Email and Server Security

Deployment Guide

Contents

Chapter 1

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.

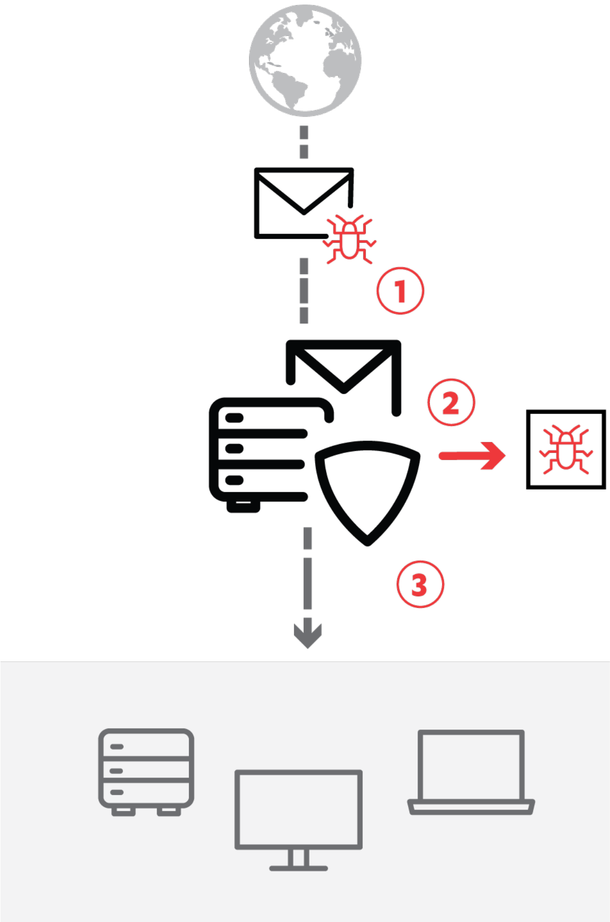


Figure 1: Email traffic

(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.

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.

Email and Server Security is a full-fledged antivirus solution with the same feature set as Server Security and the Exchange and Sharepoint protection-specific features.

The features that included with different product licenses:

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

Chapter

2

Deployment scenarios

Topics:

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.
4. 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.

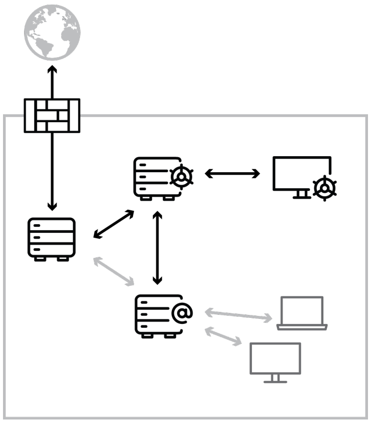
   Note: The initial installation should be done locally on the server. Upgrades can be then triggered from Policy Manager.

   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.
5. 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.

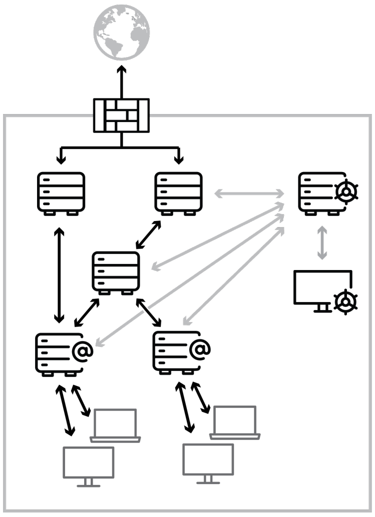
2. Install F-Secure Policy Manager Server on a dedicated server or on the same server with one of Exchange servers. You can administer the product with F-Secure Policy Manager Console.

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

3. The product installations receive 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.



1. 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.

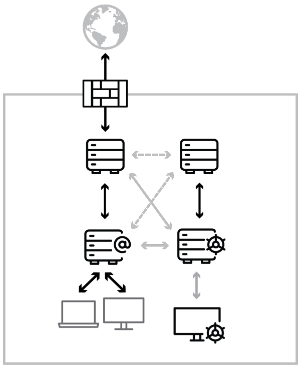
   When you install the product, configure each installation to connect to the same F-Secure Policy Manager Server.

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, 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**.
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.

2.6 Microsoft SharePoint server

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

1. 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

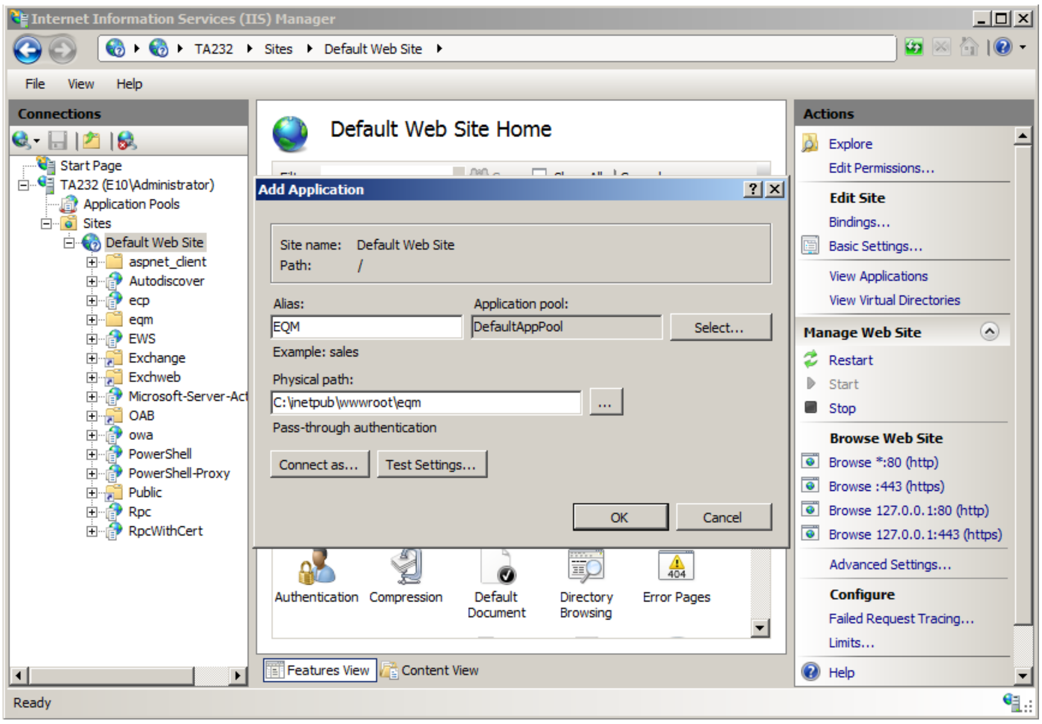
This document provides basic information for setting up F-Secure Email Quarantine Manager (EQM).

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>\Email and Server Security\EQM\`.

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 copy the contents of <F-Secure installation folder>\Email and Server Security\EQM\ 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.



Site name: Default Web Site
Path: /

Alias: EQM

Application pool: DefaultAppPool

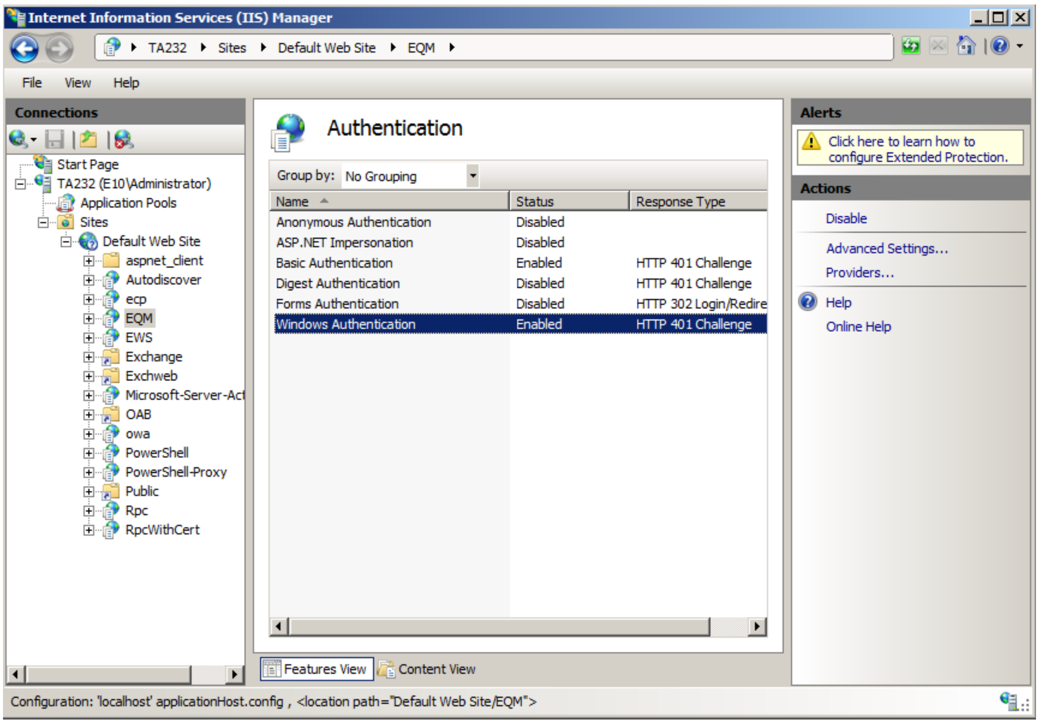
Example: sales

Physical path: C:\inetpub\wwwroot\eqm

Pass-through authentication

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

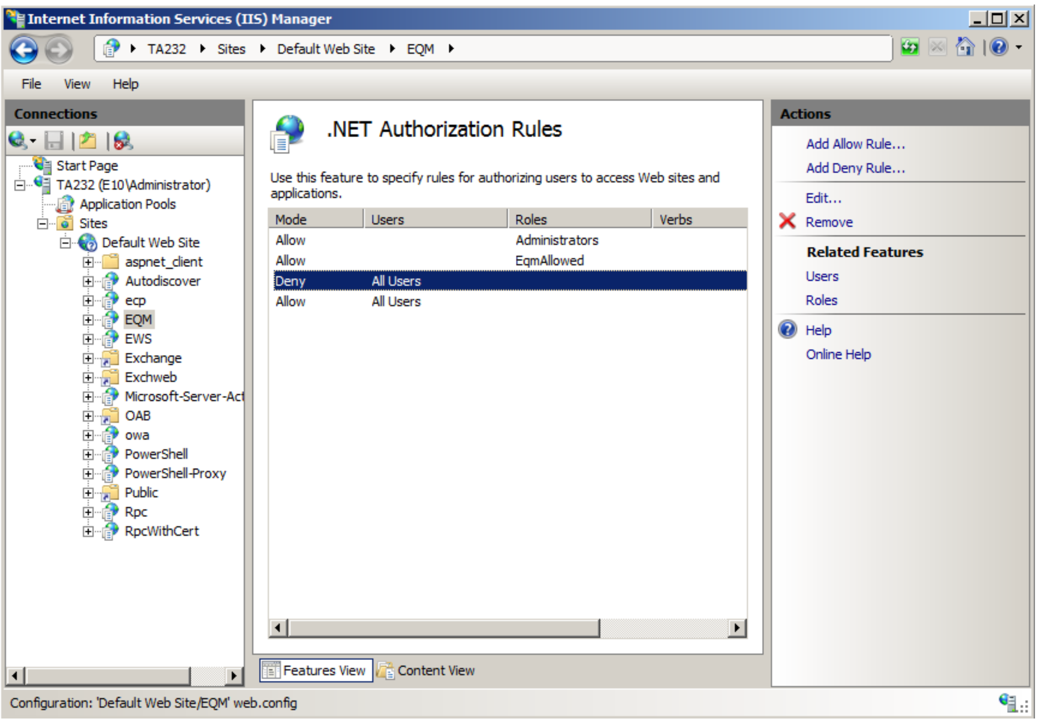


Name	Status	Response Type
Anonymous Authentication	Disabled	
ASP.NET Impersonation	Disabled	
Basic Authentication	Enabled	HTTP 401 Challenge
Digest Authentication	Disabled	HTTP 401 Challenge
Forms Authentication	Disabled	HTTP 302 Login/Redire
Windows Authentication	Enabled	HTTP 401 Challenge

Configuration: 'localhost' applicationHost.config , <location path="Default Web Site/EQM">

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



.NET Authorization Rules

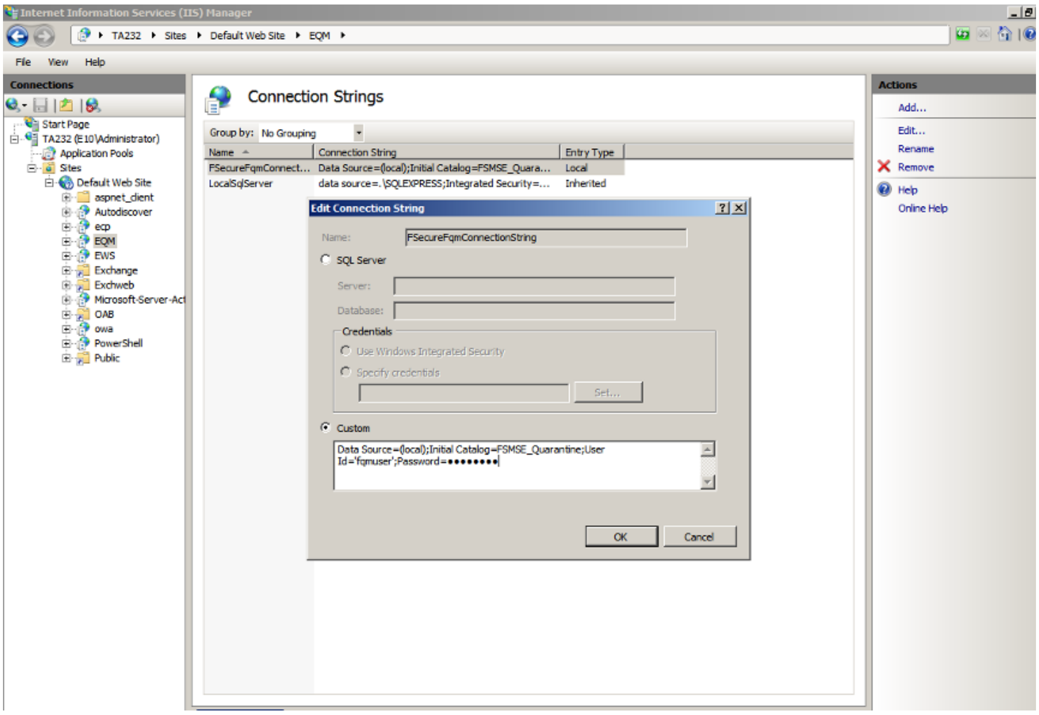
Use this feature to specify rules for authorizing users to access Web sites and applications.

Mode	Users	Roles	Verbs
Allow		Administrators	
Allow		EqmAllowed	
Deny	All Users		
Allow	All Users		

Configuration: 'Default Web Site/EQM' web.config

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.



Connection Strings

Group by: No Grouping

Name	Connection String	Entry Type
FSecureFqmConnect...	Data Source=(local);Initial Catalog=FSMSE_Quara...	Local
LocalSqlServer	data source=.\SQLEXPRESS;Integrated Security=...	Inherited

Edit Connection String

Name: FSecureFqmConnectionString

○ SQL Server

Server:

Database:

Credentials

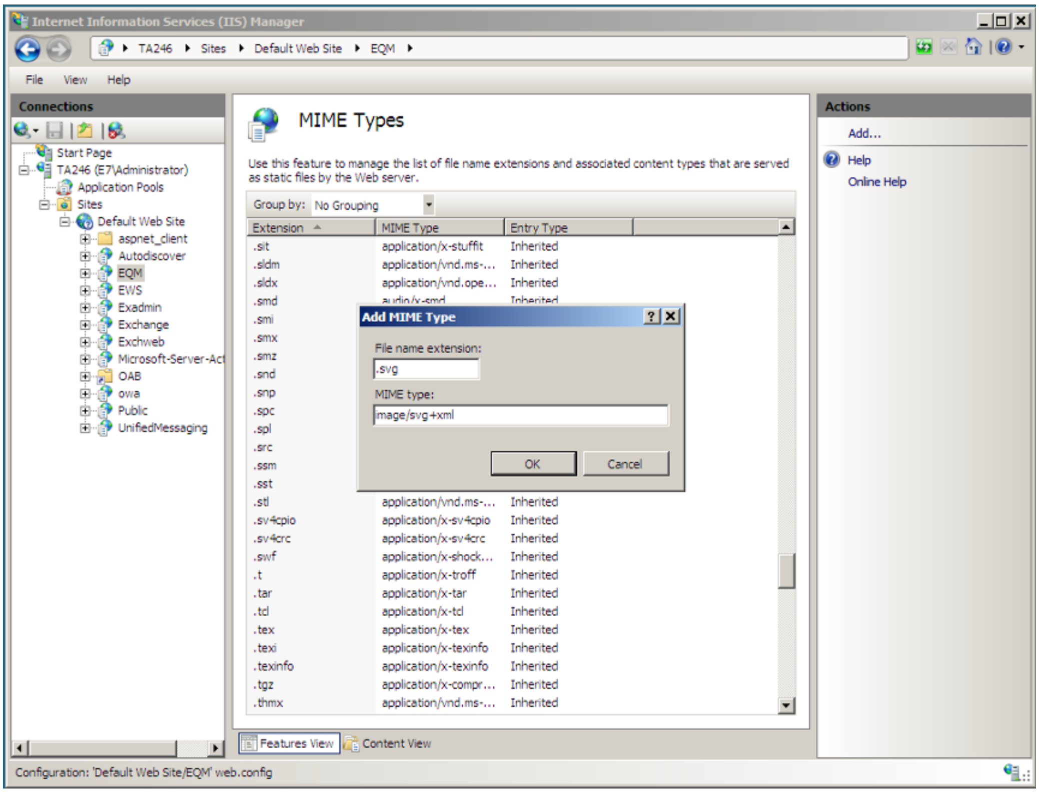
○ Use Windows Integrated Security

○ Specify credentials

● Custom

```
Data Source=(local);Initial Catalog=FSMSE_Quarantine;User
Id='fqmuser';Password=••••••••
```

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 (IIS) Manager

TA246 ▸ Sites ▸ Default Web Site ▸ EQM ▸

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.

