

F-SECURE E-MAIL AND SERVER SECURITY

Deployment Guide



F-Secure.

CONTENTS

Disclaimer	3
1. Overview	4
1.1 How the product works	4
1.2 Product contents	5
2. Deployment scenarios	6
2.1 Stand-alone server	6
2.2 Deploying the product with F-Secure Policy Manager	6
2.3 Multiple Exchange 2003 servers	7
2.4 Multiple Exchange server roles	7
2.5 Large organization using multiple Exchange servers	8
2.6 Centralized quarantine management	9
2.6.1 <i>Mixed mode authentication in the Microsoft SQL Server</i>	10
2.7 Microsoft SharePoint server	10
3. System requirements	11
3.1 Installation without Anti-Virus for Microsoft Exchange	11
3.2 Installation with Anti-Virus for Microsoft Exchange	11
3.2.1 <i>Installation on Microsoft Exchange Server 2003</i>	11
3.2.2 <i>Installation on Microsoft Exchange Server 2007</i>	12
3.2.3 <i>Installation on Microsoft Exchange Server 2010</i>	13
3.2.4 <i>Installation on Microsoft Exchange Server 2013</i>	14
3.2.5 <i>Network Requirements for E-mail and Server Security</i>	15
3.3 Centralized Management Requirements	16
3.4 Other System Component requirements	16
3.4.1 <i>SQL Server Requirements</i>	16
3.4.2 <i>Additional Windows Components</i>	17
3.4.3 <i>Web Browser Software Requirements</i>	17
3.4.4 <i>Spam Engine Requirements</i>	17
4. Installation	18
4.1 Installing the product locally	18
4.2 Upgrading from previous product versions	29
4.2.1 <i>Upgrading from F-Secure Anti-Virus for Windows Server</i>	29
4.2.2 <i>Upgrading from F-Secure Anti-Virus for Microsoft Exchange</i>	29
4.3 Registering the Evaluation Version	29
4.4 Uninstalling the Product	30
5. Configuring the Product	30
5.1 Network configuration	31
5.2 Configuring F-Secure Spam Control	32

DISCLAIMER

“F-Secure” and the triangle symbol are registered trademarks of F-Secure Corporation and F-Secure product names and symbols/logos are either trademarks or registered trademarks of F-Secure Corporation. All product names referenced herein are trademarks or registered trademarks of their respective companies.

F-Secure Corporation disclaims proprietary interest in the marks and names of others. Although F-Secure Corporation makes every effort to ensure that this information is accurate, F-Secure Corporation will not be liable for any errors or omission of facts contained herein. F-Secure Corporation reserves the right to modify specifications cited in this document without prior notice.

Companies, names and data used in examples herein are fictitious unless otherwise noted. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of F-Secure Corporation.

© 1993-2014 F-Secure Corporation. All rights reserved.

Portions Copyright © 2004 BackWeb Technologies Inc.

Portions Copyright © 1997-2014 BitDefender.

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>).

Copyright © 2000-2004 The Apache Software Foundation. All rights reserved.

This product includes PHP, freely available from <http://www.php.net/>.

Copyright © 1999-2012 The PHP Group. All rights reserved.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).

Copyright © 1998-2014 The OpenSSL Project. All rights reserved.

1. OVERVIEW

F-Secure E-mail and Server Security is designed to protect your company's mail and groupware servers and to shield the company network from any malicious code that travels in HTTP or SMTP traffic. In addition, it protects your company network against spam.

Malicious code, such as computer viruses, is one of the main threats for companies today. In the past, malicious code spread mainly via disks and the most common viruses were the ones that infected disk boot sectors. When users began to use office applications with macro capabilities - such as Microsoft Office - to write documents and distribute them via mail and groupware servers, macro viruses started spreading rapidly.

Nowadays the most common spreading mechanism for viruses is Web. Even fraudulent e-mails usually contain a link to a browser exploit or a phishing web site. F-Secure E-mail and Server Security includes Browsing Protection, which protects the Internet browsing for all users of the server.

The protection can be implemented on the gateway level to screen all incoming and outgoing e-mail (SMTP), web surfing (HTTP and FTP-over-HTTP) and file transfer (FTP) traffic. Furthermore, it can be implemented on the mail server level so that it does not only protect inbound and outbound traffic but also internal mail traffic and public sources, such as public folders on Microsoft Exchange servers.

Providing the protection already on the gateway level has plenty of advantages. The protection is easy and fast to set up and install, compared to rolling out antivirus protection on hundreds or thousands of workstations. The protection is also invisible to the end users which ensures that the system cannot be by-passed and makes it easy to maintain. Of course, protecting the gateway level alone is not enough to provide a complete antivirus solution; file server and workstation level protection is needed, also.

Why clean 1000 workstations when you can clean one attachment at the gateway level?

1.1 HOW THE PRODUCT WORKS

The product is designed to detect and disinfect viruses and other malicious code from e-mail transmissions through Microsoft Exchange Server. Scanning is done in real time as the mail passes through Microsoft Exchange Server. On-demand scanning of user mailboxes and public folders is also available.

The product scans attachments and message bodies for malicious code. It can also be instructed to remove particular attachments according to the file name or the file extension.

The product is installed on Microsoft Exchange Server and it intercepts mail traveling to and from mailboxes and public folders. The messages and documents are scanned with the scanning component, F-Secure Content Scanner Server, which also disinfects the infected messages.

If the intercepted mail contains malicious code, the product can be configured to disinfect or drop the content. Any malicious code found during the scan process can be placed in the Quarantine, where it can be further examined. Stripped attachments can also be placed in the Quarantine for further examination.

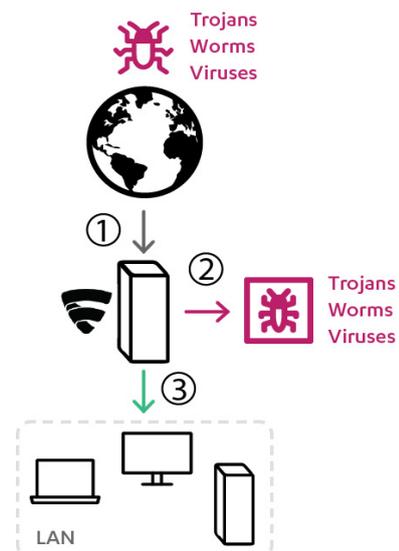


Figure 1. Email traffic.

(1) Email arrives from the Internet to F-Secure E-mail and Server Security, which (2) filters malicious content from mails and attachments, and (3) delivers cleaned files forward.

1.2 PRODUCT CONTENTS

The product can be licensed and deployed as F-Secure Server Security (Standard) or F-Secure Server Security Premium, on per-server basis, or F-Secure E-mail and Server Security (Standard) or F-Secure E-mail and Server Security Premium, on per-user or terminal connection basis.

Features with different product licenses:

Feature	F-Secure Server Security (Standard)	F-Secure Server Security Premium	F-Secure E-mail and Server Security (Standard)	F-Secure E-mail and Server Security Premium
Virus & spyware protection	X	X	X	X
DeepGuard	X	X	X	X
Web traffic scanning	X	X	X	X
Browsing protection	X	X	X	X
Anti-Virus for Microsoft Exchange			X	X
Spam Control			X	X
Offload Scanning Agent	X	X	X	X
Software Updater		X		X
Anti-Virus for Microsoft SharePoint				X
EMC CAVA support				X

2. DEPLOYMENT SCENARIOS

Depending on how the Microsoft Exchange Server roles are deployed in your environment, you might consider various scenarios of deploying the product.

There are various ways to deploy the product that are suitable to different environments.

2.1 STAND-ALONE SERVER

This is a typical scenario in companies that run Microsoft Small Business Server.

Make sure that your hardware and the system configuration meet the system and network requirements.

In corporations with one or two servers (Microsoft Exchange Server 2003/2007/2010/2013 or Microsoft Small Business Server 2003/2008/2011) that hold all mailboxes, public folders and send and receive all inbound and outbound messages over SMTP, you can administer each server in stand-alone mode.

Note: To use SharePoint Protection, Microsoft SharePoint server should be installed on the same server.

1. Install F-Secure E-mail and Server Security.

To install the product, login to the server with local administrative privileges and run the setup.

2. After you have installed the product, use the product Web Console to configure your product.

2.2 DEPLOYING THE PRODUCT WITH F-SECURE POLICY MANAGER

In corporations with multiple servers and workstations, we recommend that you use F-Secure Policy Manager to centrally manage the product. Make sure that servers where you install the product meet the system and network requirements.

To install the product to servers:

1. Download the remote installation package (jar file) of the product from F-Secure web site.
2. Import the remote installation package to F-Secure Policy Manager Console.

Note: Use the installation package based on the license that you have. F-Secure Server Security (Standard):fsss-11.00.nnn.jar

- F-Secure Server Security Premium: fssspr-11.00.nnn.jar
 - F-Secure E-mail and Server Security (Standard): fsess-11.00.nnn.jar
 - F-Secure E-mail and Server Security Premium: fsesspr-11.00.nnn.jar
3. Install F-Secure E-mail and Server Security to the target servers.

If target servers are in the policy domain already, use the policy-based installation. Otherwise, use the push-installation.

4. After the installation is complete, import new hosts to the Policy Manager domain.
5. Install E-mail Security components locally to servers running Microsoft Exchange Server.

Use the centralized administration mode and connect the product to the same Policy Manager.

