F-Secure Email and Server Security Deployment Guide

Contents

Chapter 1: Overview	4
1.1 How the product works	5
1.2 Product contents	5

Chapter 2: Deployment scenarios	7
2.1 Stand-alone server	8
2.2 Deploying the product with F-Secure Policy Manager	8
2.3 Multiple Exchange server roles	8
2.4 Large organization using multiple Exchange servers	9
2.5 Centralized quarantine management	9
2.5.1 Mixed mode authentication in the Microsoft SQL Server	10
2.6 Microsoft SharePoint server	10
2.7 Integrating Email Quarantine Manager	11
2.8 Allowing hosts to access the web console	14
2.9 Restricting website access to specific IP addresses	

Chapter 3: System requirements	
3.1 Operating system requirements	
3.2 Network requirements for Email and Server Security	21
3.3 Centralized management requirements	
3.4 Other system component requirements	
3.4.1 SQL Server requirements	
3.4.2 Spam engine requirements	23

Chapter 4: Installation24		
4.1 Installing the product locally	25	
4.2 Upgrading from the previous version of F-Secure Email and Server Security		
4.3 Uninstalling the product		

Chapter 5: Configuring the product		
5.1 Network configurat	ion	
5.2 Configuring F-Secu	re Spam Control	

Chapter 6: Deploying the product on a cluster		
6.1 Installation overview	35	
6.2 Creating quarantine storage	35	
6.2.1 Creating the quarantine storage for a single copy cluster Environment	35	
6.2.2 Creating the quarantine storage for a Continuous Cluster Replication environment	36	

6.2.3 Creating the quarantine storage for a Database Availability Group environment	
6.3 Installing the product	41
6.3.1 Installing on clusters with quarantine as cluster resource	41
6.3.2 Installing on clusters with quarantine on a dedicated computer	44
6.4 Administering the cluster installation with F-Secure Policy Manager	47
6.5 Using the quarantine in the cluster installation	48
6.6 Uninstallation	48
6.7 Troubleshooting	48

Appendix A: Installing Microsoft SQL Server.	
A.1 Installation steps	

Chapter

Overview

Topics:

- How the product works
- Product contents

F-Secure Email 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 emails usually contain a link to a browser exploit or a phishing website. F-Secure Email 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 email (SMTP), web surfing (HTTP and FTP-over-HTTP), and file transfer (FTP) traffic. Furthermore, it can be implemented on dedicated SharePoint servers and on the mail server level so that it does not only protect incoming and outgoing 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 email 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 product scans the messages and documents and handles any 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.

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



Figure 1: Email traffic

1.2 Product contents

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

The features that included with different product licenses:

Feature	F-Secure Email and Server Security	F-Secure Email and Server Security Premium
Malware protection	Х	Х

Feature	F-Secure Email and Server Security	F-Secure Email and Server Security Premium
DeepGuard	Х	Х
DataGuard		Х
Application control		X
Firewall	Х	X
Web traffic scanning	Х	X
Browsing protection	Х	Х
Software Updater		X
Offload Scanning Agent	Х	Х
Microsoft Exchange protection	Х	Х
Spam Control	Х	Х
Email Quarantine Manager	Х	Х
Microsoft SharePoint protection	X	X

Chapter

Deployment scenarios

Topics:

- Stand-alone server
- Deploying the product with F-Secure Policy Manager
- Multiple Exchange server roles
- Large organization using multiple Exchange servers
- Centralized quarantine management
- Microsoft SharePoint server
- Integrating Email Quarantine Manager
- Allowing hosts to access the web console
- Restricting website access to specific IP addresses

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.

Administration modes

You can deploy the product either in the standalone or centralized administration mode. In the standalone mode, the product is managed with Web Console that can be accessed also remotely. In the centralized administration mode, the product is monitored and managed typically with F-Secure Policy Manager Console.

Note: When you install the product for the first time, F-Secure Anti-Virus for Microsoft Exchange and F-Secure Anti-Virus for Microsoft SharePoint components must be configured during the installation. These configurations cannot be preconfigured with F-Secure Policy Manager, so they need to be installed with a locally run installation.

Local or centralized quarantine

F-Secure Email and Server Security can quarantine emails. You can install the quarantine either in the local or centralized mode. When the quarantine is installed locally, it uses a local folder to store the quarantined attachments and Microsoft SQL Server for the quarantine management. We recommend that the Microsoft SQL Server is installed locally.

When the quarantine is installed in the centralized mode, it can be shared by multiple instances of F-Secure Email and Server Security. It uses a file share for storing quarantined attachments and an instance of Microsoft SQL Server for the quarantine management.

Note: The quarantine mode can be installed in either the local or centralized mode, regardless of the standalone or centralized administration mode.

2.1 Stand-alone server

In corporations with one or two servers (Microsoft Exchange Server 2013/2016/2019) that hold all mailboxes, public folders and send and receive all incoming and outgoing messages over SMTP, you can administer each server in stand-alone mode.

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

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

- 1. Download the installation package (jar file) from the F-Secure website.
- 2. Import the package to Policy Manager.
- 3. Configure the package with your keycode and the selected features, and export it to an MSI package.
- Install F-Secure Email and Server Security using the exported MSI package.
 To install the product, login to the server with local administrative privileges and run the setup.
- 5. 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 the F-Secure website.
- 2. Import the remote installation package to F-Secure Policy Manager Console.
- 3. Install the product to the target servers.

Note: The initial installation should be done locally on the server. Upgrades can be then triggered from Policy Manager.

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

- 4. After the installation is complete, new hosts are automatically imported to the Policy Manager domain.
- Install Email and Server Security to servers running Microsoft Exchange Server and Microsoft SharePoint Server. Use the centralized administration mode and connect the product to the same Policy Manager.

2.3 Multiple Exchange server roles

Your organization has multiple Microsoft Exchange Server 2013/2016/2019 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.

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

- 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 updates to malware and spam databases from F-Secure Policy Manager Server, which receives updates from F-Secure Update Server.
- 4. Use the Web Console to manage and search quarantined content.

2.4 Large organization using multiple Exchange servers

Your organization has multiple Microsoft Exchange Server 2013/2016/2019 installations. All Exchange roles are deployed on dedicated servers. Mailbox servers are possibly clustered.



- Install the product to the server where Exchange Edge, Hub and Mailbox Server roles are deployed. Do not install the product to Client Access or Unified Messaging Server roles.
- 2. 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.

- 3. The product installations receive updates to malware and spam databases from F-Secure Policy Manager Server, which receives updates from F-Secure Update Server.
- 4. Use the Web Console to manage and search quarantined content.

2.5 Centralized quarantine management

Your organization has multiple Microsoft Exchange Server installations. For example, you have a network configuration with Edge and Mailbox roles running Exchange Server 2013/2016/2019.



- 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 email traffic, it is recommended to use a Microsoft SQL server installed on a separate server. When using the free Microsoft SQL Server 2014 SP2 Express included with the product, the Quarantine database size is limited to 10 GB, CPU utilization is limited to one processor or four cores, and memory utilization is limited to 1 GB.
- 3. Use the Web Console to manage and search quarantined content.

2.5.1 Mixed mode authentication in the Microsoft SQL Server

If you install Microsoft SQL Server 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.
- 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.

2.6 Microsoft SharePoint server

Your organization has one or several dedicated SharePoint Servers 2013/2016/2019.

 Install the product locally on all SharePoint machines with the Web Server role (SharePoint Web Front End server). This guarantees that on-access scanning protects the server.

Note: Redirected traffic does not pass through Email and Server Security in the Web Front End server role. If a Web Front End server redirects traffic to a different SharePoint role in the farm, the product must be installed on both the Web Front End server and the target SharePoint role.

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.

2.7 Integrating Email Quarantine Manager

This document provides basic information for setting up F-Secure Email Quarantine Manager (EQM).

This section explains the steps that are required to integrate the product with Internet Information Services (IIS) for use within your network.

After installing F-Secure Email and Server Security, you can find the EQM binaries in the following archive: <F-Secure installation folder>\Quarantine Manager\tools\eqm\eqm.zip.

Note: Some Web server (IIS) role services may be missing on your server. To complete the installation steps below, you may need to add the missing role services to Web server (IIS) using the Server Manager console.

