F-Secure Messaging Security Gateway Deployment Guide

Contents

Chapter 1: Deploying F-Secure Messaging Security Gateway	3
1.1 The typical product deployment model	4
1.2 Configuring the firewall	4
1.3 Installing the virtual appliance from OVF	5
1.4 Setting up the appliance through a console	7
1.5 Changing the network settings	8
1.6 Changing the keyboard layout	11
1.7 Allowing remote SSH access	13
1.8 Completing the setup in the web interface	16

Chapter 2:	Updating	to the	latest	recommended	settings	24
2.1 Import	ing settings					

		~
2.2	Configuring the environment settings2	6

Appendix A: Adding agents to the cluster	34
A.1 Adding a new agent to the cluster	35

Deploying F-Secure Messaging Security Gateway

Topics:

- The typical product deployment model
- Configuring the firewall
- Installing the virtual appliance
 from OVF
- Setting up the appliance through a console
- Changing the network settings
- Changing the keyboard layout
- Allowing remote SSH access
- Completing the setup in the web interface

This guide describes how to install F-Secure Messaging Security Gateway.

1.1 The typical product deployment model

The diagram shows a typical deployment model of the product.



1.2 Configuring the firewall

You need to configure your company firewalls to allow the network traffic through.

E-mail traffic

Source and destination	Protocol	Port
Internet $\leftarrow \rightarrow$ F-Secure Messaging Security Gateway	TCP	25
Microsoft Exchange ← → F-Secure Messaging Security Gateway	ТСР	25
F-Secure Messaging Security Gateway $\leftarrow \rightarrow$ DNS Server	TCP/UDP	53

Updates

Source and destination	Protocol	Port
F-Secure Messaging Security Gateway → Internet	ТСР	80, 443

Administration

Source and destination	Protocol	Port
Administrator → F-Secure Messaging Security Gateway	ТСР	10000
Administrator → F-Secure Messaging Security Gateway	ТСР	22

Importing users (optional)

Source and destination	Protocol	Port
F-Secure Messaging Security Gateway -> LDAP Server	ТСР	389 or 636

End-user commands

Source and destination	Protocol	Port
End-user \rightarrow F-Secure Messaging Security Gateway	ТСР	443

1.3 Installing the virtual appliance from OVF

The following steps provide instructions for installing the OVF image.

If you are using a hardware appliance, you can skip this step.

- 1. Verify the OVF files are available in a directory or URL that you can navigate to using the vSphere Client.
- 2. From the vSphere Client File menu, select Deploy OVF Template.
- 3. In the **Deploy OVF Template** pop-up window, browse to the directory where OVF file is located, and then click **Next**.
- 4. Enter a name for the virtual appliance (for example, F-Secure Messaging Security Gateway). Click Next.
- 5. Select a datastore. Highlight the datastore and click Next.
- 6. For the Disk Format, select the Thick provisioned format radio button and then click Next.

Thick Provisioning Lazy Zeroed: Allocates the disk space statically (no other volumes can take the space), but doesn't write zeros to the blocks until the first write takes place to that block during runtime (which includes a full disk format).

Thick Provisioning Eager Zeroed: Allocates the disk space statically (no other volumes can take the space), and writes zeros to all the blocks.

- 7. Click Finish to complete the installation. It will take several minutes for the installation to complete.
- 8. Before you start the OVF image, you will need to edit the instance settings:

F-Secure Messaging Security Gateway		
	P	Power Guest Snapshot Open Console
	5	Edit Settings
		Migrate Upgrade Virtual Hardware
	2 ⁸⁰	Clone Template
		Fault Tolerance
		VM Storage Profile
		Add Permission Ctrl+P Alarm
		Report Performance
		Rename
		Open in New Window Ctrl+Alt+N Remove from Inventory Delete from Disk

9. Remove the default flexible type adapter:

ardware Options Resources	Profiles VServices	Virtual Machine Version:
Show All Devices	Add Remove	Device Status Connected
lardware	Summary	Connect at power on
Memory CPUs Video card SCSI controller 0 Hard disk 1 CD/DVD drive 1 Network adapter 1 Floppy drive 1	4996 MB 2 Video card LSI Logic Parallel Virtual Disk CD-ROM 1 GTN_502_10.133.4.0 Floppy 1	Adapter Type Current adapter: Flexible MAC Address 00:50:56:b3:33:93 C Automatic C Manual DirectPath 1/0 Status: Not supported Network Connection Network label:
Help		OK Cancel

- **10.** Add a new network adapter:
 - a) Select adapter type E1000 and click Next.
 - b) Confirm the settings.
 - c) Click Finish.

Hardware Summary ■ Memory 4096 MB □ CPUs 2 Video card Video card SSCSI controller 0 LSI Logic Parallel □ Hard disk 1 Virtual Disk ○ CD/DVD drive 1 CD-ROM 1 ■ Floppy drive 1 Floppy 1 S1 State S1 State □ CPUs 2 □ Hard disk 1 Virtual Disk ○ CD/DVD drive 1 CD-ROM 1 ■ Floppy drive 1 Floppy 1	iardware Options Resource	Add Remov	e Mer	Device Type What sort of device do	you wish to add to your virtual m	adhine?
	Hardware Memory CPUs Video card SCSI controller 0 Hard disk 1 CD/DVD drive 1 Floppy drive 1	Summary 4096 MB 2 Video card LSI Logic Parallel Virtual Disk CD-ROM 1 Floppy 1	3 1 51: 25: 12: 64	Device Type Network connection Ready to Complete	Choose the type of device Serial Port Parallel Port CD/DVD Drive US Controller Ethernet Adapter Hard Disk	you wish to add. - Information

For highest reliability, F-Secure strongly recommends the E1000 network adapter over the Flexible.

- **11.** Everything is now configured and you can start to use the image.
 - Note: The OVF image size is either 80 GB or 250 GB. We recommend that you use the larger image for the first server (master). You can download the OVF images from this link: http://www.f-secure.com/en/web/business_global/support/downloads/-/carousel/view/96.

1.4 Setting up the appliance through a console

Follow these instructions to set up F-Secure Messaging Security Gateway with the console.

- 1. Log in to the appliance with the following user name and password:
 - · Login: admin
 - · Password: password



The welcome screen opens.

