Management Server's clock.

▼ To set the rest of the OS settings

1. Type in the name of the firewall.



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

- (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.

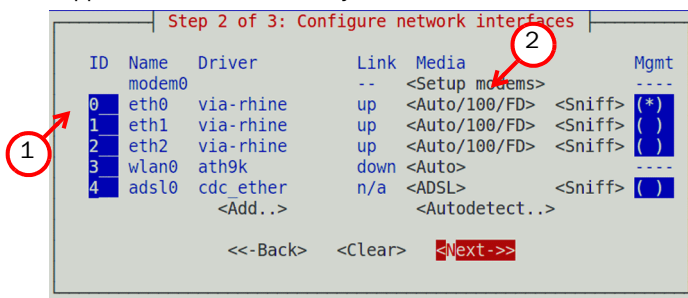
Note – It is not necessary to enable the SSH daemon now for ongoing management, as this option can also be set through the Management Client. We recommend that you enable the SSH access in the Management Client when needed and then disable the access again when you are done.

- Highlight **Next** and press ENTER. The Configure Network Interfaces window is displayed.

Configuring the Network Interfaces

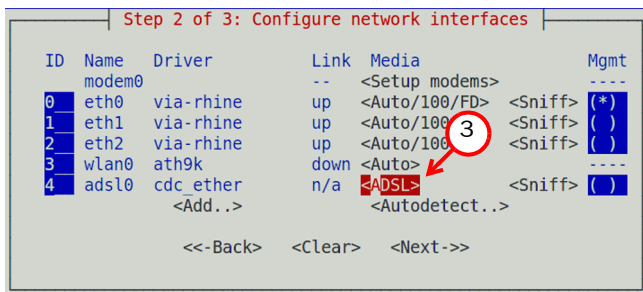
▼ To map the physical interfaces to interface IDs

- Type in the Interface IDs to define how physical interfaces are mapped to the Interface IDs you defined in the Firewall element.



- Highlight the **Media** column for the physical interfaces and (optionally) the wireless interface and press ENTER to match the speed/duplex settings to those used in each network.
 - Make sure that the speed/duplex settings of network cards are identical at both ends of each cable.
- (Appliances with DSL port) Highlight the **Media** column for the ADSL interface and press ENTER to define the Virtual Path ID (VPI)

and virtual channel ID (VCI) settings according to the information that you have received from your service provider.



4. Highlight the **Mgmt** column and press the spacebar on your keyboard to select the correct interface for contact with the Management Server.

Note – The Management interface must be the same that you configured as the Primary Control Interface for the corresponding Firewall element in the Management Center. You cannot select the WLAN (wireless) interface as the Management interface.

5. Highlight **Next** and press ENTER to continue. The Prepare for Management Contact window opens.

Contacting the Management Server

If you imported the initial configuration from a USB stick, most of the information in the Prepare for Management Contact window is filled in. This task has two parts. First, you activate an initial configuration on the firewall.

- The initial configuration contains the information that the engine needs to connect to the Management Server for the first time.
- The initial configuration is replaced with a working configuration when you install a Firewall Policy from the Management Server on this engine using the Management Client.

▼ To activate the initial configuration

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

Step 3 of 3: Prepare for management contact

```
[*] Switch firewall node to initial configuration
[ ] Obtain node IP address from a DHCP server
[ ] Use PPPoE <Settings>
[*] Enter node IP address manually
  IP address:*
  Netmask:*
  Gateway to management:
  [ ] Use VLAN Identifier:
  Contact management server:
```

Callout 1 points to the first menu item. Callout 2 points to the 'Gateway to management' field.

2. Fill in according to your environment. The information must match to what you defined for the Firewall element (Primary Control IP Address).

- If the engine and the Management Server are on the same network, you can leave the **Gateway to Management** field empty.

The initial configuration contains a simple firewall policy that allows only administration-related connections and blocks everything else.