- 1. In Administrative Tools, start Active Directory Users and Computers.
- 2. Create the EqmAllowed user group and add the required users to this group.
- 3. Create a folder named EQM under IIS and extract the contents of EQM.ZIP there (C:\inetpub\wwwroot\eqm).
- 4. In Administrative Tools, start Internet Information Services (IIS) Manager.
- 5. Right-click Default Web Site and select Add application.
- 6. Enter EQM in the Alias text field, and C:\inetpub\wwwroot\eqm in the Physical path text field.

Internet Information Services (I	IS) Manager	<u>_</u> _×
	Sites 🕨 Default Web Site 🕨	📃 🖸 🗟 🖓 I 🕐 🔹
File View Help		
Connections	Default Web Site Home Add Application ? X Site name: Default Web Site Path: / Alias: Application pool: EQM DefaultAppPool Select Example: sales Physical path: C: \netpub\wwwroot\eqm Pass-through authentication Connect as Test Settings OK Cancel Authentication Compression Default Directory Error Pages	Actions
Ready		W Help ▼

- 7. Select OK.
- 8. On the navigation pane, select EQM, and then on the right side, select Authentication.
- 9. Set the status for the authentication methods as follows:
 - Basic authentication: Enabled
 - Windows authentication: Enabled
 - All other methods: Disabled

Finternet Information Services (IIS) Manager	
	🔛 🖂 🟠 I 🕐 🔹
File View Help	
Connections Conne	Alerts
Configuration: "localhost' applicationHost.config , <location path="Default Web Site/EQM"></location>	€ <u>1</u> .:

- 10. On the navigation pane, select EQM, and then on the right side, select .NET Authorization Rules.
- **11.** Set the modes for the authorization rules as follows:
 - Administrators: Allow
 - EqmAllowed: Allow
 - All users: Deny

Number Information Services (II	5) Manager		
() ↓ TA232 ↓ Sites	▶ Default Web Site ▶ EQM ▶) 🖅 🖂 👔 I 🕐 👻
File View Help			
File View Help Connections Start Page Start Page S	INET Authorization Use this feature to specify rules for aut applications. Mode Users Allow Allow	horizing users to access Web sites and Roles Verbs Administrators EgmAllowed	Actions Add Allow Rule Add Deny Rule Edit Remove Related Features Users Roles Pelp Online Help
Configuration: 'Default Web Site FOM web	Features View		

Note: For Windows Server 2008 SP2 OS, you do not need to add the following rule: All Users: Deny.

- **12.** On the navigation pane, select **EQM**, and then on the right side, select **Connection Strings**.
- **13.** Under Connection Strings, update FSecureFqmConnectionString as follows:
 - a) Update the SQL server name or address. This is set to (local) by default, and fits to the scenario of SQL Express 2014 installation from the product package.
 - b) Update or define the password for FQMUSER.

Internet Information Services (115) Manager	Site > EOM >	
File Vew Help		
Connections Connections Start Page Application Page Application Page Constructions Application Page Constructions Application Page Constructions C	h Grouping Connection String Entry Type Connection String Connection String Connection String The Connection String Security Connection String Security Secure Grouping atted Security Content Connection String Security Connection String Security Content Connection String Connection String Security Content Connection String Content Connection String Connection String Security Content Connection String Content Connection String Connection String Connecti	Actions Add Edit Rename ➤ Remove ♥ Heb Online Heb Online Heb

14. Select OK.

15. For Windows server 2008 SP2 only: On the navigation pane, select **EQM** and then select **Mime Types**.

- a) In the Add MIME Type window, enter . svg in the File name extension field and image/svg+xml in the MIME type field.
- b) Select **OK**.

📲 Internet Information Services (II	S) Manager	
(→) (→) TA246 → Sites	► Default Web Site → EQM ►	💆 🖂 🏠 I 🕢 🛨
File View Help		
Vew Pep Connections Q Q Q Q Q <td>MIME Types Use this feature to manage the list of file name extensions and associated content types that are served as static files by the Web server.</td> <td>Add</td>	MIME Types Use this feature to manage the list of file name extensions and associated content types that are served as static files by the Web server.	Add
Configuration: 'Default Web Site/EQM' web	o.config	€ <u>1</u> .:

2.8 Allowing hosts to access the web console

To access the web console from other hosts in the network, you need to allow them via Internet Information Services (IIS).

To allow access to the web console for all hosts:

- 1. In Administrative Tools, start Internet Information Services (IIS) Manager.
- 2. Go to Sites > EssWebConsole.
- 3. Select Bindings.

Eile View Help	s > EssWebConsole >	2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2
Connections Conne	EssWebConsole Home Filter:	Actions Explore Edit Permissions Edit Site Bindings Wiew Applications View Virual Directories Manage Website © Restart ▷ Start Stop Browse Website © Browse (1:1):25023 (https)
	Authentic Compression Default Document Browsing HTTP Redirect Request Filtering SLAPI Filters Request SSL Settings Features View Content View	Advanced Settings Configure Failed Request Tracing Limits P Help

4. Click Add.

Connections		EssWebC	onsole H	lome			Actions
Start Page	Filter		. 76	o - Show A	Group by: Area	• ·	Explore Edit Permissions
 EXCH16 (EXCH1616\adminis Application Pools Sites 	Site Binding	js			Group by. Area	? >	Edit Site Bindings
 Solution Solution<	Type https	Host Name	Port 25023	IP Address 127.0.0.1	Binding Informa	Add	View Applications View Virtual Directories
	https		25023	[::1]		Remove	Manage Website
							Stop Browse Website Browse 127.0.0.1:25023 (https) Browse [::1]:25023 (https)
							Advanced Settings Configure
							Failed Request Tracing Limits
						Close	🕖 Help

5. Select https as the Type, enter the IP address for the server, and set the Port to 25023.

e	Edit Site Binding			?	×	
s	Туре:	IP address:	Port:			
)S	https	v 1.2.3.4	~ 25023			
3	Host name:					/e
					s	e
	nequire serv	ver Name Indication				
	SSL certificate:	ver Name Indication				
	SSL certificate:	Console Self Signed Cert	✓ Select	View		

6. Select the SSL certificate, then click OK.

Note: SSL 2.0 certificates are not supported due to vulnerabilities.

2.9 Restricting website access to specific IP addresses

After allowing access to the web console from other hosts in your network, you may want to restrict the access to a specific IP address or IP range.

To allow only specific hosts to access the web console:

1. Make sure that the IP and Domain Restrictions feature is installed for Internet Information Services (IIS).

elect server role	S	DESTINATION SERVER exch16.exch16.rdc.gtr
Before You Begin Installation Type	Select one or more roles to install on the selected server. Roles	Description
Server Selection	↓ Volume Activation Services ✓ Web Server (IIS) (26 of 43 installed)	IP and Domain Restrictions allow you to enable or deny content base
Server Roles	 ✓ Web Server (10) (20 of 45 installed) ✓ Web Server (20 of 34 installed) 	upon the originating IP address or
Confirmation	 Common HTTP Features (5 of 6 installed) Health and Diagnostics (4 of 6 installed) 	domain name of the request. Instea of using groups, roles, or NTFS file
Daraile	Performance (Installed)	system permissions to control acces
	 Secting (5 of 9 installed) Request Filtering (Installed) Basic Authentication (Installed) Centralized SSL Certificate Support Client Certificate Mapping Authentication IIS Client Certificate Mapping Authentication IIS Client Certificate Mapping Authentication IV and Domain Restrictions URL Authorization Windows Authentication (Installed) Application Development (4 of 11 installed) FTP Server Management Tools (6 of 7 installed) 	addresses or domain names.

2. Go to Sites > EssWebConsole.

3. Open IP and Domain Restrictions.

Filter:		• 🔻 Go 🔹 🕻	Show All	Group by: Ar	ea	•	
ASP.NET – .NET Authorizat	.NET Compilation	.NET Error Pages	.NET Globalization	.NET Profile	.NET Roles	.NET Trust Levels	~
.NET Users	Application Settings	Connection Strings	Machine Key	Pages and Controls	Providers	Session State	
MTP E-mail							
IIS Authentic	Compression	Default	Directory Browsing	404 Error Pages	Failed Request Tra	Handler Mappings	~

4. Select Add Allow Entry.

5. Enter the IP address or IP range.

our bur	Add Allow Restriction Rule	?	×		Remove
odp by:	Allow access for the following IP address or domain name:		-	_	Revert To Parent View Ordered List
ow	Specific IP address: 1.2.3.4	1			Edit Dynamic Restriction Settings
	O IP address range:			0	Help
	Mark ar Drofin]			
]			
	ОК	Cancel			

Note: Make sure that you add the local IP address if you need to open the web console locally.