Group by: No Grouping

Extension	MIME Type	Entry Type
.sit	application/x-stuffit	Inherited
.sldm	application/vnd.ms-...	Inherited
.sldx	application/vnd.ope...	Inherited
.smd	audio/x-smd	Inherited
.smi		
.smx		
.smz		
.snd		
.snp		
.spc		
.spl		
.src		
.ssm		
.sst		
.stl	application/vnd.ms-...	Inherited
.sv4cpio	application/x-sv4cpio	Inherited
.sv4crc	application/x-sv4crc	Inherited
.swf	application/x-shock...	Inherited
.t	application/x-troff	Inherited
.tar	application/x-tar	Inherited
.tcl	application/x-tcl	Inherited
.tex	application/x-tex	Inherited
.texi	application/x-texinfo	Inherited
.texinfo	application/x-texinfo	Inherited
.tgz	application/x-compr...	Inherited
.thmx	application/vnd.ms-...	Inherited

Add MIME Type

File name extension: .svg

MIME type: mage/svg+xml

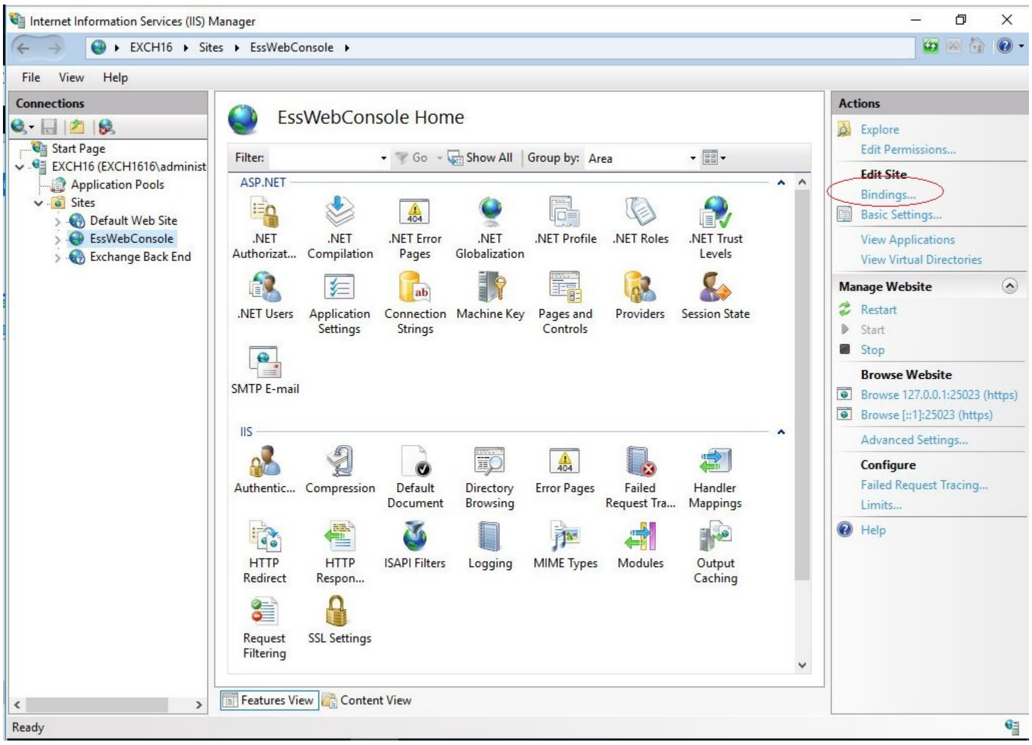
Configuration: 'Default Web Site/EQM' web.config

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**.



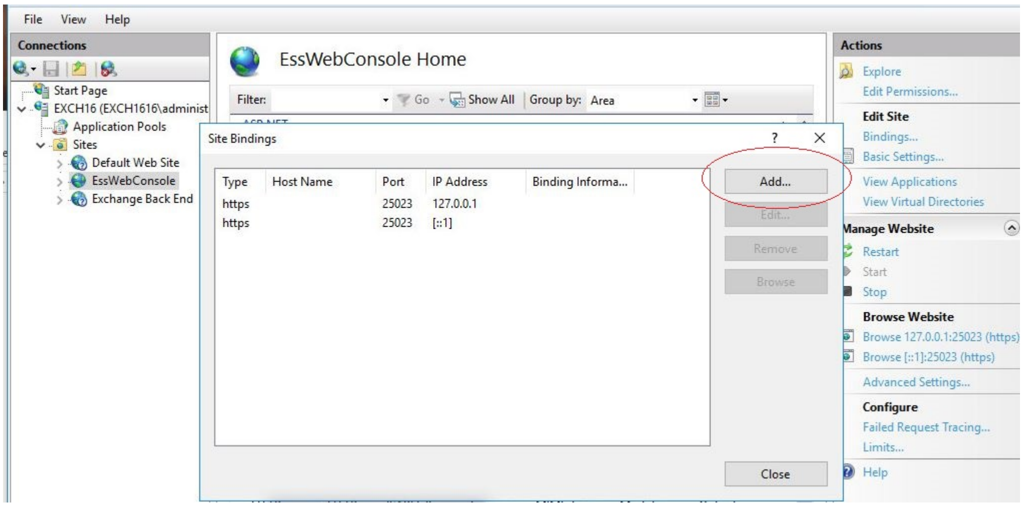
Internet Information Services (IIS) Manager

EXCH16 ▸ Sites ▸ EssWebConsole ▸

EssWebConsole Home

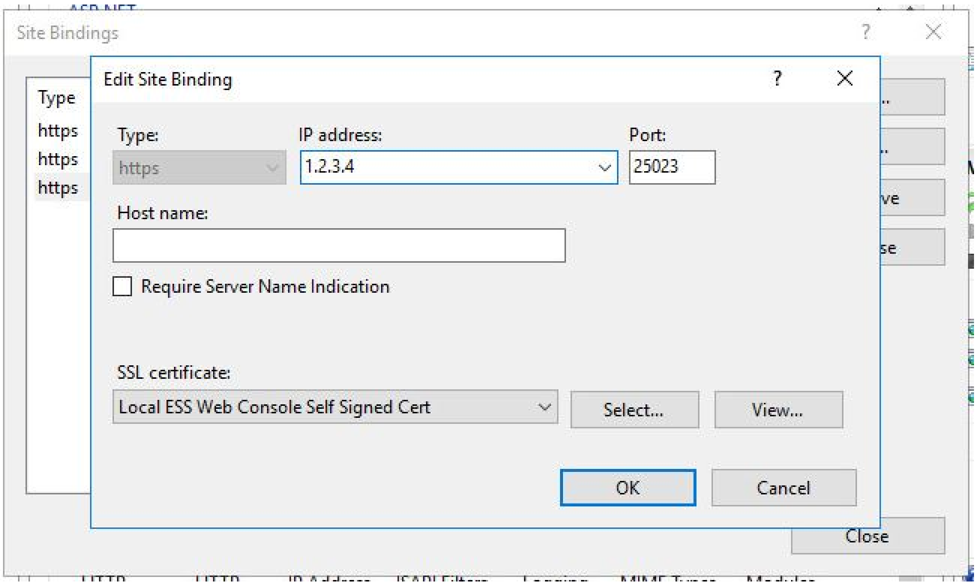
Ready

4. Click **Add**.



Type	Host Name	Port	IP Address	Binding Informa...
https		25023	127.0.0.1	
https		25023	[::1]	

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



Type: https

IP address: 1.2.3.4

Port: 25023

Host name:

□ Require Server Name Indication

SSL certificate: Local ESS Web Console Self Signed Cert

6. Select the **SSL certificate**, then click **OK**.

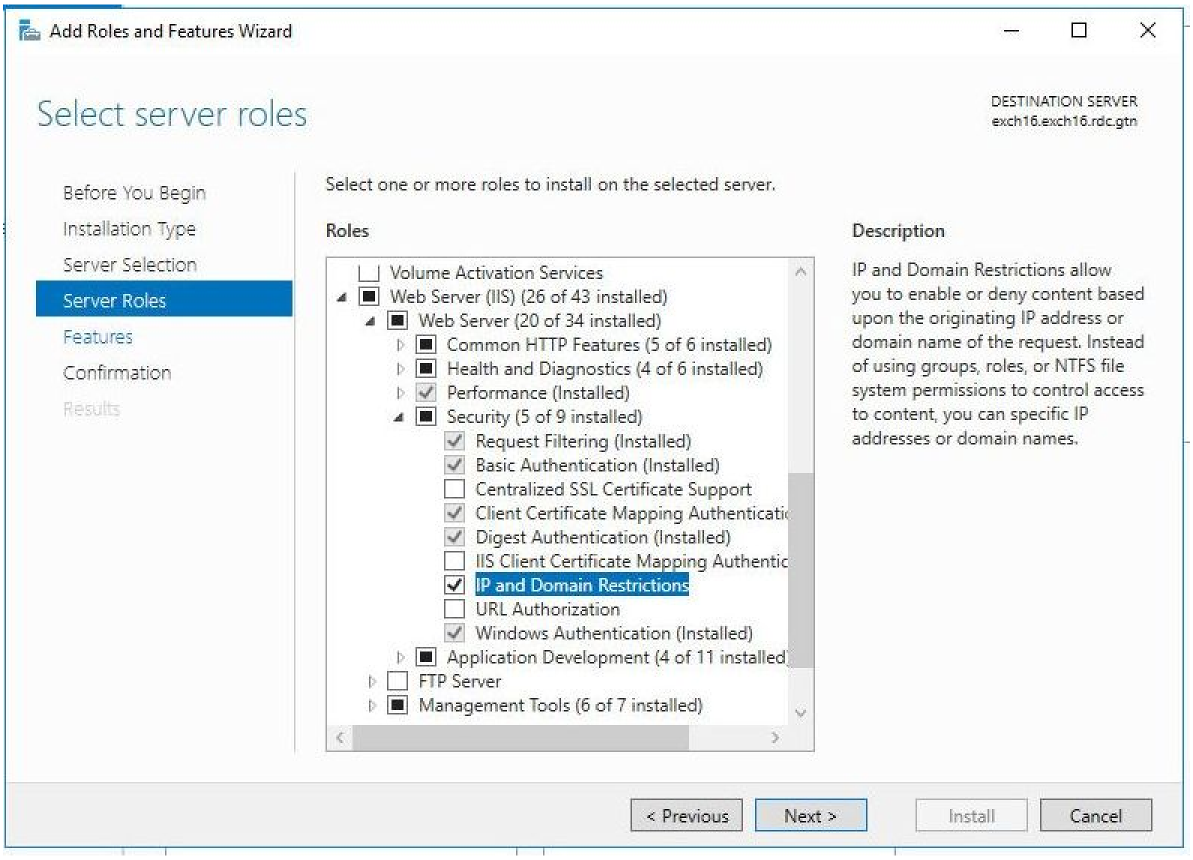
   Note: SSL 2.0 certificates are not supported due to vulnerabilities.

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).



Select server roles

DESTINATION SERVER
exch16.exch16.rdc.gtn

Select one or more roles to install on the selected server.

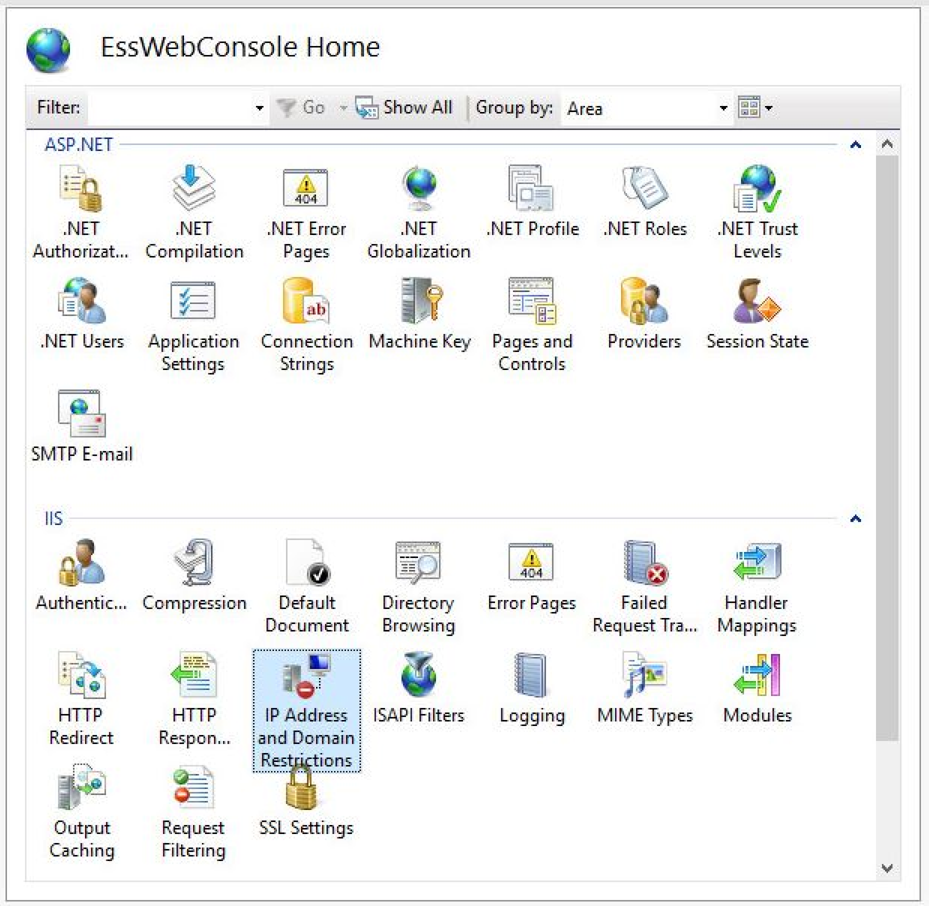
Roles

- □ Volume Activation Services
- ■ Web Server (IIS) (26 of 43 installed)
  - ■ Web Server (20 of 34 installed)
    - ■ Common HTTP Features (5 of 6 installed)
    - ■ Health and Diagnostics (4 of 6 installed)
    - ☑ Performance (Installed)
    - ■ Security (5 of 9 installed)
      - ☑ Request Filtering (Installed)
      - ☑ Basic Authentication (Installed)
      - □ Centralized SSL Certificate Support
      - ☑ Client Certificate Mapping Authenticati
      - ☑ Digest Authentication (Installed)
      - □ IIS Client Certificate Mapping Authentic
      - ☑ IP and Domain Restrictions
      - □ URL Authorization
      - ☑ Windows Authentication (Installed)
    - ■ Application Development (4 of 11 installed)
  - □ FTP Server
  - ■ Management Tools (6 of 7 installed)

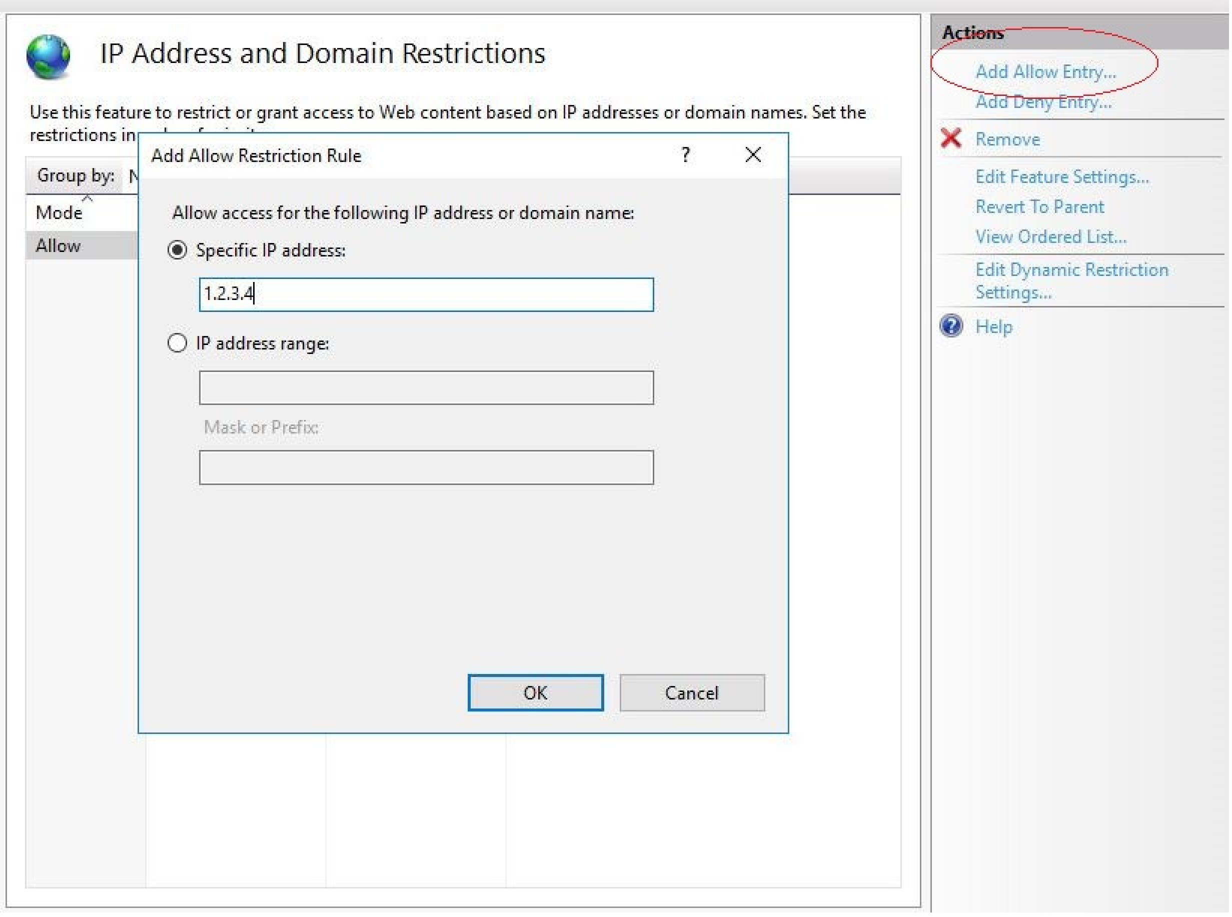
Description

IP and Domain Restrictions allow you to enable or deny content based upon the originating IP address or domain name of the request. Instead of using groups, roles, or NTFS file system permissions to control access to content, you can specific IP addresses or domain names.