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

▼ To fill in the Management Server information

1. Highlight **Contact Management Server** and press spacebar to activate.

```
Contact management server:
[ ] Do not contact
[ ] Contact
[ ] Contact at reboot
Management server
IP address:*
One-time password:*
Key fingerprint:
192.168.10.200
kU4aL6SmsA
8D:38:10:B3:04:56:DC:9E:A0:B7:18:65:E5:0B:FD:2F
<<-Back> <Finish>
```

Callout 1 points to the 'Contact' option. Callout 2 points to the 'IP address' field. Callout 3 points to the 'One-time password' field.

2. Fill in the Management Server IP address and the one-time password that was created for this engine when you saved the initial configuration.
- If you do not have a one-time password for this firewall, see the *Firewall/VPN Installation Guide* for instructions on how to save an initial configuration.

3. (Optional) Fill in the Key fingerprint (also shown when you saved the initial configuration). Filling it in increases the security of the communications.
4. Highlight **Finish** and press ENTER.

The engine now tries to make initial Management Server contact.

- If you see a “connection refused” error message, ensure that the one-time password is correct and the Management Server IP address is reachable from the node. Save a new initial configuration if unsure about the password.
- If the engine is unable to contact the Management Server, make sure there are no networking problems, that all information defined in the Firewall element corresponds to what you entered in the configuration wizard and, if NAT is in use, that you have configured contact addresses for NAT as explained in the *Firewall/VPN Installation Guide*.

Note – Once initial contact has been made, the engine receives a certificate from the Management Center for identification. If the certificate is deleted or expires, you must repeat the initial contact using a new one-time password.

After Successful Management Server Contact

After you see a notification that Management Server contact has succeeded, or the appliance has rebooted itself after plug-and-play configuration or automatic configuration with a USB stick, the firewall engine installation is complete and the firewall is ready to receive a policy. After a while, the firewall’s status changes in the Management Client from **Unknown** to **No Policy Installed**, and the connection state is **Connected** indicating that the Management Server can connect to the node.

If a firewall policy was included in the initial configuration, the policy is automatically installed on the appliance after successful contact to the Management Server. Otherwise, the next step is creating a policy and installing it on the engine. See the *Online Help* of the Management Client for detailed instructions.



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

Maintenance Operations

Connecting to the Engine Command Line

You may need to connect to the engine command line, for example, to undo a software upgrade.

▼ To connect to the engine command line

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.

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 to the engine command line as described above in *Connecting to the Engine Command Line* (page 23).
2. (Re)start the appliance:
 - If the appliance is powered on, press `Enter`, log in as the user `root` with the password you have set for the appliance, and issue the command `reboot`.
3. Wait until a list of the appliance partitions is shown. The currently active partition is highlighted in the list of partitions.
4. Select the inactive partition and press `Enter`. A list of available commands opens.
5. Select or **Boot SG FW/VPN** <name of partition> and press `Enter`. The appliance switches partitions and boots up.

6. Refresh the policy on the firewall or firewall cluster to synchronize the policy and other configuration data between components.

Note – If the certificate for system communications on the previously used partition is not valid anymore, see the *Troubleshooting* section in the Management Client's *Online Help* for renewal instructions.

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 to the engine command line as described in *Connecting to the Engine Command Line* (page 23).
2. (Re)start the appliance:
 - If the appliance is powered on, press `Enter`, log in as the user `root` with the password you have set for the appliance, and issue the command `reboot`.
3. Wait until a list of partitions is shown. The currently active partition is highlighted. Press `Enter`. A list of available commands opens.
4. Select **System Restore Options** and press `Enter`.
5. Type `1` and press `Enter` to clear the settings. A confirmation prompt is shown.
6. 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 *Initial Configuration* (page 13).

Default Port Settings

This section explains the port settings that are used when the appliance is configured using the plug-and-play method. It also explain the order in which the different types of ports are used to connect to the Stonesoft Installation Server.

Note – Use the default port settings explained below also in the properties of the corresponding engine interfaces that you have defined in the Management Client. The initial configuration fails if the port settings on the physical appliance and the interface definitions in the firewall element properties are not the same.