- 6. Click **OK**.
- 7. Select Edit feature settings.

8. Set Access for unspecified clients to Deny.

	Addross and Domain Postrictions	Actions
Jse this featu	Address and Domain Restrictions ure to restrict or grant access to Web content based on IP addresses or d	omain names. Set the
Group by:	No Grouping	Edit Festure Settings
Mode	Requestor Entry Type	Revert To Parent
Allow	¹ Edit IP and Domain Restrictions Settings ? X	Edit Dynamic Restriction
	Access for unspecified clients:	Help
	Deny ~	Cherp
	Enable Proxy Mode Deny Action Type: Forbidden OK Cancel	

9. Click OK.

10. Restart the EssWebConsole site.

Chapter

System requirements

Topics:

- Operating system requirements
- Network requirements for Email and Server Security
- Centralized management requirements
- Other system component requirements

3.1 Operating system requirements

The product can be installed on any computer that meets the requirements for the supported operating system.

Operating system:

- **Note:** Microsoft .NET 4.7.2 must be installed on the system.
- Microsoft[®] Windows Server 2008 R2
- Microsoft[®] Windows Small Business Server 2011
- Microsoft[®] Windows Server 2012
- Microsoft[®] Windows Server 2012 Essentials
- Microsoft[®] Windows Server 2012 R2
- Microsoft[®] Windows Server 2012 R2 Essentials
- Microsoft[®] Windows Server 2012 R2 Foundation
- Microsoft[®] Windows Server 2016 Standard
- Microsoft[®] Windows Server 2016 Essentials
- Microsoft[®] Windows Server 2016 Datacenter
- Microsoft[®] Windows Server 2016 Core
- Microsoft[®] Windows Server 2019 Standard
- Microsoft[®] Windows Server 2019 Essentials
- Microsoft[®] Windows Server 2019 Datacenter
 - Microsoft[®] Windows Server 2019 Core

Note: Windows Server 2016 Nano is not supported.

All Microsoft Windows Server editions are supported except:

- Windows Server for Itanium processor
- Windows HPC editions for specific hardware
- Windows Storage editions
- Windows MultiPoint Server
- Windows Home Server

Note: All operating systems are required to have the latest Service Pack installed.

Note: For performance and security reasons, you can install the product only on an NTFS partition.

- Supported Microsoft Exchange Server versions:
- Microsoft[®] Exchange Server 2013 without service pack, service pack 1 (CU23, CU22, CU21)
- Microsoft[®] Exchange Server 2016 (CU15, CU14, CU13, CU12, CU11)
- Microsoft[®] Exchange Server 2019 (CU3, CU2, CU1)

The cumulative updates (CU) that support .NET Framework 4.7.2 are indicated in parentheses. For more detailed information, see the Microsoft support pages.

Note: Microsoft Exchange Server 2013 SP1 requires a special fix, which allows third-party or custom-developed transport agents to be installed correctly. The fix and its installation instructions are available in Microsoft Knowledge Base article 2938053.

Supported Microsoft SharePoint Server versions:

- Microsoft[®] SharePoint 2013 with the latest service pack
- Microsoft[®] SharePoint 2016
- Microsoft[®] SharePoint 2019

Supported terminal servers:	• Microsoft Windows Terminal/RDP Services (on the above mentioned Windows Server platforms)
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 Security Cloud
Web browser:	 Microsoft Internet Explorer 11 Mozilla Firefox (up-to-date versions) Google Chrome (up-to-date versions)

To use Email Quarantine Manager, you need Microsoft Internet Information Server running in your environment. This is available as part of Microsoft Exchange Server.

Cluster environments

The current version of the product supports Microsoft Exchange Server 2013, 2016, and 2019 high-availability solutions based on Database Availability Groups (DAG).

3.2 Network requirements for Email 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 Email and Server Security WebUI	W3wp.exe / IIS Worker Process	25023	DNS (53, UDP and TCP), 1433 (TCP), only with the dedicated SQL server
F-Secure Host Process	%ProgramFiles%\F-Secure\Email and Server Security\fshoster32.exe	-	DNS (53, UDP and TCP), HTTP (80), HTTPS (443) or another port used for HTTP(S) proxy
F-Secure Quarantine Manager	%ProgramFiles%\F-Secure\Email and Server Security\Anti-Virus For Microsoft Services\F-Secure.Ess.Fqm.exe	-	DNS (53, UDP/TCP), 1433 (TCP), only with the dedicated SQL server
F-Secure ORSP Client	%ProgramFiles%\F-Secure\Email and Server Security\Ultralight\ulcore\ <update number>\fsorsp64.exe</update 	-	DNS (53, UDP/TCP), HTTP (80) or another port used for HTTP proxy
F-Secure Software Updater	%ProgramFiles%\F-Secure\Email and Server Security\swup\fssua.exe	-	DNS (53, UDP/TCP), HTTPS (443), HTTP (80) or another port used for HTTP proxy

3.3 Centralized management requirements

F-Secure Policy Manager 14.30 is required to centrally manage F-Secure Email and Server Security version 14.x.

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

F-Secure Email and Server Security requires Microsoft SQL Server for the email quarantine management. Depending on the selected deployment and administration method, you may need 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:

- 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 2014
- Microsoft SQL Server 2016
- Microsoft SQL Server 2017
- Microsoft SQL Server 2019

Important: We do not recommend that you use MSDE or Microsoft SQL Server Express Edition with the centralized quarantine management or if your organization sends and receives a large amount of emails.

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 incoming and outgoing 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



Important: If you are using a previous version of F-Secure Email and Server Security and you use Microsoft SQL Server 2005 for the quarantine, update Microsoft SQL Server to version 2008 R2 or later before you update F-Secure Email and Server Security.

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

Microsoft SQL Server Express Edition

- When using Microsoft SQL Server Express Edition, the quarantine database size is limited to 10 GB.
- It is **not** recommended to use Microsoft SQL Server Express Edition if you are planning to use centralized quarantine management with multiple product installations.

Microsoft SQL Server

- If your organization sends and receives a large amount of emails, it is recommended to use the licensed version of Microsoft SQL Server.
- 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, you must purchase it and obtain your own license before you deploy the product. To purchase Microsoft SQL Server, contact your Microsoft reseller.

3.4.2 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.

Chapter



Installation

Topics:

- Installing the product locally
- Upgrading from the previous version of F-Secure Email and Server Security
- Uninstalling the product

4.1 Installing the product locally

Follow these instructions to install the product.

Use a user account that meets the following conditions for installation:

Microsoft Exchange

- The account must belong to the local Administrators group
- The account must have access rights to add and configure applications in the Program Files folder
- The account must have permission to install and configure local services
- The account must have permission to run PowerShell scripts
- The account must be a member of the Organization Management role group this can be added in the Microsoft Exchange security group or via Exchange admin center (EAC) > Permissions

Microsoft SharePoint

- The account must belong to the local **Administrators** group
- For scanning and service access (the credentials are entered during installation or using the configuration tool after installation):
 - The account must belong to the Farm Administrators SharePoint Group
 - The account must have the Logon as a service privilege switched on
- 1. Download the installation file exported from F-Secure Policy Manager.
- 2. Run the installation file to start the installation.

F-Secure Email and Server Security		×
F-Secure Email and Server Security		
To complete the installation, there are a few steps needed to configure your pro	duct.	
Continue		

3. When you install the Microsoft SharePoint component, enter the account details to manage Microsoft Sharepoint. This account needs local administrative permissions on the SharePoint server.