2. Select Yes to change the admin password.

CHANGE ADMIN PASSWORD Welcome to the F-Secure Messaging Security Gateway. Since this is the first time you are logging onto the system, you must change the password for this account. Select 'Yes' to continue, or 'No' to logout.	CHANGE ADMIN PASSWORD Welcome to the F-Secure Messaging Security Gateway. Since this is the first time you are logging onto the system, you must change the password for this account. Select 'Yes' to continue, or 'No' to logout. <u>Yes ></u> (No >
CHANGE ADMIN PASSWORD Welcome to the F-Secure Messaging Security Gateway. Since this is the first time you are logging onto the system, you must change the password for this account. Select 'Yes' to continue, or 'No' to logout. ∠Yes > < No >	CHANGE ADMIN PASSWORD Welcome to the F-Secure Messaging Security Gateway. Since this is the first time you are logging onto the system, you must change the password for this account. Select 'Yes' to continue, or 'No' to logout. < You >
<u>< Yes</u> → < No →	<u>< Yes</u> < No >

3. Enter your new admin password.

At this stage, the keyboard input language is US English. When you enter a new password, make sure that you use characters that are available after you change the keyboard layout.



4. Press Enter.

Next, you need to change the network settings.

1.5 Changing the network settings

You need to change the network settings the first time you log in to the system.

1. Select Yes to change the network settings.

F-Seci	ure Messaging Security Gateway System ID:00:0C:29:DE:61:08
	CHANGE NETWORK SETTINGS Welcome to the F-Secure Messaging Security Gateway. Since this is the first time you are logging onto the system, you must change the network settings. Select 'Yes' to continue, or 'No' to logout.
	<pre></pre>
l	

The network configuration wizard opens.

2. Enter Yes to continue.



3. Enter the IP address of the appliance.



4. Enter the subnet mask of the appliance.



5. Enter y for the automatic negotiation mode, unless you want to manually configure the transmission parameters of your network device.



6. Enter the IP address of the default gateway.



7. Enter the host name of the appliance.



8. Enter the domain name.



Enter the IP addresses of the DNS servers in use.

We recommend that you use at least two different DNS server addresses for redundancy.



10. Enter a host name override if you are creating two nodes cluster. Add the agent information to the first server (master), and add the master server information if you are installing the agent.



11. Enter Yes to confirm the network settings.

Your new settings are saved.

12. When the new settings have been saved, press ENTER.



Next, change the keyboard layout to suit your needs.

1.6 Changing the keyboard layout

Change the keyboard layout the first time you log in to the system.

1. In the F-Secure Messaging Security Gateway menu, select **Console Keyboard Selector** and press ENTER.

Welcome to This menu can run. 1	MAIN MENU the F-Secure Messaging Security Gateway Menu contains the most often used items that the admin user Please select one of the items below.
	 F-Secure Appliance Setup Assistant Guide Display F-Secure Appliance Network Settings Change Password Console Keyboard Selector Advanced System Control Operations Logout of the F-Secure Appliance

2. Select the preferred keyboard from the list and press ENTER.

F-Secure Messaging Security Gatew	ay System ID:00:0C:29:DE:61:08						
Console Keyboard Selector The Console Keyboard Selector will setup the type of keyboard attached to the console of the F-Secure Appliance. Please select the new keyboard type from the list below. The currently selected keyboard is: 'ILS English'							
ê(-) fi i-intini fr fr-latin0 fr-latin1 fr-pc cf de de-latin1-nodeadkeys S(+)	Finnish Finnish (latin1) French French (latin0) French (latin1) French (pc) French Canadian German German (latin1 ω/ no deadkeys)						
	<cancel></cancel>						

3. Select **Yes** and press ENTER to confirm the change.

F-Secure	e Messaging Security Gateway Syste	m ID:00:0C:29:DE:61:08
	Console Keuboard Selector	
	The new keyboard type selected:	
	Finnish (latin1)	hand time?
	Hre you sure you want to change the key	
	<mark><⊻es></mark> < No >	

4. Press ENTER to return to the main menu.

Console Keyboard Selector The keyboard type has successfully been changed to: Finnish (latin1) Select the OK button to leave the Console Keyboard Selector.	

1.7 Allowing remote SSH access

You need to allow a remote SSH access to the system.

1. From the main menu, select Advanced System Control Operations.

MAIN MENU- Welcome to the F-Secure Messaging Sec This menu contains the most often use	urity Gateway Menu
can run. Thease select one of the ft	d items that the admin user ems below.
1 F-Secure Appliance Setup 2 Display F-Secure Applian 3 Change Password 4 Console Keyboard Selecto 4 Advanced System Control 6 Logout of the F-Secure A	Assistant Guide ce Network Settings r O <mark>perations</mark> ppliance
<u>د ۵</u> ۴ ×	

2. Select Remote SSH Access.



3. Select Enable Remote SSH Access for all.

ecure	Messaging Security Gateway System ID:00:00:29:DE:61:08
	Enable Remote SSH Access This menu provides options for restoring access to the SSH server.
	1 Enable Remote SSH Access for support Enable Remote SSH Access for all 3 Disable Remote SSH Access 4 Return to Advanced System Control Menu
	<u>< <u>0</u>K ></u>

4. Select Yes to confirm that you want to allow the SSH access to the appliance.

F-Secure Mess	aging Security Gateway System ID:00:0C:29:DE:61:08
	Reset SSH in Host Firewall? WARNING: You have chosen to reset the SSH (port 22) configuration in the host firewall. This will reset the configuration to allow all hosts to access the SSH server. Are you sure?

5. Press ENTER to return to the menu.



6. Select Return to Advanced System Control Menu.

Enable Remote SSH Access This menu provides options for restoring access to the SSH server. 1 Enable Remote SSH Access for support 2 Enable Remote SSH Access for all 3 Disable Remote SSH Access Return to Advanced System Control Menu	Secure	Messaging Security Gateway System ID:00:0C:29:DE:61:08
This menu provides options for restoring access to the SSH server. 1 Enable Remote SSH Access for support 2 Enable Remote SSH Access 3 Disable Remote SSH Access Return to Advanced System Control Menu COM		Enable Remote SSH Access
1 Enable Remote SSH Access for support 2 Enable Remote SSH Access 3 Disable Remote SSH Access ■ Return to Advanced System Control Menu		This menu provides options for restoring access to the SSH server.
2 Enable Remote SSH Access for all 3 Disable Remote SSH Access Return to Advanced System Control Menu (OK >		1 Enable Remote SSH Access for support
3 Disable Remote SSH Access Return to Advanced System Control Menu COM		2 Enable Remote SSH Access for all
		3 Disable Remote SSH Access Return to Advanced System Control Manu
<u>< ⊡k ></u>		Metarii to havancea system control hena
K OK >		
		<u>< <u>0</u>K →</u>

7. Select Return to the Main Menu.



8. Select Logout of the F-Secure Appliance.

Welcome This me	MAIN MENU to the F-Secure Messaging Security Gateway Menu nu contains the most often used items that the admin user
can run	. Please select one of the items below.
	1 F-Secure Appliance Setup Assistant Guide 2 Display F-Secure Appliance Network Settings
	3 Unange rassword 4 Console Keuboard Selector
	5 Advanced System Control Operations
	Logout of the F-Secure Appliance

9. Select Yes to log out.

F-Secure	Messaging	Security	Gateway	Syster	n ID:00:00	C:29:DE:61:0)8
		You have F-Secure Would ye	LOGOU e chosen to e Appliance ou like to	T? log out of continue?	the		
			< <u>Y</u> es >	< No >			

After you log out, open your browser and go to

https://[appliance_ip_address_or_dns_name]:10000 to continue setting up F-Secure Messaging Security Gateway with the web interface.