2. Go to Sites > EssWebConsole.
3. Open IP and Domain Restrictions.



4. Select **Add Allow Entry**.
5. Enter the IP address or IP range.



IP Address and Domain Restrictions

Use this feature to restrict or grant access to Web content based on IP addresses or domain names. Set the restrictions in

Add Allow Restriction Rule

Allow access for the following IP address or domain name:

● Specific IP address:

1.2.3.4

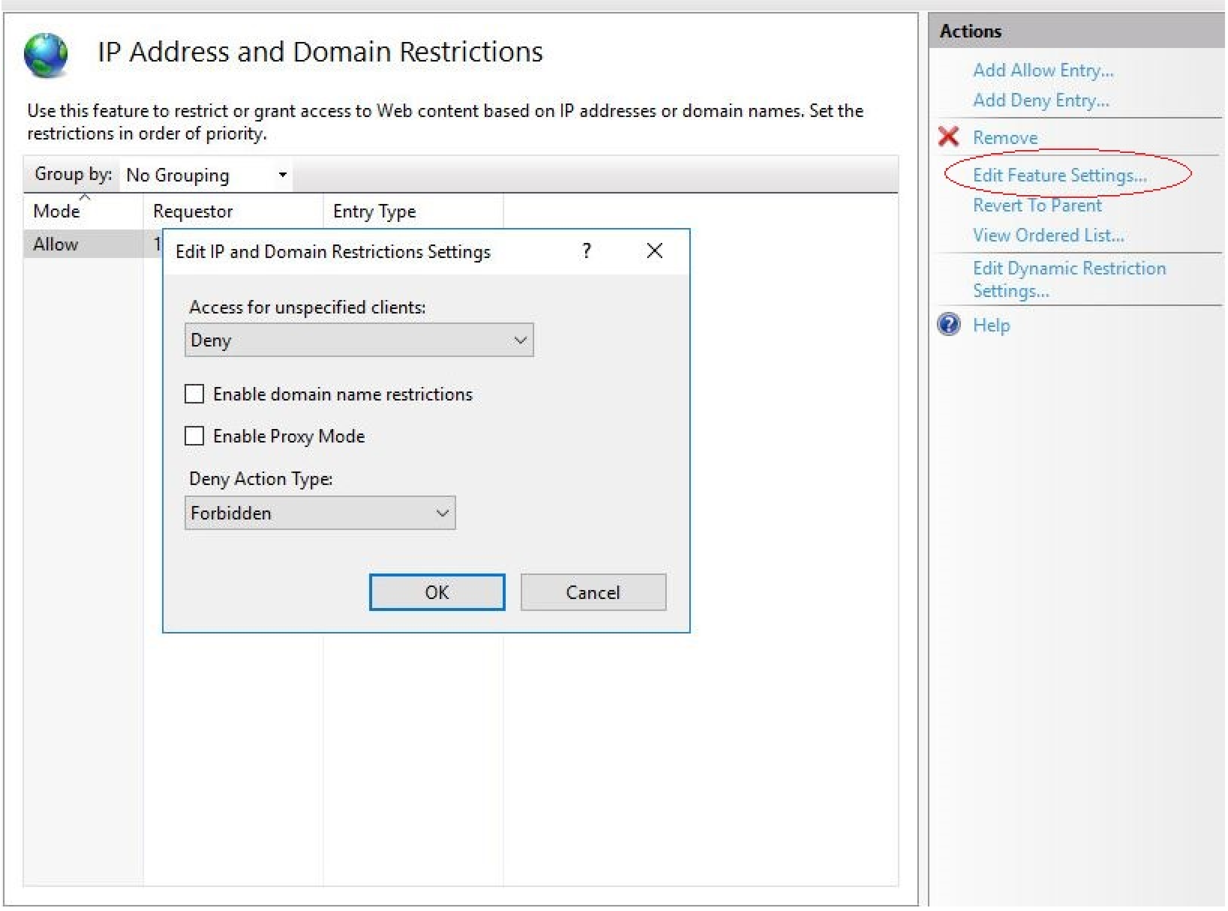
○ IP address range:

Mask or Prefix:

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**.



IP Address and Domain Restrictions

Use this feature to restrict or grant access to Web content based on IP addresses or domain names. Set the restrictions in order of priority.

Edit IP and Domain Restrictions Settings

Access for unspecified clients: Deny

□ Enable domain name restrictions

□ Enable Proxy Mode

Deny Action Type: Forbidden

9. Click **OK**.

10. Restart the **EssWebConsole** site.

Chapter

3

System requirements

Topics:

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 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
- Microsoft® Windows Server 2022 Standard
- Microsoft® Windows Server 2022 Datacenter

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 (up to CU21)
- Microsoft® Exchange Server 2019 (up to CU10)

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 / Microsoft Edge (up-to-date versions) • 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

Service	Process	Inbound ports	Outbound ports
F-Secure ORSP Client	%ProgramFiles%\F-Secure\Email and Server Security\Ultralight\ulcore\<update number>\fsorsp64.exe	-	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 15.20 is required to centrally manage F-Secure Email and Server Security version 15.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.

Cloud Connectivity Test

In order for the engine to do anything useful, it needs to be able to connect to the cloud service. To check that the connection is working properly, you can attempt to fetch a URL from the cloud detection server by other means.

If you can successfully connect to https://aspam.sp.f-secure.com/bdnc/config and get back a piece of JSON, the connection is working. If not, you have a network problem.

If the connection fails, you need to allow `*.f-secure.com` and `*.fsapi.com` on your Firewall.

3.4.3 WebUI system requirements

The Web Server (IIS) role is required for the WebUI to run.

Do the following:

- Check that the **Static Content** Windows feature is enabled.
- Check that the **Windows Authentication** Windows feature is enabled.

Chapter 4

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:

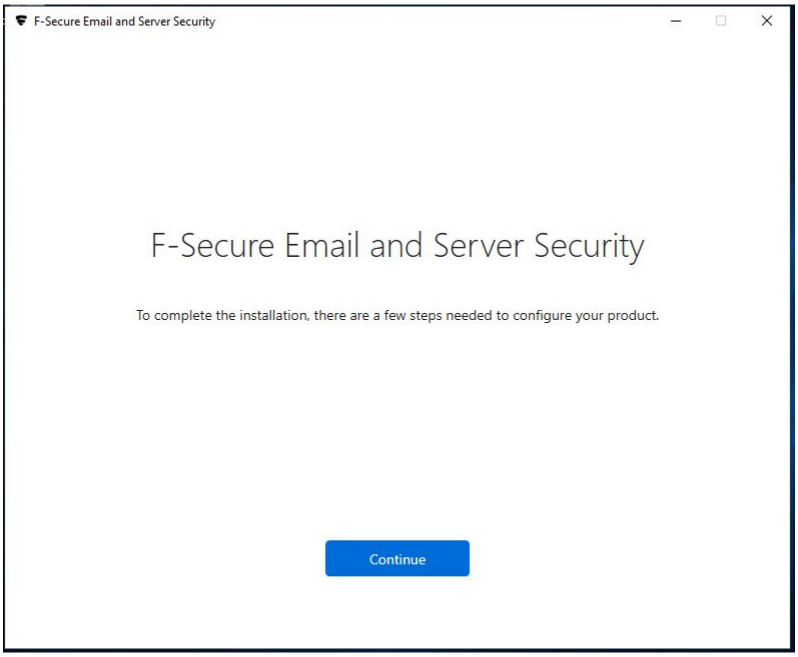
Microsoft Exchange

- 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**
- The account must have the Logon as a service privilege switched on
- The user must be a member of the built-in **Administrators** group and have permission to access and edit items in the public folders

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.

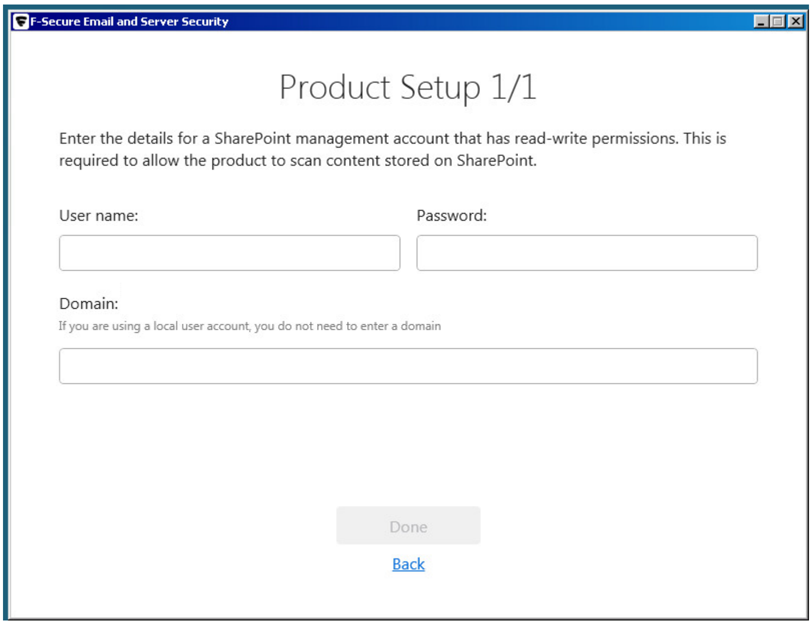


F-Secure Email and Server Security

F-Secure Email and Server Security

To complete the installation, there are a few steps needed to configure your product.

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.



F-Secure Email and Server Security

Product Setup 1/1

Enter the details for a SharePoint management account that has read-write permissions. This is required to allow the product to scan content stored on SharePoint.

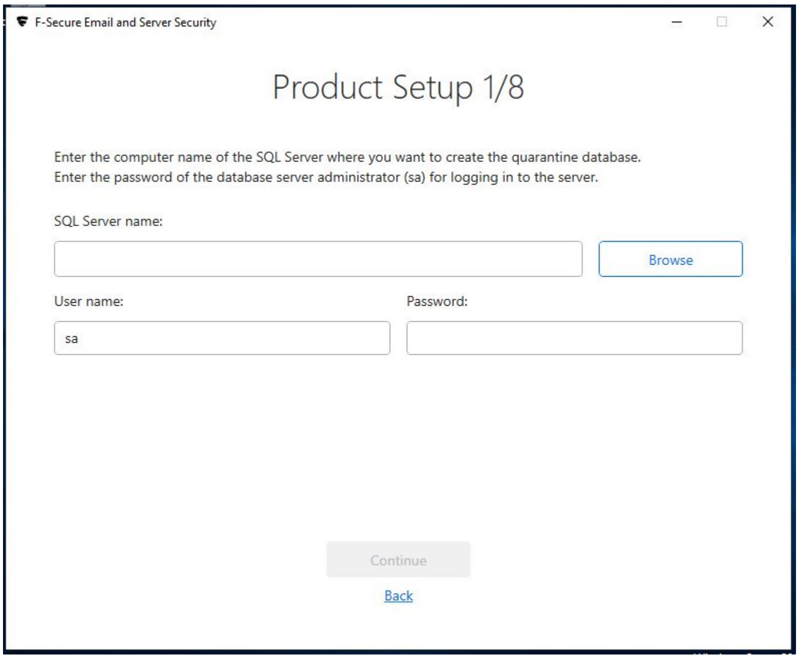
User name:

Password:

Domain:

If you are using a local user account, you do not need to enter a domain

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



F-Secure Email and Server Security

Product Setup 1/8

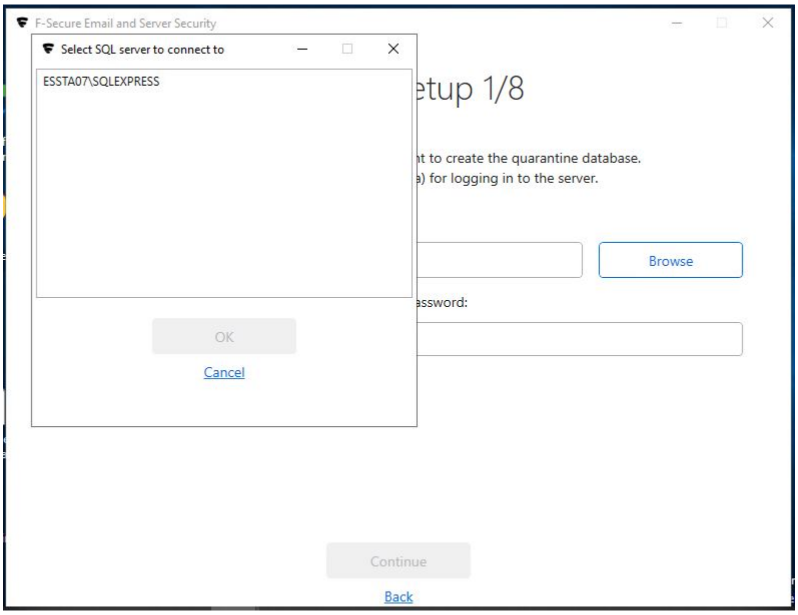
Enter the computer name of the SQL Server where you want to create the quarantine database.
Enter the password of the database server administrator (sa) for logging in to the server.

SQL Server name:

User name: sa

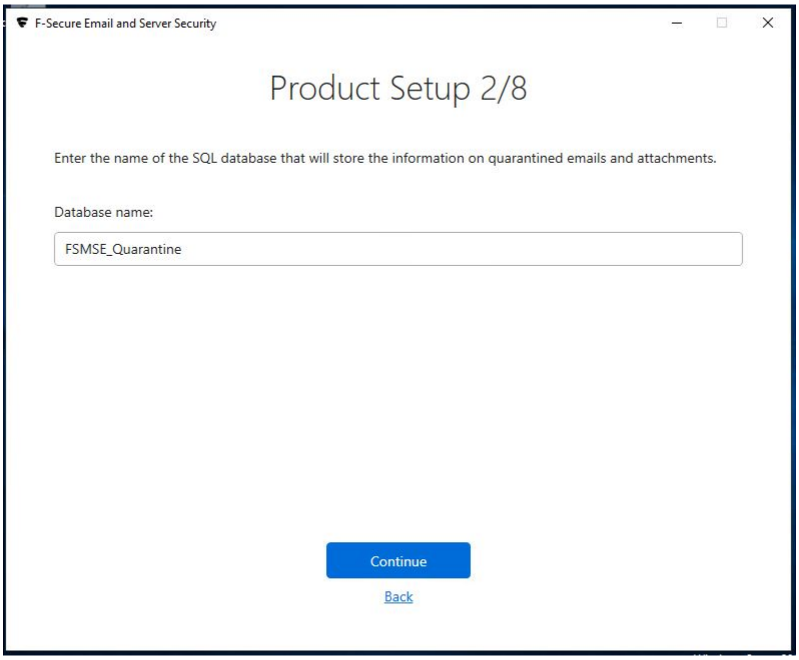
Password:

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



F-Secure Email and Server Security
Select SQL server to connect to
ESSTA07\SQLEXPRESS
OK
Cancel
etup 1/8
nt to create the quarantine database.
a) for logging in to the server.
Browse
assword:
Continue
Back

5. Enter the quarantine database name.

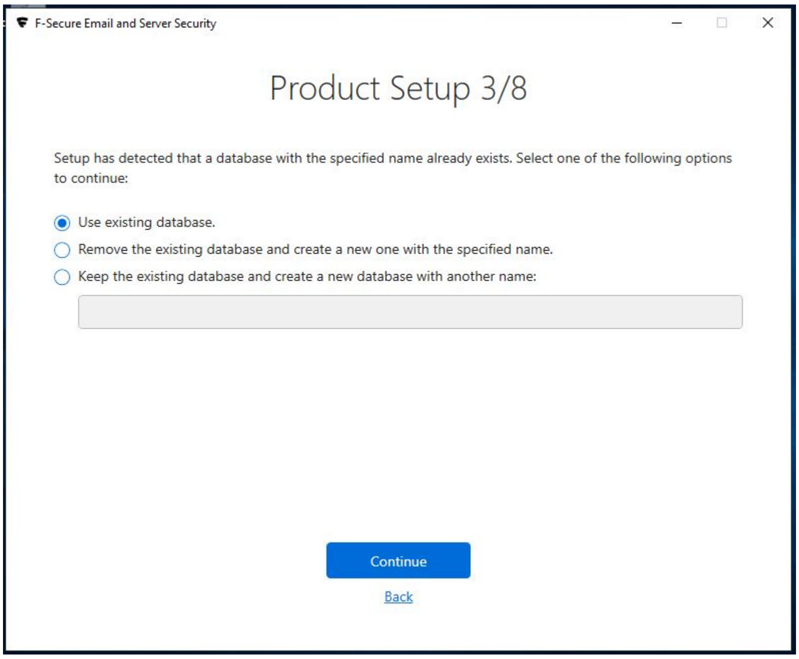


Product Setup 2/8

Enter the name of the SQL database that will store the information on quarantined emails and attachments.