		_
	Product Setup 1/1	
Enter the details for a ShareP required to allow the product	oint management account that has read-write permissions. Th t to scan content stored on SharePoint.	nis is
User name:	Password:]
Domain:		
Domain: If you are using a local user account, yo	ou do not need to enter a domain	
Domain: If you are using a local user account, yo	ou do not need to enter a domain	
Domain: If you are using a local user account, yo	ou do not need to enter a domain	
Domain: If you are using a local user account, yo	ou do not need to enter a domain	
Domain: If you are using a local user account, yo	Done	

4. When you install the Microsoft Exchange component, start by entering your SQL Server configuration.

Secure Email and Server Security		_ □
	Product Setup 1/7	
Enter the computer nar Enter the password of t	ne of the SQL Server where you want to create the he database server administrator (sa) for logging in	quarantine database. 1 to the server.
SQL Server name:		Browse
User name:	Password:	
sa		
	Continue	
	Back	

F-Secure Email and Server Security					- 0	×
	Product Setu	ip 1/7	7			
Enter the computer nar Enter the password of t SQL Server name: User name: sa	Select SQL server to connect to TA73\SQLEXPRESS TA73\SQLSERVER17	-		×	rantine database. the server. Browse	
	OK <u>Cancel</u>					
L	Back]	

Click **Browse** to select the server from a list of automatically detected options.

5. Enter the quarantine database name.

♥ F-Secure Email and Server Security -		×
Product Setup 2/7		
Enter the name of the SQL database that will store the information on quarantined emails attachments.	and	
Database name:		
FSMSE_Quarantine		
Continue		
Back		

If the database name that you enter already exists, choose how to proceed.



6. Enter the user credentials to use for the quarantine database.

-Secure Email and Server Security			-	
Р	roduct Set	up 4/7		
Enter the user name and passwor specified account does not exist,	d to use for connecti it will be created auto	ng to the quarantined datab matically during installation	ase. If the	
User name:				
Password:	Cont	irm password:		
•••••	••	•••••		
	Continue			
	Back			
				_

7. Select how you want to manage the quarantine.



- 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.
- 8. Enter the path to the quarantine directory.

F-Secure Email and Server Security	-		×
Product Setup 6/7			
Enter the path to the directory where quarantined email messages and attachn placed. If you are installing the product to a cluster node, make sure that the q is located on the shared disk. Quarantine Directory:	nents will be uarantine dire	ectory	
C:\ProgramData\F-Secure\EssQuarantine	Browse		
Continue			
UGLA			

9. Enter the SMTP address if necessary.

Note: The address is detected automatically using Active Directory, but you can override it if necessary.

F-Secure Email and Server Security	_		<
Product Setup 7/7			
Enter a valid SMTP address. This address will be used by F-Secure Anti-Virus for Mic Exchange to send warning and informational messages to the users (recipients, sen owners, etc.). To ensure proper reporting, this SMTP address should exist in the organization and allowed to send email messages.	rosoft ders, mailb should be	ox	
Reporting SMTP address:			
Administrator@ex16.psbess.rdc.gtn			
Done			
Back			

10. Click Done to complete the installation.

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.

Note: After installing the product on Windows Server 2016 or newer, you need to explicitly disable or uninstall Windows Defender.

If you need to reconfigure the products, you can run the following configuration tool using a Windows admin account to start this configuration wizard later on: C:\Program Files (x86)\F-Secure\Email and Server Security\ui\F-Secure.Ess.Config.exe

4.2 Upgrading from the previous version of F-Secure Email and Server Security

To upgrade the product, you can use the installation MSI package or run the operation from Policy Manager.



Note: During upgrades, the product restarts IIS on the servers with SharePoint and Microsoft Exchange Transport to register the new scanner and new transport agent respectively.

Supported upgrade methods

For Microsoft Exchange:

- Local upgrade using MSI
- Local silent upgrade using MSI
- Policy-based upgrade from Policy Manager •

Note: For policy-based upgrades, always use the **Upgrade** link in Policy Manager Console.



For Microsoft SharePoint:

- Local upgrade using MSI
- Local silent upgrade using MSI

Note: Policy-based upgrades are not supported for Microsoft SharePoint protection.



4.3 Uninstalling the product

You can uninstall the product via Windows Control Panel.

To uninstall the product:

- 1. Go to Windows Control Panel > Programs and features.
- 2. Select F-Secure Email and Server Security Premium (standard) and select Uninstall.

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

Chapter

Configuring the product

Topics:

- Network configuration
- Configuring F-Secure Spam Control

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. If you plan to manage the product with other computers through Web Console, follow the instructions in Allowing hosts to access the web console on page 14.
- **3.** Specify the IP addresses of hosts that belong to your organization. For more information, see Network configuration on page 33.
- **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 Email and Server Security on page 21.

5. 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 incoming, outgoing, 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),
- a network/nnn CIDR specification (for example, 10.1.0.0/16), or
- IPv6 address (for example, 1::, 2001::765d 2001::0-5, 2001:db8:abcd:0012::0/64, 2001:db8:abcd:abcd::/52, ::1).

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 email client to send and receive email, 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 outgoing mails.

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

4. Specify incoming mails.

Email messages that come from hosts that are not defined as internal SMTP sender hosts are considered incoming.

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

Note: If email 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.

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 email client.

Chapter

6

Deploying the product on a cluster

Topics:

- Installation overview
- Creating quarantine storage
- Installing the product
- Administering the cluster installation with F-Secure Policy Manager
- Using the quarantine in the cluster installation
- Uninstallation
- Troubleshooting

6.1 Installation overview

Follow these steps to deploy and use the product on a cluster.

- Install F-Secure Policy Manager on a dedicated server. If you already have F-Secure Policy Manager installed in the network, you can use it to administer the product. For more information, see F-Secure Policy Manager Administrator's Guide.
- 2. Install Microsoft SQL Server 2008, 2012, 2014, or 2016 on a dedicated server. Microsoft SQL Server must be installed with the mixed authentication mode (Windows Authentication and SQL Server Authentication). After the installation, make sure that **Named Pipes** and **TCP/IP protocols** are enabled in SQL Server network configuration.
- 3. Create the quarantine storage where the product will place quarantined email messages and attachments.
 - In the Single Copy Cluster (SCC) environment, continue to Creating the quarantine storage for a single copy cluster Environment on page 35.
 - In the Continuous Cluster Replication (CCR) environment, continue to Creating the quarantine storage for a Continuous Cluster Replication environment on page 36.
 - In the Database Availability Group (DAG) environment continue to Creating the quarantine storage for a Database Availability Group environment on page 39.
- **4.** Install the product locally on one node at the time in the centralized administration mode, starting from the active node. Make sure the product is fully up and running before starting the installation on the passive node.



Note: Do not move cluster resources to the passive node before you install the product at all passive nodes first.

- In the environment with Quarantine as cluster resource, see more information on Installing on clusters with quarantine as cluster resource on page 41.
- In the environment with Quarantine on dedicated computer, see more information on Installing on clusters with quarantine on a dedicated computer on page 44.
- Create a policy domain for the cluster in F-Secure Policy Manager and import cluster nodes there. See Administering the cluster installation with F-Secure Policy Manager on page 47. For more information, see the Policy Manager documentation.
- 6. Log on to each node and configure IIS to accept connections from authorized hosts. See Allowing hosts to access the web console on page 14.
- **7.** To use the spam detection engine, permit **outgoing** HTTPS connections to **aspam.sp.f-secure.com** (TCP port 443) in your firewall rules.

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

6.2 Creating quarantine storage

Follow instructions in this section to create the Quarantine Storage in the cluster environment.

6.2.1 Creating the quarantine storage for a single copy cluster Environment

For single copy cluster, the Quarantine Storage can be created on a dedicated computer or as a cluster resource.

To install the Quarantine Storage on a dedicated computer, see Creating the quarantine storage for a Continuous Cluster Replication environment on page 36 for more instructions.

To install Quarantine Storage as a cluster resource, follow these instructions:

- 1. Log on to the active node of the cluster with the domain administrator account.
- 2. Create a directory for the quarantine storage on the physical disk shared by the cluster nodes.

You can create it on the same disk where the Exchange Server storage and logs are located.

3. After the quarantine directory is created, it has to be shared. When you share the quarantine directory, it becomes visible in the Failover Cluster Manager. To share the directory, right-click the quarantine folder and select Share.

