

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 Importing settings.....	25
2.2 Configuring the environment settings.....	26
Appendix A: Adding agents to the cluster.....	34
A.1 Adding a new agent to the cluster.....	35

Deploying F-Secure Messaging Security Gateway

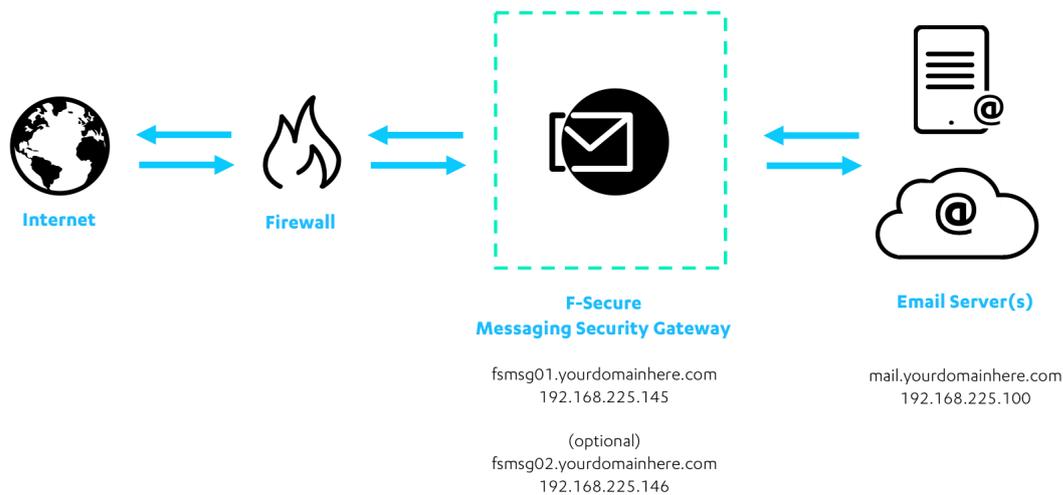
Topics:

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

- *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*

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 ← → F-Secure Messaging Security Gateway	TCP	25
Microsoft Exchange ← → F-Secure Messaging Security Gateway	TCP	25
F-Secure Messaging Security Gateway ← → DNS Server	TCP/UDP	53

Updates

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

Administration

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

Importing users (optional)

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

End-user commands

Source and destination	Protocol	Port
End-user → F-Secure Messaging Security Gateway	TCP	443

1.3 Installing the virtual appliance from OVF

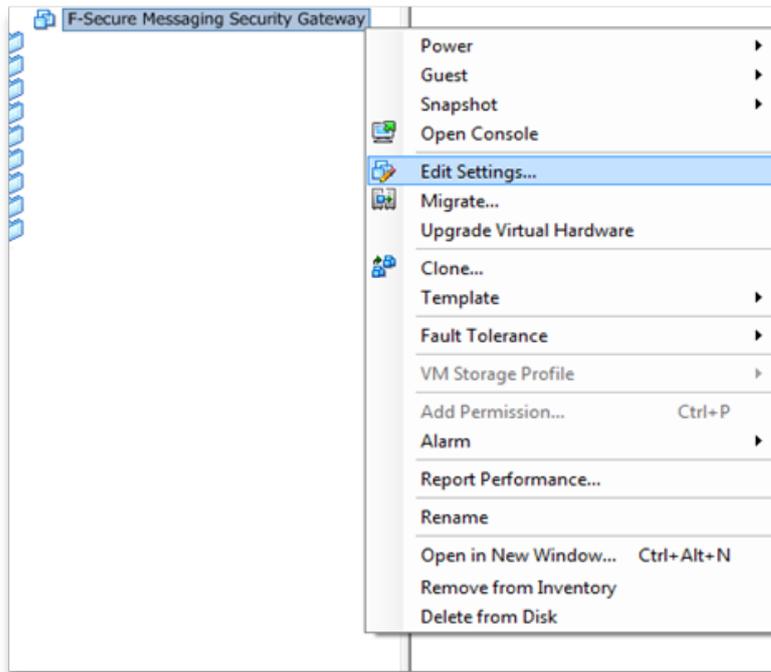
The following steps provide instructions for installing the OVF image.

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

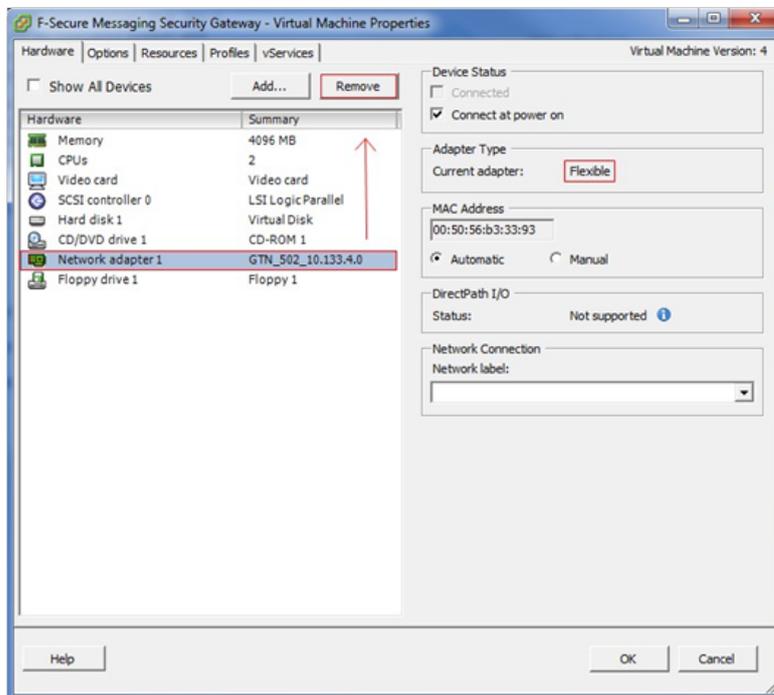
1. Verify the OVF files are available in a directory or URL that you can navigate to using the vSphere Client.
2. From the vSphere Client **File** menu, select **Deploy OVF Template**.
3. In the **Deploy OVF Template** pop-up window, browse to the directory where OVF file is located, and then click **Next**.
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:

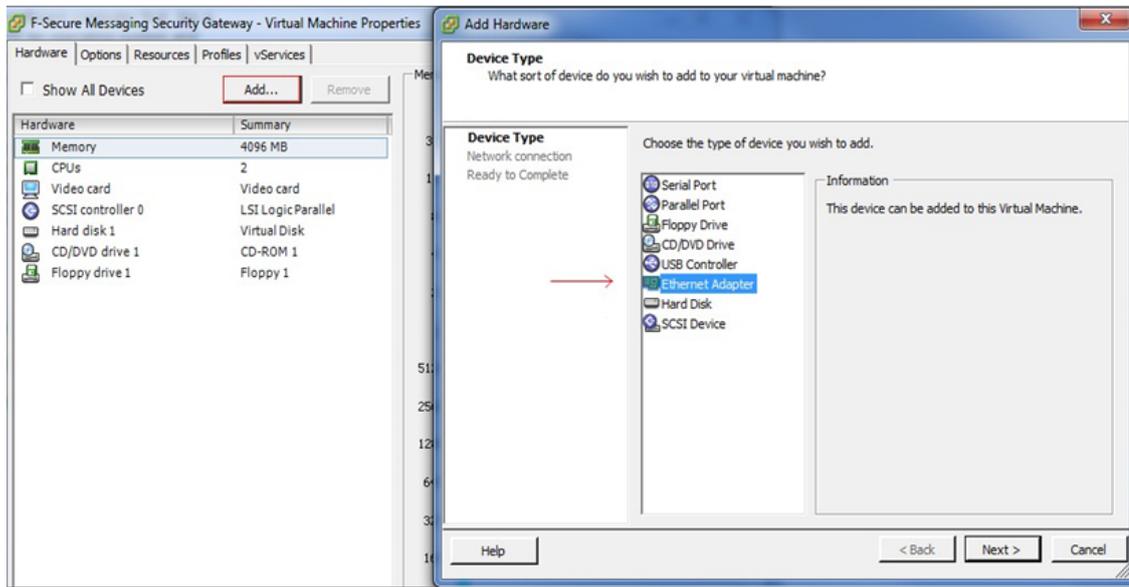


9. Remove the default flexible type adapter:



10. Add a new network adapter:

- a) Select adapter type E1000 and click **Next**.
- b) Confirm the settings.
- c) Click **Finish**.



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

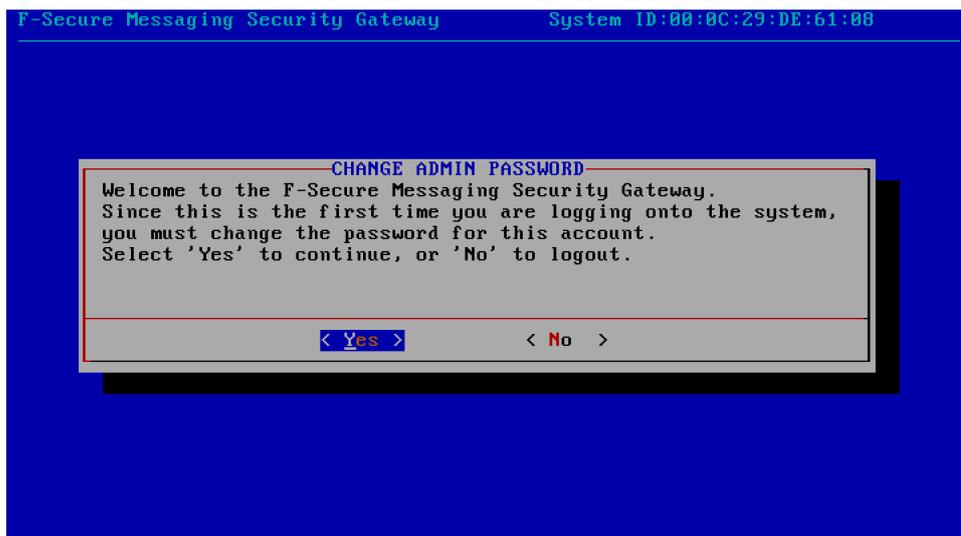
Follow these instructions to set up F-Secure Messaging Security Gateway with the console.