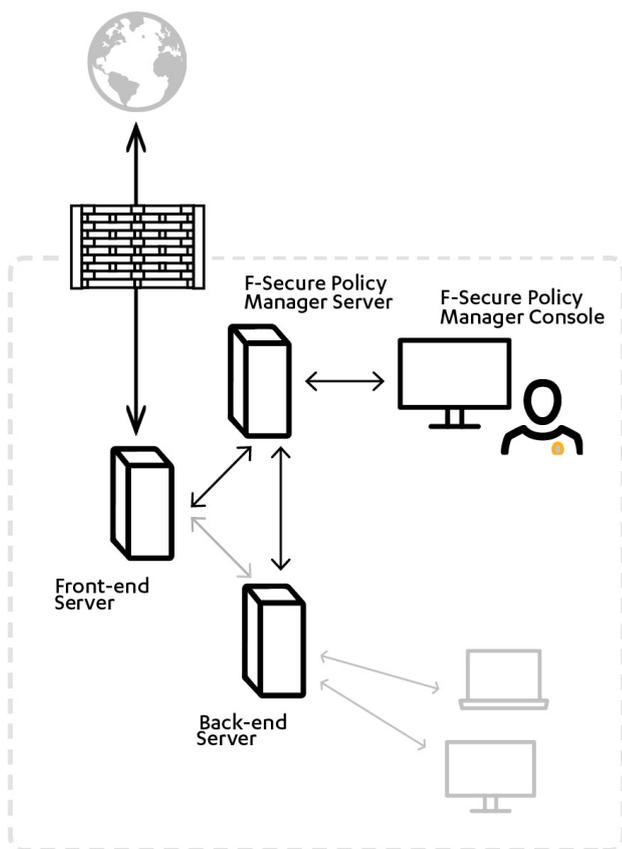
6. Install Anti-Virus for Microsoft SharePoint component locally to servers that are running Microsoft SharePoint Server.

Use the centralized administration mode and connect the product to the same Policy Manager.

Note: Anti-Virus for Microsoft SharePoint is available only with the Premium license.

2.3 MULTIPLE EXCHANGE 2003 SERVERS

Your organization has multiple Microsoft Exchange Server 2003 installations. Usually, the front-end server is located in the perimeter network and receives inbound mail using SMTP and forwards all messages to the back-end server. The back-end Exchange server holds all mailboxes and public folders. In a larger organization, back-end servers may be clustered.



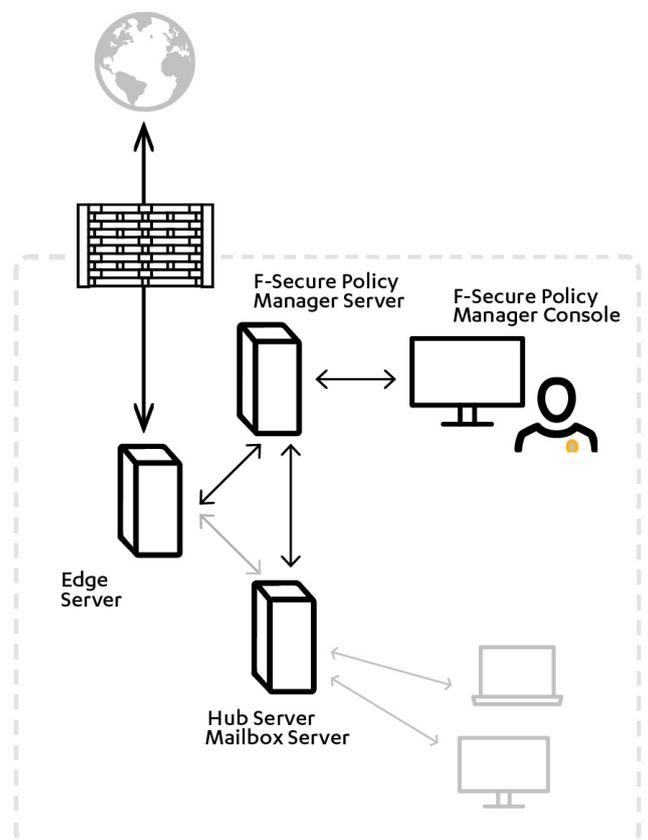
1. Install the product to both front-end and back-end Exchange servers. In addition, the front-end server can be protected with F-Secure Spam Control.
2. Install F-Secure Policy Manager Server on a dedicated server or on the same server with one of Exchange servers. You can administer the product with F-Secure Policy Manager Console.

When you install the product, configure each installation to connect to the same F-Secure Policy Manager Server.

3. The product installations receive anti-virus and spam database updates from F-Secure Policy Manager Server, which receives updates from F-Secure Update Server.

2.4 MULTIPLE EXCHANGE SERVER ROLES

Your organization has multiple Microsoft Exchange Server 2007/2010/2013 installations. Exchange Edge and Mailbox Server roles are deployed to separate servers and the Hub Server is deployed either on a separate server or on the same server with the Mailbox Server. The Edge Server handles incoming and outgoing messages using SMTP and Mailbox Server holds all mailboxes and public folders and Hub Server routes mail traffic between Exchange servers.



1. Install the product to all servers where Exchange Edge, Hub and Mailbox Server roles are deployed. In addition, the Edge server can be protected with F-Secure Spam Control.

Note: If the Exchange role is changed later, the product has to be reinstalled.

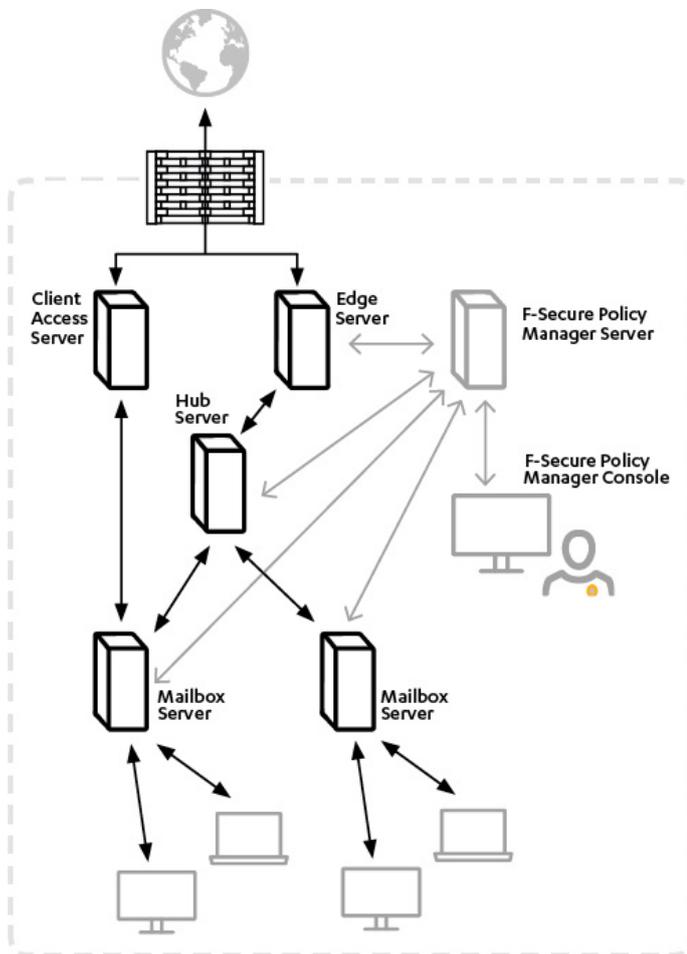
2. Install F-Secure Policy Manager Server on a dedicated server or on the same server with one of Exchange servers. You can administer the product with F-Secure Policy Manager Console.

When you install the product, configure each installation to connect to the same F-Secure Policy Manager Server.

3. The product installations receive anti-virus and spam database updates from F-Secure Policy Manager Server, which receives updates from F-Secure Update Server.

2.5 LARGE ORGANIZATION USING MULTIPLE EXCHANGE SERVERS

Your organization has multiple Microsoft Exchange Server 2007/2010/2013 installations. All Exchange roles are deployed on dedicated servers. Mailbox servers are possibly clustered.



1. Install the product to the server where Exchange Edge, Hub and Mailbox Server roles are deployed. In addition, the Edge server can be protected with F-Secure Spam Control.

Do not install the product to Client Access or Unified Messaging Server roles.