1.8 Completing the setup in the web interface

After you have completed the setup in the console, finish the setup with the web interface.

Messaging Security Gateway does not have a valid certificate installed the first time that you log in.

€∋	Mttps://fsmsg01.yourdomainhere.com:10000/ タマ ひ @ Certificate Error: Navigation×			
8	There is a problem with this website's security certificate.			
The security certificate presented by this website was not issued by a trusted certificate authority.				
	Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.			
	We recommend that you close this webpage and do not continue to this website.			
	Ø Click here to close this webpage.			
	Sontinue to this website (not recommended).			
	More information			

This is normal, so when you receive the certification warning message, continue to the website to complete the setup.

1. Log in to the web interface.

F-Secure				
		Language	English (US)	~
Login: Password:	admin •••••••••••• Log In			
8 2002-2014 F-Secure				

2. Read the introductory screen.

- Step 1 of 12	
Introduction	Welcome to the Setup Assistant Guide for the F-Secure Messaging Security Gateway appliance. The configuration settings you make with the setup assistant are essential for operation of the
License Agreement	appliance. Once you complete your configuration and activate the appliance for updates, the appliance will be ready to protect your email infrastructure from spam and viruses.
Server Information	If you complete the configurations correctly, the F-Secure Protection Server management interface will display, where you can make additional selections and configurations for the appliance.
Network Settings	Fields with an asterisk (*) require an entry.
DNS Settings	Click Next to get started.
Proxy Settings	
Inbound Mail	
Outbound Mail	
Regional Settings	
Alert Profile	
Administrator	
Finish	
	Kant> Cancel

3. Read and accept the license agreement.

- Step 2 of 12	
Introduction	F-Secure License Agreement
License Agreement	
Server Information	E SECUDE DUDCHASE AND LICENSE ACDEEMENT
Network Settings	
DNS Settings	
Proxy Settings	PLEASE READ THIS F-SECURE PURCHASE AND LICENSE AGREEMENT (AGREEMENT) CAREFOLLY, F-SECURE IS WILLING TO SELL THE APPLIANCE AND LICENSE THE SOLUTION THAT LICENSE THE SOLUTION THAT LICENSE AGREEMENT (CAREFOLITY) CAREFOLITY IN THE CONTROL THAT LICENSE AGREEMENT (CAREFOLITY) CAREFOLITY IN THE CONTROL THAT LICENSE AGREEMENT (CAREFOLITY) CAREFOLITY IN THE CONTROL THAT LICENSE AGREEMENT (CAREFOLITY) CAREFOLITY (CAREFOLITY) CAREFOLITY) CAREFOLITY (CAREFOLITY) CAREFOLITY (CAREFOLITY) CAREFOLITY) (CAREFOLITY)
Inbound Mail	CONTAINED IN THIS AGREEMENT, BY CLUCKING ON THE "I ACCEPT BUTTON BELOW OR Y IN INFALLING OF USING THE APPLIANCE THAT OF TAILS THE SOFTWARE LOCKINGE ANY INVESSION ACCEPTING AND A CONTRACT AND AN A CONTRACT AND AND AND AND AND A CONTRACT AND
Outbound Mail	LOCISELE CLINER DE LOCALE LIKE ANY WRITTEN CONTRACT SIGNED SY LACES EL FA WRITTEN AND REACLES (V) TO DE DOGIN DI TALLO TES LEXANS, RED (V) TO DE LOCIS DI TALLO TES LEXANS, RED (V) TES
Regional Settings	EDUNDER AND FTHE TERMS OF THAT WRITTEN AGREEMENT. LICENSEES CONTINUED USE OF THE APPLICACE UNDER AND ALLO SO CONSTITUE ASSENT TO THE SOUTH AND ALLO SO CONSTITUE ASSENT TO THE APPLICACE ON THAT WRITTEN AGREEMENT.
Alert Profile	TIGHNS OF THIS SPACE/AREN LOST AN EXISTING WATTERSAFEDIENT. TIGENSEE (ID) DECEMPE (ID) TIGENSEE (ID)
Administrator	CONTAINS THE SUPTIVARE, AND (OLICENSEE MAY RELOVED THE APPLICATURE ON WHICH THE SUPTIVARE WOULD OTHERWISE BE INSTALLED FOR A FULL REFUND. LICENSEES RIGHT TO REFUND EXPRES 30 DAYS AFTER PURCHASE FROM F-SECURE.
Finish	
	1. DEFINITIONS.
	Affiliate' means any company controlled by, controlling or under common control with License. For purposes of this definition, "control" means the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of such person or entity, whether through ownership of more than fifty percent (50%) of the outstanding voting securities of othermation interests, by contract. "Applicance(s)" means the Applicance, Documentation, Software purchased by Licensee. "Contidential Information which, in accordance with Section 11 below, is considered confidential. "Information means the applicable of the use of the Applicance access code is to F-Secure's support sites, and all information which, in accordance with Section 11 below, is considered confidential." The means the adaption the use of the Applicance and Software part of the provided on the or disorder with the Software to the second of the outstanding and the second of the sec

4. Check the server host name and domain settings, select **Master** as the appliance type, and enter the **Activation ID** from the license that you received from F-Secure.

- Step 3 of 12				
Introduction	Enter the hostname of the appliance, and a fully qualified domain name.			
License Agreement	Salart the spectrum of you called Marter you pand to other your E Secure Activities ID			
Server Information	Select me appliance type. It you select master, you need to enter your F-Secure Activation IU.			
Network Settings	Server Identity			
DNS Settings	* Hostname fsmsg01			
Proxy Settings	Domain Name yourdomainhere.com			
Inbound Mail	Activation Information			
Outbound Mail	Appliance Type Master Agent			
Regional Settings	F-Secure Activation ID fsecure_fi-youractivationid			
Alert Profile				
Administrator				
Finish				
	<pre><code con<="" control="" th=""></code></pre>			

5. Check the network settings.

- Step 4 of 12		
Introduction	Enter the IP addresses you want to assign to	he network interfaces and the accompanying netmask addresses.
License Agreement		
Server Information	Network Interface	
Network Settings	Network Interface 1	
DNS Settings	* IPv4 Address	192.168.225.200
Proxy Settings	* Netmask	255.255.255.0
Inbound Mail	MAC Address	00:0C:29:DE:61:08
Outbound Mail	IPv4 Network Gateway	
Regional Settings	* Default IPv4 Gateway:	192.168.225.2
Alert Profile		
Administrator		
Finish		

6. Check the DNS settings.

- Step 5 of 12	
Introduction	Enter an IP address for the Primary Name Server.
License Agreement	
Server Information	DNS Settings
Network Settings	Primary Name Server 192.168.225.2
DNS Settings	Secondary Name Server 192.168.225.3
Proxy Settings	Tertiary Name Server
Inbound Mail	Hostname Override 192.168.225.201 fsmsg02.yourdomainhere.com fsm
Outbound Mail	(ie: 192.168.1.1 host.example.com)
Regional Settings	
Alert Profile	
Administrator	~
Finish	< >>
	Seal Next>> Cancel

- Note: Depending on how your network is set up, DNS servers may not recognize the IP addresses or host names of the F-Secure Messaging Security Gateway Servers on your network. In this case, add IP addresses and host names of each F-Secure Messaging Security Gateway Server to the Hostname Override text box. If you are creating a two-node cluster, make sure that you add also the host name and IP address of the agent.
- 7. Check the proxy settings.