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

```
F-Secure Messaging Security Gateway 8.0.1.1446:8.0.1.1368 (00:0C:29:DE:61:08)
MessagingSecurityGateway login: admin
Password: _
```

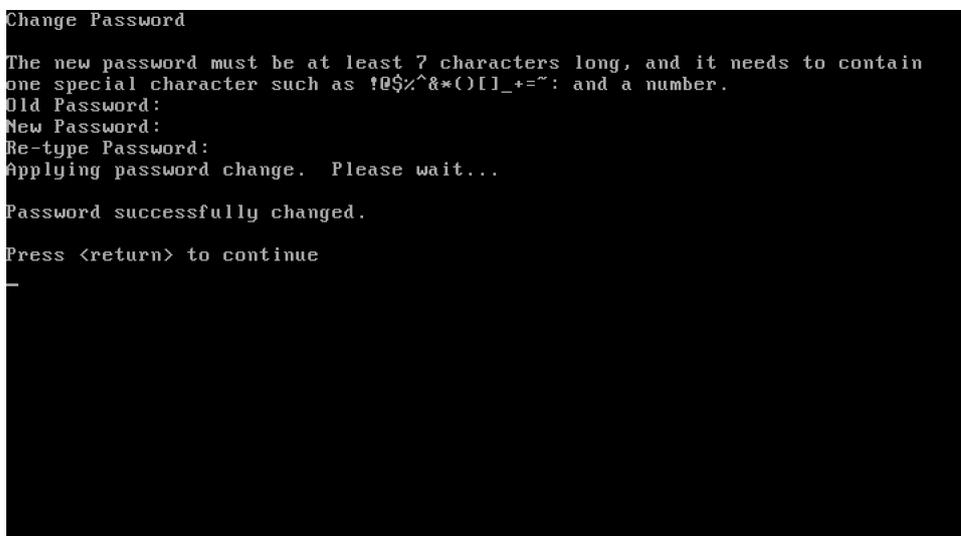
The welcome screen opens.

2. Select **Yes** to change the admin password.



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.



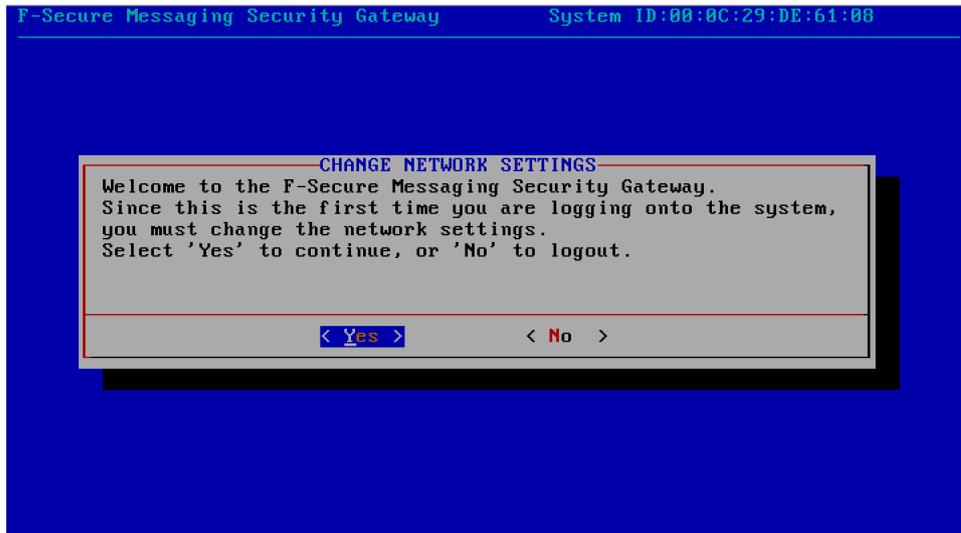
4. Press Enter.

Next, you need to change the network settings.

1.5 Changing the network settings

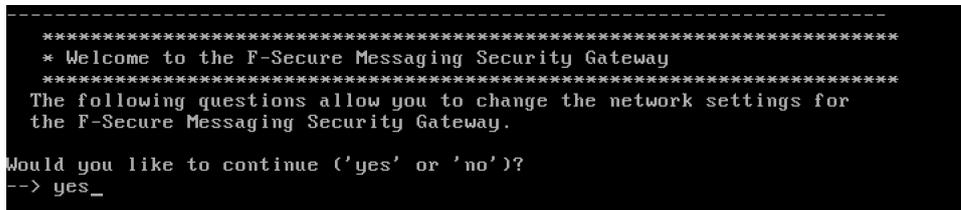
You need to change the network settings the first time you log in to the system.

1. Select **Yes** to change the network settings.

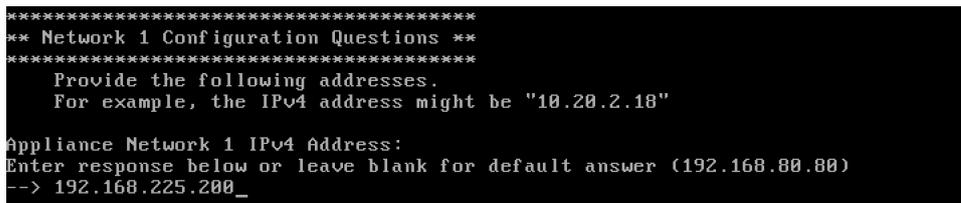


The network configuration wizard opens.

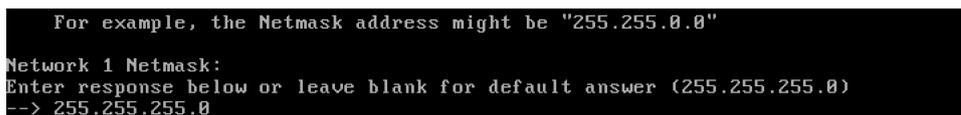
2. Enter `Yes` to continue.



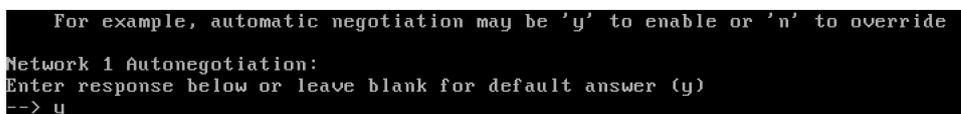
3. Enter the IP address of the appliance.



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.

```

    For example, the Default IPv4 Gateway address might be "10.20.0.1"
Default Gateway IPv4 Address:
Enter response below or leave blank for default answer (192.168.80.1)
--> 192.168.225.2_

```

7. Enter the host name of the appliance.

```

*****
** Group 2: Hostname and DNS Questions **
*****
Provide a name for the Hostname and Domain Name.
Provide IPv4 addresses for the DNS Servers.
The Hostname parameter should be the unqualified Hostname, for example
"appliance". Do not use a fully qualified Hostname, for example
"appliance.example.com".

Hostname:
--> fsmsg01_

```

8. Enter the domain name.

```

    The Domain name, for example would be something like "example.com".
Domain name:
--> yourdomainhere.com_

```

9. Enter the IP addresses of the DNS servers in use.

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

```

    A DNS Server translates a host or domain name into an IP Address.
    The Primary DNS Server is mandatory.

Primary DNS Server IPv4 Address:
Enter response below or leave blank for default answer (204.127.129.1)
--> 192.168.225.2
-----
    If no secondary DNS Server is available, press return.

Secondary DNS Server IPv4 Address:
--> 192.168.225.3
-----
    If no tertiary DNS Server is available, press return.

Tertiary DNS Server IPv4 Address:
--> _

```

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.

```

Hostname override (e.g. 192.168.1.1 host.example.com)
Hostname override:
--> 192.168.225.201 fsmsg02.yourdomainhere.com fsmsg02_

```

11. Enter Yes to confirm the network settings.

```

*****
** Confirm Your Responses **
*****
Please verify that the responses you have given are correct.

  1-Appliance Network 1 IPv4 Address: . . . . . 192.168.225.200
  2-Network 1 Netmask: . . . . . 255.255.255.0
  3-Network 1 Autonegotiation: . . . . . y
  4-Default Gateway IPv4 Address: . . . . . 192.168.225.2
  5-Hostname: . . . . . fsmsg01
  6-Domain name: . . . . . yourdomainhere.com
  7-Primary DNS Server IPv4 Address: . . . . . 192.168.225.2
  8-Secondary DNS Server IPv4 Address: . . . . . 192.168.225.3
  9-Tertiary DNS Server IPv4 Address: . . . . .
 10-Hostname override: . . . . . 192.168.225.201 fsmsg0
2.yourdomainhere.com fsmsg02

Confirm? (yes/no/quit)
-->

```

Your new settings are saved.

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

```

Your changes have been applied.
If this system is the Config Master, please point your web browser
to https://192.168.225.200:10000/ to continue setting up the appliance using the
web based management interface.
If this system is an agent, use the management interface on the Config Master
to add the agent to the cluster and complete its configuration.

Press <return> to continue

```

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.

```

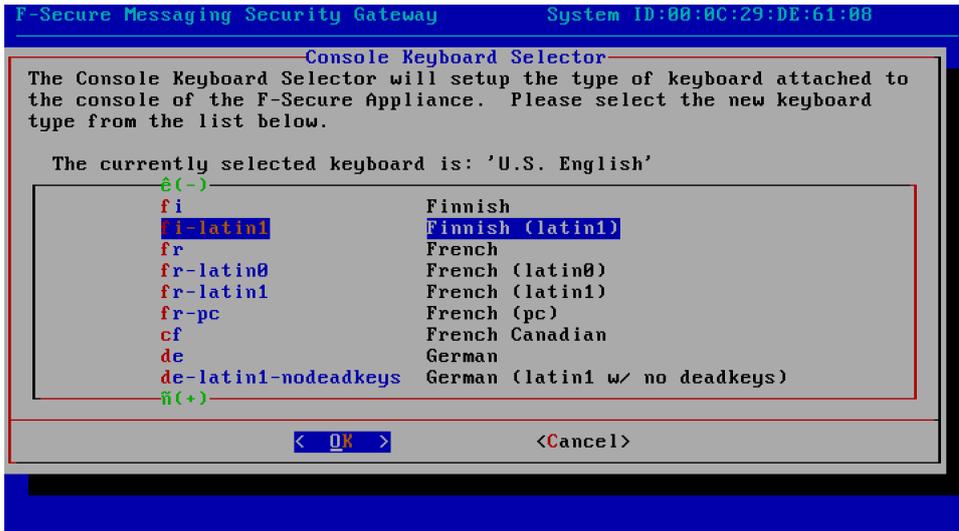
F-Secure Messaging Security Gateway      System ID:00:0C:29:DE:61:00
-----
MAIN MENU
Welcome to the F-Secure Messaging Security Gateway Menu
This menu contains the most often used items that the admin user
can run. Please select one of the items below.

  1 F-Secure Appliance Setup Assistant Guide
  2 Display F-Secure Appliance Network Settings
  3 Change Password
  4 Console Keyboard Selector
  5 Advanced System Control Operations...
  6 Logout of the F-Secure Appliance

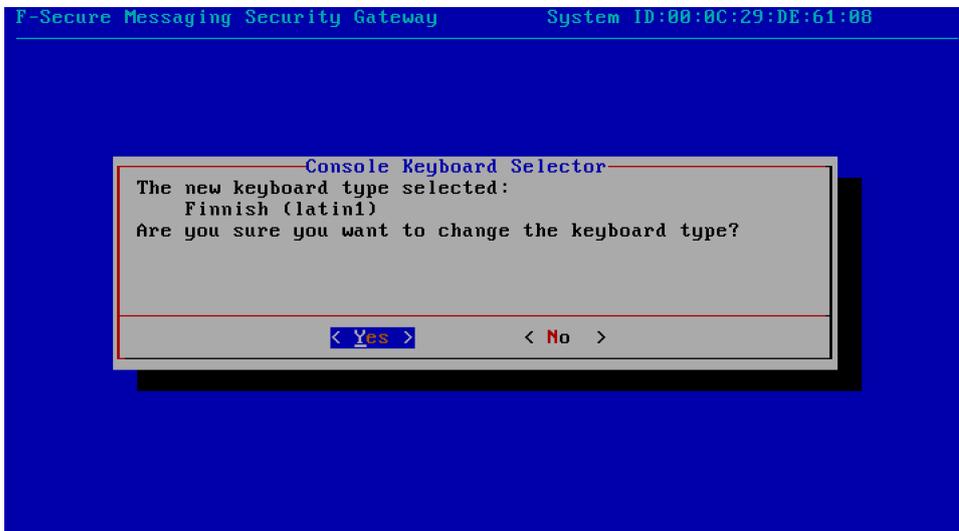
  < OK >