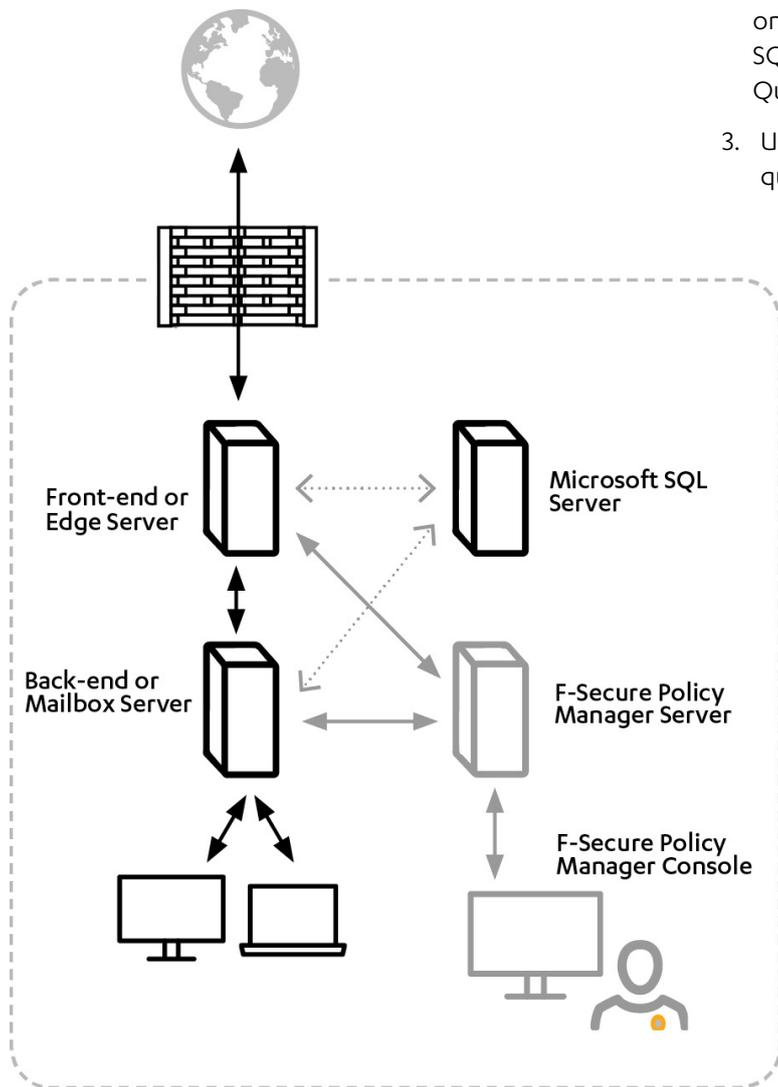
2. F-Secure Spam Control can be installed on the Edge server.
3. Install F-Secure Policy Manager Server on a dedicated server. You can administer the product with F-Secure Policy Manager Console.

When you install the product, configure each installation to connect to the same F-Secure Policy Manager Server.

4. The product installations receive anti-virus and spam database updates from F-Secure Policy Manager Server, which receives updates from F-Secure Update Server.

2.6 CENTRALIZED QUARANTINE MANAGEMENT

Your organization has multiple Microsoft Exchange Server installations. For example, you have front-end and back-end servers running Exchange Server 2003, or a network configuration with Edge and Mailbox roles running Exchange Server 2007/2010/2013.



1. Install Microsoft SQL Server on a dedicated server or on the server running F-Secure Policy Manager Server.
2. Install the product.
 - When you install the product, configure each installation to use the same SQL server and database.

- Make sure that the SQL server, the database name, user name and password are identical in the quarantine configuration for all F-Secure Anti-Virus for Microsoft Exchange installations.
 - Make sure that all the servers are allowed to communicate with the SQL server using mixed mode authentication.
 - In environments with heavy e-mail traffic, it is recommended to use a Microsoft SQL server installed on a separate server. When using the free Microsoft SQL Server 2008 R2 included with the product, the Quarantine database size is limited to 10 GB.
3. Use the Web Console to manage and search quarantined content.

2.6.1 MIXED MODE AUTHENTICATION IN THE MICROSOFT SQL SERVER

If you install Microsoft SQL Server 2005/2008 separately, it supports Windows Authentication only by default. You have to change the authentication to mixed mode during the setup or configure it later with Microsoft SQL Server user interface.

The mixed mode authentication allows you to log into the SQL server with either your Windows or SQL username and password.

Follow these steps to change the authentication mode:

1. Open Microsoft SQL Server Management Studio or Microsoft SQL Server Management Studio Express.

If you do not have Microsoft SQL Server Management Studio installed, you can freely download Management Studio Express from the [Microsoft web site](#).

2. Connect to the SQL server.
 3. In Object Explorer, go to Security > Logins.
 4. Right-click on **sa** and select **Properties**.
 5. Open the **General** page and change the password. Confirm the new password that you entered.
- Note:** Make sure that the sa password is strong when you change the authentication mode from the Windows authentication to the mixed authentication mode.
6. Open the **Status** page and select **Enabled** in the **Login** section.
 7. Click **OK**.
 8. In Object Explorer, right-click on the server name and select **Properties**.
 9. On the **Security** page, select **SQL Server and Windows Authentication mode** under **Server authentication**.
 10. Click **OK**.
 11. Right-click on the server name and select **Restart**.

- Wait for a moment for the service to restart before you continue.

12. Use Management Studio to test the connection to the SQL server with the sa account and the new password you set.

2.7 MICROSOFT SHAREPOINT SERVER

Your organization has one or several dedicated SharePoint servers.

1. Install the product locally on each server that runs SharePoint. During the installation, make sure that you select to install F-Secure Anti-Virus for Microsoft SharePoint component.

You can install the product in stand-alone mode and administer it with the Web Console.

2. You need to enter the account details to manage Microsoft Sharepoint during the installation. You can use a dedicated account in the domain and add it to farm administrators. Make sure that this account has local administrative rights on the server.

3. SYSTEM REQUIREMENTS

3.1 INSTALLATION WITHOUT ANTI-VIRUS FOR MICROSOFT EXCHANGE

The minimum and recommended requirements for installing and using the product on the server that does not have Microsoft Exchange Server.

Processor:

- Any processor based on Intel x86 (I386) or AMD x64 / Intel EM64T architecture that can run the corresponding Microsoft Windows Server (Intel Pentium 4 2GHz or higher recommended)

Operating system:

- Microsoft® Windows Server 2003 with the latest service pack
- Microsoft® Windows Server 2003 R2
- Microsoft® Windows Server 2008
- Microsoft® Windows Server 2008 R2
- Microsoft® Small Business Server 2003
- Microsoft® Small Business Server 2003 R2
- Microsoft® Small Business Server 2008
- Microsoft® Small Business Server 2011, Standard edition
- Microsoft® Small Business Server 2011, Essentials
- Microsoft® Windows Server 2012
- Microsoft® Windows Server 2012 R2
- Microsoft® Windows Server 2012 Essentials

Note: DeepGuard does not support Windows Server 2003 64-bit platform.

Memory:

512MB (1GB or more recommended)

Disk space:

1,5 GB for installation and updates

Internet connection:

Required to receive updates and to use the real-time protection network

Web browser:

Required to administer the product:

- Microsoft Internet Explorer 7.0 or later
- Mozilla Firefox 3.0 or later
- Google Chrome (up-to-date versions)
- Any other web browser that supports HTTP 1.0, SSL, JavaScript and cookies may be used as well.

3.2 INSTALLATION WITH ANTI-VIRUS FOR MICROSOFT EXCHANGE

The product is installed on the computer running Microsoft Exchange Server.

Note: The release notes document contains the latest information about the product and might have changes to system requirements and the installation procedure. It is highly recommended to read the release notes before you proceed with the installation.

3.2.1 INSTALLATION ON MICROSOFT EXCHANGE SERVER 2003

The product can be installed on a computer running Microsoft® Exchange Server 2003 with the latest service pack.

Processor:

- Any processor based on Intel x86 (I386) or AMD x64 / Intel EM64T architecture that can run the corresponding 32-bit Microsoft Windows Server
- Intel Pentium 4 2GHz or higher

Operating system:

- Microsoft® Windows Server 2003 Standard Edition with the latest service pack
- Microsoft® Windows Server 2003 Enterprise Edition with the latest service pack
- Microsoft® Windows Server 2003 R2 Standard Edition
- Microsoft® Windows Server 2003 R2 Enterprise Edition
- Microsoft® Small Business Server 2003
- Microsoft® Small Business Server 2003 R2

Memory:

1 GB minimum

Disk space to install:

2 GB for installation and updates

Disk space for processing:

10 GB or more. The required disk space depends on the number of mailboxes, amount of data traffic and the size of the Information Store.

Internet connection:

Required to receive updates and to use the real-time protection network

Web browser:

Required to administer the product:

- Microsoft Internet Explorer 7.0 or later
- Mozilla Firefox (up-to-date versions)
- Google Chrome (up-to-date versions)
- Any other web browser that supports HTTP 1.0, SSL, JavaScript and cookies may be used as well.

Cluster Environment

The product supports the following cluster models of Microsoft Exchange Server 2003:

- Active - Active Cluster
- Active - Passive Cluster

3.2.2 INSTALLATION ON MICROSOFT EXCHANGE SERVER 2007

The product can be installed on a computer running one of the following Exchange Server 2007 versions.

Supported Microsoft Exchange Server versions:

- Microsoft® Exchange Server 2007 (64-bit version) with the latest service pack
- Microsoft® Small Business Server 2008

Note: The 32-bit evaluation version of Microsoft Exchange Server 2007 is not supported.

Processor:

- Any processor based on AMD x64 / Intel EM64T architecture that can run the corresponding 64-bit Microsoft Windows Server
- Intel Pentium 4 2GHz or higher

Operating system:

- Microsoft® Windows Server 2003, Standard x64 Edition with the latest service pack
- Microsoft® Windows Server 2003, Enterprise x64 Edition with the latest service pack
- Microsoft® Windows Server 2003 R2, Standard x64 Edition
- Microsoft® Windows Server 2003 R2, Enterprise x64 Edition
- Microsoft® Windows Server 2008, Standard Edition (x64)
- Microsoft® Windows Server 2008, Enterprise Edition (x64)
- Microsoft® Small Business Server 2008

Memory:

2 GB minimum

Disk space to install:

2 GB for installation and updates

Disk space for processing:

10 GB or more. The required disk space depends on the number of mailboxes, amount of data traffic and the size of the Information Store.

Internet connection:

Required to receive updates and to use the real-time protection network

Web browser:

Required to administer the product:

- Microsoft Internet Explorer 7.0 or later
- Mozilla Firefox (up-to-date versions)
- Google Chrome (up-to-date versions)
- Any other web browser that supports HTTP 1.0, SSL, JavaScript and cookies may be used as well.