- Step 6 of 12		
Introduction	If you have configured all HTTPS communi	cation at your company to go through a proxy server, you need to provide the appliance with the hostname, login, and password for the proxy server.
License Agreement	The appliance, by default, is not configured	to use a proxy server.
Server Information	Proxy Settings	
Network Settings	HTTPS Proxy	Do Not Lise Provy (Direct connection to the Internet)
DNS Settings		
Proxy Settings		0
Inbound Mail		
Outbound Mail		
Regional Settings		
Alert Profile		
Administrator		
Finish		
		<pre><<back next="">> Cancel</back></pre>

8. Enter the settings for inbound mail.

- Step 7 of 12								
Introduction	Determine how you want to route your inbound mail. Click Add and enter the appropriate information in the table below.							
License Agreement	For example, you would enter example.com for Mail for Host / Domain and mailserver.example.com for Route to Host(s) / Domain(s).							
Server Information								
Network Settings	Click Next after you complete your entries.							
DNS Settings	Inbound Mail							
Proxy Settings	Add X Delete							
Inbound Mail	* Mail for Host / Domain	Mailer	Route to Host(s) / Domain(s)	Lookup By	Delivery Type			
Outbound Mail		manor		A record only	Ordered			
Regional Settings	vourdomainhere.com	ESMTP V	192.168.225.100	MX and A records	O Load Balanced			
Alert Profile	· · · ·							
Administrator								
Finish								
				Sector Ba	ck Next >> Cancel			

Note: Enter the domains that you use to receive e-mails, and the e-mail servers where the filtered e-mails are routed.

9. Enter the settings for outbound mail.

- Step 8 of 12						
Introduction	Determine how you want to route your outbound mail. Enter the appropriate information in the text field below, and click the right-arrow (>>) button.					
License Agreement	For example, you would enter 10.20 for Allow Relay from IP addresses starting with 10.20.0.0.					
Server Information						
Network Settings	Click Next after you complete your entries.					
DNS Settings	Allow Relay					
Proxy Settings	Durain Harkenson et 10 Advers					
Inbound Mail	Dorman, Hosimane or IP Aduress					
Outbound Mail						
Regional Settings						
Alert Profile						
Administrator						
Finish						
	Kester Cancel					



Note: Add all servers that have rights to send outbound emails to the Internet. Normally, this is your email server address.

10. Select your language, date and time settings.

- Step 9 of 12							
Introduction	During the setup procedure, several default configuration settings are created for your convenience. For example, default filtering rules in the filtering modules are created so that you can start						
License Agreement	using them right away. Select a language for the default settings.						
Server Information	Select your time zone preference.						
Network Settings	Default Language						
DNS Settings	A You will not be able to chance the language for the default settings later, using the management interface (administrative interface). If you do not select a language now.						
Proxy Settings	the default settings will appear in English.						
Inbound Mail	Language English (US) 🗸						
Outbound Mail	Date/Time						
Regional Settings	Time Zone Europe/Helsinki						
Alert Profile	Current Time 2015-08-07 08-19-29 [UTC+3:00]						
Administrator							
Finish							
	Kenter Cancel						

11. Create a profile for the alerts that are sent by the Messaging Security Gateway server.

- Step 10 of 12				
Introduction	Enter the hostname of the alert email server.			
License Agreement	Alext Dee Sle			
Server Information	Alen Profile			
Network Settings	* Hostname	127.0.0.1		
DNS Settings	* Port	25		
Proxy Settings	From Address	fsmsg@yourdomainhere.com		
Inbound Mail	HELO Domain	yourdomainhere.com		
Outbound Mail	Login]	
Regional Settings	Password]	
Alert Profile	Retype Password]	
Administrator				
Finish				
				<< Back Next >> Cancel

12 Enter the e-mail address that receives all the alerts sent by Messaging Security Gateway.

- Step 11 of 12	
Introduction	Enter an email address for receiving alert email.
License Agreement	
Server Information	Alert Email
Network Settings	System Alerts Email Address email.admin@yourdomainhere.com
DNS Settings	
Proxy Settings	
Inbound Mail	
Outbound Mail	
Regional Settings	
Alert Profile	
Administrator	
Finish	
	K Back Next> Cancel

13. Click **Finish** to complete the installation.

- Step 12 of 12	
Introduction	Click Finish to save your configuration and connect to the F-Secure Dynamic Update Service to activate your appliance.
License Agreement	
Server Information	If you cack Cancel or close the Setup Assistant Guide window, you will be automatically logged out: Until you successfully compute the Setup Assistant Guide, it will continue to appear each time you login.
Network Settings	
DNS Settings	
Proxy Settings	
Inbound Mail	
Outbound Mail	
Regional Settings	
Alert Profile	
Administrator	
Finish	
	< Back Finish Cancel



14. Click OK to continue.

weicome
Congratulations, you have successfully setup and activated your appliance. You can now begin using the management interface to make additional selections and configurations for the appliance and the F-Secure Protection Server.
Press the OK button to continue.
N

You have now completed the setup of F-Secure Messaging Security Gateway.

Updating to the latest recommended settings

Topics:

- Importing settings
- Configuring the environment settings

We recommend that you use the latest recommended settings with the product.

2.1 Importing settings

Follow these instructions to import the configuration.

1. Go to System > Licenses and Updates > General and make sure that all patches are installed. The status should be *Up to date* in all lines.