Database name: FSMSE_Quarantine

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

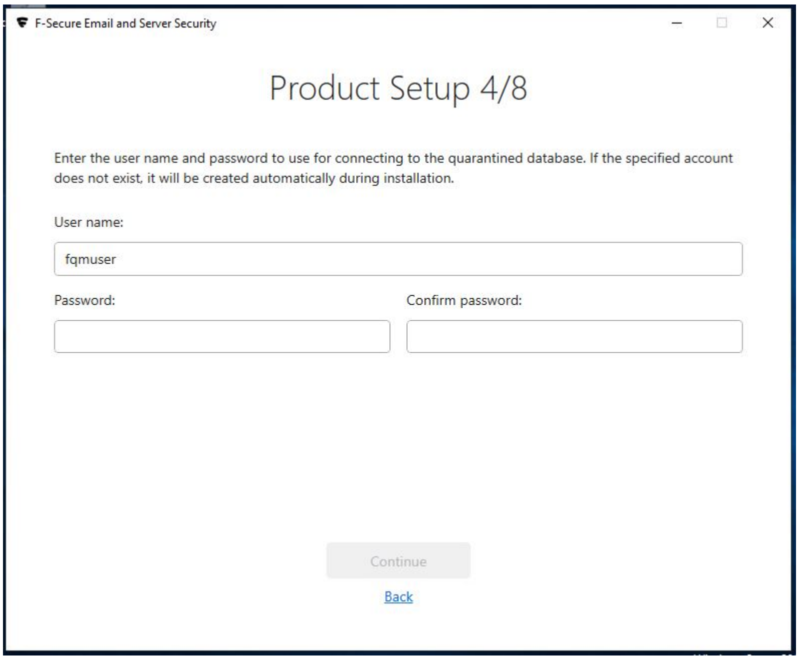


Product Setup 3/8

Setup has detected that a database with the specified name already exists. Select one of the following options to continue:

● 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:

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



Product Setup 4/8

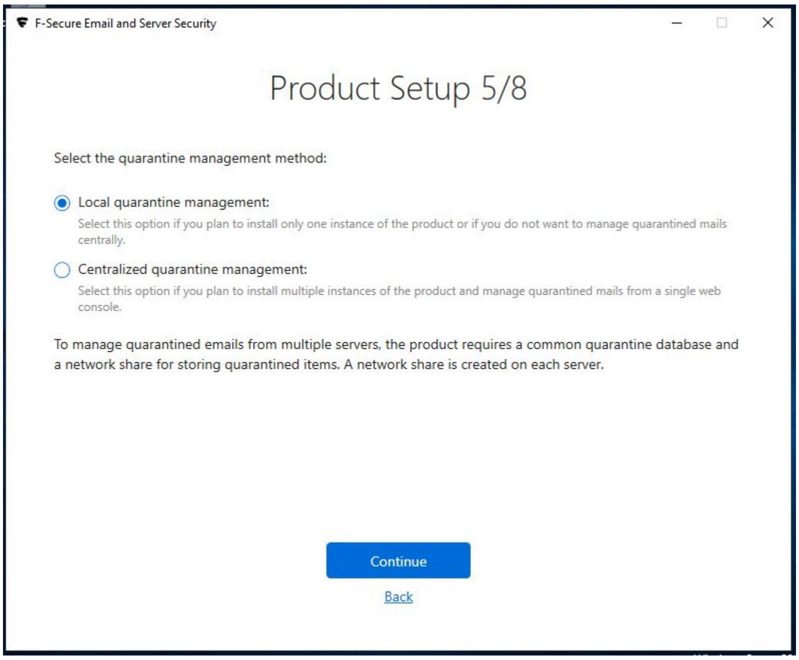
Enter the user name and password to use for connecting to the quarantined database. If the specified account does not exist, it will be created automatically during installation.

User name: fqmuser

Password:

Confirm password:

7. Select how you want to manage the quarantine.



Product Setup 5/8

Select the quarantine management method:

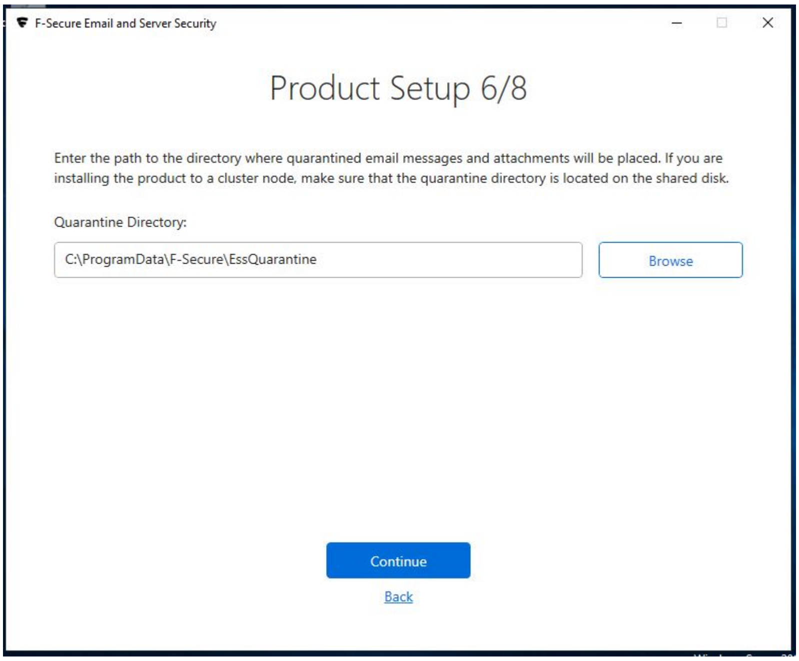
● Local quarantine management:
Select this option if you plan to install only one instance of the product or if you do not want to manage quarantined mails centrally.

○ Centralized quarantine management:
Select this option if you plan to install multiple instances of the product and manage quarantined mails from a single web console.

To manage quarantined emails from multiple servers, the product requires a common quarantine database and a network share for storing quarantined items. A network share is created on each server.

- 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.

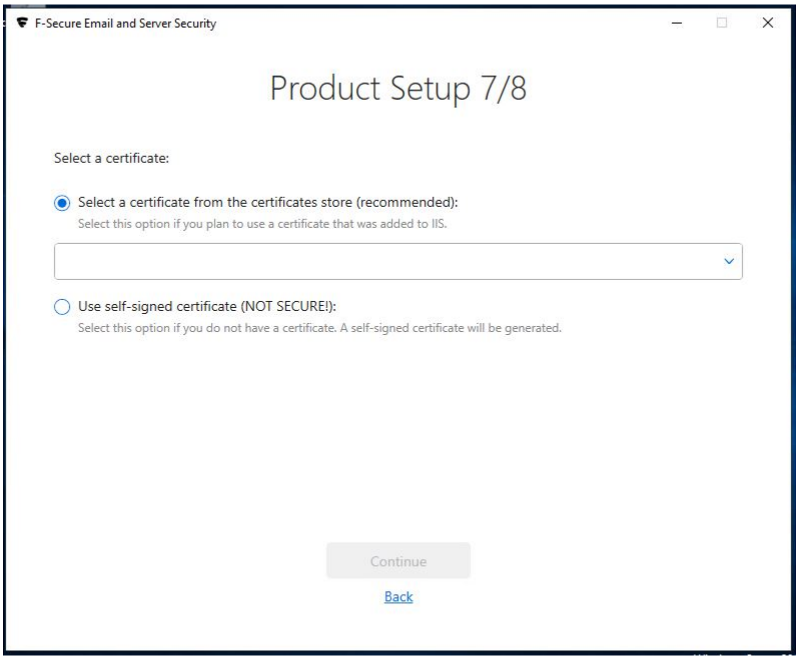


Product Setup 6/8

Enter the path to the directory where quarantined email messages and attachments will be placed. If you are installing the product to a cluster node, make sure that the quarantine directory is located on the shared disk.

Quarantine Directory: C:\ProgramData\F-Secure\EssQuarantine

9. Select a certificate.



F-Secure Email and Server Security

Product Setup 7/8

Select a certificate:

● Select a certificate from the certificates store (recommended):

Select this option if you plan to use a certificate that was added to IIS.

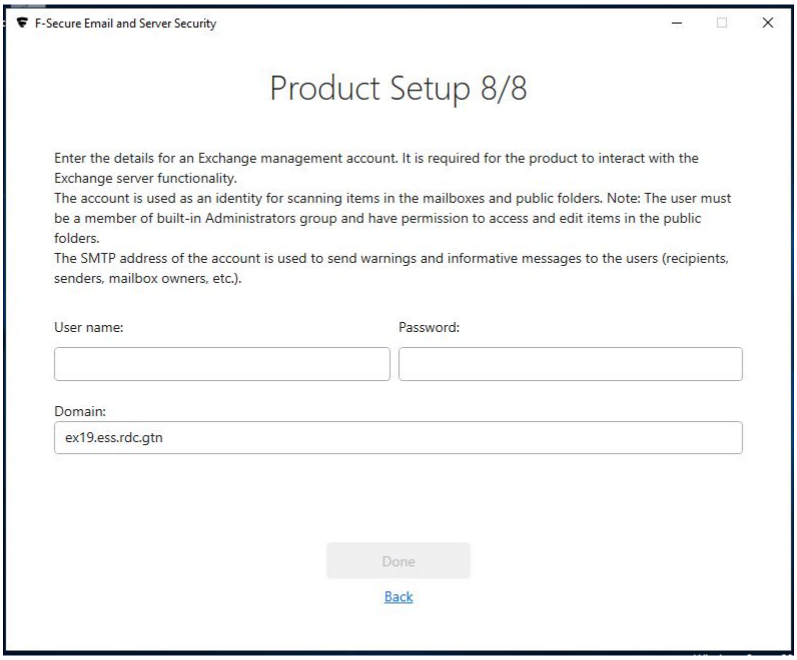
○ Use self-signed certificate (NOT SECURE!):

Select this option if you do not have a certificate. A self-signed certificate will be generated.

10. Enter the details for an Exchange management account.

Note: The user must be a member of the built-in **Administrators** group and have permission to access and edit items in the public folders.

Note: This user is utilized in the storage scanning service. Hence, we recommend that you create a new company-shared user for this service.



F-Secure Email and Server Security

Product Setup 8/8

Enter the details for an Exchange management account. It is required for the product to interact with the Exchange server functionality.
The account is used as an identity for scanning items in the mailboxes and public folders. Note: The user must be a member of built-in Administrators group and have permission to access and edit items in the public folders.
The SMTP address of the account is used to send warnings and informative messages to the users (recipients, senders, mailbox owners, etc.).

User name:

Password:

Domain: ex19.ess.rdc.gtn

11. 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.

Important: To set user credentials for the ODS service, the F-Secure Config tool should be started locally after upgrading from an older version to Email and Server Security version 15.10 (both local and policy-based upgrades). The path to the config tool: `<F-Secure installation folder>\Email and Server Security\ui\F-Secure.ESS.Config.exe`.

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

5

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:

6.1 Installation overview

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

1. 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, 2016, or 2019 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 37 .
   - 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 45 .

5. 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 48 . 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.

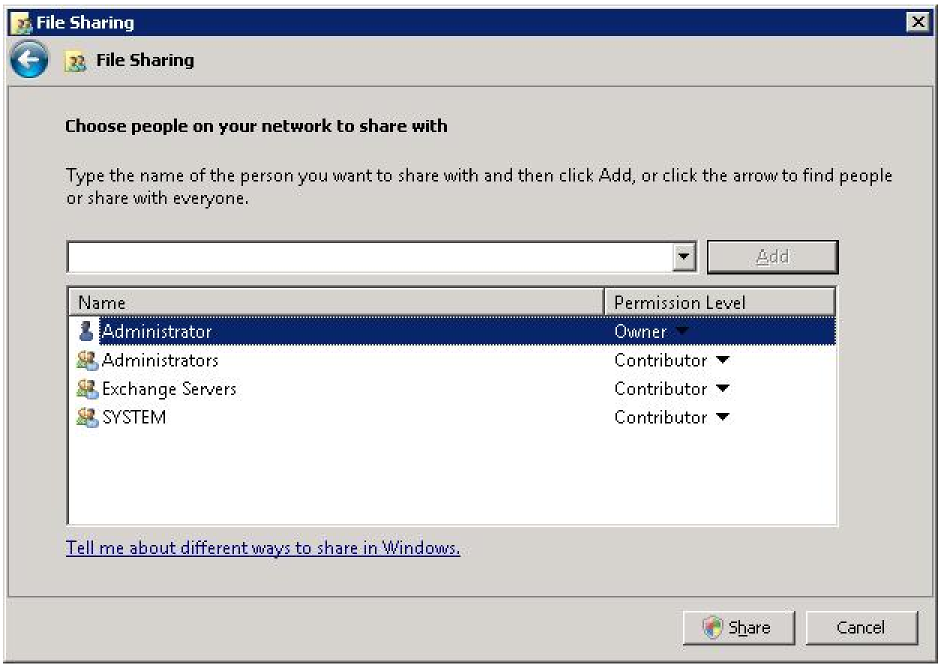
To install the Quarantine Storage on a dedicated computer, see Creating the quarantine storage for a Continuous Cluster Replication environment on page 37 for more instructions.

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**.



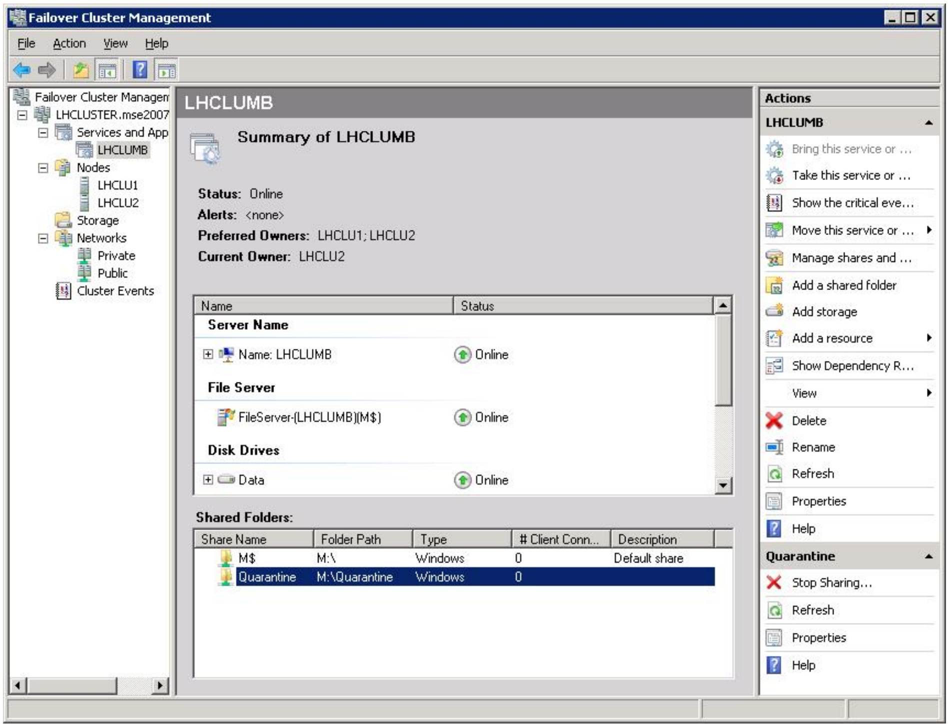
Choose people on your network to share with

Type the name of the person you want to share with and then click Add, or click the arrow to find people or share with everyone.

Name	Permission Level
Administrator	Owner
Administrators	Contributor
Exchange Servers	Contributor
SYSTEM	Contributor

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:



LHCLUMB

Summary of LHCLUMB

Status: Online
Alerts: <none>
Preferred Owners: LHCLU1; LHCLU2
Current Owner: LHCLU2

Name	Status
Server Name	
Name: LHCLUMB	Online
File Server	
FileServer-(LHCLUMB)(M$)	Online
Disk Drives	
Data	Online

Shared Folders:

Share Name	Folder Path	Type	# Client Conn...	Description
M$	M:\	Windows	0	Default share
Quarantine	M:\Quarantine	Windows	0	

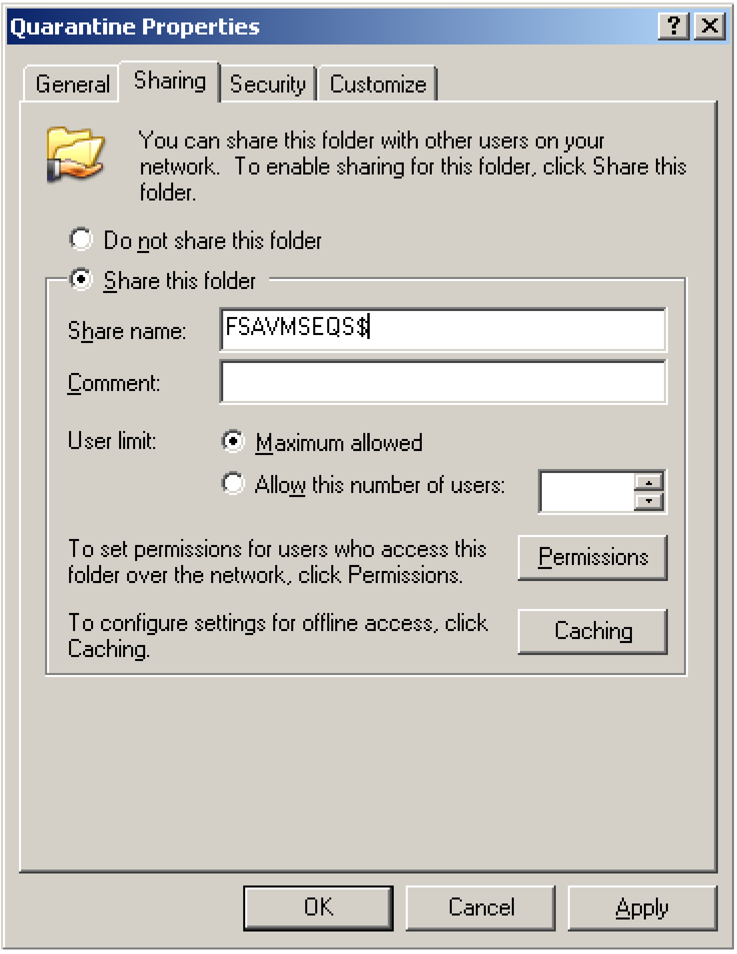
5. During the product installation, select the quarantine share you just created when the installation asks for the quarantine path.