Important: If you install the product on on Microsoft Exchange Server 2007 that is running on Microsoft Windows Server 2008 R2, you must install the Collaboration Data Objects for Exchange (CDOEX) update first. To install the CDOEX update, see the Microsoft Knowledge Base article 98270.

Microsoft Exchange Server Roles

The product supports the following roles of Microsoft Exchange Server 2007:

- Edge Server role
- Hub Server role
- Mailbox Server role
- Combo Server (Mailbox Server and Hub Server roles)

Cluster Environment

The product supports the following cluster models of Microsoft Exchange Server 2007:

- Cluster Continuous Replication (CCR)
- Single Copy Cluster (SCC)

3.2.3 INSTALLATION ON MICROSOFT EXCHANGE SERVER 2010

The product can be installed on a computer running the following versions of Exchange Server 2010.

Supported Microsoft Exchange Server versions:

- Microsoft® Exchange Server 2010 (without service pack or with service pack 1 or 2)
- Microsoft® Small Business Server 2011

Processor:

- Any processor based on AMD x64 / Intel EM64T architecture that can run the corresponding 64-bit Microsoft Windows Server

Operating system:

- Microsoft® Windows Server 2008, Standard Edition (x64)
- Microsoft® Windows Server 2008, Enterprise Edition (x64)
- Microsoft® Windows Server 2008 R2, Standard Edition
- Microsoft® Windows Server 2008 R2, Enterprise Edition
- Microsoft® Small Business Server 2008
- Microsoft® Small Business Server 2011, Standard edition

Memory:

4 GB minimum

Disk space to install:

2 GB for installation and updates

Disk space for processing:

10 GB or more. The required disk space depends on the number of mailboxes, amount of data traffic and the size of the Information Store.

Internet connection:

Required to receive updates and to use the real-time protection network

Web browser:

Required to administer the product:

- Microsoft Internet Explorer 7.0 or later
- Mozilla Firefox (up-to-date versions)
- Google Chrome (up-to-date versions)
- Any other web browser that supports HTTP 1.0, SSL, JavaScript and cookies may be used as well.

Microsoft Exchange Server Roles

- The product supports the following roles of Microsoft Exchange Server 2010: Edge Server role
- Hub Server role
- Mailbox Server role
- Combo Server (Mailbox Server and Hub Server roles)

Cluster Environment

The current version of the product supports Microsoft Exchange Server 2010 high-availability solutions based on Database Availability Groups (DAG).

3.2.4 INSTALLATION ON MICROSOFT EXCHANGE SERVER 2013

The product can be installed on a computer running the following Microsoft Exchange Server 2013 (with or without service pack 1).

Processor:

- x64 architecture-based computer with Intel processor that supports Intel 64 architecture (formerly known as Intel EM64T)
- AMD processor that supports the AMD64 platform

Operating system:

- Microsoft® Windows Server 2012 Standard or Datacenter
- Microsoft® Windows Server 2012 R2 Standard or Datacenter
- Microsoft® Windows Server 2008 R2 Standard with Service Pack 1 (SP1)
- Microsoft® Windows Server 2008 R2 Enterprise with Service Pack 1 (SP1)
- Microsoft® Windows Server 2008 R2 Datacenter RTM or later

Memory:

- Mailbox role: 8GB minimum
- Client Access role: 4GB minimum
- Mailbox and Client Access roles combined: 8GB minimum

Disk space to install:

2 GB for installation and updates

Disk space for processing:

10 GB or more. The required disk space depends on the number of mailboxes, amount of data traffic and the size of the Information Store.

Internet connection:

Required to receive updates and to use the real-time protection network

Web browser:

Required to administer the product:

- Microsoft Internet Explorer 7.0 or later
- Mozilla Firefox (up-to-date versions)
- Google Chrome (up-to-date versions)
- Any other web browser that supports HTTP 1.0, SSL, JavaScript and cookies may be used as well.

Microsoft Exchange Server Roles

The product supports the following roles of Microsoft Exchange Server 2013:

- Client Access Server role
- Mailbox Server role

The product can be installed on a server with any role.

Cluster Environment

The current version of the product does not support clusters.

3.2.5 NETWORK REQUIREMENTS FOR E-MAIL AND SERVER SECURITY

This network configuration is valid for all scenarios described in this chapter.

Make sure that the following network traffic can pass through:

Service	Process	Inbound ports	Outbound ports
F-Secure Content Scanner Server	%ProgramFiles%\F-Secure\Content Scanner Server\fsavsd.exe	18971 (TCP) (on localhost only)	DNS (53, UDP/TCP), HTTP (80) or another known port used for HTTP proxy
F-Secure E-mail and Server Security WebUI Daemon	%ProgramFiles%\F-Secure\Web User Interface\bin\fswebuid.exe	25023	DNS (53, UDP and TCP), 1433 (TCP), only with the dedicated SQL server
F-Secure Automatic Update Agent	%ProgramFiles%\F-Secure\FSAUA\program\fsaua.exe	-	DNS (53, UDP and TCP), HTTP (80) and/or another port used to connect to F-Secure Policy Manager Server
F-Secure Network Request Broker	%ProgramFiles%\F-Secure\?Common\fnrb32.exe	-	DNS (53, UDP/TCP), HTTP (80) or another port used to connect to F-Secure Policy Manager Server
F-Secure Management Agent	%ProgramFiles%\F-Secure\Common\fameh32.exe	-	DNS (53, UDP/TCP), SMTP (25)
F-Secure Quarantine Manager	%ProgramFiles%\F-Secure\Quarantine Manager\fqm.exe	-	DNS (53, UDP/TCP), 1433 (TCP), only with the dedicated SQL server
F-Secure ORSP Client	%ProgramFiles%\F-Secure\ORSP Client\fsorsp.exe	-	DNS (53, UDP/TCP), HTTP (80, or the port used for HTTP proxy)

3.3 CENTRALIZED MANAGEMENT REQUIREMENTS

The product supports the following F-Secure Policy Manager versions.

- Standard installations: F-Secure Policy Manager (Windows) 11.10 or newer, 11.20 is recommended
- F-Secure Policy Manager (Linux) 10.30 or newer, 10.40 is recommended
- Premium installations: F-Secure Policy Manager (Windows) 11.20
- F-Secure Policy Manager (Linux) 10.40

If you are using a previous version of F-Secure Policy Manager, upgrade it to the latest version before you install the product.

3.4 OTHER SYSTEM COMPONENT REQUIREMENTS

When you install the product with Anti-Virus for Microsoft Exchange, it requires Microsoft SQL Server for the e-mail quarantine management. Depending on the selected deployment and administration method, you may need have some additional software as well.

3.4.1 SQL SERVER REQUIREMENTS

The product requires Microsoft® SQL Server for the quarantine management.

The following versions of Microsoft SQL Server are recommended to use:

- Microsoft SQL Server 2005 (Enterprise, Standard, Workgroup or Express edition) with the latest service pack
- Microsoft SQL Server 2008 (Enterprise, Standard, Workgroup or Express edition)
- Microsoft® SQL Server 2008 R2 (Enterprise, Standard, Workgroup or Express Edition)
- Microsoft® SQL Server 2012 (Enterprise, Business Intelligence, Standard, or Express Edition)

Microsoft SQL Server 2008 R2 Express Edition SP1 is distributed with the product and can be installed during F-Secure E-Mail and Server Security setup.

The product supports also Microsoft SQL Server 2000 with Service Pack 4 and Microsoft SQL Server 2000 Desktop Engine (MSDE) with Service Pack 4.

Note: To install Microsoft SQL Server 2008 R2 Express Edition, you must have Microsoft .NET Framework version 2.0 SP2 and Microsoft Windows Installer 4.5 installed. You can download installation packages from Microsoft Download Center.

If you install Microsoft SQL Server on the same server with the product, install these components first.

Note: When centralized quarantine management is used, the SQL server must be reachable from the network and file sharing must be enabled.

Important: We do not recommend that you use MSDE or Microsoft SQL Server 2005/2008/2008R2/2012 Express Edition with the centralized quarantine management or if your organization sends and receives a large amount of e-mails.

Which SQL Server to Use for the Quarantine Database?

As a minimum requirement, the Quarantine database should have the capacity to store information about all inbound and outbound mail to and from your organization that would normally be sent during 2-3 days.

The upgrade installation does not upgrade the SQL server if you choose to use the existing database and the remote upgrade installation does not install or upgrade SQL Server and change the Quarantine database.

If you want to upgrade the SQL Server version that you use, follow the recommendations on the Microsoft web site: <http://www.microsoft.com/sqlserver/en/us/default.aspx>

Take the following SQL server specific considerations into account when deciding which SQL server to use:

Microsoft SQL Server 2005/2008 Express Edition

- When using Microsoft SQL Server 2005/2008 R2 Express Edition, the Quarantine database size is limited to 4 GB (2005 version) or 10 GB (2008 R2 version).
- Microsoft SQL Server 2005/2008 Express Edition supports Microsoft Windows Server 2008.
- It is **not** recommended to use Microsoft SQL Server 2005/2008 Express Edition if you are planning to use centralized quarantine management with multiple product installations.

Note: Microsoft SQL Server 2008 R2 Express Edition is delivered with F-Secure E-mail and Server Security, and you can install it during the setup.