F-Secure Server 🚟	System > Licenses and U	pdates > General							
C Appliance	🕰 Check for Updates 📩 Dow	nload 🏼 Apply Upda	ate(s) Last	checked for updates: 2015-08-	-08 00:15	:03 [UTC+0300]			
W System	Module	Current Vers	ion	Version Date		Available Version	Available Description	Available Date	Status
Summary	Spam MLX Engine	8.0.1-1506180	000	2015-06-26 07:25:00 [UTC+	+0300]				Up to Date
Settings	Spam MLX Definitions	main-1508070	362	2015-08-08 00:12:41 [UTC+	+0300]				Up to Date
Inbound Mail	Regulatory Compliance	141114_1128	35	2014-11-14 21:28:35 [UTC+	+0200]				Up to Date
Outbound Mail	Content Extraction Engine	10.20.0.0p1_14102	4_132239	2014-10-24 23:22:38 [UTC+	+0300]				Up to Date
SMTP Encryption	Zero-Hour Anti-Virus Engine	7.5.0_20130516	1025	2013-05-17 03:05:21 [UTC+	+0300]				Up to Date
SMTP Server Summary	F-Secure Anti-Virus Definitions	2015-08-07_21-	02-41	2015-08-08 00:02:01 [UTC+	+0300]				Up to Date
SMTP Queue Summary	F-Secure Anti-Virus Engine	8.0.1-25010432_140	910_2236	2014-09-11 08:36:44 [UTC+	+0300]				Up to Date
SMTP Messages									
Servers	System Upgrades					Last check	ed for upgrades: 2015-08	-08 00:15:03 [UTC+	+0300]
Jobs	Check for Upgrades	wnload 📿 Lingrade	Last check	ed for upgrades: 2015-08-08 0	0.12.03 [UTC+03001			
Alerts		inicad 🛃 opgrado	1 2401 011000	54 161 apgradot. 2010 00 00 0	0.10.00 [510.0000			
Policy Routes	Module	Current Version		Version Date	Availa	able Version A	vailable Description	Available Date	Status
Certificates	Proofpoint Protection Server	8.0.1.1446	2014-12	2-13 04:28:03 [UTC+0200]					Up to Date
File Type Profiler									
DNS Block List									
Custom Modules									
⊿ Licenses and Updates									
> General									
Licenses									
Settings									
History									

2. Go to System > Backup and Restore and download the configuration backup from https://www.f-secure.com/en/web/business_global/downloads/messaging-security-gateway/latest.

F-Secure Server		System > Backup and Resto	re
Appliance	^	Save Changes	
🍿 System		Backup Options	
Summary		Backup Schedule	Daily V at 2:00 AM
Settings			
Inbound Mail		Backup and Restore	
Outbound Mail			
SMTP Encryption		Restore Backup Xelete Backu	ip Đ Import Configuration Comment:
SMTP Server Summary		Time	Version
SMTP Queue Summary		No Information Available.	
SMTP Messages			
Servers			
Jobs			
Alerts			
Policy Routes			
Certificates			
File Type Profiler			
DNS Block List			
Custom Modules			
Licenses and Updates			
Config History			
Backup and Restore			

3. Browse to your downloaded backup file.

Import Configuration File		
Configuration Filename:	pure_Defauls_801_v1.pbc Browse	
		Import Close

4. Select the imported backup file and click **Restore backup**.

sy	stem > Ba	ckup and Restore			
	Save Change	\$			
Ba	ckup Optic	ns			
	Back	up Schedule Daily V at 2:00 AM			
Ba	ickup and	Restore Entri	es 1-1 🗸 of	1	
a	Restore Back	up 🙀 Delete Backup 🏐 Import Configuration 🛛 Comment: 🤤 Create Backup			
	Time	Version	Comment	User	
1	Fri Aug 7 16:06:40 EEST 2015	8.0.11446 (patch-0002143, patch-0002151, patch-0002153, patch-0002153, patch-0002167, patch-0002167, patch-0002167, patch-0002216, patch-0002226, patch-0002226, patch-0002226, patch-000225, patch-000226, patch-000286, patch-000226, patch-000226, patch-000226, patch-00	FSecure_Defaults_801_v1	admin	Download

5. Click Yes.



6. Wait while the backup is restored.

System > Backup and Restore		
	\$** ₽₀°	Restoring backup

7. Refresh your browser after the backup has been restored.

Success: The configuration was restored

2.2 Configuring the environment settings

Configure your environment settings.

1. Go to Appliance > SMTP Settings > General to configure the postmaster email address and the system administrator email address.

F-Se	cure Server		Appliance > SMTP Settings > General	
🖵 Ap	opliance	<u>^</u>	Save Changes	
Þ	Network		MTA Host Settings	
	Host Firewall		Banner Hostname	
4	SMTP Settings		Banner Text	
>	> General		HELO Hostname	
	Advanced			
	Default LDAP		Email Notification Settings	
	LDAP Routing		Postmaster Email Address	email.admin@yourdomainhere.com
	Access		System Administrator Email Address	email.admin@yourdomainhere.com

 If you use an external email relay for outbound emails, for example an ISP, go to Appliance > SMTP Settings > Advanced and click Add Smart host.

F-Secure Server	Appliance > SMTP Settings > Advanced				
Appliance	Save Changes				
Network	Filter Settings				
Host Firewall	SMTP Turbocharge	Off On			
SMTP Settings	Mail Delivery Options	Refuse Connections Accept Connections			
General	When Filter Unavailable	Retry Messages Deliver Unfiltered			
> Advanced	Queue Settings				
LDAP Routing	Message Expiration	5 days			
Access	Message Queue Interval	30 minutes V 0 minutes V			
Aliases	Message Queue Minimum Age				
Virtual Domains	Alert Sender Message Is Still in Queue After	4 hours V			
Rewrite Domains	Relay Settings				
Rewrite Header	Smart Host	operatormailserver.com			
Masquerade Domains	Relay Option	Relay Subdomains Relay Hosts Only			
Date and Time	Unresolvable Domains	Reject O Accept			
SNMP	Mailer Settings				
📆 System	Maximum Number of Messages Per SMTP Connection	Messages			
Summary	Maximum Number of Recipients Per SMTP Connection	Recipients			
Settings	Maximum Message Header Length	131072 Bytes			

- 3. Go to Appliance > Date and Time to add NTP server if want keep date and time updated automatically.
 - **Tip:** Use ntp.proofpoint.com if you do not have an ntp server that you use already.

F-Secure Server		Appliance > Date and Time
Appliance	~	Save Changes
 Network Host Firewall SMTP Settings General Advanced Default LDAP LDAP Routing Access Alases Vitro I Benzine 		Date and Time Options Time Zone Europe/Helsinki Network Time Protocol O off @ On NTP Server #1 intp.proof/point.com NTP Server #2
Rewrite Domains Rewrite Header Masquerade Domains Sendmail Expert Config Date and Time SNMP	9	

 Go to System > Inbound mail and enter the domains that you are use to receive emails, and email servers where filtered emails are routed.