   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.



Quarantine Properties

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:

To set permissions for users who access this folder over the network, click Permissions.

To configure settings for offline access, click Caching.

   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.

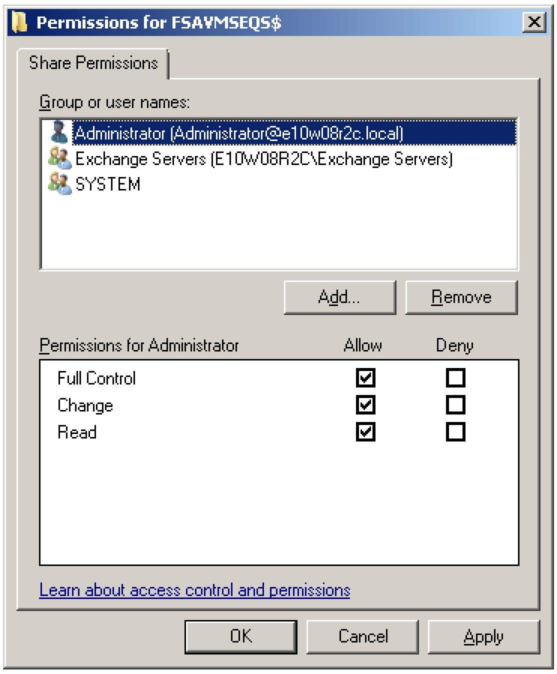
   b. Make sure that **User Limit** is set to **Maximum allowed**.

   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:

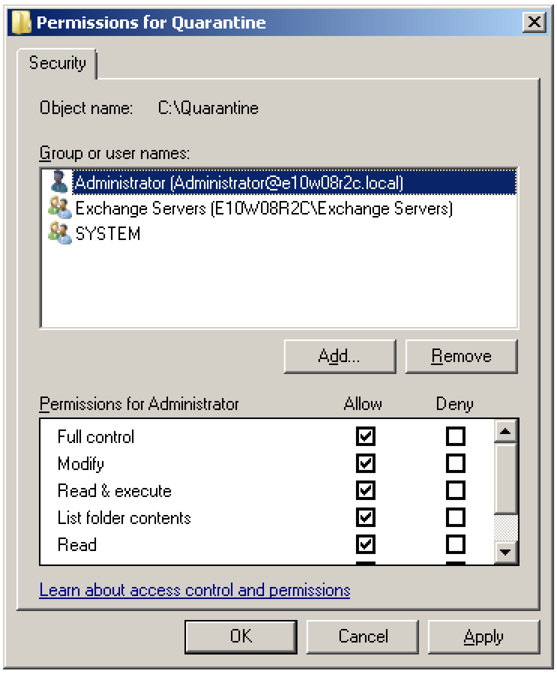
- Administrator (Administrator@e10w08r2c.local)
- Exchange Servers (E10W08R2C\Exchange Servers)
- SYSTEM

Permissions for Administrator	Allow	Deny
Full Control	☑	□
Change	☑	□
Read	☑	□

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

Group or user names:

- Administrator (Administrator@e10w08r2c.local)
- Exchange Servers (E10W08R2C\Exchange Servers)
- SYSTEM

Permissions for Administrator	Allow	Deny
Full control	☑	□
Modify	☑	□
Read & execute	☑	□
List folder contents	☑	□
Read	☑	□

Click **OK** to finish.

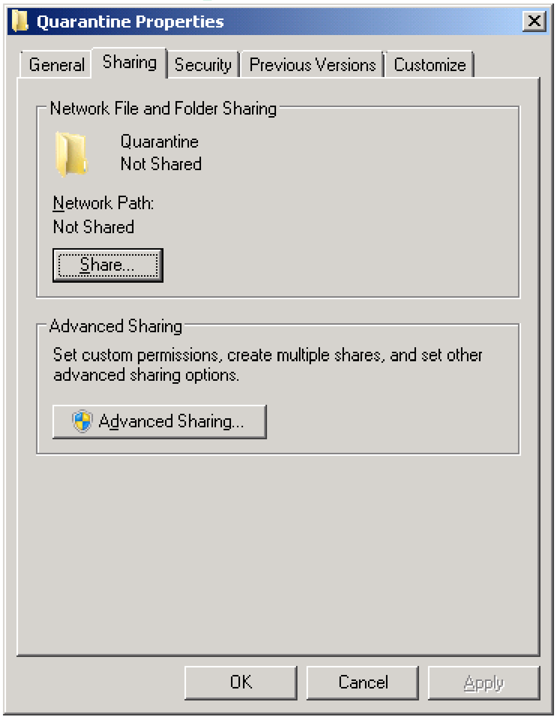
To make sure that the quarantine storage is accessible, follow these instructions:

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.

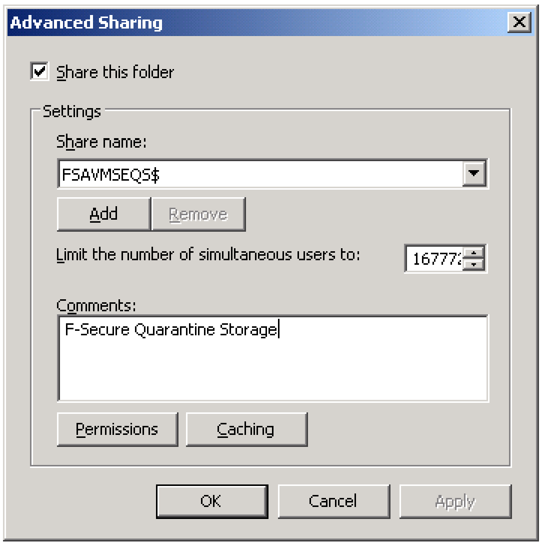


Quarantine
Not Shared

Network Path:
Not Shared

Set custom permissions, create multiple shares, and set other advanced sharing options.

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



☑ Share this folder

Share name: FSAVMSEQS$

Limit the number of simultaneous users to: 16777

Comments: F-Secure Quarantine Storage

   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.

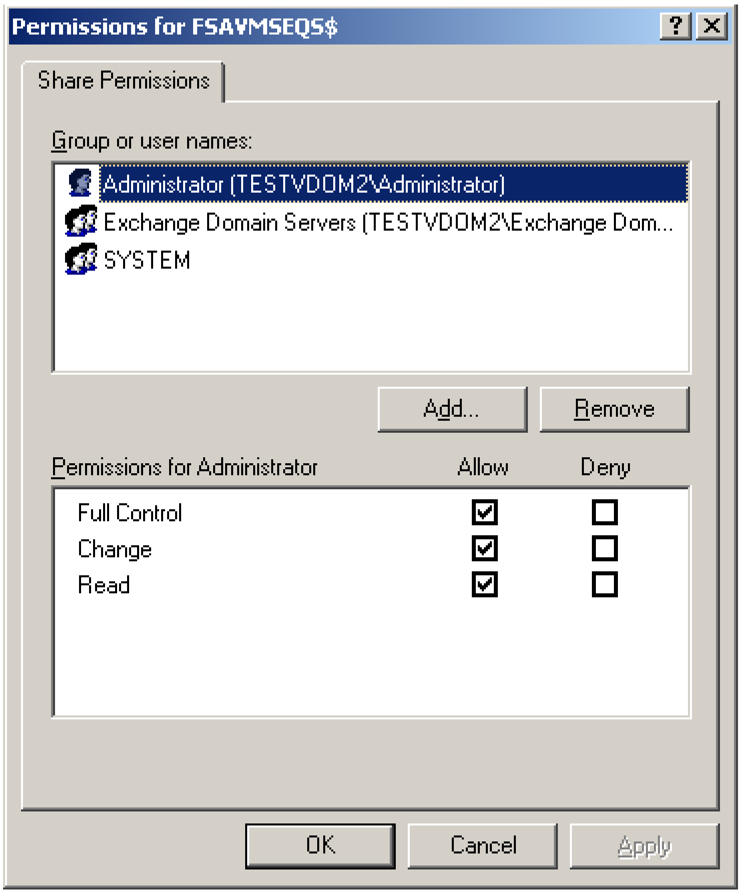
8. Change permissions as follows:

   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.



Group or user names:

- Administrator (TESTVDOM2\Administrator)
- Exchange Domain Servers (TESTVDOM2\Exchange Dom...
- SYSTEM

Permissions for Administrator	Allow	Deny
Full Control	☑	□
Change	☑	□
Read	☑	□

9. Click **OK** to continue.

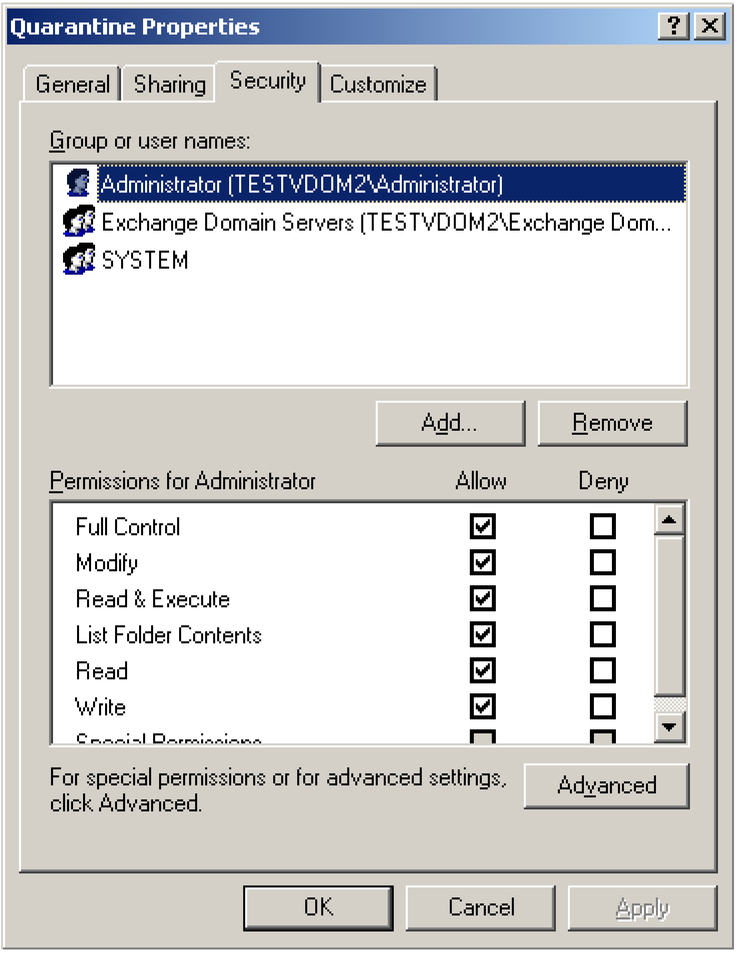
10. Go to the **Security** tab and click **Edit**.

    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.



Group or user names:

- Administrator (TESTVDOM2\Administrator)
- Exchange Domain Servers (TESTVDOM2\Exchange Dom...
- SYSTEM

Permissions for Administrator	Allow	Deny
Full Control	☑	□
Modify	☑	□
Read & Execute	☑	□
List Folder Contents	☑	□
Read	☑	□
Write	☑	□
Special Permissions	□	□

For special permissions or for advanced settings, click Advanced.

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 quarantine storage share.

6.3 Installing the product

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

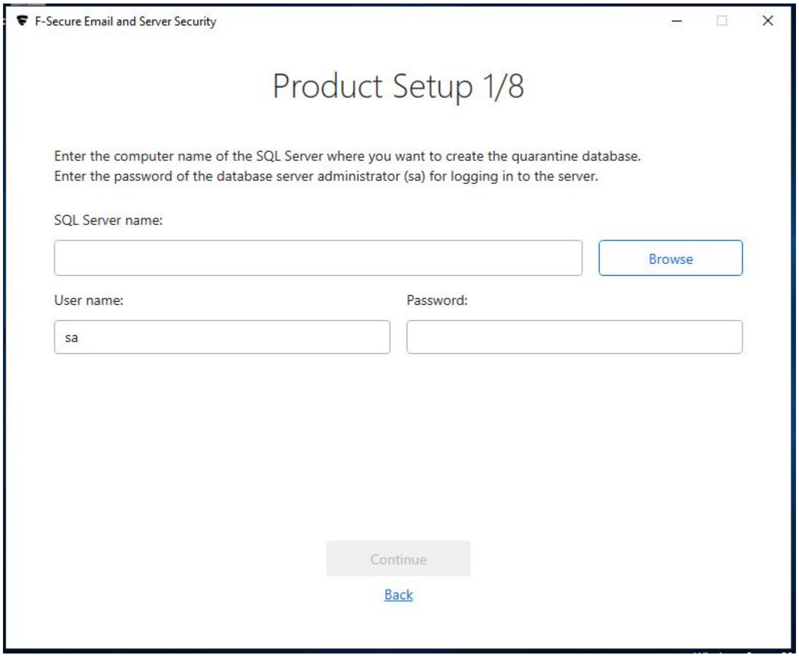
6.3.1 Installing on clusters with quarantine as cluster resource

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

Product Setup 1/8

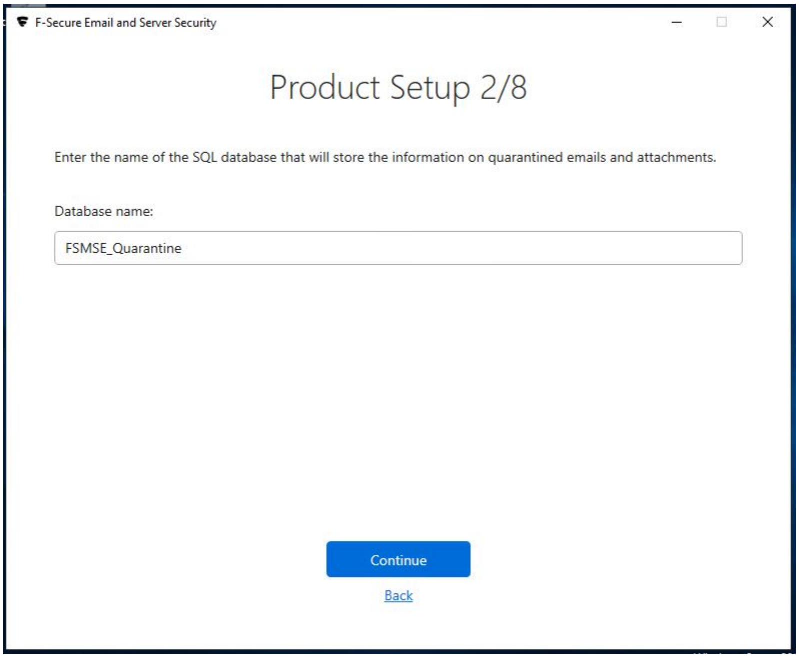
Enter the computer name of the SQL Server where you want to create the quarantine database.
Enter the password of the database server administrator (sa) for logging in to the server.

SQL Server name:

User name: sa

Password:

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



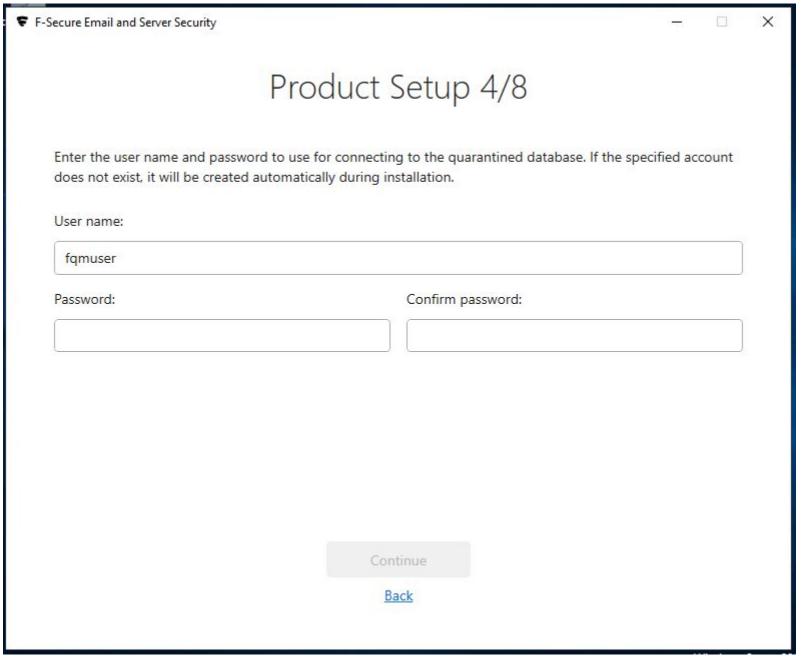
F-Secure Email and Server Security

Product Setup 2/8

Enter the name of the SQL database that will store the information on quarantined emails and attachments.