102 · 2	
Choose people on your network to share w	ith
Type the name of the person you want to sha	re with and then click Add, or click the arrow to find people
or share with everyone.	
	► Add
Name	Permission Level
👗 Administrator	Owner 🖛
Administrators	Contributor 🔻
😹 Exchange Servers	Contributor 🔻
SYSTEM	Contributor 🔻
Tell me about different ways to share in Wind	<u>ows.</u>

Add **Administrators**, **Exchange Servers** and **SYSTEM** with **Contributor** permission levels. Press **Share** to close the window and enable the share.

4. Check that everything is configured correctly. The Failover Cluster Manager view should look like this:

ailover Cluster Manager	LHCLUMB					1	Actions
LHCLUSTER.mse2007	Summa Status: Online	ry of LHCLU	мв				.HCLUMB Bring this service or Take this service or Show the critical ev
Curter Events	Alerts: <none> Preferred Owne Current Owner:</none>	rs: LHCLU1; LHC LHCLU2	CLU2				Move this service or Manage shares and
En Cluster Evenes	Name		Statu	5			Add storage
	E In Name: LH	CLUMB	💽 Or	line			 Add a resource Show Dependency I View
	FileServer Disk Drives	(LHCLUMB)(M\$)	💿 Or	line		8	K Delete Rename
	🗄 🕮 Data		💿 Or	line		-	Ca Rerresh
	Shared Foldore						Properties
	Share Name	Folder Path	Tune	# Client Conn	Description		🛛 Help
	M\$	M:\	Windows	0	Default share	- I	Quarantine
	👰 Quarantin	e M:\Quarantine	e Windows	0			🗙 Stop Sharing
						1	a Refresh
						1	Properties

5. During the product installation, select the quarantine share you just created when the installation asks for the quarantine path.

Use the UNC path in form of \\CLUSTERNAME\QUARANTINE. (In the example above, \\LHCLUMB\Quarantine.)

6.2.2 Creating the quarantine storage for a Continuous Cluster Replication environment

For a Continuous Cluster Replication (CCR) cluster installation, the quarantine storage must be set on a dedicated computer. This computer has to be a member in the same domain with Exchange Servers.

- 1. Log on to the server where you plan to create the quarantine storage (for example, APPSERVER) with the domain administrator account.
- 2. Open Windows Explorer and create a directory (for example, C:\Quarantine) for the quarantine storage on the physical disk.
- 3. Right-click the directory and select Sharing and Security.
- 4. Go to the Sharing tab.

General Sharing Security Customize Vou can share this folder with other users on your network. To enable sharing for this folder, click Share this folder. O pot share this folder Do not share this folder Share name: FSAVMSEQS\$ Comment:	iarantine Proper	ties		<u>?</u> >
You can share this folder with other users on your network. To enable sharing for this folder, click Share this folder. Do not share this folder Share this folder Share name: FSAVMSEQS\$ Comment: User limit: Maximum allowed Allow this number of users: Image: Permissions To set permissions for users who access this folder over the network, click Permissions. Permissions To configure settings for offline access, click Caching	General Sharing	Security Customize	1	
 ○ Do not share this folder ● Share this folder Share name: FSAVMSEQS\$ © comment: User limit: ● Maximum allowed ○ Allow this number of users: ■ To set permissions for users who access this folder over the network, click Permissions. To configure settings for offline access, click Caching. 	You can network. folder.	share this folder with o To enable sharing for	other users on your r this folder, click Share	this
	C Do <u>n</u> ot share	e this folder		
Share name: FSAVMSEQS\$ Comment:	─● Share this for	lder		
Comment:	S <u>h</u> are name:	FSAVMSEQS\$		
User limit:	Comment:			-
Oser limit. Imaximum allowed O Allow this number of users: Imaximum allowed To set permissions for users who access this folder over the network, click Permissions. Permissions To configure settings for offline access, click Caching. Caching	—	C. N		
To set permissions for users who access this folder over the network, click Permissions. To configure settings for offline access, click Caching.	User limit:	Maximum allowed	- (-
To set permissions for users who access this folder over the network, click Permissions. To configure settings for offline access, click Caching Caching.		Allow this number of the second se	or users:	
To configure settings for offline access, click Caching Caching.	To set permissio folder over the n	ns for users who acces etwork, click Permissio	ss this <u>P</u> ermissions	
	To configure sel Caching.	tings for offline access	; click Caching	
OK Cancel Apolu		ΠΚ	Cancel An	nlu

a. Type FSAVMSEQS\$ as the share name and F-Secure Quarantine Storage as comment.

Note: The dollar (\$) character at the end of the share name makes the share hidden when you view the network resources of the cluster with Windows Explorer.

b. Make sure that **User Limit** is set to **Maximum allowed**.

Click **Permissions** to set permissions.

- 5. Change permissions as follows:
 - **a.** Remove all existing groups and users.
 - b. Add Administrator, Exchange Domain Servers and SYSTEM to the Group or user names list.
 - c. Grant Change and Read permissions for Exchange Domain Servers and SYSTEM.

d. Grant Full Control, Change and Read permissions for the Administrator account.

Permissions for FSAVMSEQS	\$	×
Share Permissions		
Group or user names:		
Administrator (Administrator & Exchange Servers (E10W0) & SYSTEM	≥e10w08r2c.local) 3R2C\Exchange Se	ervers)
	A <u>d</u> d	<u>R</u> emove
Permissions for Administrator	Allow	Deny
Full Control		
Change Bead		
Learn about access control and r	permissions	
		1
UK	Cancel	

Click **OK** to continue.

- 6. Go to the Security tab.
 - **a.** Remove all existing groups and users.
 - b. Add Administrator, Exchange Domain Servers and SYSTEM to the Group or user names list.
 - c. Grant all except Full Control permissions for Exchange Domain Servers and SYSTEM.
 - **d.** Grant all permissions for the **Administrator** account.

🕌 Permissions for Quarantine		×
Security		
Object name: C:\Quarantine		
<u>G</u> roup or user names:		
👗 Administrator (Administrator@	e10w08r2c.local)	
SYSTEM	R2C\Exchange S	ervers)
1	A <u>d</u> d	<u>R</u> emove
Permissions for Administrator	Allow	Deny
Full control	$\mathbf{\nabla}$	
Modify	\checkmark	
Read & execute	\checkmark	
List folder contents	\checkmark	
Read		
Learn about access control and p		
	ermissions	

Click **OK** to finish.

To make sure that the quarantine storage is accessible, follow these instructions:

- 1. Log on as the domain administrator to any node of the cluster.
- 2. Try to open \\<Server>\FSAVMSEQS\$\ with Windows Explorer, where <Server> is the name of the server where you just created the quarantine storage share.

6.2.3 Creating the quarantine storage for a Database Availability Group environment

For the Database Availability Group (DAG) installation, the quarantine storage must be set on a dedicated computer. This computer has to be a member in the same domain with Exchange Servers.

- **1.** Log on to the server where you will create the quarantine storage (for example, APPSERVER) with the domain administrator account.
- 2. Open Windows Explorer and create a directory (for example, C:\Quarantine) for the quarantine storage.
- 3. Right-click the directory and select **Properties** from the menu.
- 4. Go to the Sharing tab.

📙 Quarantine Properties	×
General Sharing Security Previous Versions Cus	tomize
Network File and Folder Sharing	
Not Shared	
<u>N</u> etwork Path: Not Shared	
Share	
Advanced Sharing	
Set custom permissions, create multiple shares, and advanced sharing options.	set other
🚱 A <u>d</u> vanced Sharing	
	(

- 5. Click Advanced Sharing to share the directory.
- 6. Select Share this folder.

Advanced Sharing
☑ Share this folder
Settings
Share name:
FSAVMSEQS\$
Add Remove
Limit the number of simultaneous users to:
Comments: F-Secure Quarantine Storage
Permissions Caching
OK Cancel Apply

a. Type FSAVMSEQS\$ as the share name and F-Secure Quarantine Storage as a comment.



Note: The dollar (\$) character at the end of the share name hides the share when you view the network resources of the cluster with Windows Explorer.

- **b.** Make sure that **User Limit** is set to Maximum that is allowed (16777216).
- 7. Click **Permissions** to set permissions for the share.
- 8. Change permissions as follows:

- **a.** Remove all existing groups and users.
- **b.** Add Administrator, Exchange Servers and SYSTEM to the Group or user names list.
- c. Grant Change and Read permissions for Exchange Servers and SYSTEM.
- d. Grant Full Control, Change and Read permissions for the Administrator account.