```

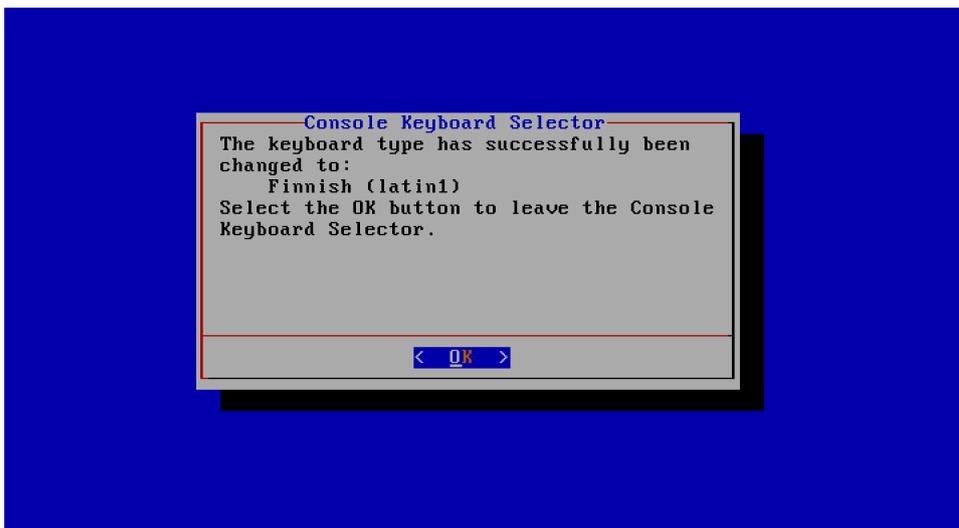
2. Select the preferred keyboard from the list and press ENTER.



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



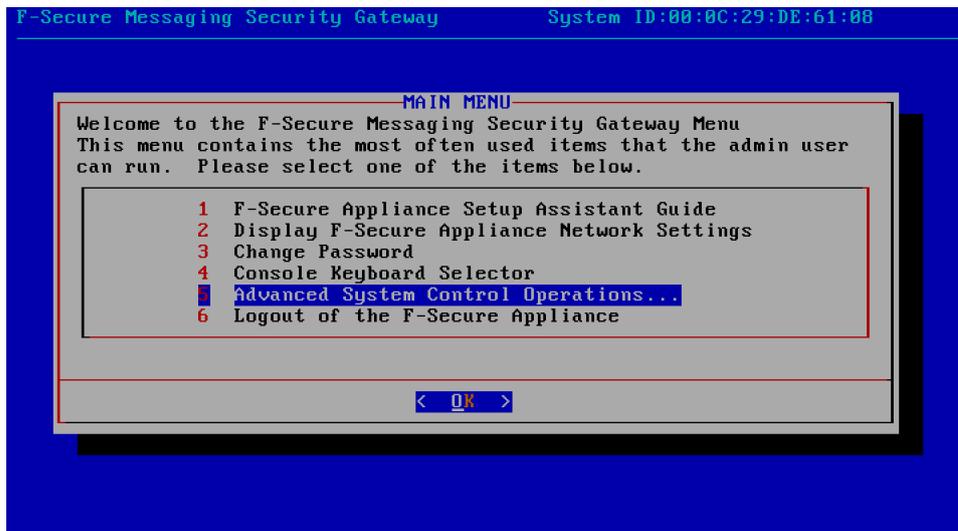
4. Press **ENTER** to return to the main menu.



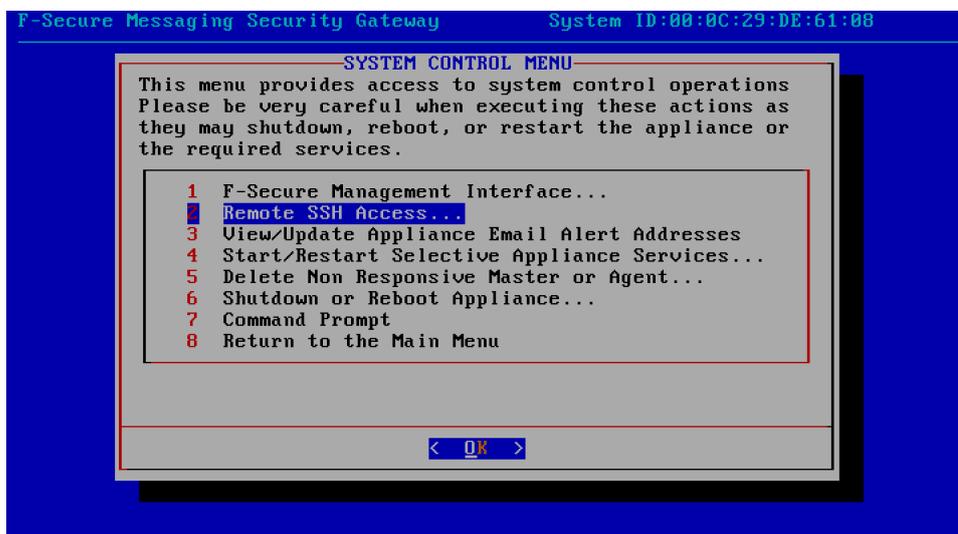
1.7 Allowing remote SSH access

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

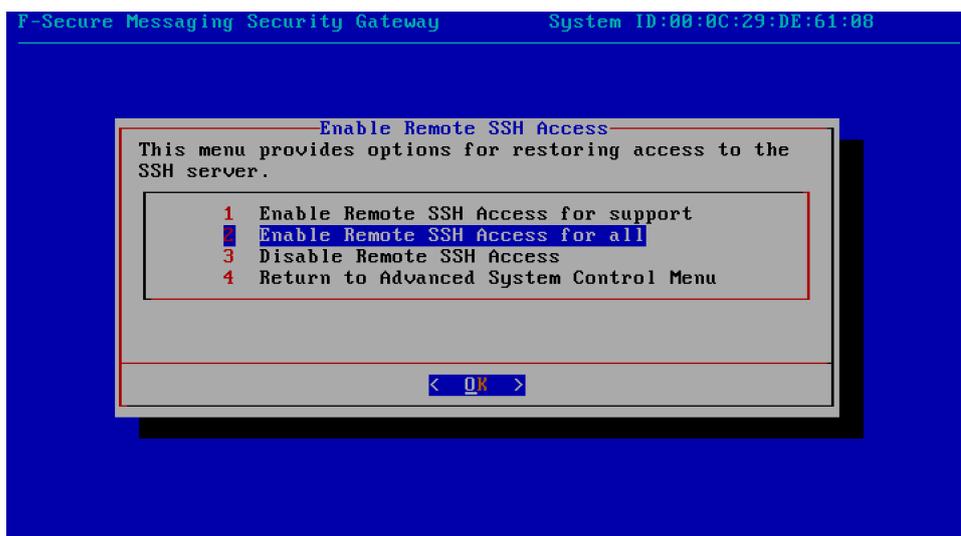
1. From the main menu, select **Advanced System Control Operations**.



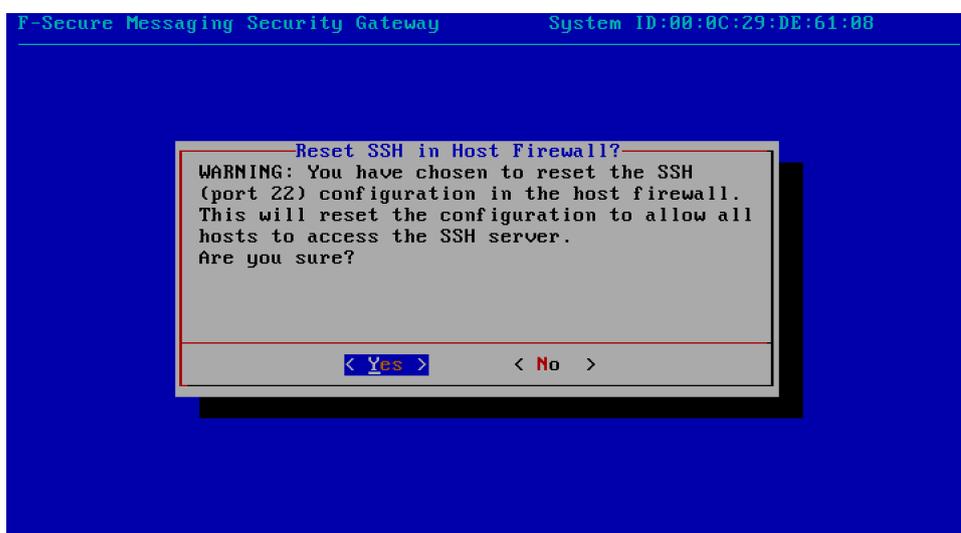
2. Select **Remote SSH Access**.



3. Select **Enable Remote SSH Access for all**.



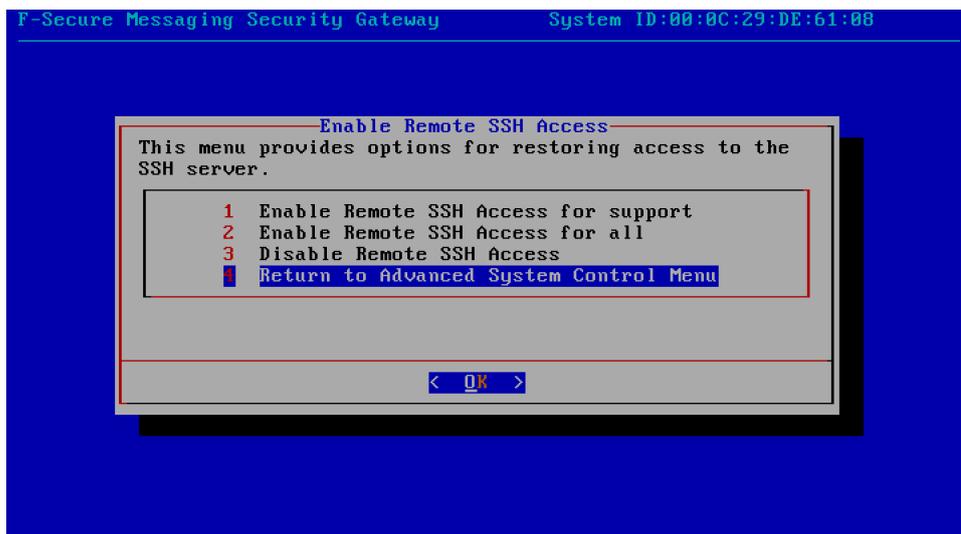
4. Select **Yes** to confirm that you want to allow the SSH access to the appliance.