Microsoft SQL Server 2000, 2005 and 2008

- If your organization sends a large amount of e-mails, it is recommended to use Microsoft SQL Server 2000, 2005 or 2008.
- It is recommended to use Microsoft SQL Server if you are planning to use centralized quarantine management with multiple product installations.
- Note that the product does not support Windows Authentication when connecting to Microsoft SQL Server. The Microsoft SQL Server that the product will use for the Quarantine database should be configured to use Mixed Mode authentication.

Note: If you plan to use Microsoft SQL Server 2000, 2005 or 2008, you must purchase it and obtain your own license before you start to deploy the product. To purchase Microsoft SQL Server, contact your Microsoft reseller.

3.4.2 ADDITIONAL WINDOWS COMPONENTS

The product may require additional Windows components, depending on how you deploy the product to your network system.

- The following Windows components may be required: Microsoft .NET Framework version 3.5 SP1 and Windows Installer 4.5 are required to install Microsoft SQL Server 2008 R2 Express Edition.
- If you plan to have Microsoft SQL Server on the same server, Microsoft .NET Framework must be installed before installing F-Secure E-mail and Server Security. Microsoft .NET Framework can be downloaded from the Microsoft Download Center.

3.4.3 WEB BROWSER SOFTWARE REQUIREMENTS

In order to administer the product with the Web Console, one of the following web browsers is required.

- Supported web browsers: Microsoft Internet Explorer 7.0 or later
- Mozilla Firefox (up-to-date versions)
- Google Chrome (up-to-date versions)

You can use any other web browser that supports HTTP 1.0, SSL, javascripts and cookies.

3.4.4 SPAM ENGINE REQUIREMENTS

To use the spam detection engine, you need to make a change to your firewall rules.

- Permit **outbound** HTTPS connections to `aspam.sp.f-secure.com` (TCP port 443).

Note: Alternatively, you can use a CONNECT-capable HTTPS proxy instead of changing the firewall rules.

4. INSTALLATION

4.1 INSTALLING THE PRODUCT LOCALLY

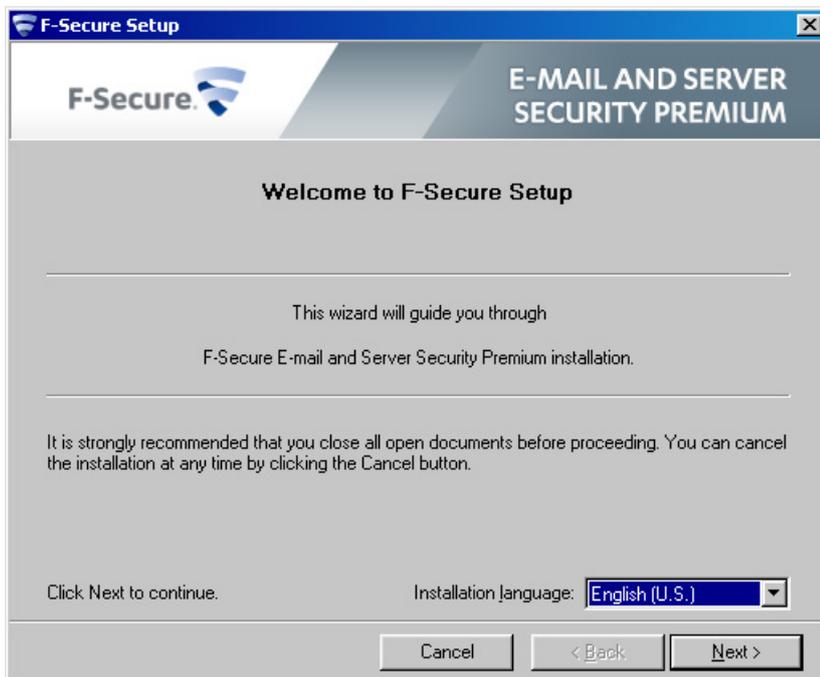
Follow these instructions to install the product.

1. Download the installation file (ess1100-nnn-rtm.exe) from the [F-Secure web site](#).
2. Run the installation file to start the installation.
3. Click **Install**.

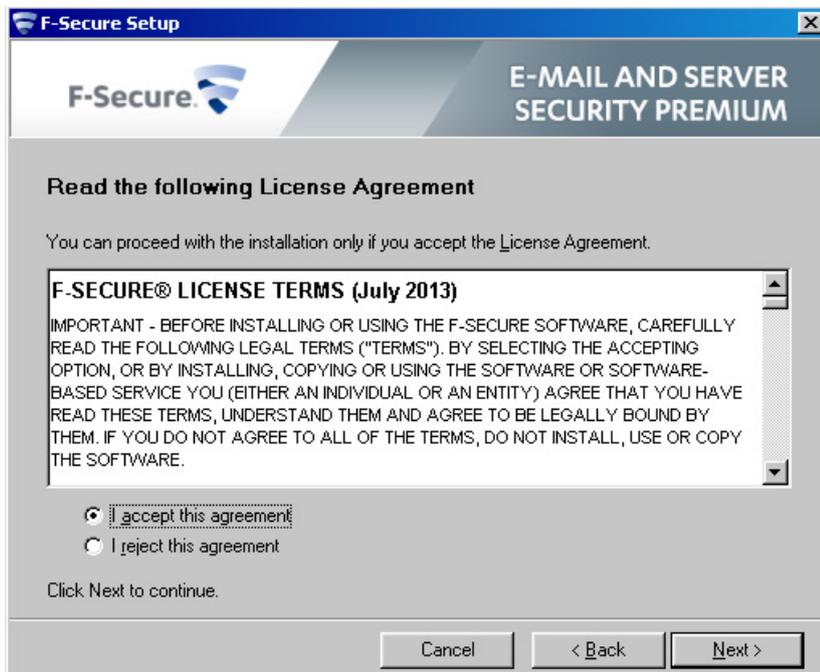


Note: If you plan to install Microsoft SQL Server 2008 R2 Express Edition SP1 that is included in the package, and you want to control the installation, click the link under Extras to start the SQL Server installation before you install the product. Depending on your system configuration, Microsoft SQL Server installation may require that you restart the server. In this case, install the product after the restart.

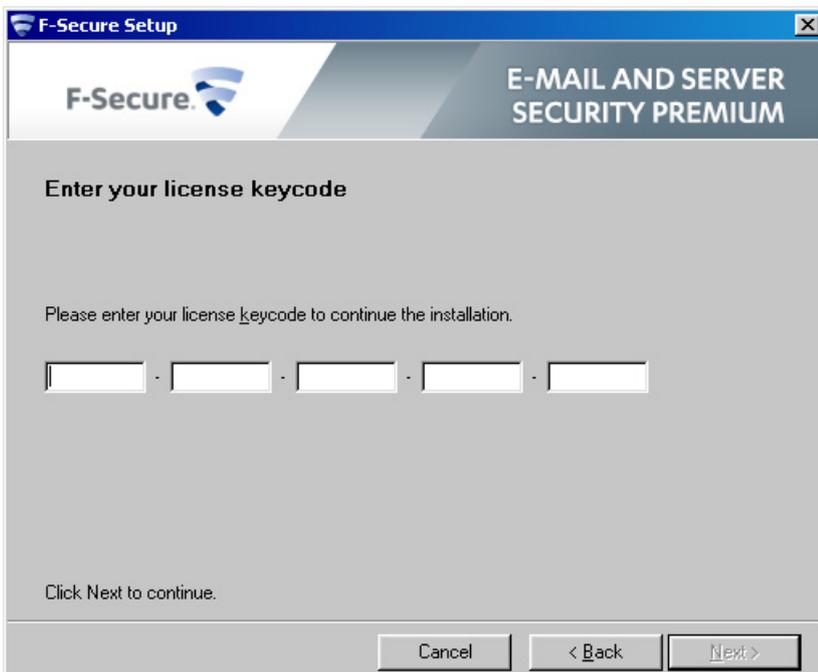
4. Read the information in the Welcome screen.