Database name: FSMSE_Quarantine

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



Product Setup 4/8

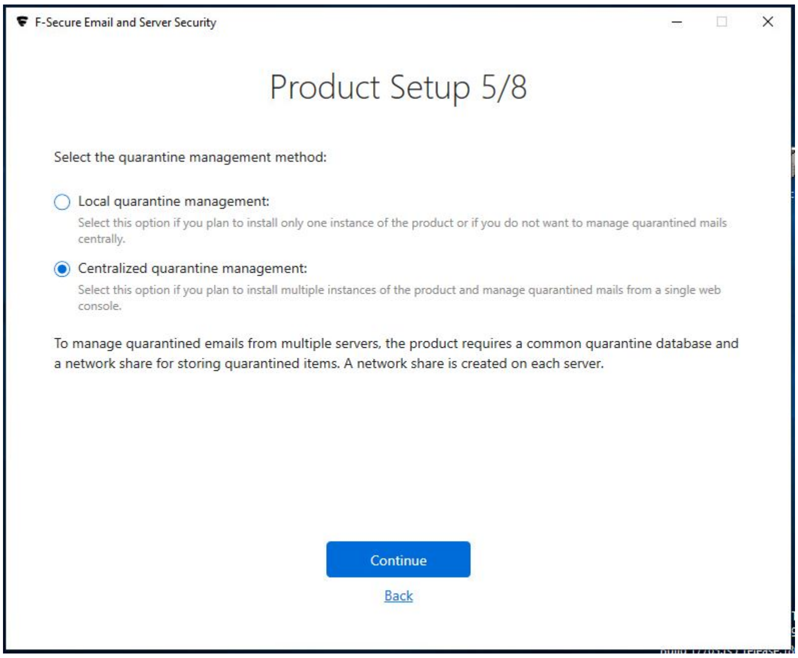
Enter the user name and password to use for connecting to the quarantined database. If the specified account does not exist, it will be created automatically during installation.

User name: fqmuser

Password:

Confirm password:

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



Product Setup 5/8

Select the quarantine management method:

○ Local quarantine management:

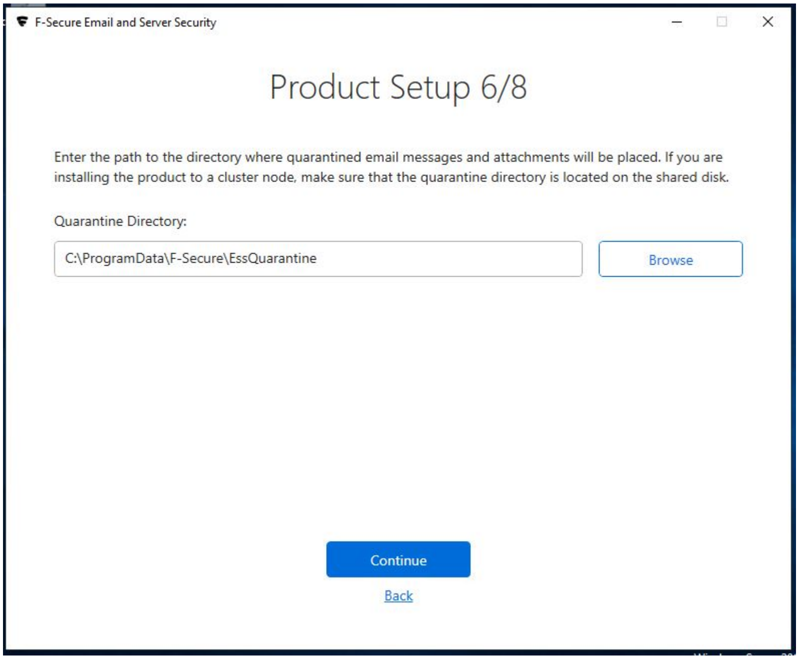
Select this option if you plan to install only one instance of the product or if you do not want to manage quarantined mails centrally.

● Centralized quarantine management:

Select this option if you plan to install multiple instances of the product and manage quarantined mails from a single web console.

To manage quarantined emails from multiple servers, the product requires a common quarantine database and a network share for storing quarantined items. A network share is created on each server.

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



F-Secure Email and Server Security

Product Setup 6/8

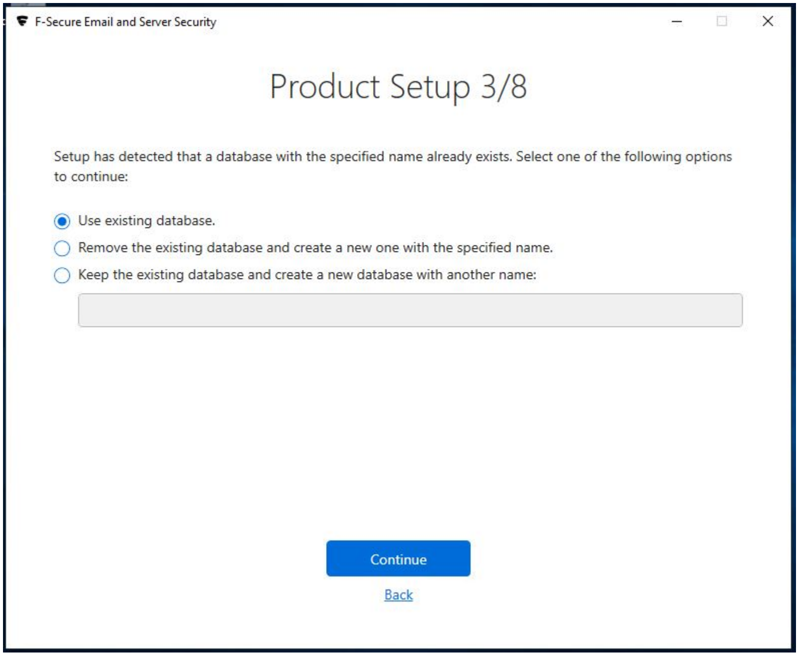
Enter the path to the directory where quarantined email messages and attachments will be placed. If you are installing the product to a cluster node, make sure that the quarantine directory is located on the shared disk.

Quarantine Directory: C:\ProgramData\F-Secure\EssQuarantine

Specify the UNC path to the Quarantine Storage share that you created before the installation as the Quarantine Directory. For example, `\\<EVSName>\FSAVMSEQS$`, where `<EVSName>` 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.



F-Secure Email and Server Security

Product Setup 3/8

Setup has detected that a database with the specified name already exists. Select one of the following options to continue:

● 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:

Select **Use existing database** and click **Continue**.

11. Complete the installation on the passive node.

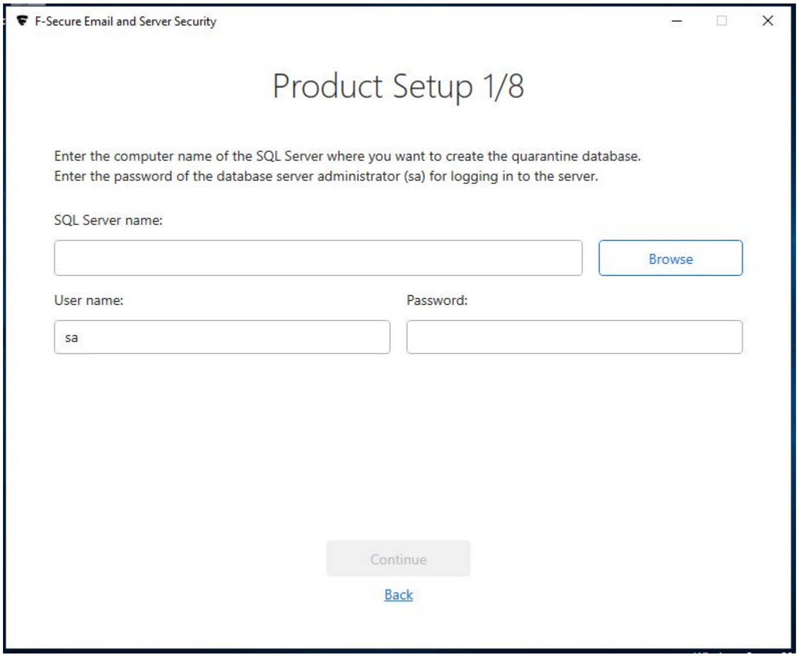
6.3.2 Installing on clusters with quarantine on a dedicated computer

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 1/8

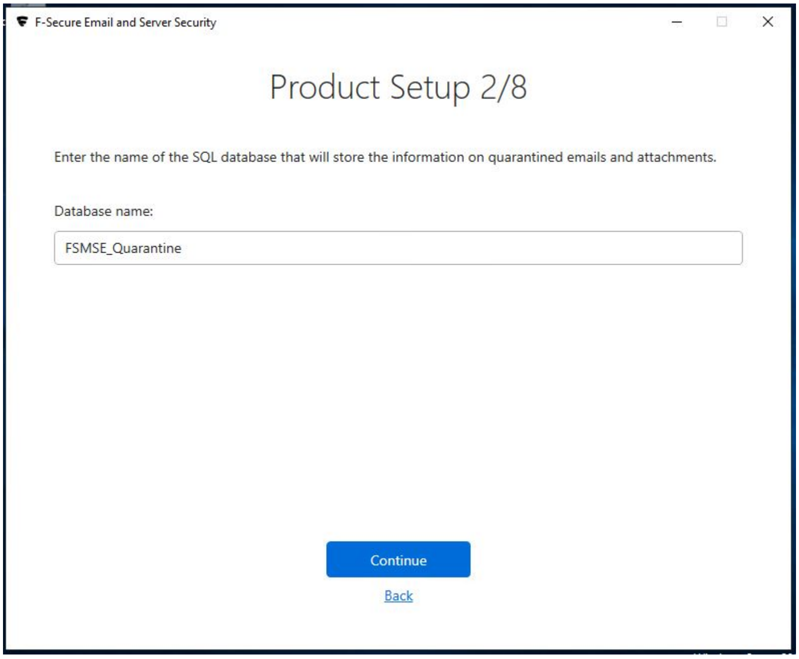
Enter the computer name of the SQL Server where you want to create the quarantine database.
Enter the password of the database server administrator (sa) for logging in to the server.

SQL Server name:

User name: sa

Password:

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



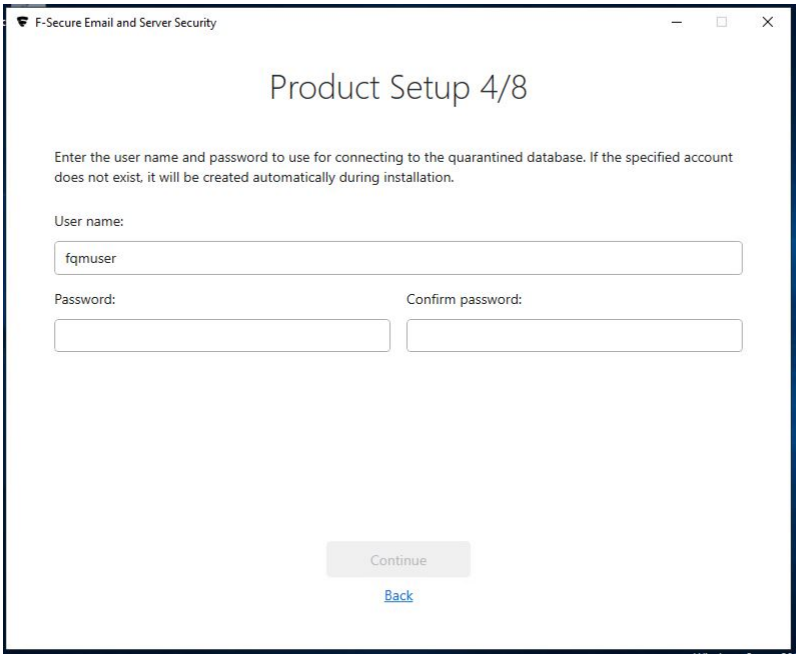
F-Secure Email and Server Security

Product Setup 2/8

Enter the name of the SQL database that will store the information on quarantined emails and attachments.

Database name: FSMSE_Quarantine

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



Product Setup 4/8

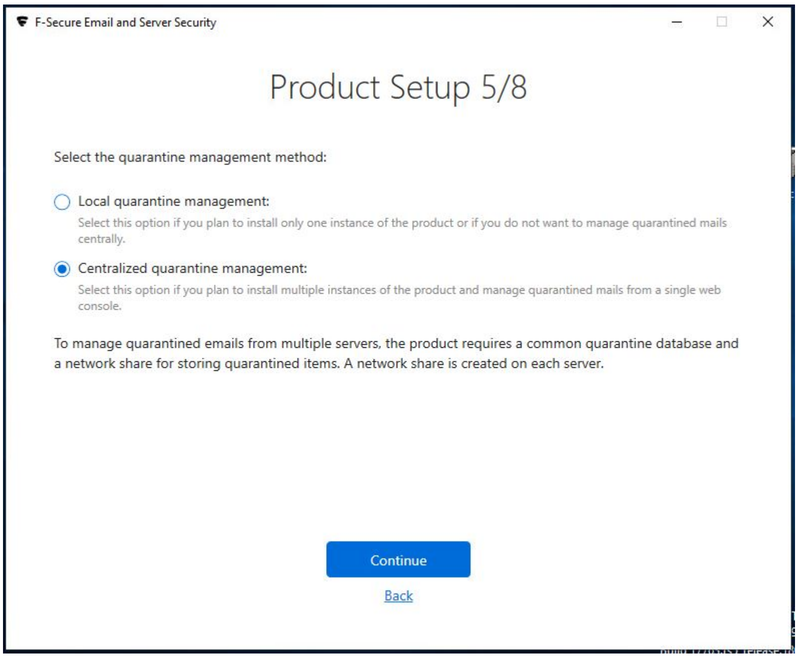
Enter the user name and password to use for connecting to the quarantined database. If the specified account does not exist, it will be created automatically during installation.

User name: fqmuser

Password:

Confirm password:

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



Product Setup 5/8

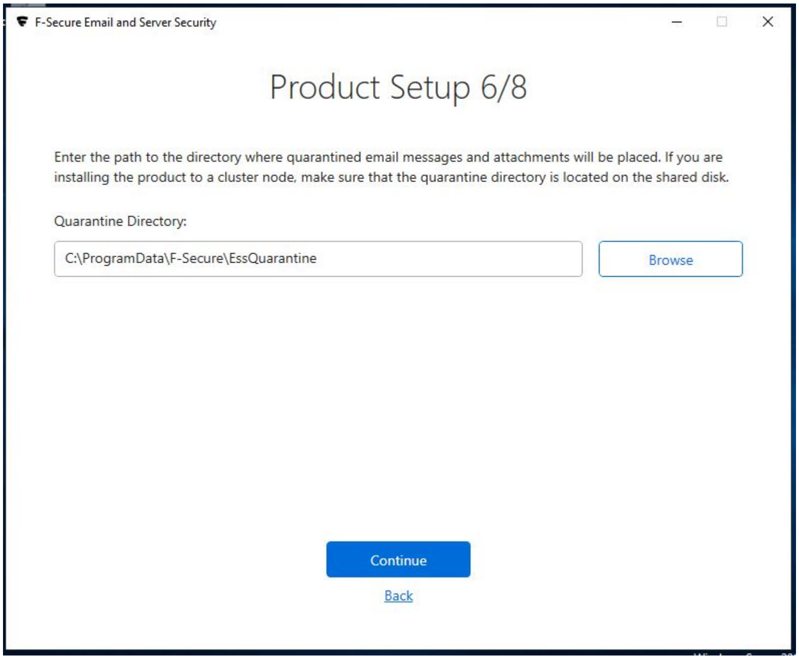
Select the quarantine management method:

○ Local quarantine management:
Select this option if you plan to install only one instance of the product or if you do not want to manage quarantined mails centrally.

● Centralized quarantine management:
Select this option if you plan to install multiple instances of the product and manage quarantined mails from a single web console.

To manage quarantined emails from multiple servers, the product requires a common quarantine database and a network share for storing quarantined items. A network share is created on each server.

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



Product Setup 6/8

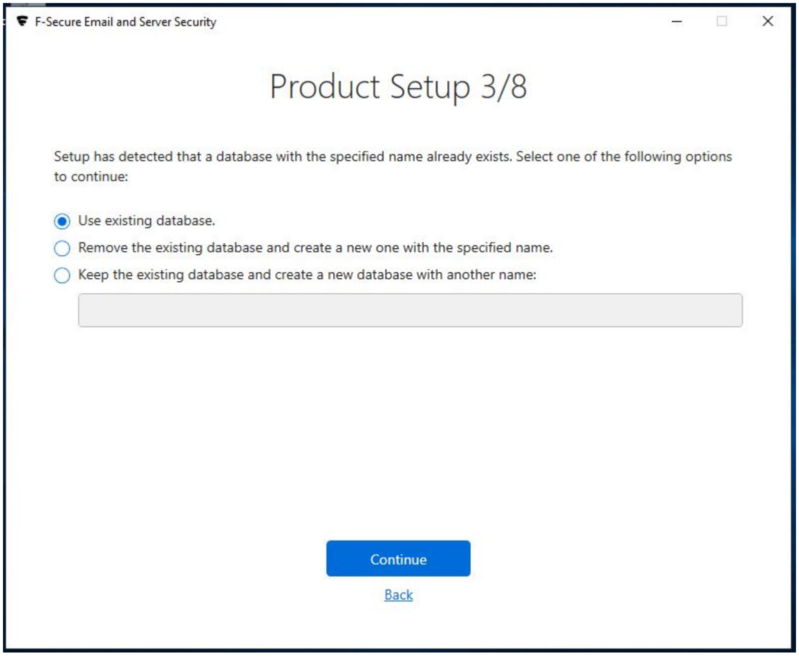
Enter the path to the directory where quarantined email messages and attachments will be placed. If you are installing the product to a cluster node, make sure that the quarantine directory is located on the shared disk.

Quarantine Directory: C:\ProgramData\F-Secure\EssQuarantine

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.



Product Setup 3/8

Setup has detected that a database with the specified name already exists. Select one of the following options to continue:

● 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:

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

To solve quarantine issues, if any:

- 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.

1. **Check permissions**

   in WebUI:

   - Check that the SQL server is accessible. You can do it through the WebUI page by selecting **Email quarantine** > **Options** > **Test database connection**.

   in Windows:

The F-Secure Quarantine Manager for Microsoft Exchange service should be run under the LocalSystem account.