Permissions for FSAVMSEQ5\$? ×
Share Permissions		
<u>Group or user names:</u> Administrator (TESTVDOM2) Exchange Domain Servers (T SYSTEM	Administrator) ESTVDOM2\Exc	hange Dom
Permissions for Administrator	A <u>d</u> d	<u>R</u> emove
Full Control Change Read	2	
OK	Cancel	Apply

- 9. Click OK to continue.
- 10. Go to the Security tab and click Edit.
 - **a.** Remove all existing groups and users.
 - **b.** Add Administrator, Exchange Servers and SYSTEM to the Group or user names list.
 - c. Grant all except Full Control permissions for Exchange Servers and SYSTEM.

d. Grant all permissions for the Administrator account.

uarantine Properties		?
General Sharing Security Cust	tomize	
Group or user names:		
Administrator (TESTVD0M2 Exchange Domain Servers (SYSTEM	\Administrator) TESTVD0M2\Exc	change Dom
Permissions for Administrator	A <u>d</u> d	<u>R</u> emove Deny
Full Control Modify Read & Execute List Folder Contents Read Write		
For special permissions or for adva click Advanced.	anced settings,	Advanced
ОК	Cancel	Apply

11. Click OK to continue.

After you have configured the quarantine storage, make sure that it is accessible. Follow these instructions:

- 1. Log on as the domain administrator to any node of the cluster.
- 2. Open \\<Server>\FSAVMSEQS\$\ with Windows Explorer, where <Server> is the name of the server where you created the guarantine storage share.

6.3 Installing the product

Follow the instructions in this section to install the product on CCR, SCC, and DAG installations.

6.3.1 Installing on clusters with quarantine as cluster resource

This section describes how to install the product on clusters where quarantine is configured as cluster resource in Exchange Virtual Server.

- 1. Log on to the active node of the cluster using a domain administrator account.
- 2. Run F-Secure Email and Server Security setup wizard.

For more information, see Installing the product locally on page 25.

3. Select the Microsoft SQL Server to use for the quarantine database, then click **Continue**.

 F-Secure Email and Server Security 		– 🗆 ×
Pr	roduct Setup 1/7	
Enter the computer name of the SC Enter the password of the database SOL Server name:	QL Server where you want to create the server administrator (sa) for logging	e quarantine database. in to the server.
		Browse
User name:	Password:	
sa		
	Continue	
	Back	

4. Enter the quarantine database name, then click **Continue**.

-Secure Email and Server Security			-		;
Produc	t Setup 2/	7			
Enter the name of the SQL database that wil attachments.	store the informatio	n on quarantined er	nails an	d	
Database name:					
FSMSE_Quarantine					
_					
	Continue				
	Back				

5. Enter the user credentials to use for accessing the database, then click **Continue**.

F-Secure Email and Server Security		-		2
Prod	uct Setup 4/7			
Enter the user name and password to us specified account does not exist, it will b	e for connecting to the quarantined databa e created automatically during installation.	se. If the	e	
User name:				
fqmuser				
Password:	Confirm password:			
•••••	•••••			
	Continue			
	Back			

6. Select Centralized quarantine management as the quarantine management method, then click Continue.

F-Secure Email and Server Security	-		×
Product Setup 5/7			
Select the quarantine management method:			
 Local quarantine management: Select this option if you plan to install only one instance of the product or if you do not want to n quarantined mails centrally. Centralized quarantine management: Select this option if you plan to install multiple instances of the product and manage quarantined single web console. To manage quarantined emails from multiple servers, the product requires a comm 	nanage mails from non quara	a ntine	
database and a network share for storing quarantined items. A network share is cru server.	ated on e	each	
Continue Back			

7. The setup wizard asks for the location of the quarantine directory.

F-Secure Email and Server Security	-		×
Product Setup 6/7			
Enter the path to the directory where quarantined email messages and attach placed. If you are installing the product to a cluster node, make sure that the is located on the shared disk. Quarantine Directory:	iments will be quarantine dire	ectory	
C:\ProgramData\F-Secure\EssQuarantine	Browse		
Continue			
Back			

Specify the UNC path to the Quarantine Storage share that you created before the installation as the Quarantine Directory. For example, $\$ SAVMSEQS\$, where SVSName is the network name of your Exchange Virtual Server.

Click Continue.

- 8. Complete the installation on the active node.
- 9. Log on to the passive node of the cluster using a domain administrator account. Repeat the steps given above.
- 10. After you specify the SQL Server to use, the setup wizard asks you to specify the quarantine database.

Product Setup 3/7			
tup has detected that a database with the specified name already exists. Select llowing options to continue:	one of th	e	
Use existing database.			
Remove the existing database and create a new one with the specified name.			
Keep the existing database and create a new database with another name:			
Continuo			
Continue			
Back			

Select Use existing database and click Continue.

11. Complete the installation on the passive node.

6.3.2 Installing on clusters with quarantine on a dedicated computer

This section describes how to install the product on clusters where Quarantine is installed on a dedicated computer.

- 1. Log on to the first node of the cluster using a domain administrator account.
- 2. Run F-Secure Email and Server Security setup wizard.

For more information, see Installing the product locally on page 25.

3. Select the Microsoft SQL Server to use for the quarantine database, then click **Continue**.

F-Secure Email and Server Security		- 🗆	×
	Product Setup 1/7		
Enter the computer name of th Enter the password of the data	e SQL Server where you want to create the base server administrator (sa) for logging in	quarantine database. to the server.	
SQL Server name:		Browse	
User name:	Password:		
sa			
	Continue		
	Back		

4. Enter the quarantine database name, then click **Continue**.

Secure Email and Server Security				/=		×
	Product	Setup	2/7			
Enter the name of the SQL da attachments.	tabase that will s	tore the infor	mation on quarar	tined emails	and	
Database name:						
FSMSE_Quarantine						
	Co	ontinue				
		Back				

5. Enter the user credentials to use for accessing the database, then click **Continue**.

F-Secure Email and Server Security		-		×	
Produc	t Setup 4/7				
Enter the user name and password to use for specified account does not exist, it will be cre	connecting to the quarantined databas ated automatically during installation.	se. If the	e		
User name:					
fqmuser					
Password:	Confirm password:				
••••••					
	Continue				
	Back				

6. Select Centralized quarantine management as the quarantine management method, then click Continue.

F-Secure Email and Server Security	-		×
Product Setup 5/7			
Select the quarantine management method:			
Local quarantine management: Select this option if you plan to install only one instance of the product or if you do not want to ma quarantined mails centrally.	nage		
 Centralized quarantine management: Select this option if you plan to install multiple instances of the product and manage quarantined n single web console. 	nails from	а	
To manage quarantined emails from multiple servers, the product requires a commo database and a network share for storing quarantined items. A network share is crea server.	n quara ited on e	ntine each	
Continue Back			

7. The setup wizard asks for the location of the quarantine directory.

F-Secure Email and Server Security	—		×
Product Setup 6/7			
Enter the path to the directory where quarantined email messages and attact placed. If you are installing the product to a cluster node, make sure that the is located on the shared disk. Quarantine Directory:	hments will be quarantine dir	ectory	
C:\ProgramData\F-Secure\EssQuarantine	Browse		
Continue Back			

Specify the UNC path to the Quarantine Storage share that you created before the installation as the Quarantine Directory. For example, \\<Server>\FSAVMSEQS\$, where <Server> is the name of the server where you created the quarantine storage share.

Click Continue.

- 8. Complete the installation on the first node.
- 9. Log on to the second node of the cluster using a domain administrator account. Repeat the steps given above.
- **10.** After you specify the SQL Server to use, the setup wizard asks you to specify the quarantine database.

iecure Email and Server Security	-	
Product Setup 3/7		
Setup has detected that a database with the specified name already following options to continue:	exists. Select one of the	
• Use existing database.		
O Remove the existing database and create a new one with the spe	ecified name.	
\bigcirc Keep the existing database and create a new database with anot	her name:	
Continue		
Back		

Select Use existing database and click Continue.

11. Complete the installation on the second node.

6.4 Administering the cluster installation with F-Secure Policy Manager

To administer the product installed on a cluster, create a new subdomain under your organization or network domain. Import all cluster nodes to this subdomain.