5. Read the license agreement. If you accept the agreement, check the **I accept this agreement** checkbox to continue.

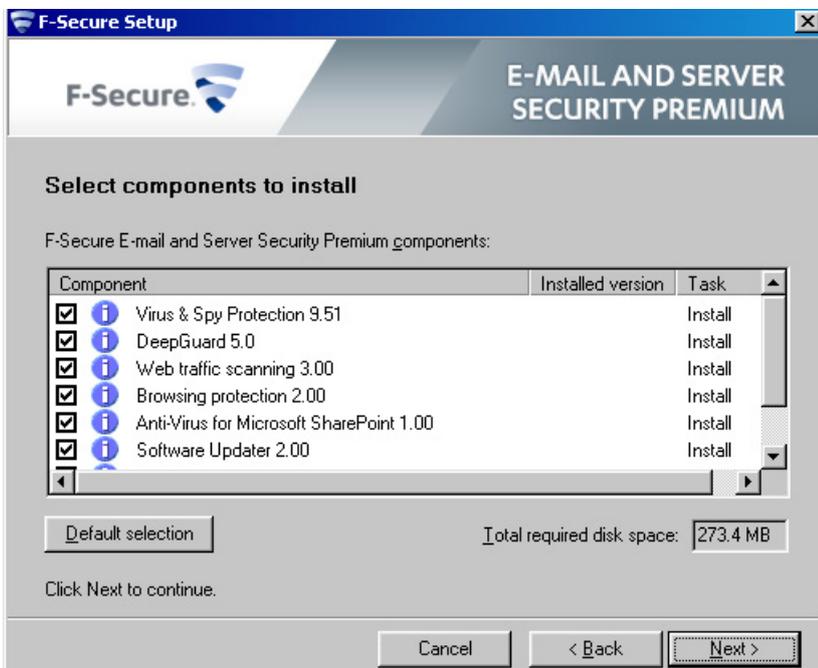


6. Enter the product keycode.



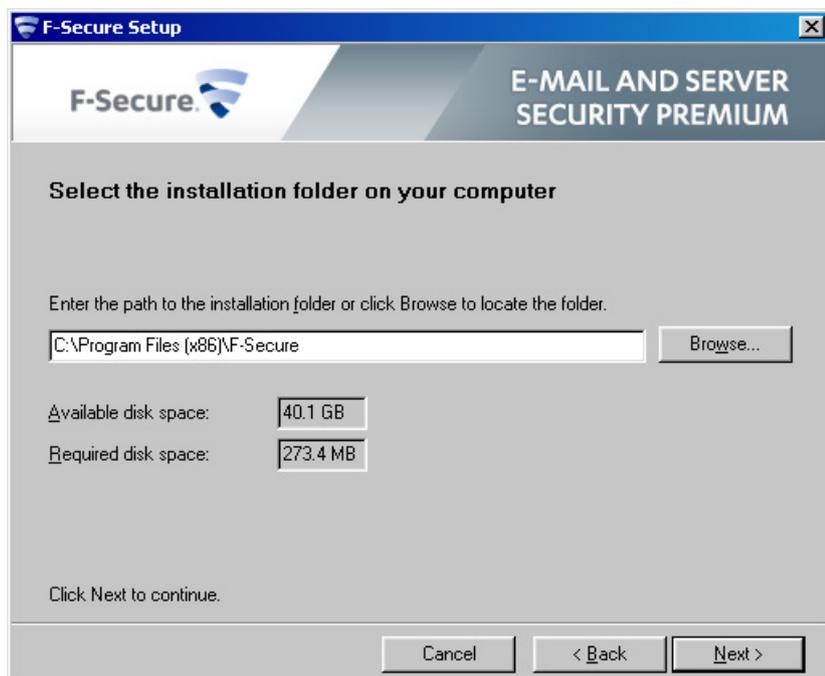
Note: This step is skipped if you install the evaluation version of the product.

7. Choose the components to install.

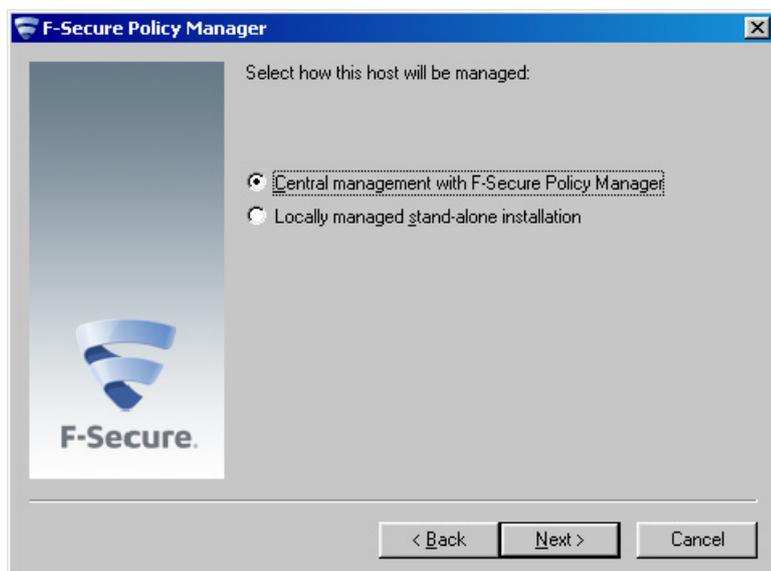


Note: Based on the product licence that you have, some components may not be available. For more information, see [Product contents](#).

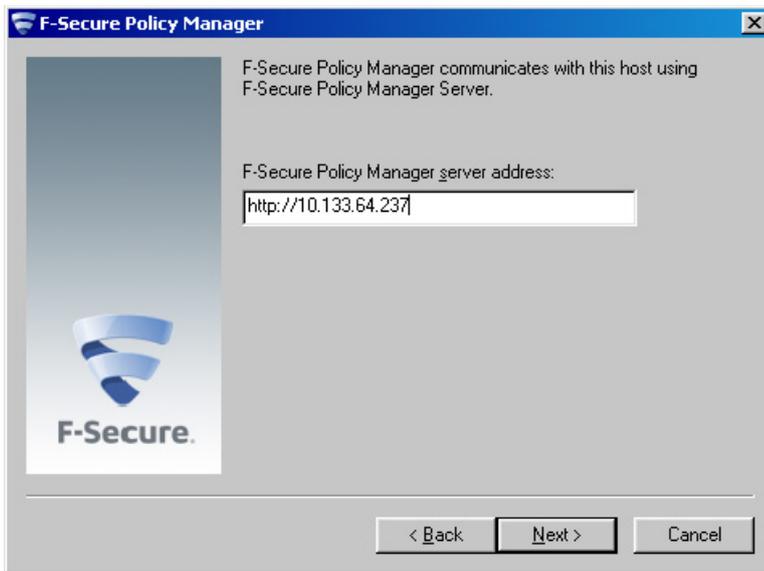
8. Choose the destination folder for the installation.



9. Choose the administration method.

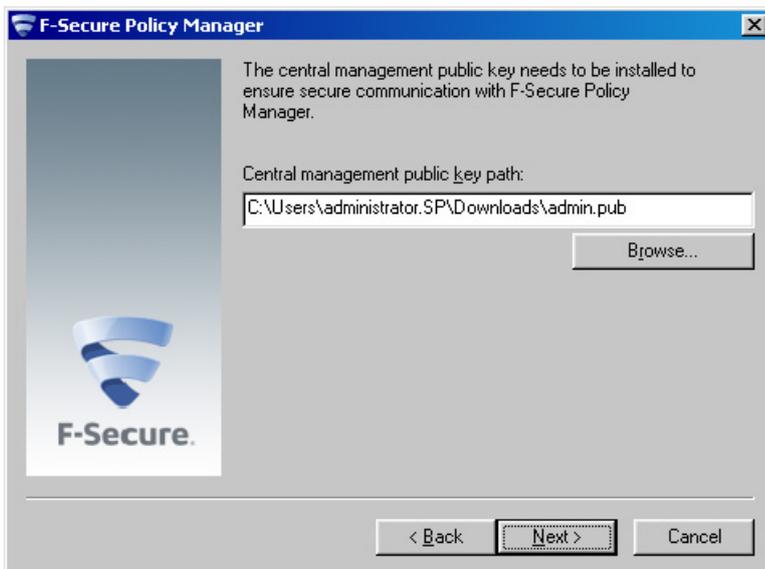


- Select the stand-alone mode to use the Web Console to change product settings and to view statistics.
- Select the central management to configure settings and receive alerts and status information in F-Secure Policy Manager Console.
 - a. In the centrally managed administration mode, enter the IP address or URL of the F-Secure Policy Manager Server you have installed earlier.



Note: If you do not use the default port (80) for the host communication, specify the port that you use here.

- b. The centrally managed administration mode requires the public management key. Enter the path to the public management key file `admin.pub` that was created during F-Secure Policy Manager setup.



You can retrieve the **admin.pub** file directly from Policy Manager Server.

- i. Open your web browser.
- ii. Go to the Policy Manager Server address, for example: `http://fspm.example.local`
- iii. At the page that opens, find the following text:

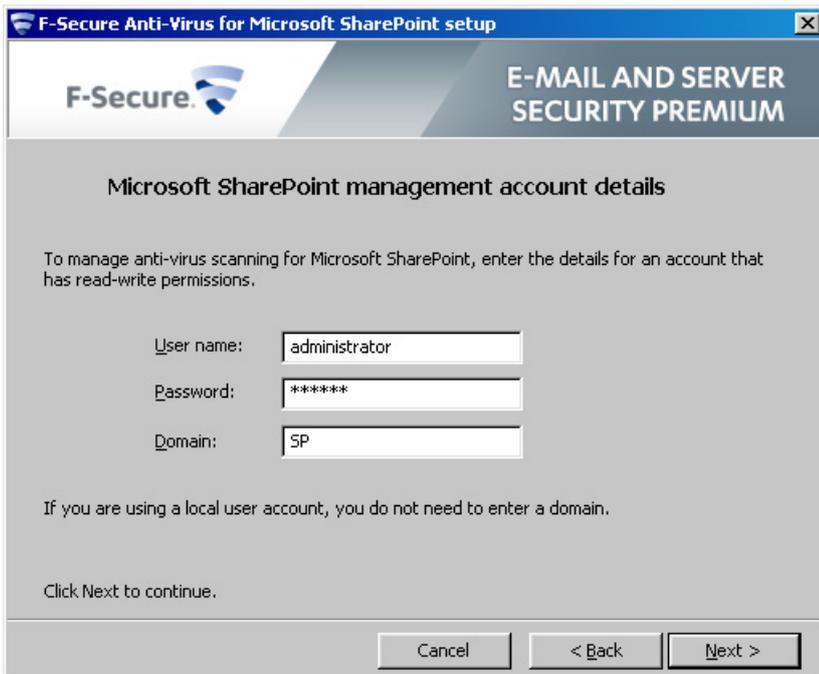
F-Secure Policy Manager Server's management public key used by clients to verify validity of distributed policies can be downloaded from here.