Check the permission locally in the following way:

a. The Microsoft Exchange Transport service and hence our Transport Agent is running under **NETWORK SERVICE**. **NETWORK SERVICE** should have **Read** and **Execute** permissions on the `...Anti-Virus For Microsoft Services/` folder.

b. The `C:\ProgramData\F-Secure\EssTemp\` folder should have the following permissions:

LocalSystem - **Full**

Administrators - **Full**

NETWORK SERVICE - **Read**, **Write** and **Delete**

c. The `C:\ProgramData\F-Secure\EssLimited\` folder should have the following permissions:

LocalSystem - **Full**

Administrators - **Full**

NETWORK SERVICE - **Read** and **Delete**

d. The `C:\ProgramData\F-Secure\EssQuarantine\` quarantine folder should have the following permissions:

LocalSystem - **Full**

Administrators - **Full**

Check permissions for the network share if the centralized mode is used:

a. The F-Secure Quarantine Manager for Microsoft Exchange service account (SYSTEM by default) should have **Read**, **Write**, and **Change** permissions to the remote centralized quarantine (share & folder security tabs).

b. The Exchange Servers or specific Exchange computers and hosts should have **Read**, **Write** and **Delete** permissions on the Security and Share pages.

in the SQL management studio:

Check the following:

- the SQL instance is running;
- the mixed authentication mode is enabled;
- the database exists;
- the FQM user has **Write** permissions in database.

2. **The SQL path can't be found during setup**

   The setup will find the path if the SQL server is installed on the same server as Email and Server Security. If, for some reason, it can't find it, enter `.\sqlexpress` to locate it.

   If the SQL server is not installed on the same server, enter the network path to the SQL instance.

3. **Configuration tool (F-Secure.Ess.Config)**

   Make sure that the configuration tool is run under an admin account. If it it doesn't work, run as administrator.

   Important: Once all permissions have been set properly, you need to restart the F-Secure Quarantine Manager for Microsoft Exchange service.

Appendix A

Installing Microsoft SQL Server

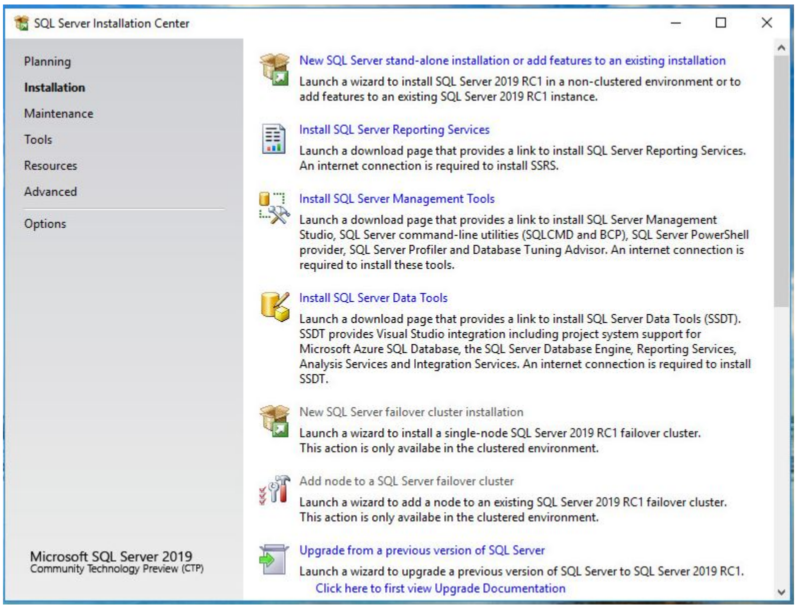
Topics:

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
Planning
Installation
Maintenance
Tools
Resources
Advanced
Options
Microsoft SQL Server 2019
Community Technology Preview (CTP)

New SQL Server stand-alone installation or add features to an existing 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.

Install SQL Server Reporting Services

Launch a download page that provides a link to install SQL Server Reporting Services. An internet connection is required to install SSRS.

Install SQL Server Management Tools

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.

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.

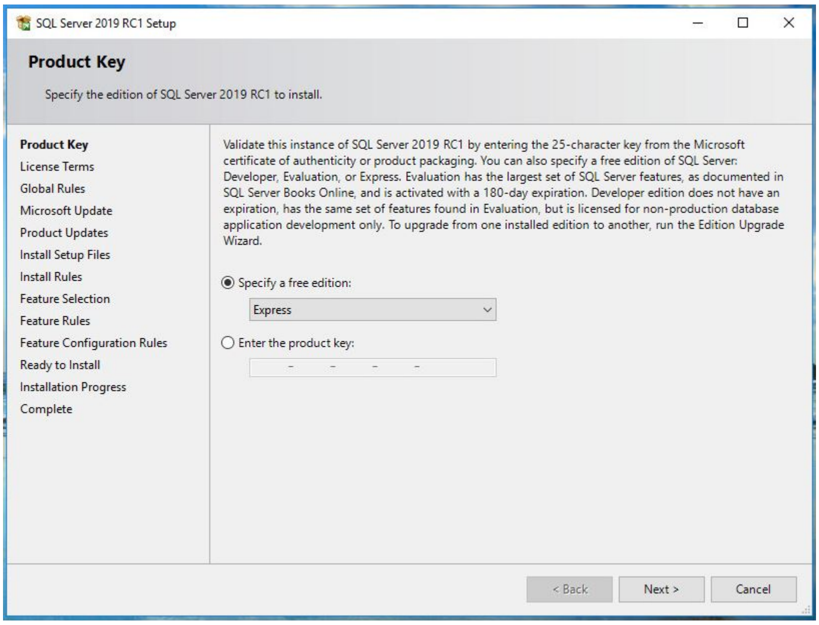
Add node to a SQL Server failover cluster

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.

Upgrade from a previous version of SQL Server

Launch a wizard to upgrade a previous version of SQL Server to SQL Server 2019 RC1.
Click here to first view Upgrade Documentation

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



Product Key

Specify the edition of SQL Server 2019 RC1 to install.

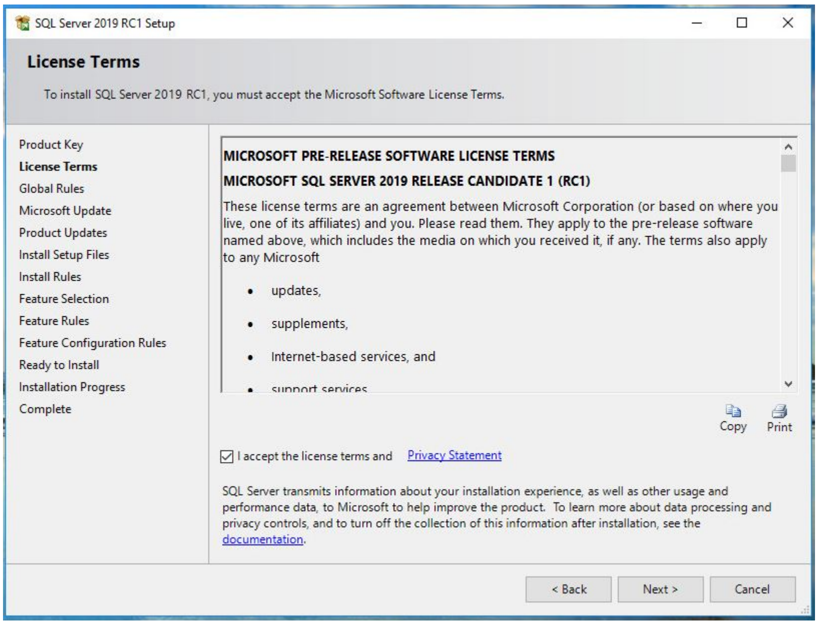
Validate this instance of SQL Server 2019 RC1 by entering the 25-character key from the Microsoft certificate of authenticity or product packaging. You can also specify a free edition of SQL Server: Developer, Evaluation, or Express. Evaluation has the largest set of SQL Server features, as documented in SQL Server Books Online, and is activated with a 180-day expiration. Developer edition does not have an expiration, has the same set of features found in Evaluation, but is licensed for non-production database application development only. To upgrade from one installed edition to another, run the Edition Upgrade Wizard.

● Specify a free edition: Express

○ Enter the product key: - - - -

4. Click **Next**.

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



License Terms

To install SQL Server 2019 RC1, you must accept the Microsoft Software License Terms.

MICROSOFT PRE-RELEASE SOFTWARE LICENSE TERMS

MICROSOFT SQL SERVER 2019 RELEASE CANDIDATE 1 (RC1)

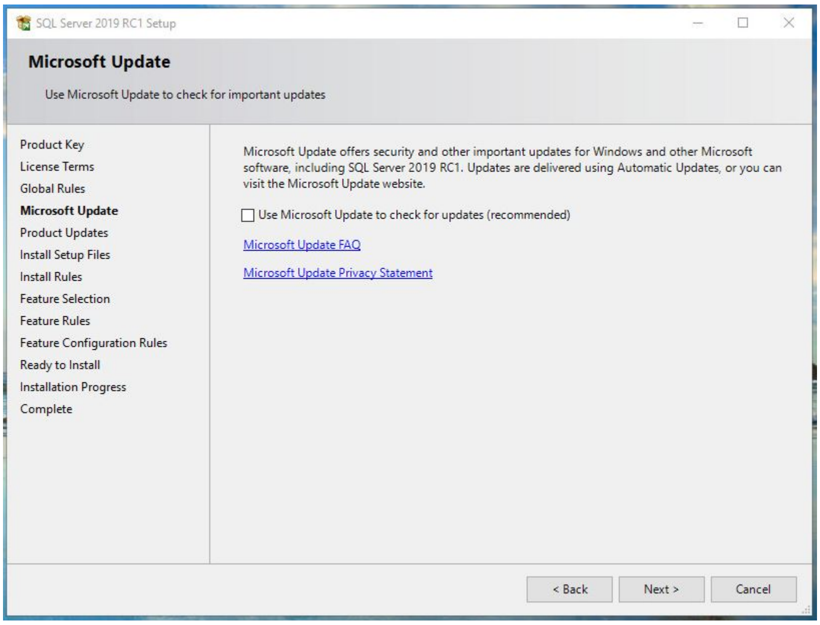
These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to the pre-release software named above, which includes the media on which you received it, if any. The terms also apply to any Microsoft

- updates,
- supplements,
- Internet-based services, and
- support services

☑ I accept the license terms and Privacy Statement

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**.



Microsoft Update

Use Microsoft Update to check for important updates

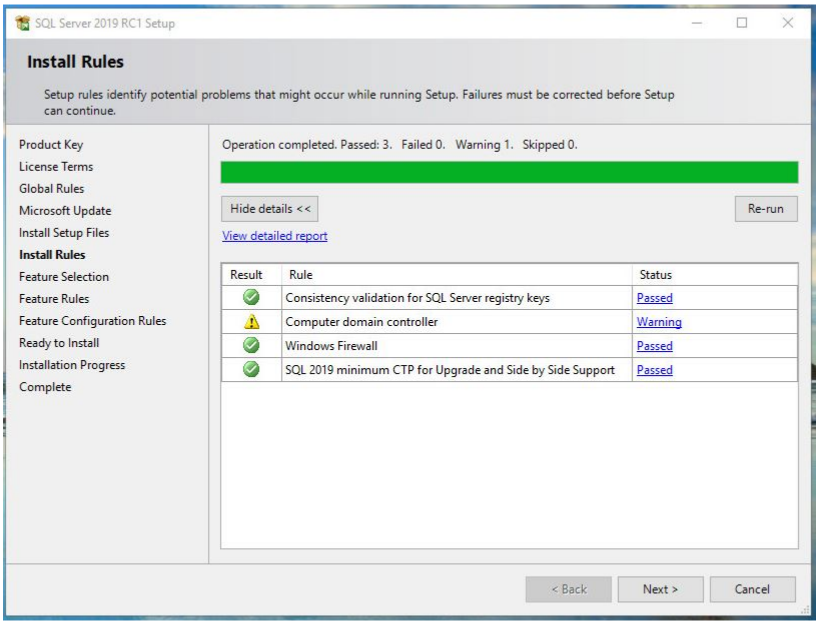
Microsoft Update offers security and other important updates for Windows and other Microsoft software, including SQL Server 2019 RC1. Updates are delivered using Automatic Updates, or you can visit the Microsoft Update website.

☐ Use Microsoft Update to check for updates (recommended)

Microsoft Update FAQ

Microsoft Update Privacy Statement

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



SQL Server 2019 RC1 Setup

Install Rules

Setup rules identify potential problems that might occur while running Setup. Failures must be corrected before Setup can continue.

Product Key
License Terms
Global Rules
Microsoft Update
Install Setup Files
Install Rules
Feature Selection
Feature Rules
Feature Configuration Rules
Ready to Install
Installation Progress
Complete

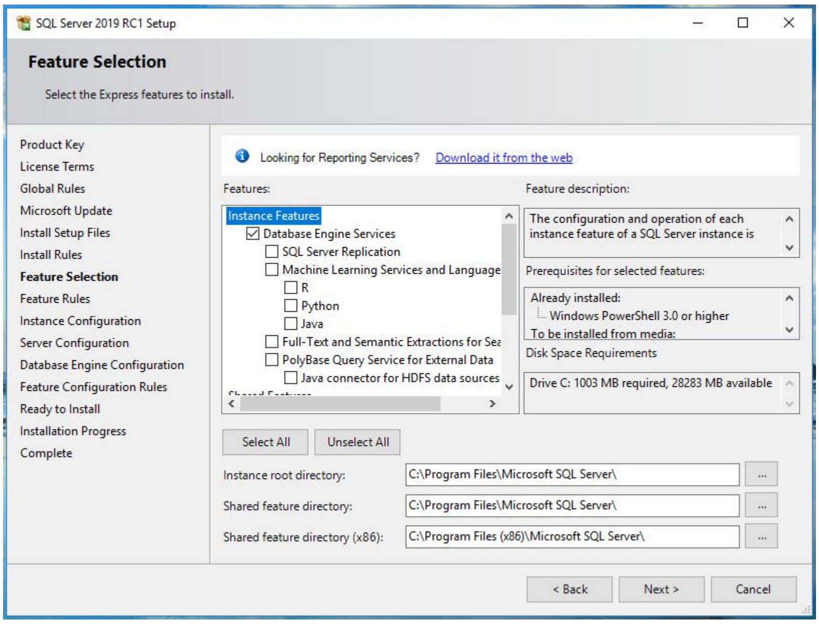
Operation completed. Passed: 3. Failed 0. Warning 1. Skipped 0.

View detailed report

Result	Rule	Status
✓	Consistency validation for SQL Server registry keys	Passed
⚠	Computer domain controller	Warning
✓	Windows Firewall	Passed
✓	SQL 2019 minimum CTP for Upgrade and Side by Side Support	Passed

8. Click **Next**.

9. Select the **Database Engine Services** feature.



SQL Server 2019 RC1 Setup

Feature Selection

Select the Express features to install.

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

Looking for Reporting Services? Download it from the web

Features:

Instance Features
☑ Database Engine Services
□ SQL Server Replication
□ Machine Learning Services and Language
□ R
□ Python
□ Java
□ Full-Text and Semantic Extractions for Sea
□ PolyBase Query Service for External Data
□ Java connector for HDFS data sources

Feature description:

The configuration and operation of each instance feature of a SQL Server instance is

Prerequisites for selected features:

Already installed:
Windows PowerShell 3.0 or higher
To be installed from media:

Disk Space Requirements

Drive C: 1003 MB required, 28283 MB available

Instance root directory: C:\Program Files\Microsoft SQL Server\

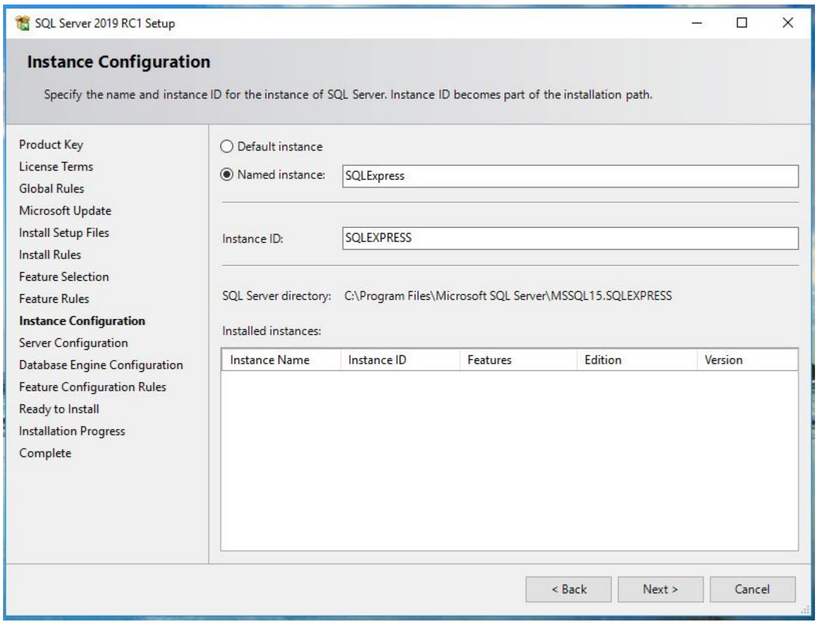
Shared feature directory: C:\Program Files\Microsoft SQL Server\

Shared feature directory (x86): C:\Program Files (x86)\Microsoft SQL Server\

10. Click **Next**.

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

You can use the default name (`SQLExpress`).



SQL Server 2019 RC1 Setup

Instance Configuration

Specify the name and instance ID for the instance of SQL Server. Instance ID becomes part of the installation path.