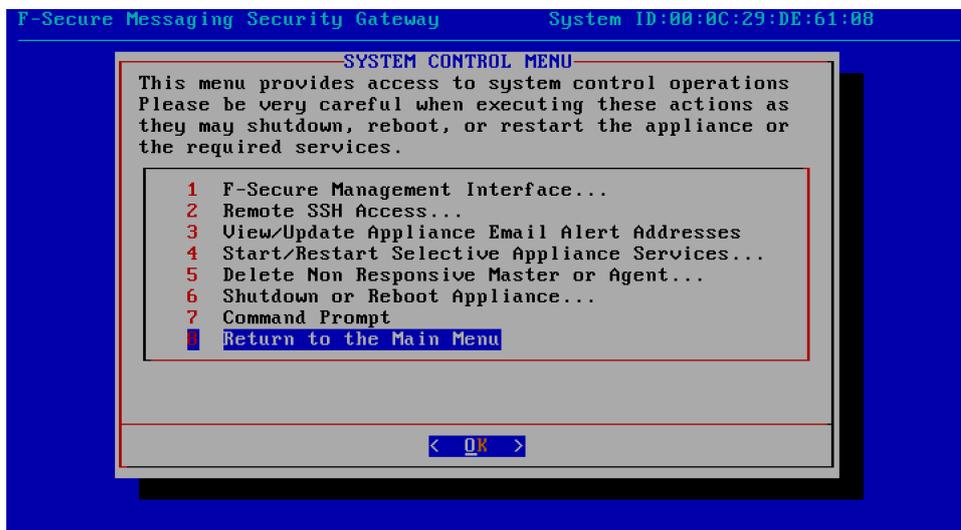
5. Press **ENTER** to return to the menu.



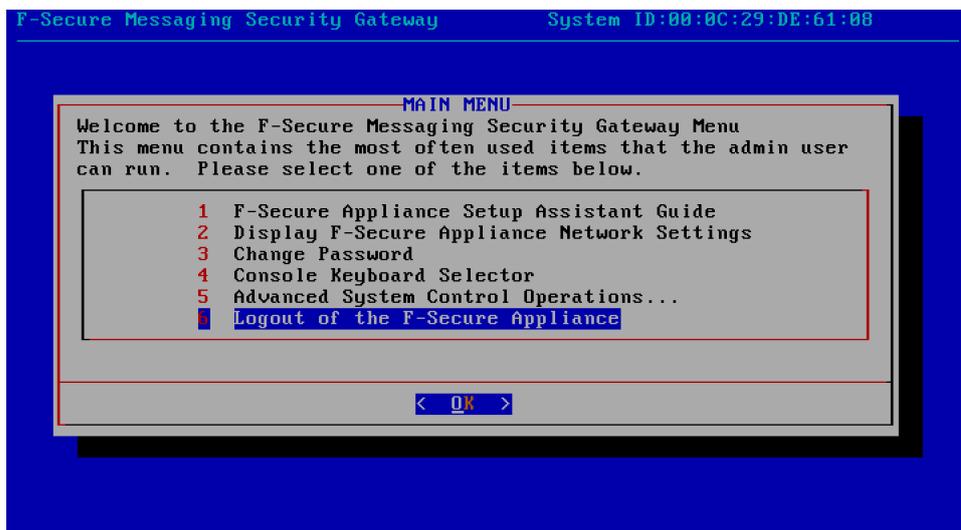
6. Select **Return to Advanced System Control Menu**.



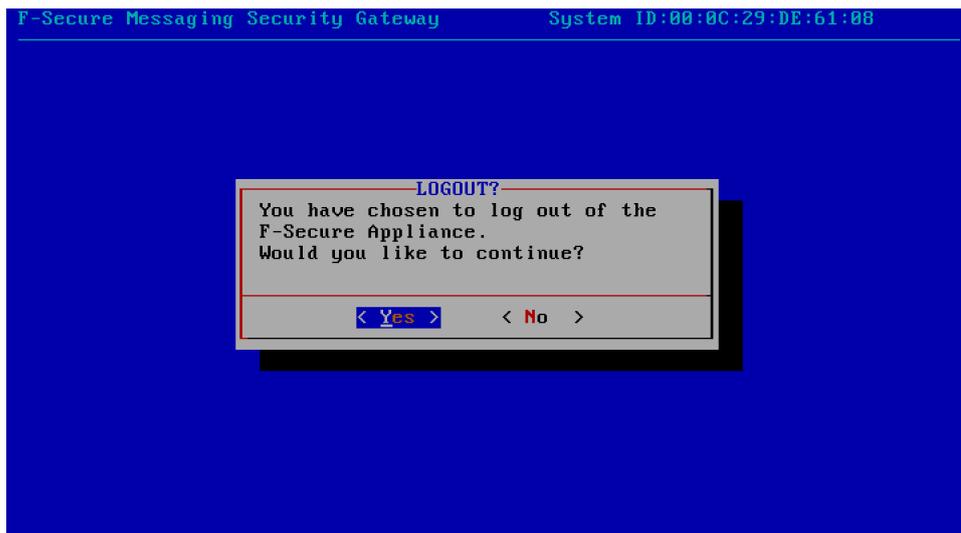
7. Select **Return to the Main Menu**.



8. Select **Logout of the F-Secure Appliance**.



9. Select **Yes** to log out.

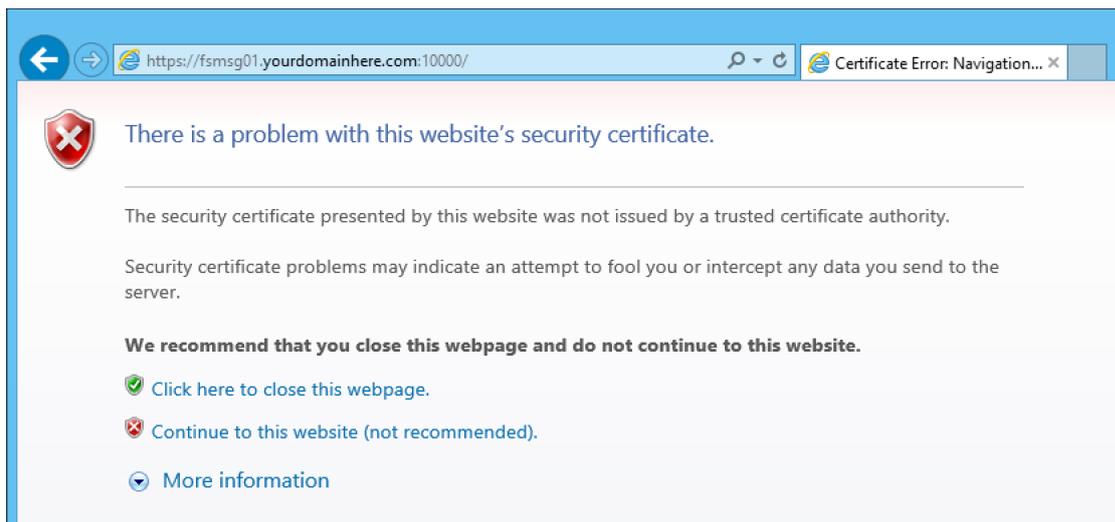


After you log out, open your browser and go to `https://[appliance_ip_address_or_dns_name]:10000` to continue setting up F-Secure Messaging Security Gateway with the web interface.

1.8 Completing the setup in the web interface

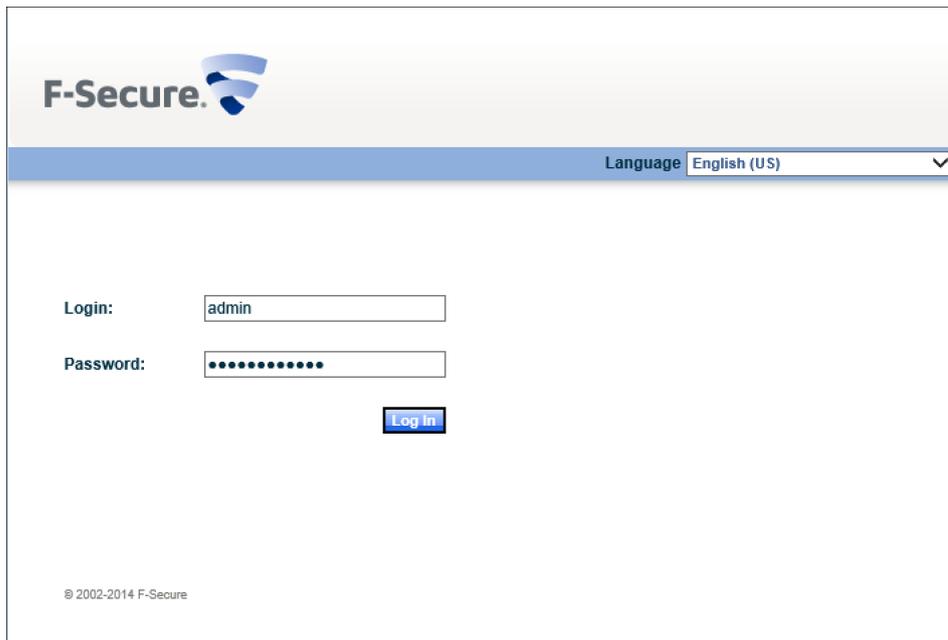
After you have completed the setup in the console, finish the setup with the web interface.

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



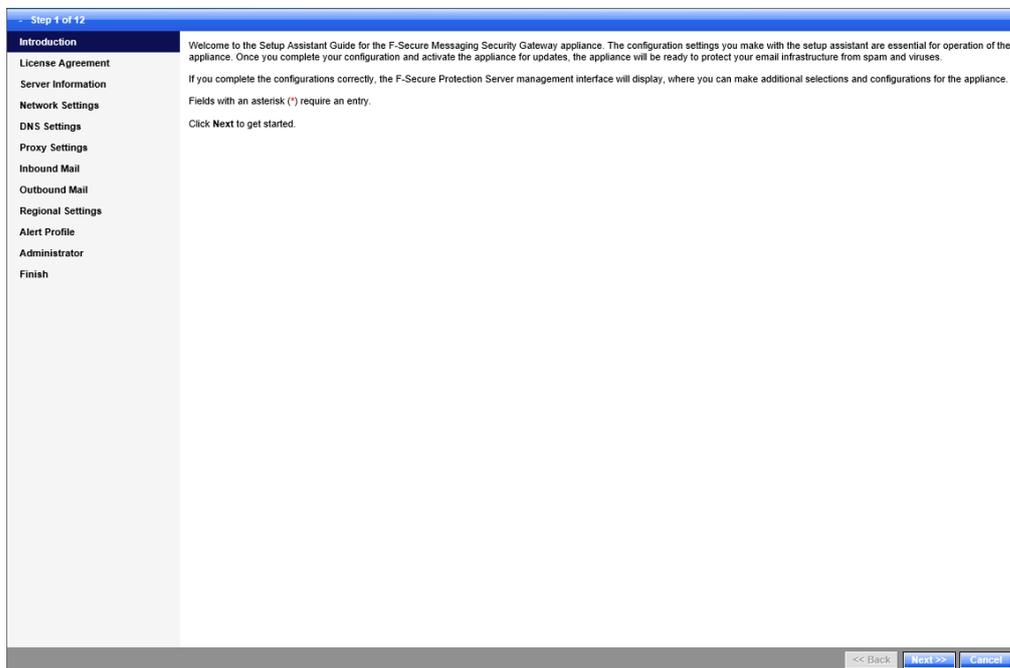
This is normal, so when you receive the certification warning message, continue to the website to complete the setup.

