Symantec™ Mail Security for Microsoft® Exchange 7.10 Release Notes

Copyright statement

About Symantec Mail Security for Microsoft Exchange

Symantec™ Mail Security for Microsoft® Exchange (Mail Security) provides a complete, customizable, and scalable solution that scans the emails that transit or reside on the Microsoft Exchange Server.

Mail Security protects your Exchange server from the following:

- Threats (such as viruses, Trojan horses, worms, and denial-of-service attacks)
- Security risks (such as adware and spyware)
- Unwanted content
- Unwanted file attachments
- Unsolicited email messages (spam)

Mail Security also lets you manage the protection of one or more Exchange servers from a single console.

The Exchange environment is only one avenue by which a threat or a security risk can penetrate a network. For complete protection, ensure that you protect every computer and workstation by an antivirus solution.

What's new in Mail Security 7.10

Feature	Description
Active content filtering	Mail Security contains a new antivirus rule that filters active content from your documents. Active content in a file is functionality that runs without a user's knowledge (such as a macro or a script). Active content can execute malicious code. Mail Security can remove active content from certain document types. However, it does not determine if the active content is malicious or benign. Mail Security deletes the content based on the content type. Active content filtering is disabled by default.
High-intensity detection	This release of Mail Security replaces Bloodhound antivirus detections with High-intensity detection (HID). HID lets you control the intensity for detecting threats and acting on them. You also control how frequently possible threats are reported. HID ensures that you do not automatically block files without understanding their behavior or risk, which retains maximum visibility on the newly detected files.
Microsoft Exchange Server 2010	Mail Security no longer supports Microsoft Exchange Server 2010.
Background scanning	Since background scanning was only supported on Microsoft Exchange Server 2010, this feature has been removed from the console and documentation.
Rapid Release definitions	Mail Security no longer supports Rapid Release definitions. References to Rapid Release has been removed from the console and documentation.
Whitelist	The Whitelist is now referred to in the console and documentation as the Allow list. No other changes are made to this feature.

System requirements

Ensure that you meet the appropriate system requirements for the type of installation that you want to perform.

Server system requirements

Console system requirements

Port requirements

Console system requirements

You can install the Mail Security console on a computer on which Mail Security is not installed.

Table 1: Console system requirements

Requirement	Description
Operating system	Mail Security supports the following operating systems: • Windows 7 • Windows 8 • Windows 2012 • Windows 10 • Windows Server 2016 Standard or Datacenter • Windows Server 2019 Standard or Datacenter Mail Security Console supports 64-bit processors on all supported operating systems.
Memory	2 GB
Available disk space	2 GB This requirement does not include the space that Mail Security requires for items such as quarantined messages and attachments, reports, and log data.
.NET Framework	Version 4.5 Ensure that .NET Framework is installed before you install Mail Security.

Adobe Acrobat Reader is not a requirement to install and run the Mail Security console. However, it is required to view the reports that are generated in .pdf format. You can download Adobe Acrobat Reader from http://www.adobe.com. You must also have Internet Explorer 8.0 or later to view the reports.

The following list provides the supported browsers for the Mail Security online help.

- Google Chrome[1]
- Microsoft Edge[1]
- Mozilla Firefox[1]
- Apple Safar on MacOS[1]
- Apple Safar on iOS 12.x or later

[1] These browsers have release updates every few months. Support levels will be maintained for upcoming versions of these browsers.

Server system requirements

You must have domain administrator-level privileges to install Mail Security.

The server system requirements are as follows:

Exchange platform	• Exchange Server 2013 (Mailbox, Edge Role) – Windows Server 2012 R2 Standard or Datacenter – Windows Server 2012 Standard or Datacenter – Windows Server 2008 R2 Standard SP1 – Windows Server 2008 R2 Enterprise SP1 – Windows Server 2008 R2 Datacenter RTM or later • Exchange Server 2016 (Mailbox, Edge Role) – Windows Server 2016 Standard or Datacenter – Windows Server 2012 R2 Standard or Datacenter – Windows Server 2012 Standard or Datacenter • Exchange Server 2019 (Mailbox, Edge Role) – Windows Server 2019 Standard or Datacenter – Windows Server 2019 Core
Minimum system requirements	• 2 GB of memory for Mail Security besides the minimum requirements for the operating system and Exchange. Approximately 4GB or more of memory is required. • 4 GB disk space is required for Mail Security. This space does not include the disk space that is required for items such as quarantined messages and attachments, reports, and log data. • Microsoft Internet Information Services (IIS) Manager • Microsoft .NET Framework – Exchange Server 2013 and later: .NET Framework 4.5 • Microsoft ASP.NET – Exchange Server 2013 and later: Microsoft ASP.NET 4.5 extension • MDAC 2.8 or later • DirectX 9 or later

Ensure that the components.NET Framework, MDAC, and DirectX are installed before you install Mail Security.

Adobe Acrobat Reader is not a requirement to install and run Mail Security. However, it is required to view the reports that are generated in .pdf format. You can download Adobe Acrobat Reader from http://www.adobe.com. You must also have Internet Explorer 8.0 or later to view the reports.

For more information, see the *Symantec Mail Security for Microsoft Exchange Implementation Guide*.

Port requirements

Symantec Mail Security for Microsoft Exchange scans the SMTP mail traffic that passes through Exchange servers on port 25. Mail Security does not interact with MAPI or any other mail protocols, such as POP3 on port 110 or IMAP on port 143.

Some Mail Security components require certain ports for communication.

Ports used by Mail Security components lists the ports that Mail Security components use by default.

Table 2: Ports used by Mail Security components

Mail Security component	Port	Process	Purpose
Conduit	443	Conduit.exe	Continuous Premium AntiSpam updates
DEXL Service	8081	Process ID: 0 or 4 (System)	Console communications

Mail Security component	Port	Process	Purpose
CmafReportSrv	58081	CmafReportSrv.exe	Reporting database

NOTE

If Symantec Premium AntiSpam is enabled, ensure that you open port 443 on the firewall for bi-directional traffic to aztec.brightmail.com. If Symantec Premium AntiSpam is not licensed and enabled, Mail Security does not initiate activity on port 443.

The port that is used for communication with Mail Security Console can be configured during installation or at any time after the installation. You can see activity only on these ports when you use the console to administer a remote server.

NOTE

There are no port conflicts or incompatibility between Mail Security and Symantec Endpoint Protection 11.x or the Symantec Endpoint Protection Manager.

Console system requirements

Server system requirements

Where to get more information about Mail Security

Resource	Description
Technical Support	• Create, track, or update support service tickets. • Download license files. • Download product updates. • Access product training. • Access knowledge base articles, product news, and community posts about Mail Security. • Access Mail Security documentation. • Register to receive notifications about Mail Security. https://support.broadcom.com/security
Context-sensitive help	Mail Security includes a comprehensive Help system that contains conceptual, procedural, and context-sensitive information. Press F1 to access information about the page you're viewing.
Online help	View the Mail Security online help, which contains topics relating to the installation and Mail Security configuration. https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/symantec-mail-security-for-microsoft-exchange-server/7-10.html
PDFs	Access the **Related Documents** topic in the online help for links to the published Mail Security .pdf files.


Symantec
A Division of Broadcom