F-Secure Server	88	System > Inbound Mail			Entries 1 - 1	V of 1 R R D D
Appliance	~	🗟 Add 🗙 Delete 🔌 Create Domain	Search 🔊 Reset			
Network		Mail for Host / Domain 🛆	Mailer	Destination / Error Message	Lookup By	Delivery Type
Host Firewall				192 168 226 100	A record only	Ordered
SMTP Settings		yourdomainhere.com	ESMTP V	52.100.223.100	MX and A records	O Load Balanced
Date and Time						
SNMP						
📆 System						
Summary						
Settings						
Inbound Mail						
Outbound Mail						
SMTP Encryption						
SMTP Server Summary						
SMTP Queue Summary						

5. Go to System > Outbound Mail > Allow Relay to add all servers that have rights to send outbound emails to the Internet. Normally, this is your email server address.

F-Secure Server	3	System > Outbound Mail > Allow Relay
Appliance	~	🛃 Save Changes 🛛 🔿 Import 🗢 Export
 Network Host Firewall SMTP Settings Date and Time SNMP 		Allow Relay Domain, Hostname or IP Address Domain, Hostname or IP Address List: 192.166.225.100
System Summary Settings Inbound Mail		
Outbound Mail Mail Routes Allow Relay SMTP Encryption		

6. Go to System > Alerts > Alert Profiles to add the email address where the product can send alerts.

F-Secure Server	麗	Sy	stem > Alert	s > Alert Profiles		Entries 1 - 1 V of 1	
Appliance	~		Add 🄀 Delete	Find Member:			
Network			ID	Action	Language	Recipients	
 SMTP Settings 						email.admin@yourdomainhere.com	
Date and Time			default	Send HTML alert message	Default (English (US))		
SNMP						1	
W System							
Summary							
Settings							
Inbound Mail							
Outbound Mail							
SMTP Encryption							
SMTP Server Summary							
SMTP Queue Summary							
SMTP Messages							
Servers							
Jobs							
 Alerts 							
General							
> Alert Profiles							
Rules							

 Go to System > Policy Routes to add all those IP addresses that you added to System > Outboud Mail > Allow Relay to the outbound policy route.

F-Secure Server		Sys	tem >	Policy Routes		Entries 1-9 🗸 of 9 🔣 🗹 🕑 🔄
SNMP	~	🗟 A	dd 🔀	Delete 🚽 Save Chang	ges	
📆 System		E	nabled	ID	Description	Route
Summary				internalnet	Connections From Internal Networks	Sender IB address in "127.0.0.1/32" OD Sender IB address in "~1/128"
Settings		-	•			
Inbound Mail			\checkmark	outbound	Outbound Messages	Sender IP address equals "192.168.225.100"
Outbound Mail			1	spfsafe	SPF Safe Networks	
SMTP Encryption	-	-				
SMTP Server Summary			\checkmark	tls_fallback	TLS fallback route	Sender IP address equals "127.0.0.1" AND Sender HELO domain name equals "pps.tlsfallback"
SMTP Queue Summary			~	xclient_trusted	Trusted route for XCLIENT command	
SMTP Messages Servers			-	allow_relay	Connection is allowed to do outbound relay	
Jobs				tis	TLS route	
Alerts			1	default inbound	Default Inbound Mail Policy	Recipient Email Address is in domain "yourdomainhere com"
Policy Routes		-		annan Cumpania		
Certificates			\checkmark	disable_ip_reputation	Disable IP Reputation	
File Type Profiler						
DNS Block List						
Custom Modules						

- 8. If you have a *Protection Bundle* license and you use email encryption, change following settings:
 - a) Go to Encryption > Settings > Secure Reader.
 - b) Turn on Enable External Message Initiation.
 - c) Turn on Enable Recipient Domain Restrictions.
 - d) Turn on Enable Allowed Domains.
 - e) Move your inbound domains to Selected domains list.

F-Secure Server	Encryption > Settings > Secure Reader
Appliance	Save Changes
🍿 System	Secure Reader Login
Administrator	Enabling External Message Initiation allows users external to your organization to log in and authenticate using an email address to compose a secure message. The LIDL is created in the Branding Template. You can restrict both the sender and recipient domains.
Logs and Reports	Enable External Message Initiation Orff O Off On
User Management	Enable Sender Domain Restrictions Off O Cn
C End User Services	Enable Recipient Domain Restrictions O on On
C Smart Search	Allow Sender Domain ● Off O on Enable Allowed Domains ○ Off ● On
Virus Protection	Secure Reader Allowed Domains
Spam Detection DLP Summary	The list of allowed domains applies to secure messages that are composed, replied to, or forwarded using Secure Reader. Response Profiles determine whether users can reply to or forward secure messages. When you enable Reply or Forward settings in a Response Profile, secure messages can be replied to or forward to domain a didresser that below to the forward in the allowed to the topologina in the Allowed to Topologina in the Allowed to Topologina in the Allowed topologina.
DLP Incidents	Select Domains From List
C Encryption	Add Other Domains
▲ Settings General	Inbound Domains: Selected Domains: yourdomainhere.com
Secure Reader Diagnostics	
Domain Profiles ▷ Trusted Partner Encryption Response Profiles Secure Reader Proxy Key Management	
Regulatory Compliance	

9. Choose the language that you want to use in email encryption (DLP) and Digest.

Digest: Go to User Management > Organization > Services and choose the language.

F-Secure Server	EE C	User Management > Organiza	tion > Services						
💭 Appliance	~	🛃 Save Changes	Save Changes						
🍿 System		Digest							
Administrator		Enable	Yes 🗸						
Logs and Reports		Digest Format	HTML Only + HTTP Commands						
C Quarantine		Send Digest	Yes 🗸						
😳 User Management		Send Empty Digest	No						
Settings		Audit Folder in Digest	No 🗸						
Password Policies		Web Application							
Import/Auth Profiles			N						
 Organization 		Enable	res 🗸						
Filtering		Language							
DLP		Language	Englieh (IIS)	Contrara l'anguage					
> Services			Liigiiaii (03)	manage Languages					
Authentication		Branding Template							
Routing		Branding Template	System_Default_Digest_Branding - System Default E 🗸	Manage Branding Templates					
Advanced									
Sub-Orgs									
Groups									
Users									

Encryption: Go to **User Management > Organization > DLP** and choose the language.

F-Secure Server	User Management > Organiz	ation > DLP	
Appliance	Save Changes		
🍿 System	Encryption		
Administrator	Enable Secure Reader	Yes 🗸	
hi Logs and Reports	Secure Reader Read-Only	No	
G Quarantine	Response Profile	System_Response_Profile - System Recipient Respc V	Manage Response Profiles
Ser Management	External Password Policy	Encryption_Users - Encryption Users	Manage External Password Policies
Settings Password Policies	Branding Template	System_Default_Encryption_Branding - System Defa	Manage Branding Templates
Import/Auth Profiles	Language	English (US)	Manage Languages
 Organization 	Regulatory Compliance		
Filtering DIP	Enforce Regulatory Compliance	Yes 🗸	
Services	Digital Assets		
Authentication	Enforce Digital Assets	Yes 🗸	
Routing	Document Creation Allowed	No	
Advanced Sub-Orns	Smart Send		
Groups	Allow Smart Send	Yes 🗸	
Users			

- **10.** Admin and all end user connections are encrypted with HTTPS. We recommend that you use a signed SSL certificate and that you use wildcard or SAN certificates, because you need to use the same SSL certificate with multiple services (admin, enduser services, and encryption).
 - a) If you need to create a certificate request, go to System > Certificates > Certificates and click Generate Certificate Request.