To change product configuration on all cluster nodes, follow these instructions:

1. Select the cluster subdomain in the **Domain tree** in Policy Manager Console.

- 2. Check the settings under the Microsoft Exchange branch on the Settings tab.
- 3. Change required settings.
- 4. Distribute the policy.
- 5. All nodes receive new settings the next time they poll the Policy Manager Server.

If you need to change settings on a particular node, follow these instructions:

- 1. Select the corresponding host in the **Domain tree** in Policy Manager Console.
- 2. Check the settings under the Microsoft Exchange branch on the Settings tab.
- 3. Change required settings.
- **4.** Distribute the policy.
- 5. The host receives new settings the next time it polls the Policy Manager Server.

6.5 Using the quarantine in the cluster installation

You can manage quarantined items with the web console by connecting to any node of the cluster.

Note: You need to configure IIS to accept connections from authorized hosts.



You can release, reprocess and download quarantined messages and attachments when at least one node of the cluster is currently online.

6.6 Uninstallation

Follow these instructions to uninstall the product in the cluster environment.

- 1. Uninstall the product from the active node with **Programs and Features** in Windows. The uninstallation removes the cluster resource automatically.
- 2. After the uninstallation in the active node is finished, uninstall the product from passive nodes.
- 3. After the product has been uninstalled from every node, reboot computers one at the time.

6.7 Troubleshooting

- If the product fails to quarantine a message or attachment or reports that the email quarantine storage is not accessible, make sure that directory sharing and security permissions are set as follows: **change**, **write** and **read** operations are allowed for **SYSTEM** and **Exchange Domain Servers**, and **full control** is allowed for **Administrator**.
- To change the location of the email quarantine storage from F-Secure Policy Manager Console, use the **Final** flag to override the setting set during product installation on the host.

Appendix



Installing Microsoft SQL Server

Topics:

• Installation steps

This section contains instructions for installing Microsoft SQL Server 2019 for use with F-Secure Email and Server Security.

A.1 Installation steps

Follow these steps to install and configure Microsoft SQL Server 2019 for use with Email and Server Security.

- 1. Download SQL Server 2019 from the Microsoft website and run the installer.
- 2. In SQL Server Installation Center select New SQL Server stand-alone installation.

🐮 SQL Server Installation Center		- 0	×
Planning		New SQL Server stand-alone installation or add features to an existing installation	^
Installation		Launch a wizard to install SQL Server 2019 RC1 in a non-clustered environment or to add features to an existing SQL Server 2019 RC1 instance.	
Maintenance	-		
Tools		Install SQL Server Reporting Services	
Resources		Launch a download page that provides a link to install SQL Server Reporting Services. An internet connection is required to install SSRS.	
Advanced		Install SQL Server Management Tools	
Options	X	Launch a download page that provides a link to install SQL Server Management Studio, SQL Server command-line utilities (SQLCMD and BCP), SQL Server PowerShell provider, SQL Server Profiler and Database Tuning Advisor. An internet connection is required to install these tools.	
	2	Install SQL Server Data Tools	
	•••	Launch a download page that provides a link to install SQL Server Data Tools (SSDT). SSDT provides Visual Studio integration including project system support for Microsoft Azure SQL Database, the SQL Server Database Engine, Reporting Services, Analysis Services and Integration Services. An internet connection is required to install SSDT.	
		New SQL Server failover cluster installation	
		Launch a wizard to install a single-node SQL Server 2019 RC1 failover cluster. This action is only availabe in the clustered environment.	
	, all	Add node to a SQL Server failover cluster	
	\$1 .	Launch a wizard to add a node to an existing SQL Server 2019 RC1 failover cluster. This action is only availabe in the clustered environment.	
Microsoft SQL Server 2019		Upgrade from a previous version of SQL Server	
Community Technology Preview (CTP)		Launch a wizard to upgrade a previous version of SQL Server to SQL Server 2019 RC1. Click here to first view Upgrade Documentation	v

3. Select the edition and enter your product key if you have one.

📸 SQL Server 2019 RC1 Setup				×
Product Key Specify the edition of SQL Se Product Key	rver 2019 RC1 to install. Validate this instance of SQL Server 2019 RC1 by entering the 25-character ke	y from the Micr	osoft	
License Terms Global Rules Microsoft Update Product Updates Install Setup Files Install Rules Feature Selection Feature Rules Feature Configuration Rules Ready to Install Installation Progress Complete	Contract of valuation, or Express. Evaluation has the largest set of SQL Server SQL Server Books Online, and is activated with a 180-day expiration. Develop expiration, has the same set of features found in Evaluation, but is licensed fo application development only. To upgrade from one installed edition to anoth Wizard. Specify a free edition: Express C Enter the product key:	for o de Se features, as do er edition does r non-productio rer, run the Edit	cumented not have - on databa ion Upgra	J in an ade
	< Back	Next >	Cance	:

4. Click Next.

5. Accept the license terms and click **Next**.

To install SQL Server 2019 R	C1, you must accept the Microsoft Software License Terms.
Product Key License Terms Global Rules Microsoft Update Product Updates Install Setup Files Install Rules Feature Rules Feature Rules Feature Configuration Rules Ready to Install	MICROSOFT PRE-RELEASE SOFTWARE LICENSE TERMS MICROSOFT SQL SERVER 2019 RELEASE CANDIDATE 1 (RC1) These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to the pre-release software named above, which includes the media on which you received it, if any. The terms also apply to any Microsoft • updates, • supplements, • Internet-based services, and • cupped tenders
Complete	Copy Print Copy Print Copy Print Copy Print SQL Server transmits information about your installation experience, as well as other usage and performance data, to Microsoft to help improve the product. To learn more about data processing and privacy controls, and to turn off the collection of this information after installation, see the documentation.

6. Select whether or not you want to check for updates, then click Next.

📸 SQL Server 2019 RC1 Setup		-		×
SQL Server 2019 RC1 Setup Microsoft Update Use Microsoft Update to check: Product Key License Terms Global Rules Microsoft Update Product Updates Install Setup Files Install Rules Feature Selection Feature Rules Feature Configuration Rules	for important updates Microsoft Update offers security and other important updates for Windows and othe software, including SQL Server 2019 RC1. Updates are delivered using Automatic Up visit the Microsoft Update website. Use Microsoft Update to check for updates (recommended) Microsoft Update FAQ Microsoft Update Privacy Statement	er Micra	Desoft pr you ca	× an
Feature Configuration Rules Ready to Install Installation Progress Complete	< Back Next >		Cancel	

7. Check if there were any issues during the initial setup and resolve them as necessary.

	operation	completed. Passed: 3. Failed U. Warning T. Skipped U.		
cense Terms				
opai Rules icrosoft Update	Hide det	tails <<		Re-ru
stall Setup Files	View deta	iled report		
stall Rules				
ature Selection	Result	Rule	Status	
ature Rules		Consistency validation for SQL Server registry keys	Passed	
adure Configuration Rules			warning	
stallation Progress		COL 2010 minimum CTD for Unrende and Cide by Side Surrent	Passed	
omplete		SQL 2019 minimum CTP for Opgrade and side by side support	Passed	

- 8. Click Next.
- 9. Select the Database Engine Services feature.

📸 SQL Server 2019 RC1 Setup			- 0	×
Feature Selection Select the Express features to i	install.			
Product Key License Terms Global Rules	Cooking for Reporting Servi Features:	ces? <u>Download it fro</u>	<u>m the web</u> Feature description:	
Microsoft Update Install Setup Files	Instance Features ✓ Database Engine Services SQL Server Replication	^	The configuration and operation of each instance feature of a SQL Server instance is	< >
Feature Selection	Machine Learning Ser	vices and Language	Prerequisites for selected features:	
Feature Rules Instance Configuration	R Python Java		Already installed: Windows PowerShell 3.0 or higher	^ ~
Server Configuration Database Engine Configuration Feature Configuration Rules Ready to Install	Full-Text and Semant PolyBase Query Servic Java connector fo	ic Extractions for Sea te for External Data r HDFS data sources	Disk Space Requirements Drive C: 1003 MB required, 28283 MB available	<
Installation Progress Complete	Select All Unselect All]		
	Instance root directory:	C:\Program Files\Mi	crosoft SQL Server\	
	Shared feature directory:	C:\Program Files\Mie	crosoft SQL Server\	j.
	Shared feature directory (x86):	C:\Program Files (x86	5)\Microsoft SQL Server\]
	1		< Back Next > Cancel	

10. Click Next.

11. Enter a name for the SQL instance, then click **Next**.

You can use the default name (SQLExpress).