○ Default instance

● Named instance: SQLExpress

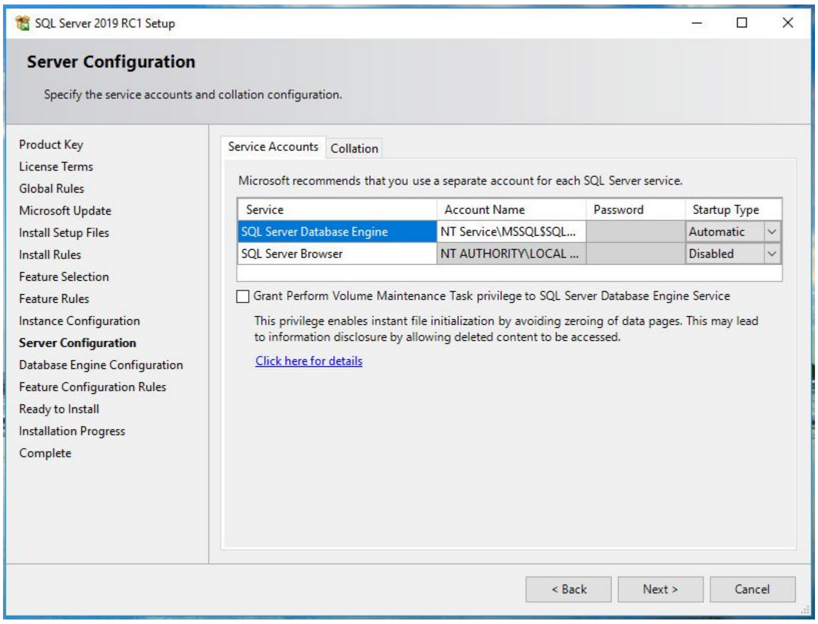
Instance ID: SQLEXPRESS

SQL Server directory: C:\Program Files\Microsoft SQL Server\MSSQL15.SQLEXPRESS

Installed instances:

Instance Name	Instance ID	Features	Edition	Version

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



SQL Server 2019 RC1 Setup

Server Configuration

Specify the service accounts and collation configuration.

Microsoft recommends that you use a separate account for each SQL Server service.

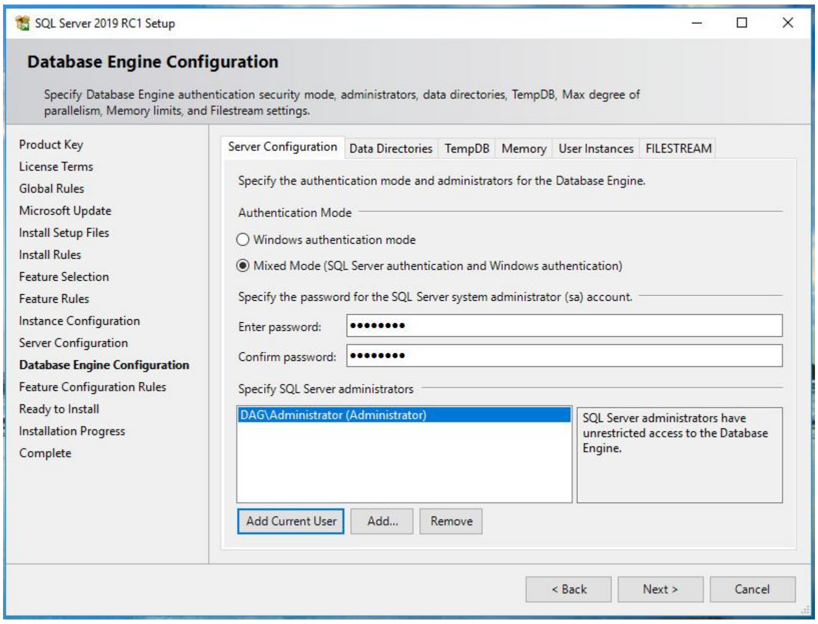
Service	Account Name	Password	Startup Type
SQL Server Database Engine	NT Service\MSSQL$SQL...		Automatic
SQL Server Browser	NT AUTHORITY\LOCAL ...		Disabled

□ Grant Perform Volume Maintenance Task privilege to SQL Server Database Engine Service

This privilege enables instant file initialization by avoiding zeroing of data pages. This may lead to information disclosure by allowing deleted content to be accessed.

Click here for details

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



SQL Server 2019 RC1 Setup

Database Engine Configuration

Specify Database Engine authentication security mode, administrators, data directories, TempDB, Max degree of parallelism, Memory limits, and Filestream settings.

Specify the authentication mode and administrators for the Database Engine.

Authentication Mode

○ Windows authentication mode

● Mixed Mode (SQL Server authentication and Windows authentication)

Specify the password for the SQL Server system administrator (sa) account.

Enter password: ••••••••

Confirm password: ••••••••

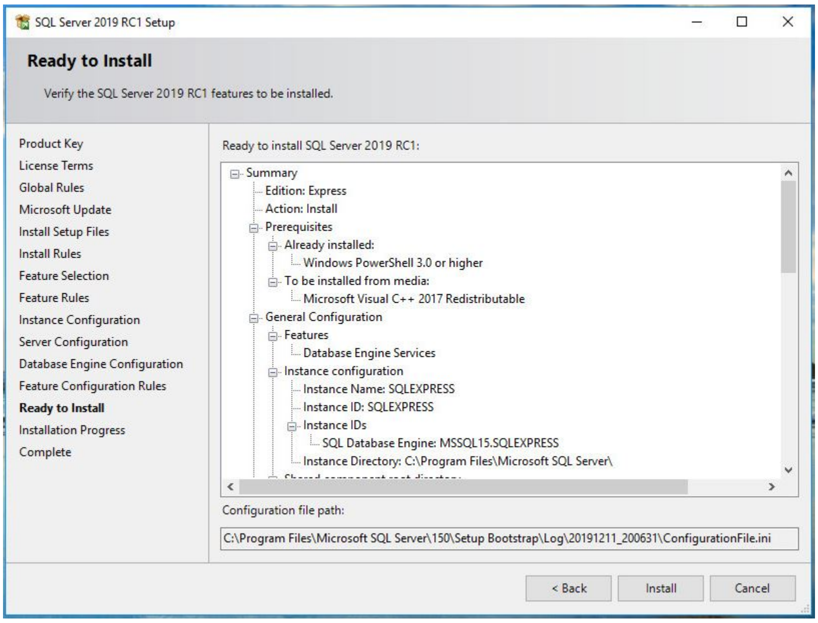
Specify SQL Server administrators

DAG\Administrator (Administrator)

SQL Server administrators have unrestricted access to the Database Engine.

14. Click **Next**.

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



SQL Server 2019 RC1 Setup

Ready to Install

Verify the SQL Server 2019 RC1 features to be installed.

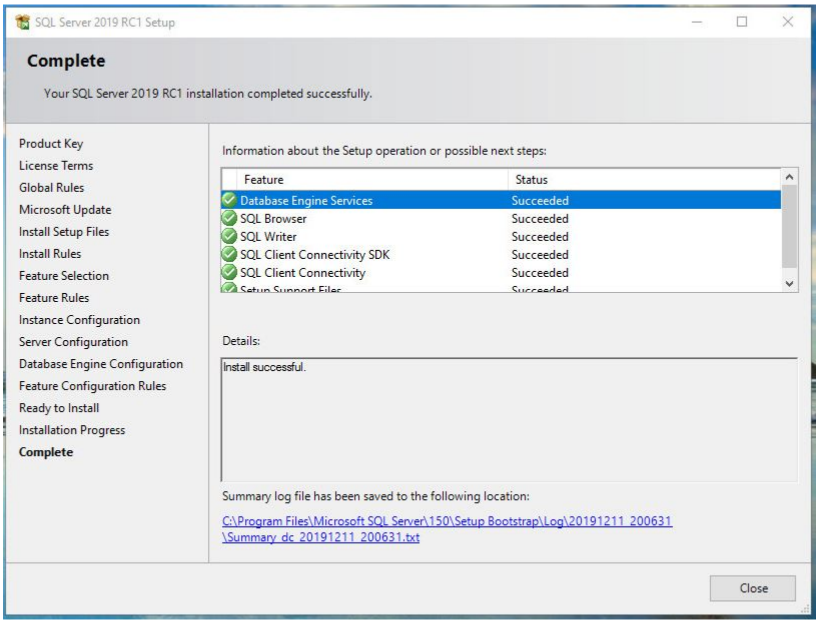
Ready to install SQL Server 2019 RC1:

```
Summary
  Edition: Express
  Action: Install
  Prerequisites
    Already installed:
      Windows PowerShell 3.0 or higher
    To be installed from media:
      Microsoft Visual C++ 2017 Redistributable
  General Configuration
    Features
      Database Engine Services
    Instance configuration
      Instance Name: SQLEXPRESS
      Instance ID: SQLEXPRESS
      Instance IDs
        SQL Database Engine: MSSQL15.SQLEXPRESS
      Instance Directory: C:\Program Files\Microsoft SQL Server\
```

Configuration file path:

C:\Program Files\Microsoft SQL Server\150\Setup Bootstrap\Log\20191211_200631\ConfigurationFile.ini

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



Complete

Your SQL Server 2019 RC1 installation completed successfully.

Information about the Setup operation or possible next steps:

Feature	Status
Database Engine Services	Succeeded
SQL Browser	Succeeded
SQL Writer	Succeeded
SQL Client Connectivity SDK	Succeeded
SQL Client Connectivity	Succeeded
Setup Support Files	Succeeded

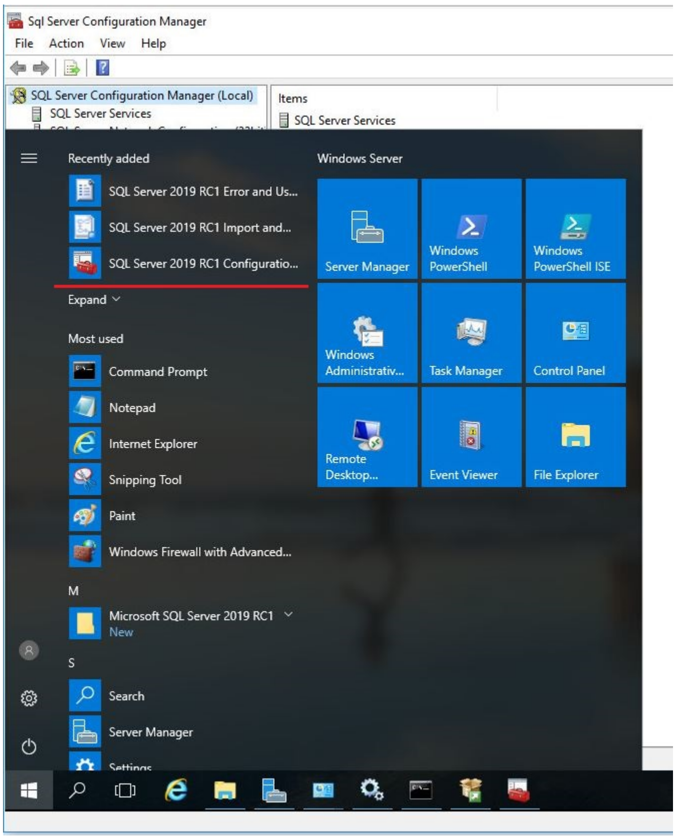
Details:

Install successful.

Summary log file has been saved to the following location:

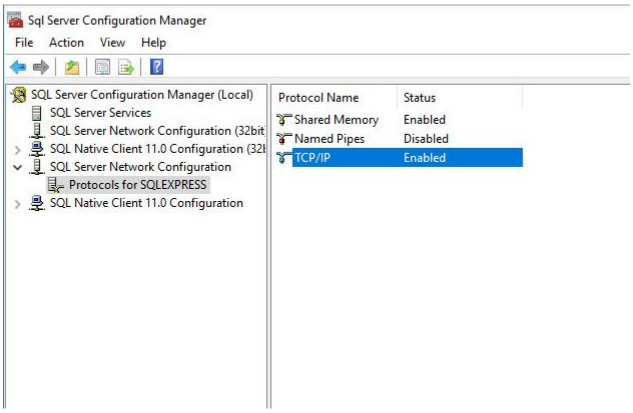
C:\Program Files\Microsoft SQL Server\150\Setup Bootstrap\Log\20191211_200631\Summary_dc_20191211_200631.txt

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



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

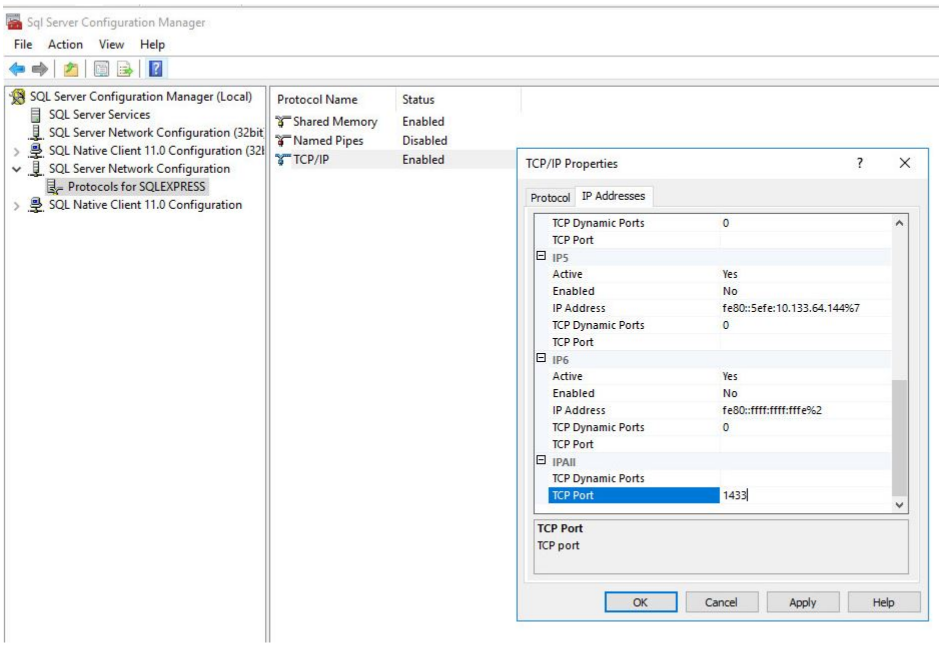
If you did not use the default name for the SQL instance, you will see Protocols for <name> instead.



- SQL Server Configuration Manager (Local)
  - SQL Server Services
  - SQL Server Network Configuration (32bit
  - SQL Native Client 11.0 Configuration (32l
  - SQL Server Network Configuration
    - Protocols for SQLEXPRESS
  - SQL Native Client 11.0 Configuration

Protocol Name	Status
Shared Memory	Enabled
Named Pipes	Disabled
TCP/IP	Enabled

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).



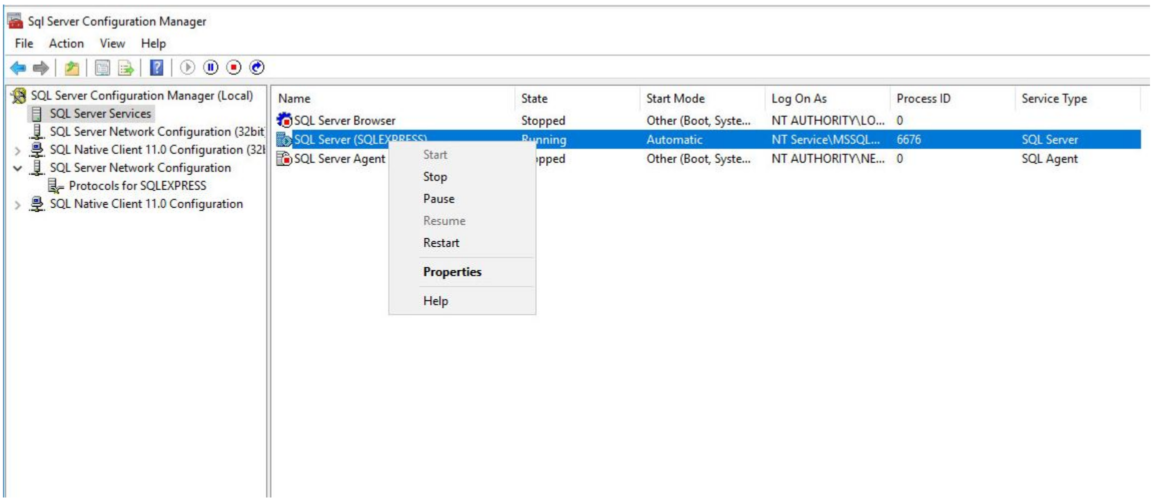
- SQL Server Configuration Manager (Local)
  - SQL Server Services
  - SQL Server Network Configuration (32bit
  - SQL Native Client 11.0 Configuration (32l
  - SQL Server Network Configuration
    - Protocols for SQLEXPRESS
  - SQL Native Client 11.0 Configuration

Protocol Name	Status
Shared Memory	Enabled
Named Pipes	Disabled
TCP/IP	Enabled

TCP Dynamic Ports	0
TCP Port	
⊟ IP5	
Active	Yes
Enabled	No
IP Address	fe80::5efe:10.133.64.144%7
TCP Dynamic Ports	0
TCP Port	
⊟ IP6	
Active	Yes
Enabled	No
IP Address	fe80::ffff:ffff:fffe%2
TCP Dynamic Ports	0
TCP Port	
⊟ IPAll	
TCP Dynamic Ports	
TCP Port	1433

TCP Port
TCP port

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 (Local)
  - SQL Server Services
  - SQL Server Network Configuration (32bit
  - SQL Native Client 11.0 Configuration (32l
  - SQL Server Network Configuration
    - Protocols for SQLEXPRESS
  - SQL Native Client 11.0 Configuration

Name	State	Start Mode	Log On As	Process ID	Service Type
SQL Server Browser	Stopped	Other (Boot, Syste...	NT AUTHORITY\LO...	0	
SQL Server (SQLEXPRESS)	Running	Automatic	NT Service\MSSQL...	6676	SQL Server
SQL Server Agent	...pped	Other (Boot, Syste...	NT AUTHORITY\NE...	0	SQL Agent

22. Close SQL Server Configuration Manager.