

RELEASE NOTES

F-Secure® Anti-Virus for Windows Servers
Version 9.00 build 333



Copyright © 1993-2010 F-Secure Corporation. All Rights Reserved.
Portions Copyright © 2004 BackWeb Technologies Inc.

This product may be covered by one or more F-Secure patents, including the following: GB2353372, GB2366691, GB2366692, GB2366693, GB2367933, GB2368233, GB2374260

1. General

This document contains late-breaking information about F-Secure Anti-Virus for Windows Servers 9.00. We strongly recommend you to read the entire document before installing the software.

1.1 What's in this file

Installation and system requirements

Product contents

New features

Known issues

Contact information

1.2 Product contents

F-Secure Anti-Virus for Windows Servers 9.00 contains the following components:

Virus & Spy Protection that includes Virus protection, Anti-Spyware and Blacklight features that scan the server for hidden malware.

Automatic updates, which enables you to keep the protection up-to-date against the latest threats.

2. Installation and System requirements

Before you install the product, we recommend you review sections in this topic to ensure that your network, hardware, software, and other system components meet the requirements for F-Secure Anti-Virus for Windows Servers 9.00.

Note: When running multiple services on the same system, minimum hardware requirements may not be sufficient.

2.1 System requirements

The minimum system requirements for F-Secure Anti-Virus for Windows Servers 9.00:

Processor: any processor that can run Microsoft Windows Server 2003/2008

Memory: 512MB

Operating System: Microsoft Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Small Business Server 2003, Small Business Server 2008

Disk space: at least 200MB

Display: at least 8-bit (256 colors)

Internet Connection: an Internet connection is required to validate your subscription and to receive updates

Web browser: Internet Explorer 6.0 or newer

The recommended system requirements for F-Secure Anti-Virus for Windows Servers 9.00:

Processor: Intel Pentium 4 2GHz or higher

Memory: 1GB or more

Operating System: Microsoft Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Small Business Server 2003, Small Business Server 2008

Disk space: 300MB free or more

Display: 16-bit or more (65000 colors)

Internet Connection: an Internet connection is required to validate your subscription and to receive updates

Web browser: Internet Explorer 6.0 or newer

2.2 Citrix Environments

F-Secure Anti-Virus for Windows Servers 9.00 supports the following Citrix platforms:

Citrix XenApp 5.0

Citrix Presentation Server 4.5

2.3 Centralized management requirements

Important: F-Secure Policy Manager 9.00 or later is required if you plan to install the product in the centralized administration mode and manage it with F-Secure Policy Manager Console. F-Secure Policy Manager must be upgraded before installing F-Secure Anti-Virus for Windows Servers 9.00. If the product is installed in the centrally administered mode with F-Secure Policy Manager Console version 8.11 or older, scanning will not be possible as virus definition database updates will not be received by Aquarius scanning engine.

2.4 Upgrade from previous versions

You can upgrade product versions 8.00 and 8.01 to F-Secure Anti-Virus for Windows Servers 9.00. It is also possible to upgrade from F-Secure Anti-Virus for Windows Servers 9.00 Beta or Release Candidate versions. Note that the system reboot may be required after upgrade.

3. What's new

3.1 Key features

Web-based console - F-Secure Anti-Virus for Windows Servers 9.00 is managed with the web-based administration console. The product can be managed both remotely and locally with the Web Console. The old local user interface does not exist any more.

Performance improvements - F-Secure's multi-engine protection has been upgraded to offer faster malware scanning and smaller memory usage while keeping the detection rate on highest possible level. Also, the number of active processes has been reduced and scanning components are made less CPU intensive, which result in faster boot-up time and better coexistence with backup software.

Windows Server 2008 R2 support - F-Secure Anti-Virus for Windows Servers 9.00 supports Microsoft Windows Server 2008 R2 Standard/Enterprise, and Microsoft Windows Server 2008 R2 Foundation.

Server Core support - this release supports Microsoft Windows Server 2008 x32/x64 and Windows Server 2008 R2 Server Core editions.

Common Web console for the server products - when F-Secure Anti-Virus for Windows Servers 9.00 and F-Secure Anti-Virus for Microsoft Exchange 9.00 are installed on the same server, both products are managed with a common Web Console.