Instance Configuratio	n						~
Specify the name and instanc	e ID for the instance of S	QL Server. Instance	ID becomes part of t	the installation path.			
Product Key License Terms Global Rules	Default instance Named instance:	SQLExpress					
Microsoft Update Install Setup Files Install Rules	Instance ID:	SQLEXPRESS					
Feature Selection Feature Rules Instance Configuration Server Configuration Database Engine Configuration Feature Configuration Rules Ready to Install Installation Progress Complete	SQL Server directory: Installed instances:	C:\Program Files\	Microsoft SQL Server	MSSQL15.SQLEXPRES	S		
	Instance Name	Instance ID	Features	Edition	Ve	rsion	
				< Back Next	>	Cance	el

12. Review the service accounts, then click **Next**.

📸 SQL Server 2019 RC1 Setup				- 0	×				
Server Configuration									
Specify the service accounts an	d collation configuration.								
Product Key License Terms	Service Accounts Collation								
Global Rules Misrosoft Undate	Sentice	Account Name	Descuerd Status						
Install Setup Files	SOL Server Database Epgine	NT Service\MSSOL\$SOL	rassword	Automatic					
Install Rules	SQL Server Browser	NT AUTHORITY\LOCAL		Disabled	~				
Install Rules Feature Selection Feature Rules Instance Configuration Server Configuration Database Engine Configuration Peature Configuration Rules Ready to Install Installation Progress Complete	Grant Perform Volume Maintr This privilege enables instant to information disclosure by a <u>Click here for details</u>	enance Task privilege to SQL Sen file initialization by avoiding zerc illowing deleted content to be ac	ver Database En bing of data pa <u>c</u> cessed.	gine Service ges. This may lead	ł				
		< Back	c Next	t> Can	cel				

13. Select Mixed Mode as the authentication mode and enter the details for the system administrators account.

parallelism, Memory limits, and	Filestream settings.						
Product Key License Terms Global Rules Microsoft Update Install Setup Files Install Rules Feature Rules Instance Configuration Server Configuration Database Engine Configuration Feature Configuration Rules Ready to Install Installation Progress Complete	Server Configuration Specify the authent Authentication Moi O Windows auther Mixed Mode (SC Specify the password: Confirm password: Specify SQL Server.	Data Directories tication mode and de atication mode QL Server authentic rd for the SQL Serv 	TempDB administrat ation and V ver system a	Memory tors for the Vindows au	User Instances Database Engin uthentication) or (sa) account.	FILESTREAM e.	
	DAG\Administrator (Administrator) SQL Server administrators have unrestricted access to the Database Engine. Add Current User Add						

14. Click Next.

15. Review the installation configuration, then click **Next**.

📸 SQL Server 2019 RC1 Setup	58		×
Ready to Install Verify the SQL Server 2019 RC	1 features to be installed.		
Product Key License Terms Global Rules Microsoft Update Install Setup Files Install Rules Feature Selection Feature Rules Instance Configuration Server Configuration Database Engine Configuration Feature Configuration Rules Ready to Install Installation Progress Complete	Ready to install SQL Server 2019 RC1: Summary General Configuration Features Database Engine Services Instance IDs Instance IDs Instanc		~
	Configuration file path: C:\Program Files\Microsoft SQL Server\150\Setup Bootstrap\Log\20191211_200631\Configurat	ionFile.in	i
	< Back Install	Cance	:

16. Wait for the installation to complete, then click **Close**.

rour size server 2019 KCT Ins	canación compreteu successibiliy.		
Product Key	Information about the Setup operation or p	oossible next steps:	
License Terms	Feature	Status	
Global Rules	Database Engine Services	Succeeded	
Aicrosoft Update	SOL Browser	Succeeded	
nstall Setup Files	SOL Writer	Succeeded	
nstall Rules	SOL Client Connectivity SDK	Succeeded	
eature Selection	SQL Client Connectivity	Succeeded	
Cocore o creccion	Cotun Sunnart Eilar	Succorded	
Conturo Pulor			
Feature Rules			
Feature Rules nstance Configuration			
Feature Rules Instance Configuration Server Configuration	Details:		
Feature Rules Instance Configuration Server Configuration Database Engine Configuration	Details: Install successful.		
Feature Rules Instance Configuration Server Configuration Database Engine Configuration Feature Configuration Rules	Details: Instal successful.		
Feature Rules Instance Configuration Server Configuration Database Engine Configuration Feature Configuration Rules Ready to Install	Details: Install successful.		
Feature Rules Instance Configuration Server Configuration Database Engine Configuration Feature Configuration Rules Ready to Install	Details: Install successful.		
Feature Rules Instance Configuration Server Configuration Database Engine Configuration Feature Configuration Rules Ready to Install Installation Progress	Details: Install successful.		
Feature Rules Instance Configuration Server Configuration Database Engine Configuration Feature Configuration Rules Ready to Install Installation Progress Complete	Details: Install successful.		
Feature Rules Instance Configuration Server Configuration Database Engine Configuration Feature Configuration Rules Ready to Install Installation Progress Complete	Details: Install successful.		
Feature Rules Instance Configuration Server Configuration Database Engine Configuration Feature Configuration Rules Ready to Install Installation Progress Complete	Details: Instal successful Summary log file has been saved to the foll	owing location:	
Feature Rules Instance Configuration Server Configuration Database Engine Configuration Feature Configuration Rules Ready to Install Installation Progress Complete	Details: Install successful. Summary log file has been saved to the foll	owing location: \Setup Bootstrap\Log\20191211 200631	

17. Open SQL Server Configuration Manager in the Windows Start menu.



18. Go to **Protocols for SQLEXPRESS**.

If you did not use the default name for the SQL instance, you will see **Protocols for <name>** instead.



19. Make sure that TCP/IP is enabled.

20. Open the TCP/IP properties and set the following details under **IPALL**:

- a) Set **TCP Dynamic Ports** to blank. Remove any numbers from the field if necessary.
- b) Set **TCP Port** to 1433 (the default port for SQL).

 SQL Server Configuration Manager (Local) SQL Server Services SQL Server Network Configuration (32bit) SQL Native Client 11.0 Configuration (321) SQL Server Network Configuration Configuration 	Protocol Name Shared Memory Named Pipes	Status Enabled Disabled			
	\$ ICP/IP	Lindbied	TCP/IP Properties Protocol IP Addresses		
.문 SQL Native Client 11.0 Configuration			TCP Pynamic Ports TCP Port IP5 Active Enabled IP Address TCP Dynamic Ports TCP Port IP6 Active Enabled IP Address TCP Dynamic Ports TCP Port IP6 IPAII TCP Dynamic Ports TCP Port TCP Port TCP Port TCP Port TCP Port TCP Port	0 Yes No fe00::5efe:10.133.64.144%7 0 Yes No fe00::fff:fff:fff:ffe%2 0 1433	Help

21. Go to SQL Server Services and restart SQLEXPRESS.

The name shown depends on what you entered for the instance during setup.

Sql Server Configuration Manager							
File Action View Help							
🗢 🄿 🖄 📓 🗟 🛛 💿 📀							
 SQL Server Configuration Manager (Local) SQL Server Services SQL Server Network Configuration (32bit) SQL Server (Section 1.0 Configuration (20) 	Name		State	Start Mode	Log On As	Process ID	Service Type
	🐞 SQL Server Browser		Stopped	Other (Boot, Syste	NT AUTHORITY\LO	0	
	SQL Server (SQLEX02ES)	122	Running	Automatic	NT Service\MSSQL	6676	SQL Server
✓ SOL Server Network Configuration (SEI)		Start	pped	Other (Boot, Syste	NT AUTHORITY/NE	0	SQL Agent
Protocols for SQLEXPRESS		Stop					
→ 💂 SQL Native Client 11.0 Configuration		Pause					
		Resume					
		Restart					
		Properties					
		Help					

22. Close SQL Server Configuration Manager.