3G Modem

If a 3G modem is plugged in to one of the USB ports, the appliance first tries to contact the Installation Server through the 3G modem. If connecting to the Installation Server fails after a couple of attempts, the appliance next tries to connect to the Installation Server through the integrated ADSL modem. The 3G modem and the corresponding Modem interface in the Management Client must have the following settings:

- **Access Point Name:** internet
- **Phone number:** *99#
- **PIN Code:** <empty value>

Note – PIN code must also be disabled on the 3G modem.

ADSL

If connecting to the Installation Server using the 3G modem fails and a cable is plugged in to the DSL port, the appliance tries to connect to the Installation Server using predefined ADSL settings. It tries all the predefined settings until the connection to the Installation Server either succeeds or all the predefined ADSL settings have been tried. A list of the predefined ADSL settings is available at the Stonesoft support pages at <http://www.stonesoft.com/support/>.

Note – Plug-and-play configuration requires that the ADSL Service Provider setting is set to Automatic when the initial configuration is saved in the Initial Configuration dialog in the Management Client.

Ethernet 0

If attempts to connect to the Installation Server through the 3G modem and through the DLS port fail, the appliance tries to connect to the Installation Server through Ethernet port 0. In the Management Client, the corresponding Physical Interface must have a dynamic IPv4 address.

Conformity Marks

CE Marking

The following conformity mark is added to the appliance in accordance to 2004/108/EC:



FCC Marking

The following conformity mark is added to the appliance in accordance with FCC Part 15 regulations:



Compliance Information

This section contains information on the FW-315 models that have wireless support and the compliance of these appliances with the EMC directive (2004/108/EC), and the FCC standard (FCC Part 15) for wireless devices that are meant for home and office use.

This information is valid for all dual band products (2,4 GHz, IEEE 802.11b/g/n, and 5 GHz, IEEE 802.11n).

Applied Technologies

Radio spectrum:

- Sub-bands 2400 - 2483,5 MHz, 5150 - 5250 MHz, 5250 - 5350 MHz, and 5470 - 5725 MHz

Safety:

- Dual band products

Electromagnetic Compatibility (EMC):

- Dual band products

National Restrictions and Requirements for Authorization

This appliance can be operated within FCC DFS2 band or ETSI/EC DFS band, or other countries which are regulating or are planning to regulate mid-5 GHz band. The usage of mid-5 GHz band is subject to the regulatory approval along with the resided devices.

The requirements for any country or area may evolve. We recommend that you check the latest status of national requirements for 2.4 GHz and 5 GHz wireless LANS with you local authorities.

Frequency Range

Table 5 Frequency Range Information

Country/ Area	Frequency Range
USA	2.400 ~ 2.483 GHz, 5.15 ~ 5.35 GHz, 5.5 ~ 5.7 GHz, 5.725 ~ 5.825 GHz
Europe	2.400 ~ 2.483 GHz, 5.15 ~ 5.35 GHz, 5.47 ~ 5.725 GHz
Japan	2.400 ~ 2.497 GHz, 5.15 ~ 5.35 GHz, 5.47 ~ 5.725 GHz
China	2.400 ~ 2.483 GHz, 5.725 ~ 5.85 GHz

Channel Support

Table 6 Supported Channels

Country	Mode	Channels
US/Canada	802.11b/g/n	11 (1 ~ 11)
	802.11n	23 non-overlapping channels: 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 149, 153, 157, 161
Major European country	802.11b/g/n	13 (1 ~ 13)
	802.11n	19 non-overlapping channels: 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140
France	802.11b/g/n	4 (10 ~ 13)
	802.11n	19 non-overlapping channels: 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140
Japan	802.11b/g/n	11b: 14 (1~13 or 14th); 11g/n: 13 (1 ~ 13)
	802.11n	19 non-overlapping channels: 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120,124, 128, 132, 136, 140
China	802.11b/g/n	13 (1 ~ 13)
	802.11n	5 non-overlapping channels: 149, 153, 157, 161, 165

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