1. Log in to the web interface.



The image shows the F-Secure login interface. At the top left is the F-Secure logo. To the right, there is a language selection dropdown menu currently set to "English (US)". Below this, there are two input fields: "Login:" with the text "admin" entered, and "Password:" with a masked password of ten dots. A blue "Log in" button is positioned below the password field. At the bottom left, the copyright notice "© 2002-2014 F-Secure" is visible.

2. Read the introductory screen.



The image displays the introductory screen of the F-Secure Setup Assistant. The title bar indicates "Step 1 of 12". A left-hand navigation pane lists the following steps: Introduction, License Agreement, Server Information, Network Settings, DNS Settings, Proxy Settings, Inbound Mail, Outbound Mail, Regional Settings, Alert Profile, Administrator, and Finish. The main content area contains the following text:

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 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.

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.

Fields with an asterisk (*) require an entry.

Click Next to get started.

At the bottom right, there are three buttons: "<< Back", "Next >>", and "Cancel".

3. Read and accept the license agreement.

Step 2 of 12

Introduction

License Agreement

Server Information

Network Settings

DNS Settings

Proxy Settings

Inbound Mail

Outbound Mail

Regional Settings

Alert Profile

Administrator

Finish

F-Secure License Agreement

Print the License Agreement...

F-SECURE PURCHASE AND LICENSE AGREEMENT

PLEASE READ THIS F-SECURE PURCHASE AND LICENSE AGREEMENT ("AGREEMENT") CAREFULLY. F-SECURE IS WILLING TO SELL THE APPLIANCE AND LICENSE THE SOFTWARE TO YOU OR THE ENTITY OR COMPANY THAT YOU REPRESENT ("LICENSEE") ONLY UPON THE CONDITION THAT LICENSEE ACCEPTS ALL THE TERMS CONTAINED IN THIS AGREEMENT. BY CLICKING ON THE "ACCEPT" BUTTON BELOW OR BY INSTALLING OR USING THE APPLIANCE THAT CONTAINS THE SOFTWARE, LICENSEE ACKNOWLEDGES AND AGREES THAT IT HAS READ AND UNDERSTANDS THIS AGREEMENT AND AGREES (I) TO BE BOUND BY ALL OF ITS TERMS; AND (II) THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN CONTRACT SIGNED BY LICENSEE. IF A WRITTEN AGREEMENT EXISTS BETWEEN AND HAS BEEN EXECUTED BY BOTH LICENSEE AND F-SECURE, THE TERMS OF THAT WRITTEN AGREEMENT SHALL TAKE PRECEDENCE OVER THIS AGREEMENT, AND LICENSEE ACKNOWLEDGES THAT IT IS BOUND BY THE TERMS OF THAT WRITTEN AGREEMENT. LICENSEE'S CONTINUED USE OF THE APPLIANCE AND SOFTWARE SHALL ALSO CONSTITUTE ASSENT TO THE TERMS OF THIS AGREEMENT OR OF AN EXISTING WRITTEN AGREEMENT. IF LICENSEE DOES NOT ACCEPT ALL THE TERMS OF THIS AGREEMENT, THEN: (A) F-SECURE IS UNWILLING TO LICENSE SELL THE APPLIANCE AND LICENSE THE SOFTWARE TO LICENSEE; (B) LICENSEE WILL NOT INSTALL OR ATTEMPT TO USE THE APPLIANCE THAT CONTAINS THE SOFTWARE; AND (C) LICENSEE MAY RETURN THE APPLIANCE ON WHICH THE SOFTWARE WOULD OTHERWISE BE INSTALLED FOR A FULL REFUND. LICENSEE'S RIGHT TO RETURN AND REFUND EXPIRES 30 DAYS AFTER PURCHASE FROM F-SECURE.

1. DEFINITIONS.

"Affiliate" means any company controlled by, controlling or under common control with Licensee. 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 or other interests, by contract.

"Appliance(s)" means the hardware appliance(s) containing the Software purchased by Licensee.

"Confidential Information" means the Appliance, Documentation, Software, access codes to F-Secure's support sites, and all information which, in accordance with Section 11 below, is marked as confidential or proprietary or is disclosed verbally and identified as confidential or proprietary at the time of disclosure, or which by its nature is normally and reasonably considered confidential.

"Documentation" means the user manuals relating to the use of the Appliance and Software either provided on-line or delivered with the Software.

"Effective Date" is the date Licensee signs the applicable Product Order Form.

"Extension Term" means each additional renewal period, which shall be for a period equal to the Initial Term, for which the Agreement is extended pursuant to Section 16.

"Initial Term" means the initial license term specified on the Product Order Form, commencing on the Effective Date.

"Mailbox" means a separate account on Licensee's e-mail server for sending or receiving messages or data within Licensee's e-mail system or network. Aliases and distribution lists shall not be counted as separate mailboxes provided each person who has access to such aliases and distribution lists has a separate account on Licensee's email server for the receipt of messages or data within Licensee's e-mail system or network.

"Product Order Form" means F-Secure's standard Product Order Form or other ordering document (e.g. Licensee's Purchase Order) that specifies the Appliances, Software licenses and other products or services purchased by Licensee.

"Public Software" means any software that contains, or is derived (in whole or in part) from, any software that is distributed as free software, open source software or similar licensing or distribution models. Software does not include Public Software.

"Software" means a machine executable copy of the object code of the proprietary software products owned or distributed by F-Secure and licensed by F-Secure to Licensee under this Agreement.

"Service Updates" means generally available rule updates that F-Secure make available for each Software module licensed by Licensee under this Agreement.

"Services" means installation or other consulting services provided hereunder by F-Secure to Licensee.

"Software Updates" means all updates and enhancements that F-Secure generally makes available to its customers for each Software module licensed by Licensee under this Agreement.

"Subscription Fees" mean the fees paid by Licensee for the right to use the Software and receive Service Updates and Support during the applicable Term.

"Support" means the support services provided by F-Secure in accordance with F-Secure's support policies and procedures for small and medium enterprise customers then in effect.

"Term" means the Initial Term and any Extension Term.

"Work Product" means all work (including any tools, materials, derivative works and modifications made to the Software or Documentation) used, developed or created by F-Secure for Licensees during the course of provision of Services and Support services, provided to Licensee by F-Secure under this Agreement.

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

License Agreement

Server Information

Network Settings

DNS Settings

Proxy Settings

Inbound Mail

Outbound Mail

Regional Settings

Alert Profile

Administrator

Finish

Enter the hostname of the appliance, and a fully qualified domain name.

Select the appliance type. If you select **Master**, you need to enter your F-Secure Activation ID.

Server Identity

* Hostname

* Domain Name

Activation Information

* Appliance Type Master Agent

* F-Secure Activation ID

<< Back Next >> Cancel

5. Check the network settings.

Step 4 of 12

Introduction
License Agreement
Server Information
Network Settings
DNS Settings
Proxy Settings
Inbound Mail
Outbound Mail
Regional Settings
Alert Profile
Administrator
Finish

Enter the IP addresses you want to assign to the network interfaces and the accompanying netmask addresses.

Network Interface

Network Interface 1

• IPv4 Address:

• Netmask:

MAC Address: 00:0C:29:DE:61:08

IPv4 Network Gateway

• Default IPv4 Gateway:

<< Back Next >> Cancel

6. Check the DNS settings.

Step 5 of 12

Introduction
License Agreement
Server Information
Network Settings
DNS Settings
Proxy Settings
Inbound Mail
Outbound Mail
Regional Settings
Alert Profile
Administrator
Finish

Enter an IP address for the Primary Name Server.

DNS Settings

• Primary Name Server:

Secondary Name Server:

Tertiary Name Server:

Hostname Override: (ie: 192.168.1.1 host.example.com)

<< Back 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
License Agreement
Server Information
Network Settings
DNS Settings
Proxy Settings
Inbound Mail
Outbound Mail
Regional Settings
Alert Profile
Administrator
Finish

If you have configured all HTTPS communication 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. The appliance, by default, is not configured to use a proxy server.

Proxy Settings

HTTPS Proxy

Do Not Use Proxy (Direct connection to the Internet)
 Use Proxy

<< Back Next >> Cancel

8. Enter the settings for inbound mail.

Step 7 of 12

Introduction
License Agreement
Server Information
Network Settings
DNS Settings
Proxy Settings
Inbound Mail
Outbound Mail
Regional Settings
Alert Profile
Administrator
Finish

Determine how you want to route your inbound mail. Click **Add** and enter the appropriate information in the table below.

For example, you would enter *example.com* for **Mail for Host / Domain** and *mailserver.example.com* for **Route to Host(s) / Domain(s)**.

Click **Next** after you complete your entries.

Inbound Mail

	* Mail for Host / Domain	Mailer	Route to Host(s) / Domain(s)	Lookup By	Delivery Type
<input type="checkbox"/>	<input type="text" value="yourdomainhere.com"/>	ESMTP	192.168.225.100	<input checked="" type="radio"/> A record only <input type="radio"/> MX and A records	<input checked="" type="radio"/> Ordered <input type="radio"/> Load Balanced

<< Back 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
License Agreement
Server Information
Network Settings
DNS Settings
Proxy Settings
Inbound Mail
Outbound Mail
Regional Settings
Alert Profile
Administrator
Finish

Determine how you want to route your outbound mail. Enter the appropriate information in the text field below, and click the right-arrow (>>) button.
For example, you would enter 10.20 for **Allow Relay** from IP addresses starting with 10.20.0.0.
Click **Next** after you complete your entries.

Allow Relay

Domain, Hostname or IP Address >>
<<

Domain, Hostname or IP Address List
192.168.225.100

<< Back Next >> 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
License Agreement
Server Information
Network Settings
DNS Settings
Proxy Settings
Inbound Mail
Outbound Mail
Regional Settings
Alert Profile
Administrator
Finish

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 using them right away. Select a language for the default settings.
Select your time zone preference.

Default Language

 You will not be able to change the language for the default settings later, using the management interface (administrative interface). If you do not select a language now, the default settings will appear in English.