- iv. Click the link and save the file that opens.
- v. Return to the setup and click **Browse**.

Browse to the admin.pub file that you saved.

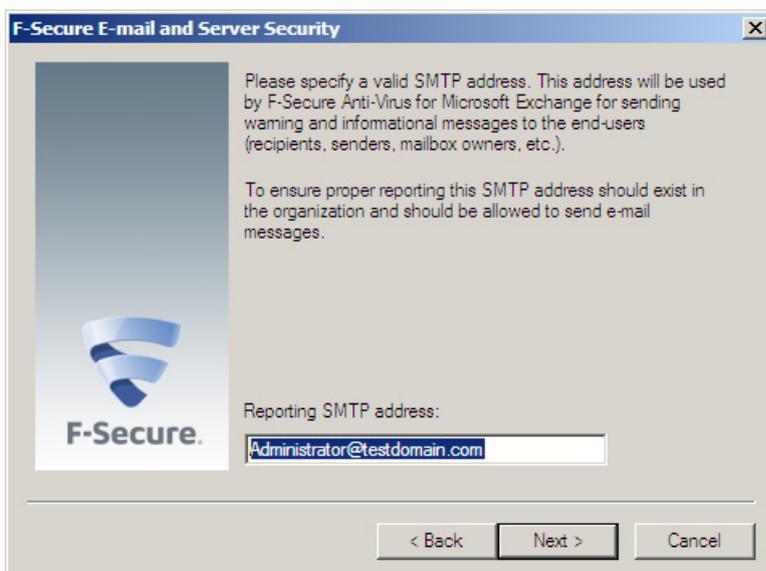
You can also transfer the public key other ways (use a shared folder on the file server, a USB device, or send the key as an attachment in an e-mail message).

10. When you install F-Secure Anti-Virus for Microsoft SharePoint component, enter the account details to manage Microsoft Sharepoint. This account needs read/write permissions on Sharepoint server.



The screenshot shows a Windows-style dialog box titled "F-Secure Anti-Virus for Microsoft SharePoint setup". The window has a blue header bar with the F-Secure logo and the text "E-MAIL AND SERVER SECURITY PREMIUM". Below the header, the main area is titled "Microsoft SharePoint management account details". A paragraph of text reads: "To manage anti-virus scanning for Microsoft SharePoint, enter the details for an account that has read-write permissions." There are three input fields: "User name:" with the text "administrator", "Password:" with "*****", and "Domain:" with "SP". Below these fields, a note states: "If you are using a local user account, you do not need to enter a domain." At the bottom, there is a prompt "Click Next to continue." and three buttons: "Cancel", "< Back", and "Next >".

11. When you install F-Secure Anti-Virus for Microsoft Exchange component, enter an SMTP address that will be used by the product to send warning and informational messages to end-users. The SMTP address should be a valid, existing address that is allowed to send messages.



The screenshot shows a Windows-style dialog box titled "F-Secure E-mail and Server Security". The window has a blue header bar with the F-Secure logo. The main area contains two paragraphs of text: "Please specify a valid SMTP address. This address will be used by F-Secure Anti-Virus for Microsoft Exchange for sending warning and informational messages to the end-users (recipients, senders, mailbox owners, etc.)." and "To ensure proper reporting this SMTP address should exist in the organization and should be allowed to send e-mail messages." Below the text, there is a label "Reporting SMTP address:" followed by an input field containing the text "Administrator@testdomain.com". At the bottom, there are three buttons: "< Back", "Next >", and "Cancel".

12. When you install F-Secure Anti-Virus for Microsoft Exchange component, specify the Quarantine management method.

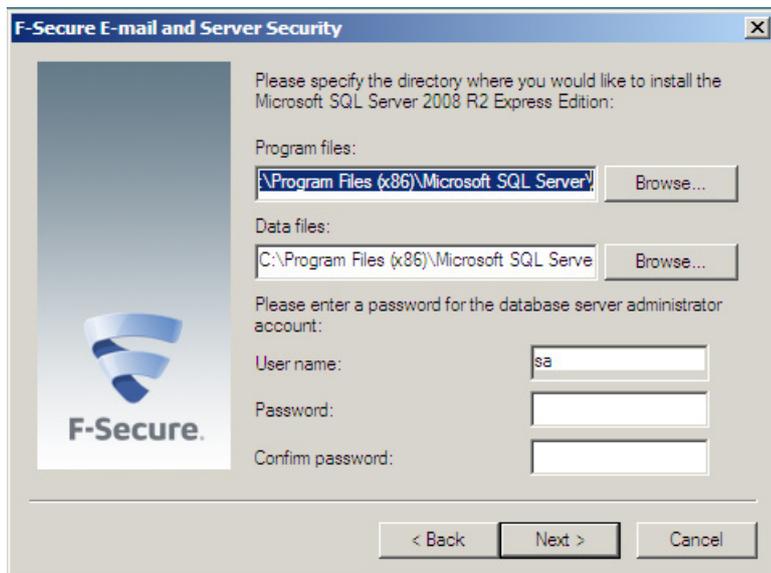


- If you want to manage the Quarantine database locally, select **Local quarantine management**.
- Select **Centralized quarantine management** if you install the product on multiple servers.

13. When you install F-Secure Anti-Virus for Microsoft Exchange component, specify Microsoft SQL Server instance that you use to store the Quarantine database.



- If you want to install Microsoft SQL Server 2008 R2 Express Edition and the Quarantine database on the same server as the product installation, select **Install and use Microsoft SQL Server 2008 R2 Express Edition**.



- Specify the installation and the database directory for Microsoft SQL Server 2008 R2 Express Edition.
 - Enter the password for the database server administrator account (sa) that will be used to create the new database.
- If you are using Microsoft SQL Server already, select **Use an existing installation of Microsoft SQL Server**.



- Specify the computer name and instance of the SQL Server where you want to create the Quarantine database.
- Enter the password for the sa account that you use to log on to the server.

14. When you install F-Secure Anti-Virus for Microsoft Exchange component, specify the name for the SQL database that stores information about the quarantined content.

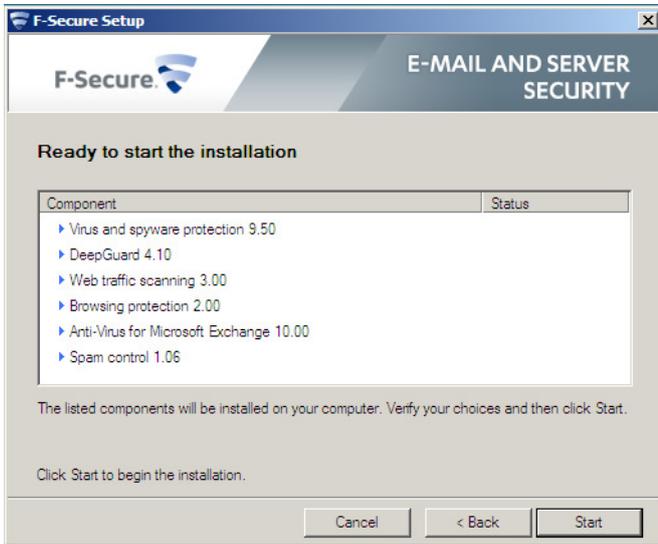
- a. Enter the user name and the password that you want to use to connect to the quarantine database.

Use a different account than the server administrator account. If the new account does not exist, the product creates it during the installation.

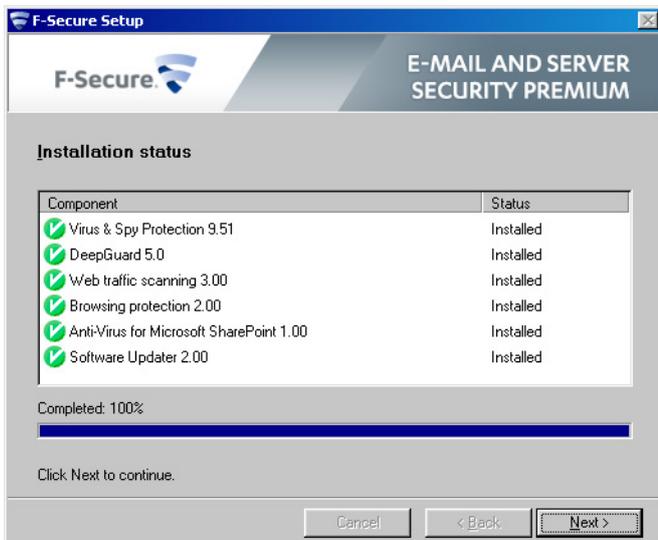
Use a password that is strong enough to comply with your current Windows password security policy.

- b. If the server has a database with the same name, you can either use the existing database, remove the existing database and create a new one or keep the existing database and create a new one with a new name.

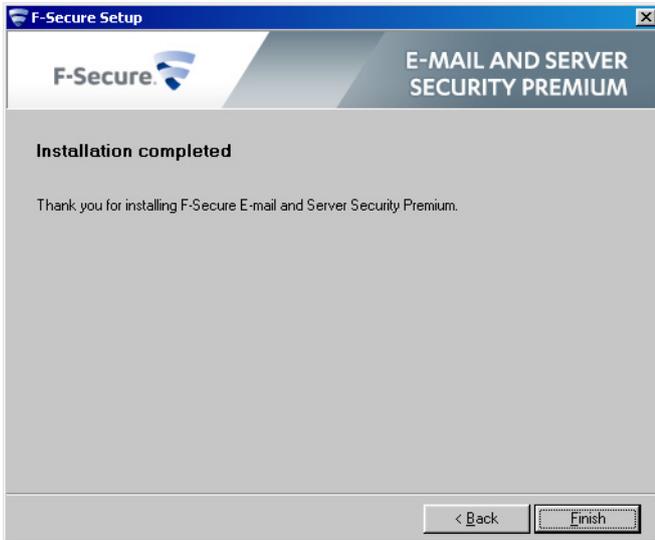
15. The list of components that will be installed is displayed, based on the keycode you use and the components that you selected earlier.