F-Se	ecure Server	黖 (S	/stem > Certific:	ates > Cer	tificates			Entries 1 - 1	✓ of 1	
💭 A	ppliance	~	R	Generate Certificate	Request	Generate Self-signed Certifica	te 🔿 Import 🕱 Delete 👘				
📆 Sı	ystem			Status	Serial	Issued To	Issued By	Issued	Expires		
	Summary			Invalid, Self-signed	1438860999	fsmsg01.yourdomainhere.com	fsmsg01.yourdomainhere.com	2015-08-06 11:36:39 [UTC+0300]	2035-08-06 11:36:39	UTC+0300]	Download
	Settings										
	Inbound Mail										
	Outbound Mail										
	SMTP Encryption										
	SMTP Server Summary										
	SMTP Queue Summary										
	SMTP Messages										
	Servers										
	Jobs										
	Alerts										
	Policy Routes										
4	Certificates										
>	Certificates										
	Services										
	SMTP Publishers (CA)										
	Site Publishers										

b) Add your server and company details to the certificate request.

Request Certificate	
Server Hostname:	fsmsg01.yourdomainhere.com
Organization (Company/Agency):	YourCompanyName
Organizational Unit:	YourOrganizationalUnit
Locality (City/County):	Helsinki
State/Province:	Uusimaa
Country:	FI
Subject Alternative Names:	
	Include all domain profiles
	Request Certificate Clos

- c) Send your certificate request to your SSL certificate provider.
- d) After you have received the signed certificate, click **Import** to import it to Messaging Security Gateway.

Add all needed certificates in one file. The correct order is:

- 1. Private Key (if you did not create a certificate request)
- 2. Server Certificate
- 3. Intermediate Certificates
- **4.** Root Certificate (optional)

F-Sec	ure Server	X 1	Sy	stem > Certifica	ites > Cert	ificates			Entries 1 - 1	V of 1	
📮 App	liance	~		Generate Certificate	Request 🛃	Generate Self-signed Certificat	e 🛋 Import 🕱 Delete 👘				
📆 Syst	em			Status	Serial	Issued To	Issued By	Issued	Expires		
S	ummary			Invalid, Self-signed	1438860999	fsmsg01.yourdomainhere.com	fsmsg01.yourdomainhere.com	2015-08-06 11:36:39 [UTC+0300]	2035-08-06 11:36:39 [l	UTC+0300]	Download
⊳ S	ettings										
In	bound Mail										
Þo	utbound Mail										
⊳ si	MTP Encryption										
S	MTP Server Summary										
S	MTP Queue Summary										
S	MTP Messages										
S	ervers										
Jo	ibs										
⊳ Al	erts										
P	olicy Routes										
4 C	ertificates										
>	Certificates										
	Services										
	SMTP Publishers (CA)										
	Site Publishers										

e) Browse to your certificate file and add a password if you are importing private key as well, and click **Import**.

Import Certificate		
Certificate File:	rator\Desktop\bundlecer(Brows	ie
Format:	PEM	~
Password:	•••••	۲
		Import Close

f) Go to System > Certificates > Services to change your certificate to all services. Click Save to confirm the new settings.

F-Secure Server	38	System > Certificates > Services	
Appliance	~	Save Changes	
📆 System		Services	Certificate
Summary		SMTP Server	fsmsg01.yourdomainhere.com (1438860999) V
Settings		Administration Server	
Inbound Mail			rsinsgor.yourdoinainnere.com (1436666999) V
Outbound Mail		End User Web Application / Secure Reader	fsmsg01.yourdomainhere.com (1438860999) V
SMTP Encryption			
SMTP Server Summary			
SMTP Queue Summary			
SMTP Messages			
Servers			
Jobs			
Alerts			
Policy Routes			
 Certificates 			
Certificates			
Services			
SMTP Publishers (CA)			
Site Publishers			

11. The service needs to know your company email addresses.

You can use several different methods to import users (manually, file, or LDAP). The following steps instruct how to use LDAP, which is the method that we recommend.

a) Go to User Management > Import/Auth Profiles and click Add.

F	-Secure Server 🔛 🗄	User	Management >	Import/Auth Profiles								
Ģ	Appliance	🛃 Ad	😓 Add 🔯 Delete 📫 Import									
n	System		Туре	Name	Schedule	Description	Info					
2	Administrator	i) Th	e default authentica	tion profile (Authentication Source) ca	n be selected on the <u>User N</u>	Management > Organization > Authentication	<u>1 page.</u>					
11	Logs and Reports		PPS	PPS			User Repository					
C2	Quarantine											
83	User Management											
	Settings											
	Password Policies											
	Import/Auth Profiles											
	Organization											
	Sub-Orgs											
	Groups											
	Users											

b) In the Import window, click Advanced LDAP Options.

Fill in the following information:

- Data Source: Defines the location where the user data is imported. The LDAP query is sent to this location.
- **Profile Name**: ID of the import profile.
- Host/IP Address: Host name or IP address of the LDAP (Active Directory) server.
- **Base DN**: A distinguishable name for the AD scope.
- Bind DN: The user whose (read) credentials are used to access the AD.
- **Password**: Bind DN user's password.

		General	Advanced
Enable:	⊖ off ● on		
Data Source:	LDAP/Microsoft Exchange/Active Directory/Lotus E	Domino 🗸	
Profile Name:	Ad_Import	×	
Description:	Connection to yourdomain.com Active Directory Se	rver	
Settings			
Host/IP Address:	192 168 225 50	Configure	
Advanced LDAP Options <<			
Base DN:	dc=vourdomainhere.com.DC=com	Example: ou=users,dc=acme,dc=com	
Bind DN:	fsecure user@vourdomainhere.com		
Password:			
Port:	389		
Authentication Attribute:	mail		
Secure Socket Layer (SSL):	Off On		
LDAP Version:	v3 V		
Certificate File:	-none-	\checkmark	
Simple Authentication And Security Layer (SASL):	-none-		
Default Domain Name:			
Verify			
Username:			
Password:		erify Info	
			Add Entry Cancel