Language

Date/Time

Time Zone

Current Time 2015-08-07 08:19:29 [UTC+3:00]

<< Back Next >> Cancel

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

Step 10 of 12

Introduction
License Agreement
Server Information
Network Settings
DNS Settings
Proxy Settings
Inbound Mail
Outbound Mail
Regional Settings
Alert Profile
Administrator
Finish

Enter the hostname of the alert email server.

Alert Profile

* Hostname

* Port

From Address

HELO Domain

Login

Password

Retype Password

<< Back Next >> Cancel

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

Step 11 of 12

Introduction
License Agreement
Server Information
Network Settings
DNS Settings
Proxy Settings
Inbound Mail
Outbound Mail
Regional Settings
Alert Profile
Administrator
Finish

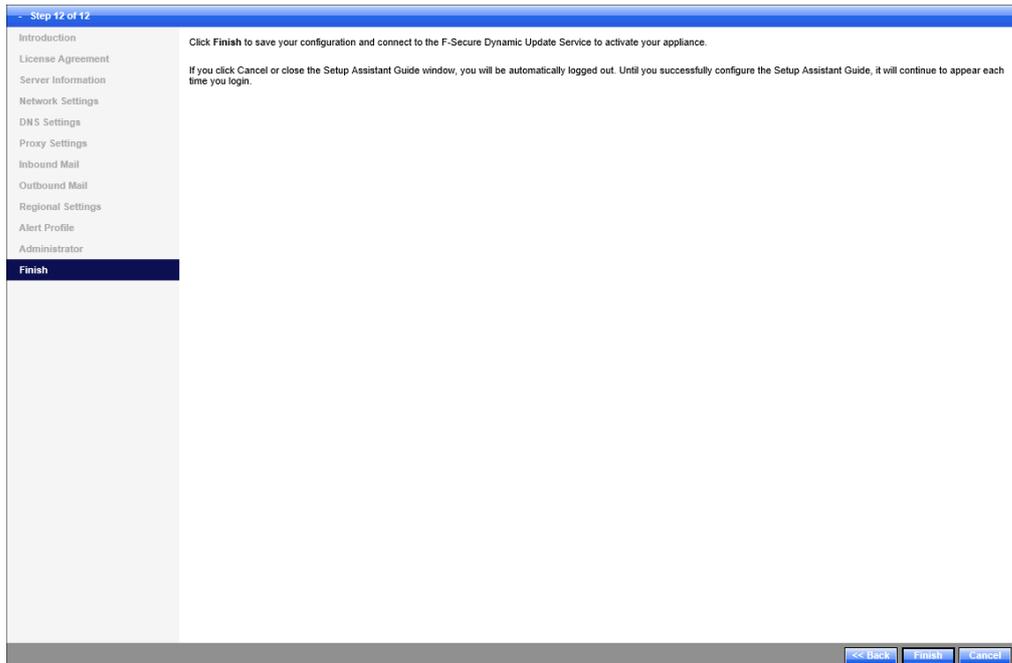
Enter an email address for receiving alert email.

Alert Email

* System Alerts Email Address

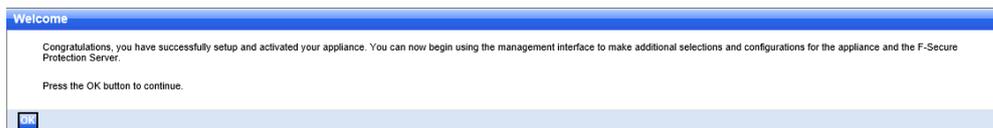
<< Back Next >> Cancel

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



Note: The Messaging Security Gateway server needs to access the Internet. If the server cannot access the Internet, the registration will not succeed.

14. Click **OK** to continue.



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

Updating to the latest recommended settings

Topics:

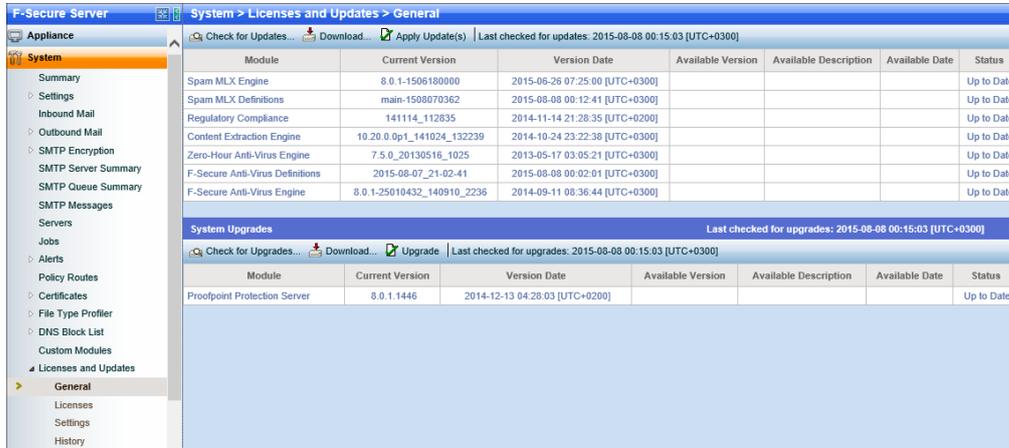
- [Importing settings](#)
- [Configuring the environment settings](#)

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

2.1 Importing settings

Follow these instructions to import the configuration.

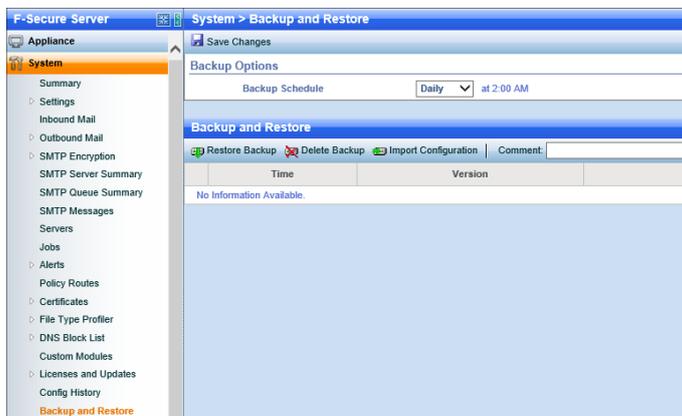
1. Go to **System > Licenses and Updates > General** and make sure that all patches are installed. The status should be *Up to date* in all lines.



Module	Current Version	Version Date	Available Version	Available Description	Available Date	Status
Spam MLX Engine	8.0.1-1506180000	2015-06-26 07:25:00 [UTC+0300]				Up to Date
Spam MLX Definitions	main-1508070362	2015-08-08 00:12:41 [UTC+0300]				Up to Date
Regulatory Compliance	141114_112835	2014-11-14 21:28:35 [UTC+0200]				Up to Date
Content Extraction Engine	10.20.0.op1_141024_132239	2014-10-24 23:22:38 [UTC+0300]				Up to Date
Zero-Hour Anti-Virus Engine	7.5.0_20130516_1025	2013-05-17 03:05:21 [UTC+0300]				Up to Date
F-Secure Anti-Virus Definitions	2015-08-07_21-02-41	2015-08-08 00:02:01 [UTC+0300]				Up to Date
F-Secure Anti-Virus Engine	8.0.1-25010432_140910_2236	2014-09-11 08:36:44 [UTC+0300]				Up to Date

Module	Current Version	Version Date	Available Version	Available Description	Available Date	Status
Proofpoint Protection Server	8.0.1.1446	2014-12-13 04:28:03 [UTC+0200]				Up to Date

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.



Backup Options

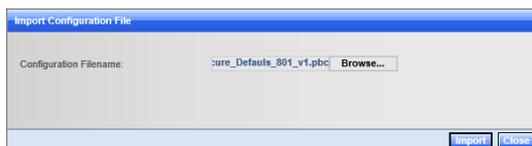
Backup Schedule: at 2:00 AM

Backup and Restore

Restore Backup Delete Backup Import Configuration Comment:

Time	Version
No Information Available.	

3. Browse to your downloaded backup file.



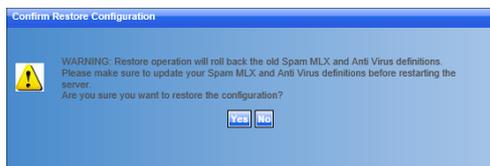
Import Configuration File

Configuration Filename:

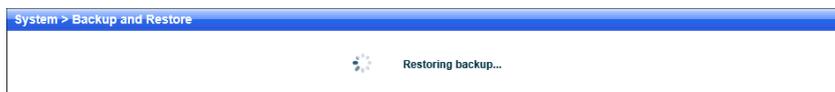
4. Select the imported backup file and click **Restore backup**.



5. Click **Yes**.



6. Wait while the backup is restored.



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



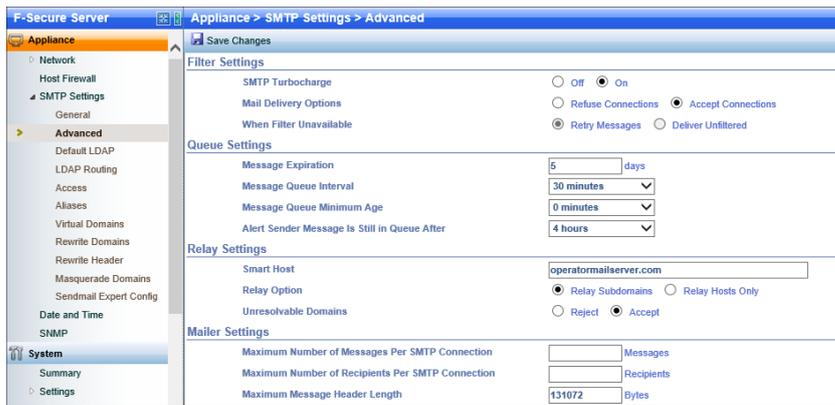
2.2 Configuring the environment settings

Configure your environment settings.

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

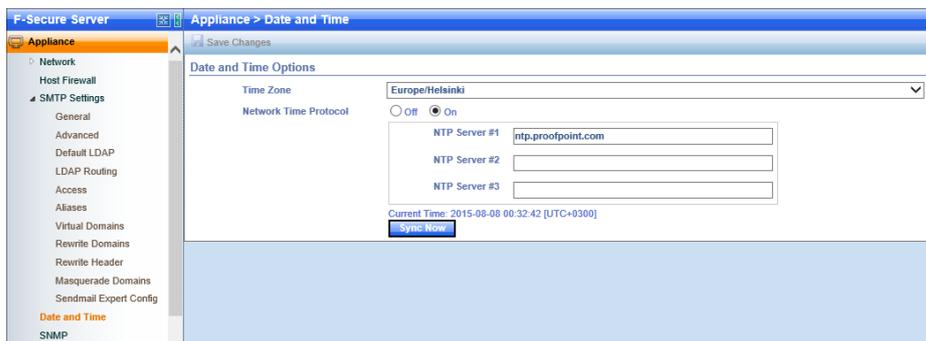


2. If you use an external email relay for outbound emails, for example an ISP, go to **Appliance > SMTP Settings > Advanced** and click **Add Smart host**.