16. Click Start to install listed components. The installation will take a while.
17. When the installation is complete, the status of the installed components is displayed.



18. The installation is complete. Click Finish to close the Setup wizard.



Note: In some cases, you may need to restart the computer to complete the installation. We recommend that you restart the server as soon as possible, as the product does not protect the server before the restart.

4.2 UPGRADING FROM PREVIOUS PRODUCT VERSIONS

Follow these instructions to install the product if you have a previous version of F-Secure Anti-Virus for Windows Servers or F-Secure Anti-Virus for Microsoft Exchange installed.

4.2.1 UPGRADING FROM F-SECURE ANTI-VIRUS FOR WINDOWS SERVER

If you have F-Secure Anti-Virus for Windows Servers installed in your domain and you want to upgrade, we recommend that you upgrade to F-Secure Policy Manager to version 11.10 or later before installing E-mail and Server Security.

With F-Secure Policy Manager, you can use Upgrade command at F-Secure Policy Manager Console to deploy and upgrade the product. You can view information about the product both in antivirus mode and in advanced mode.

4.2.2 UPGRADING FROM F-SECURE ANTI-VIRUS FOR MICROSOFT EXCHANGE

If you have F-Secure Anti-Virus for Microsoft Exchange version 9.00 - 9.10, follow the standard installation instructions. When the installation asks for the Policy Manager settings, select Keep current.

Upgrading with Policy Manager 11.10

If you have F-Secure Anti-Virus for Microsoft Exchange installed in your domain and you want to upgrade, we recommend that you upgrade to F-Secure Policy Manager to version 11.10 or later before installing E-mail and Server Security.

With F-Secure Policy Manager, you can use Upgrade command at F-Secure Policy Manager Console to deploy and upgrade the product. You can view information about the product both in antivirus mode and in advanced mode.

Note: F-Secure Anti-Virus for Microsoft Exchange and F-Secure Anti-Virus for Microsoft SharePoint components are updated only if they are installed on the host already. You cannot add these components, but you can add or upgrade other components during the upgrade installation.

4.3 REGISTERING THE EVALUATION VERSION

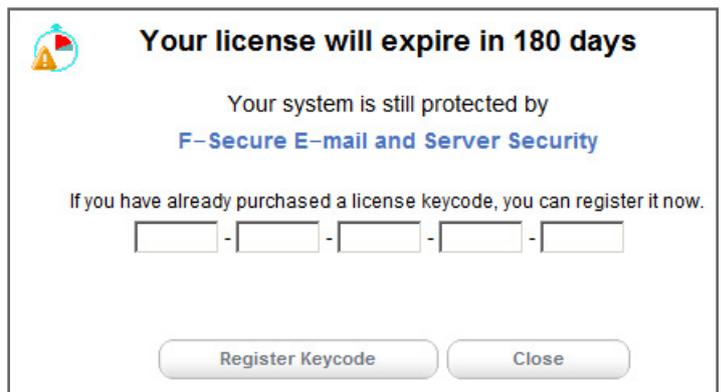
If you want to use the product after your evaluation period expires, you need a new keycode. Contact your software vendor or renew your license online.

Note: If you use F-Secure E-mail and Server Security keycode to register the product, but you have installed only the Server Security evaluation version, you need to run the installation again to add the missing components.

If you have installed F-Secure E-mail and Server Security evaluation version, you cannot use the Server Security keycode to register the product. Uninstall the evaluation version before you install the full Server Security product.

To register your new keycode:

1. Log in to the Web Console. The evaluation screen is opened.



2. Enter the new keycode you have received and click *Register Keycode*.

If you do not want to continue to use the product after your evaluation license expires, you should uninstall the software.

When the license expires, the product stops receiving anti-virus database updates, and processing e-mails and messages posted to public folders. However, the messages are still delivered to the recipients.

4.4 UNINSTALLING THE PRODUCT

To uninstall the product, select Remove Programs from the Windows Control Panel. We recommend that you uninstall the components in the following order. Skip components that you do not have installed:

1. F-Secure E-mail and Server Security - Anti-Virus for Microsoft SharePoint
2. F-Secure E-mail and Server Security - EMC CAVA support
3. F-Secure E-mail and Server Security - Offload Scanning Agent
4. F-Secure E-mail and Server Security - Spam control
5. F-Secure E-mail and Server Security - Anti-Virus for Microsoft Exchange
6. F-Secure E-mail and Server Security - Browsing protection
7. F-Secure E-mail and Server Security - Web traffic scanning
8. F-Secure E-mail and Server Security - DeepGuard
9. F-Secure E-mail and Server Security - Virus and spyware protection

Restart the server after you have uninstalled all components.

Note: Some files and directories may remain after the uninstallation and can be removed manually.

5. CONFIGURING THE PRODUCT

The product uses mostly default settings after the installation and the first update. We recommend that you go through all the settings of the installed components.

The product is fully functional only after it receives the first automatic update. The first update can take longer time than the following updates.

1. Open the Web Console to configure the product settings.
2. To make sure that the Real-time Protection Network is enabled, go to the Privacy page in the Web Console and select **Yes, I want to participate in the Real-time Protection Network**. With Real-time Protection Network, you benefit from the cloud-based F-Secure technology of exchanging information about threats with other participants all over the world.
3. Specify the IP addresses of hosts that belong to your organization. For more information, see [Network configuration](#).
4. Verify that the product is able to retrieve the virus and spam definition database updates. If necessary, reconfigure your firewalls or other devices that may block the database downloads. For more information, see [Network Requirements for E-mail and Server Security](#).
5. If the product is installed on the same computer with Microsoft Exchange Server 2010, which is in the Mailbox server role, specify the primary SMTP address for the account which is used to scan items in public folders. The user account must have permissions to access and modify items in the public folders.
6. If the organization has multiple Microsoft Exchange Server installations and Mailbox servers are deployed on dedicated servers, you have to configure the Hub Transport Role and Mailbox Role Servers so that quarantined messages can be delivered.

5.1 NETWORK CONFIGURATION

When you specify the IP addresses of hosts that belong to your organization, the product can use different settings to handle inbound, outbound, and internal mails.

Determine the mail direction as follows:

1. Use the Web Console to configure the mail direction.

The mail direction is based on the **Internal Domains** and **Internal SMTP senders** settings.

2. Specify internal mails.

Email messages are considered internal if they come from internal SMTP sender hosts and mail recipients belong to one of the specified internal domains (internal recipients).

- a. Specify **Internal Domains** and separate each domain name with a space. You can use an asterisk (*) as a wildcard. For example, ***example.com internal.example.net**.
- b. Specify all hosts within the organization that send messages to Exchange Edge or Hub servers via SMTP as **Internal SMTP Senders**. Separate each IP address with a space. An IP address range can be defined as:
 - a network/netmask pair (for example, 10.1.0.0/255.255.0.0), or
 - a network/nnn CIDR specification (for example, 10.1.0.0/16).

You can use an asterisk (*) to match any number or dash (-) to define a range of numbers.

Note: If end-users in the organization use other than Microsoft Outlook e-mail client to send and receive e-mail, it is recommended to specify all end-user workstations as Internal SMTP Senders.

Note: If the organization has Exchange Edge and Hub servers, the server with the Hub role installed should be added to the Internal SMTP Sender on the server where the Edge role is installed.

Note: Do not specify the server where the Edge role is installed as Internal SMTP Sender.

3. Specify outbound mails.

E-mail messages are considered outbound if they come from internal SMTP sender hosts and mail recipients do not belong to the specified internal domains (external recipients).

4. Specify inbound mails.

E-mail messages that come from hosts that are not defined as internal SMTP sender hosts are considered inbound.

5. E-mail messages submitted via MAPI or Pickup Folder are treated as if they are sent from the internal SMTP sender host.

Note: If e-mail messages come from internal SMTP sender hosts and contain both internal and external recipients, messages are split and processed as internal and outbound respectively.

5.2 CONFIGURING F-SECURE SPAM CONTROL

When F-Secure Spam Control is enabled, incoming messages that are considered as spam can be marked as spam automatically.

To mark mails as spam, the product adds an X-header with the spam flag or predefined text in the message header, so that end-users can create filtering rules that direct spam into a junk mail folder.

When the product stays connected to F-Secure Update Server, F-Secure Spam Control is always up-to-date. F-Secure Spam Control is fully functional only after it receives the first automatic update.

In Microsoft Exchange 2007 and 2010 environments, the Microsoft Exchange server can move messages to the Junk mail folder based on the spam confidence level value. This feature is available immediately after the product has been installed, if the end user has activated this functionality. For more information on how to configure this functionality at the end-user's workstations, consult the documentation of the used e-mail client.

SWITCH ON FREEDOM

**F-Secure is an online security and privacy company from Finland.
We offer millions of people around the globe the power to surf
invisibly and store and share stuff, safe from online threats.**

We are here to fight for digital freedom.

Join the movement and switch on freedom.

Founded in 1988, F-Secure is listed on NASDAQ OMX Helsinki Ltd.



F-Secure.