- c) Go to the **Advanced** tab.
 - Allow Mailing lists without Owner: Choose Off if you use Managed By with all email enabled groups in Active Directory. Otherwise, choose Yes.
 - **Map UID to Attribute**: Use objectGUID if your LDAP server is Active Directory. Otherwise, use your unique attribute in your LDAP server.
 - Group Attribute: memberOf

						General		Advanced
Data Source:	LDAP/Microsoft Exc	change/Ad	tive [Director	y/Lotus [Domino		
Drafie Name:	Ad Import	2						
Poperiation:	Connection to your	domain.co	m Ac	tive Dire	ectory S	erver		
Opuons								
Fallback Authentication:		۲	Off	() On	, ,	Authentication Profile PPS	~	
Force Authentication Profile for Mobile Secure Reader or ex	lernal IP Request	۲	Off	() On	, ,	Authentication Profile PPS	~	
Force Authentication:		۲	Off	() On		Allow to Login Without Password:		● Off ○ On
Allow Login With Alias:		0	Off	On		Use Primary Email Address to Authe	enticate:	⊖ off
Create User After Authentication:		۲	Off	() On	1			
Send Welcome Message		۲	Off	() On	(Set Temporary Password		🖲 Off 🔘 On
Import Settings								
Filter:	(mail=*)					Example: (mail=*)		
Insert Mode:	insert all entries				~	1		
Add to Group/Sub-Org With Profile Name (Ad_Import):	⊖ off ● On	Тур	e:	Group	p	×		
Remove User Profiles Not Imported:	🔿 Off 🖲 On	Re	strict !	Number	r Of Prof	iles To Be Deleted To Less Than 50) V	
Allow Mailing Lists without Owner:	● Off ○ On							
Map UID to Attribute:	objectGUID		_		-			
Replace Mode:	replace all aliase	s for exis	ting	users	~]		
Update Mode:	update all user d	ata	_		~			
Object Type:	auto based on ob	ojectClas	8		~	1		
Group Attribute:	memberOf				×	1		
Command Options:			_			^ ?		
						\vee		
								Save Changes Can

d) Click **Schedule** to schedule your LDAP import profile.

F-Secure Server	{ U	ser	Management >	Import/Auth Profiles			
Appliance	8	Ad	d 🔀 Delete 🛋 In	nport			
m System		8	Туре	Name	Schedule	Description	Info
	i) Th	e default authentica	tion profile (Authentication Source) ca	n be selected on the User I	Management > Organization > Authentication	1 page.
M Logs and Reports		1	Ldap	Ad_Import	Schedule	Connection to yourdomain.com Active Directo	Idap://192.168.225.50/dc=yourdomainhere.com
Ca Quarantine			PPS	PPS			User Repository
🔯 User Management						1	
Settings							
Password Policies							
Import/Auth Profiles							
Organization							
Sub-Orgs							
Groups							

e) Add how often you want to run LDAP import.

		Г	Parameters
Profile:	Ad_Import		
Туре:	● Time ○ Interval		
Time:	07:00	Import Times:	
Days:	Every Day		
		Si	ve Changes Canc

Adding agents to the cluster

Topics:

• Adding a new agent to the cluster

The following steps are optional and needed only if you want to add another agent to your current environment.

A.1 Adding a new agent to the cluster

You need to have a second installation of Messaging Security Gateway to add an agent to your current environment.

To get a second installation of Messaging Security Gateway, repeat the installation steps. You do not need to complete the setup in the web interface.

1. Log in to the web interface of the master appliance.

At this stage, the keyboard input language is English. When choosing the new password, use those characters that you can access after you change the keyboard layout.

F-Secure			
		Language English (US)	~
Login: Password:	admin •••••••		
8 2002-2014 F-Secure			

2. Go to System > Servers and click Add Agent.

F-S	ecure Server 🛛 🐰	1	System > Servers
	ppliance	~	🗟 Add Agent 🕺 Delete Agent 🏾 🗣 Reboot 🔎 Shutdown
🕅 s	ystem		
	Summary		Services: Swap: 13% Used (3.31G Avail)
Þ	Settings		CPU User: IIIIIIIII 8%
	Inbound Mail		CPU I/O Wait: 1%
Þ	SMTP Encryption		Server Profile: Config Master
	SMTP Server Summary		
	SMTP Queue Summary		
	SMTP Messages		
	Servers		

3. Fill in the agent information and click Add Agent.

System > Servers > Add Agent	
🛃 Add Agent 🗙 Cancel	
Agent Settings	
Host Name	fsmsg02.yourdomainhere.com
Admin Port Number	10000
Instance Name	instance1
Admin User Password	•••••
Clone Existing Configuration	✓
Source Host Name	fsmsg01 🗸
Import Agent Sendmail Configuration	\checkmark
Server Profile	Mail Filter
Services	Secure Reader ICAP

Note: Admin User Password is the admin password for the agent.

Note: If you are using email encryption, select **Secure Reader**.

Status	
3 8 e	Adding server
0 - 2	Please wait.

Adding the server may take several minutes.

Server added successfully

- 4. The agent is now added to the cluster.
- 5. After the agent has been added to the cluster successfully, go to **System > Summary** and wait until the agent status turns green. This can take a while.

System	> Servers						
🛃 Add A	gent 🕺 Delete	Agent 🏾 🎙 Reboot 📲 Shutdown 👘					
± 🗌 🔇	fsmsq01 Services:		PPS Version: 8.	0.1.1446	System ID: 00:0	C:29:DE:61:08	
	Swap:	12% Used (3.35G Avail)	PPS Disk:	[[[[[[[[[[[[[[[[[[[[[[[[[[[[[[[[[[[[[[System Disk:	IIIIIIIII 8% Used (10.28G Avail)	
	CPU User:	8%	CPU Nice:	5%	CPU System:	111111111 4%	
	CPU I/O Wait:	1%	CPU Busy:	111111111 17%			
	Server Profile:	Config Master	Last Update: 20	15-08-07 10:30:48 [UTC+0300]	Uptime: 0 day(s)	, 1:11, load average: 0.29, 0.52, 0.43	
H 🗌 🏈	fsmsq02 Services:		PPS Version: 8.	0.1.1446	System ID: 00:0	C:29:7E:15:FC	
	Swap:	[11111111] 0% Used (5.75G Avail)	PPS Disk:	IIIIIIII 8% Used (52.49G Avail)	System Disk:	[11111111] 8% Used (10.29G Avail)	
	CPU User:	[11111111] 5%	CPU Nice:	1111111111 2%	CPU System:	111111111 3%	
	CPU I/O Wait:	0%	CPU Busy:	111111111 11%			
	Server Profile:	Mail Filter	Last Update: 20	15-08-07 10:30:48 [UTC+0300]	Uptime: 0 day(s)	, 0:55 , load average: 0.07, 0.11, 0.10	

6. Repeat the same steps for the agent to configure the environment and click Change Certificate to all services in System > Certificates > Services.