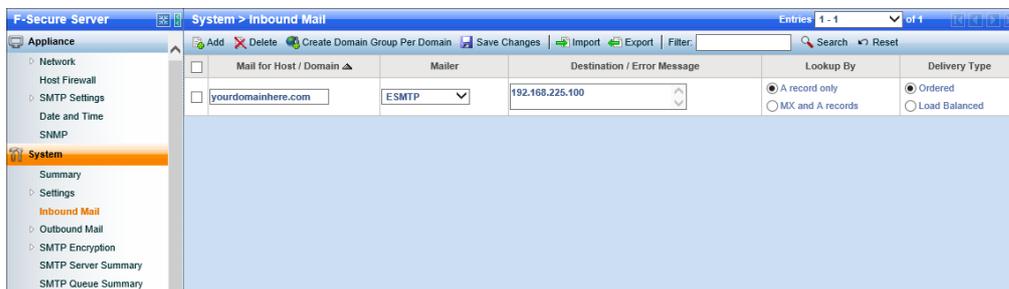


3. Go to **Appliance > Date and Time** to add NTP server if want keep date and time updated automatically.

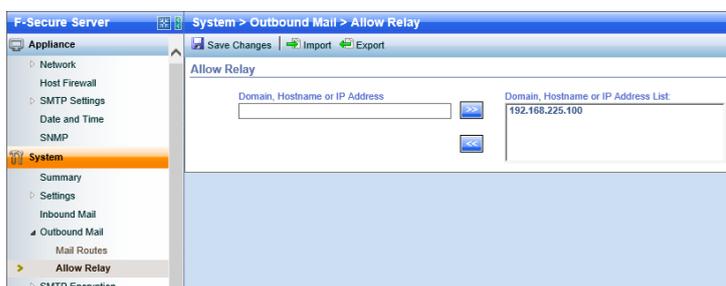
 **Tip:** Use `ntp.proofpoint.com` if you do not have an ntp server that you use already.



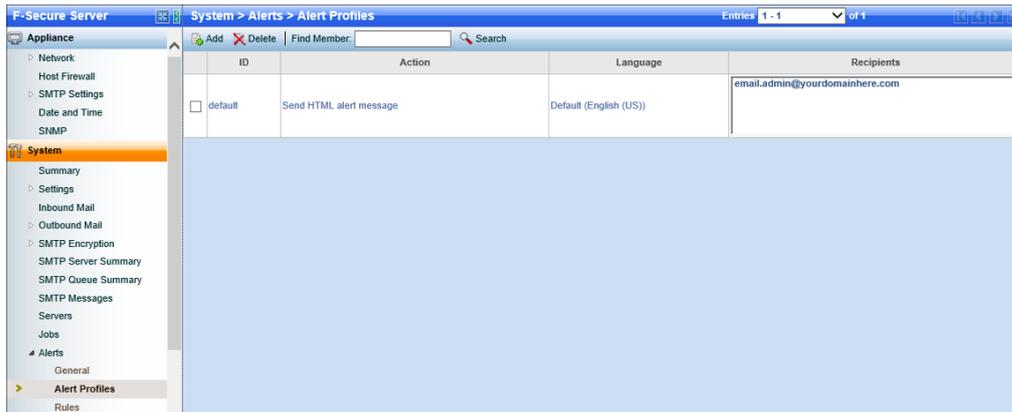
4. Go to **System > Inbound mail** and enter the domains that you are use to receive emails, and email servers where filtered emails are routed.



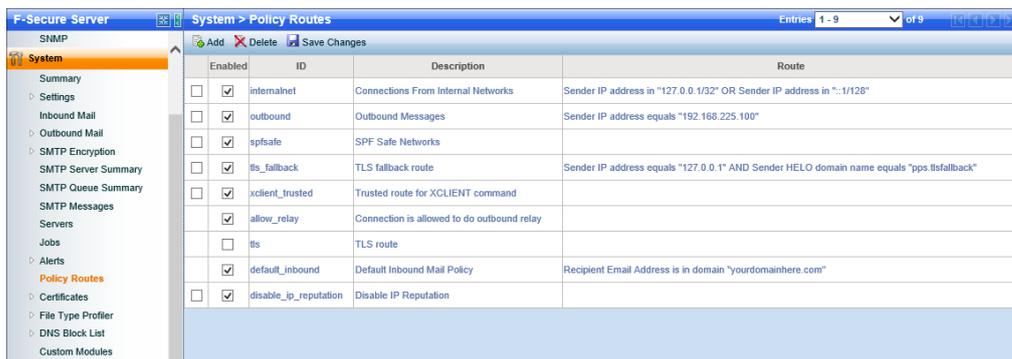
5. Go to **System > Outbound Mail > Allow Relay** to add all servers that have rights to send outbound emails to the Internet. Normally, this is your email server address.



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

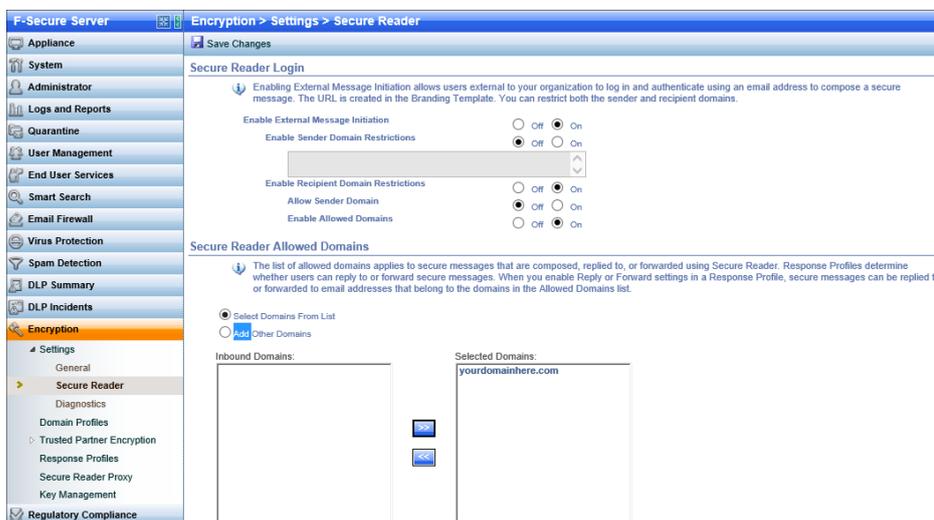


7. Go to **System > Policy Routes** to add all those IP addresses that you added to **System > Outbound Mail > Allow Relay** to the outbound policy route.



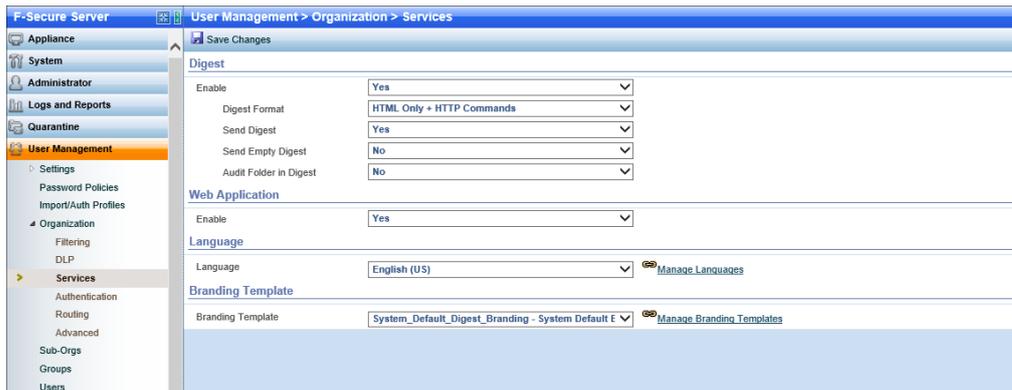
8. If you have a *Protection Bundle* license and you use email encryption, change following settings:

- Go to **Encryption > Settings > Secure Reader**.
- Turn on **Enable External Message Initiation**.
- Turn on **Enable Recipient Domain Restrictions**.
- Turn on **Enable Allowed Domains**.
- Move your inbound domains to Selected domains list.

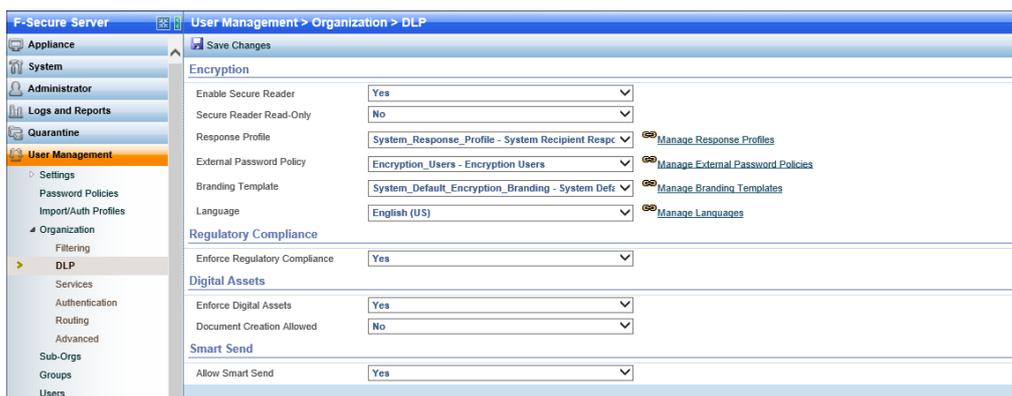


9. Choose the language that you want to use in email encryption (DLP) and Digest.

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

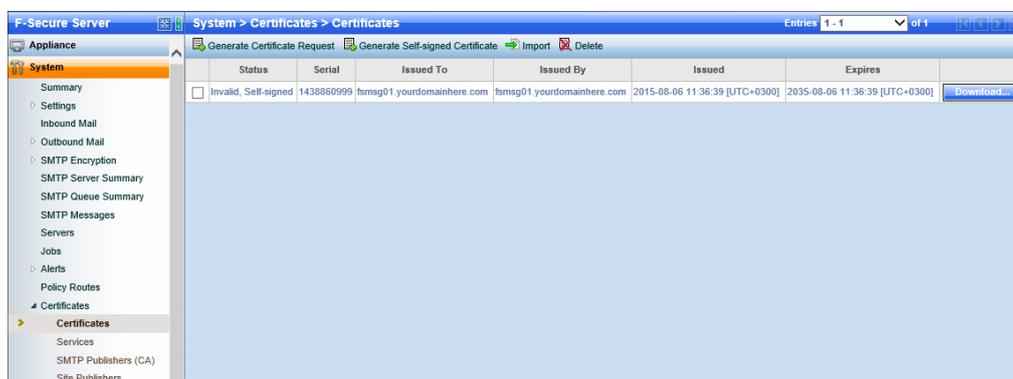


Encryption: Go to **User Management > Organization > DLP** and choose the language.

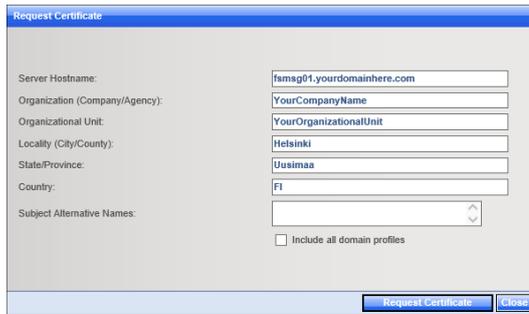


10. Admin and all end user connections are encrypted with HTTPS. We recommend that you use a signed SSL certificate and that you use wildcard or SAN certificates, because you need to use the same SSL certificate with multiple services (admin, enduser services, and encryption).

a) If you need to create a certificate request, go to **System > Certificates > Certificates** and click **Generate Certificate Request**.



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



Request Certificate dialog box with the following fields:

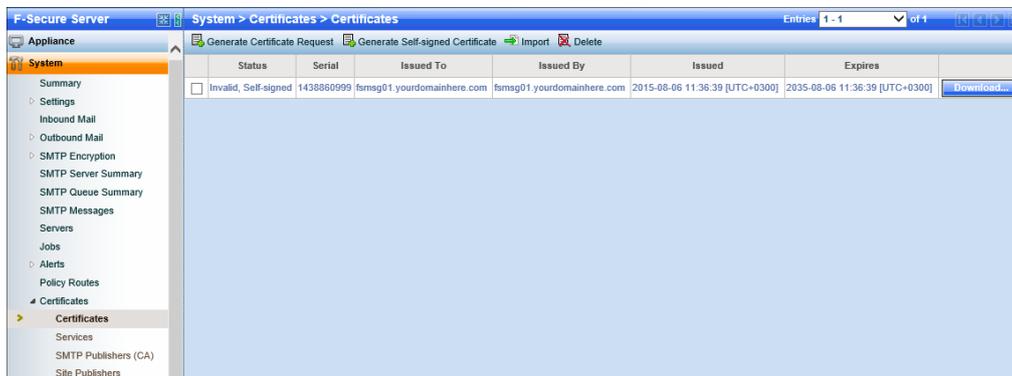
- Server Hostname: fsmag01.yourdomainhere.com
- Organization (Company/Agency): YourCompanyName
- Organizational Unit: YourOrganizationalUnit
- Locality (City/County): Helsinki
- State/Province: Uusimaa
- Country: FI
- Subject Alternative Names: (empty)
- Include all domain profiles

Buttons: Request Certificate, Close

- 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-Secure Server System > Certificates > Certificates

Status	Serial	Issued To	Issued By	Issued	Expires	
Invalid, Self-signed	1438860999	fsmag01.yourdomainhere.com	fsmag01.yourdomainhere.com	2015-08-06 11:36:39 [UTC+0300]	2035-08-06 11:36:39 [UTC+0300]	Download...

Buttons: Generate Certificate Request, Generate Self-signed Certificate, Import, Delete

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



Import Certificate dialog box with the following fields:

- Certificate File: |rator\Desktop|bundlecert| Browse...
- Format: PEM
- Password: (masked with asterisks)

Buttons: Import, Close

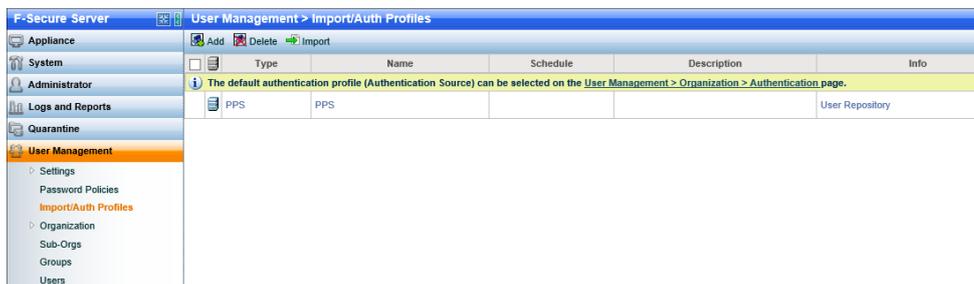
- f) Go to **System > Certificates > Services** to change your certificate to all services. Click **Save** to confirm the new settings.



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**.



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.

The screenshot shows the 'Advanced' tab of a configuration window. The 'Settings' section includes the following fields:

- Enable: Off On
- Data Source: LDAP/Microsoft Exchange/Active Directory/Lotus Domino
- Profile Name: Ad_Import
- Description: Connection to yourdomain.com Active Directory Server
- Host/Port Address: 192.168.225.50
- Advanced LDAP Options <<
- Base DN: dc=yourdomainhere.com,DC=com (Example: ou=users,dc=acme,dc=com)
- Bind DN: fsecure_user@yourdomainhere.com
- Password: [Redacted]
- Port: 389
- Authentication Attribute: mail
- Secure Socket Layer (SSL): Off On
- LDAP Version: v3
- Certificate File: -none-
- Simple Authentication And Security Layer (SASL): -none-
- Default Domain Name: [Empty]

The 'Verify' section includes:

- Username: [Empty]
- Password: [Empty]
- Buttons: Verify, Info

Buttons at the bottom: 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

The screenshot shows the 'Advanced' tab of a configuration window. The 'Options' section includes the following fields:

- Fallback Authentication: Off On
- Force Authentication Profile for Mobile Secure Reader or external IP Request: Off On
- Force Authentication: Off On
- Allow Login With Alias: Off On
- Create User After Authentication: Off On
- Send Welcome Message: Off On
- Authentication Profile: PPS
- Allow to Login Without Password: Off On
- Use Primary Email Address to Authenticate: Off On
- Set Temporary Password: Off On

The 'Import Settings' section includes the following fields:

- Filter: (mail=*) (Example: (mail=*))
- Insert Mode: insert all entries
- Add to Group/Sub-Org With Profile Name (Ad_Import): Off On Type: Group
- Remove User Profiles Not Imported: Off On Restrict Number Of Profiles To Be Deleted To Less Than: 50
- Allow Mailing Lists without Owner: Off On
- Map UID to Attribute: objectGUID
- Replace Mode: replace all aliases for existing users
- Update Mode: update all user data
- Object Type: auto based on objectClass
- Group Attribute: memberOf
- Command Options: [Empty]

Buttons at the bottom: Save Changes, Cancel.

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

Type	Name	Schedule	Description	Info
Ldap	Ad_Import	Schedule...	Connection to yourdomain.com Active Directo	Ldap://192.168.225.50/dc=yourdomainhere.co
PPS	PPS			User Repository

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

Profile: Ad_Import

Type: Time Interval

Time: 07:00

Import Times: 07:00

Days: Every Day

[Save Changes](#) [Cancel](#)

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.

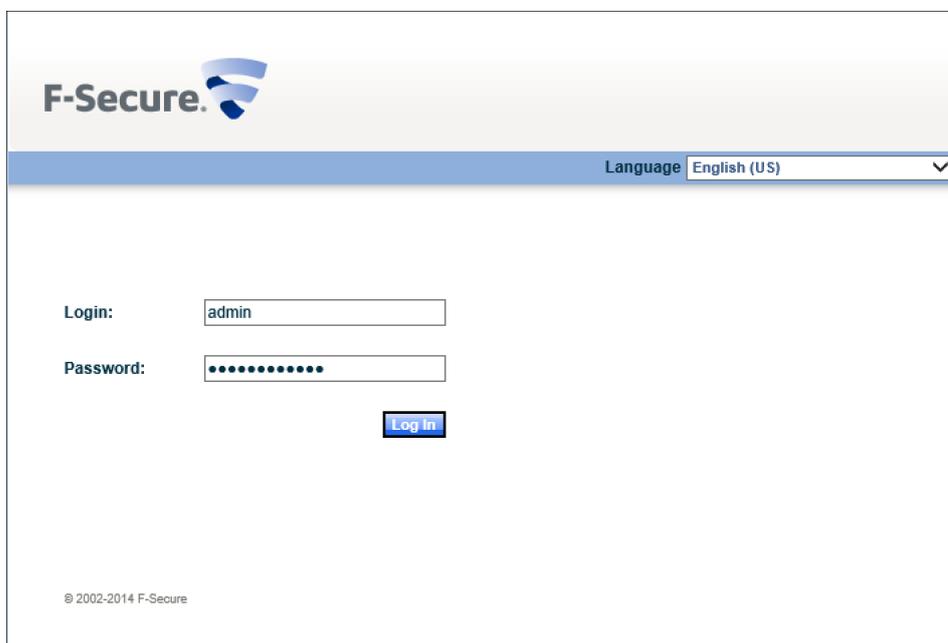
A.1 Adding a new agent to the cluster

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.

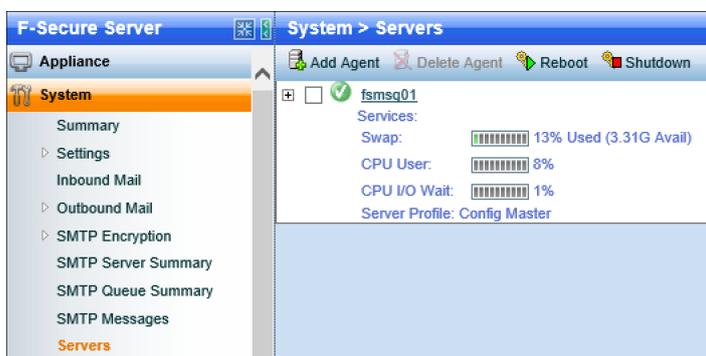
1. Log in to the web interface of the master appliance.

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.



The screenshot shows the F-Secure web interface login page. At the top left is the F-Secure logo. To the right, there is a language dropdown menu set to "English (US)". Below this, there are two input fields: "Login:" with the text "admin" and "Password:" with a masked password of ten dots. A blue "Log in" button is positioned below the password field. At the bottom left, the copyright notice "© 2002-2014 F-Secure" is visible.

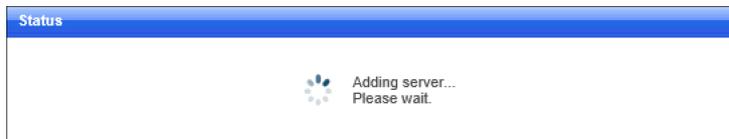
2. Go to **System > Servers** and click **Add Agent**.



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

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

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



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.

Agent Name	Services	Swap	CPU User	CPU I/O Wait	Server Profile	PPS Version	PPS Disk	CPU Nice	CPU Busy	Last Update	System ID	System Disk	CPU System	Uptime
fsmg01	Config Master	12% Used (3.35G Avail)	8%	1%	Config Master	8.0.1.1446	7% Used (70.7G Avail)	5%	17%	2015-08-07 10:30:48 [UTC+0300]	00:0C:29:DE:61:08	8% Used (10.28G Avail)	4%	0 day(s), 1:11, load average: 0.29, 0.52, 0.43
fsmg02	Mail Filter	0% Used (5.75G Avail)	5%	0%	Mail Filter	8.0.1.1446	8% Used (52.49G Avail)	2%	11%	2015-08-07 10:30:48 [UTC+0300]	00:0C:29:7E:15:FC	8% Used (10.29G Avail)	3%	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**.