Updated identification and removal of conflicting programs (sidegrade) - the product installer can detect and remove a wider range of conflicting products, and some software which does not cause any conflicts with the product is not removed anymore.

3.2 Dropped or unsupported features

Security News - the Security News feature has been removed, since it has not been in active use for several years.

Tivoli plug-in and SNMP support - the Tivoli plug-in and SNMP support has been removed, to simplify product installation and to increase performance.

Windows 2000 Server family - the product does not support Windows 2000 Server and Windows 2000 Advanced Server platforms anymore.

3.3 Fixed issues from previous releases

These issues have been fixed in this release:

FSM32 process may leak memory when starting manual scanning from the system tray [67390]

F-Secure Gatekeeper errors in Windows System event log [65398]

Blue Screen of Death interoperability issue with Parallels virtualization software [65397]

Multiple GUI related problems on Citrix environments [65411, 65479]

F-Secure Anti-Virus for Windows Servers performance issue with Symantec Enterprise Vault [68685]

4. Using Web Console

To open F-Secure Anti-Virus for Windows Servers Web Console, follow these instructions:

- Go to *Windows Start menu > Programs > F-Secure Anti-Virus for Windows Servers > F-Secure Anti-Virus for Windows Servers Web Console*, or
- Enter the IP address of F-Secure Anti-Virus for Windows Servers and the port number in your web browser. Note that the protocol used is *https*. For example:
<https://127.0.0.1:25023>

When the Web Console login page opens, enter your user name and the password and click **Log In**. Note that you need administrator rights to the host where F-Secure Anti-Virus for Windows Servers Web Console is installed to log in to Web Console.

4.1 Logging in for the First Time

Before you log in F-Secure Anti-Virus for Windows Servers Web Console for the first time, check that JavaScript and cookies are enabled in the browser.

Microsoft Internet Explorer users: You need to add the address of F-Secure Anti-Virus for Windows Servers Web Console (<https://127.0.0.1:25023/>) to the *Trusted sites* in the Internet Explorer security options to ensure that F-Secure Anti-Virus for Windows Servers Web Console works properly.

When you log in for the first time, your browser displays a *Security Alert* dialog window about the security certificate for F-Secure Anti-Virus for Windows Servers Web Console. You can install the security certificate before logging as described below. After you install the certificate, you will not see the Security Alert window again.

1. Open F-Secure Anti-Virus for Windows Servers Web Console. The Security Alert about F-

Secure Anti-Virus for Windows Servers Web Console certificate is displayed.

If you are using Internet Explorer 7 or 8, click **Continue** and then **Certificate Error**.

2. Click **View Certificate** to view the certificate information. The Certificate window opens.
3. Click **Install Certificate** to install the certificate with the Certificate Import Wizard. The Certificate window opens.

If your company has an established process for creating and storing certificates, follow that process to create and store the security certificate for F-Secure Anti-Virus for Windows Servers Web Console.

4. Click **Install Certificate** to proceed to the Certificate Import Wizard.
5. Follow the instructions in the Certificate Import Wizard.
If you are using Internet Explorer 7 or 8, select the Trusted Root Certification Authorities store in the *Place all certificates in the following store* selection. If you are using Internet Explorer 6, Click **Yes** when you are prompted to add the new certificate in the Certificate Root Store.
6. If the Security Alert window is still displayed, click **Yes** to proceed or log back in to F-Secure Anti-Virus for Windows Server Web Console.
7. Log in to the Web Console with your user name and the password when the login page opens.
8. The Web Console displays the product Home page when you log in. You can check server protection state on this page.

4.2 Using Web Console remotely

To access Anti-Virus for Windows Servers Web Console remotely, follow these instructions:

1. Log in to the Web Console locally on the server (<https://127.0.0.1:25023>).
2. Go to the *General > Administration* page and open the *Web Console* tab.
3. In *Allowed hosts* section, click **Add new hosts** link and enter the IP address of the remote host where you want to access the server.
4. On remote host, open <https://<IP address of the server>:25023> to open the Web Console.

5. Compatibility with F-Secure and third party products

5.1 Compatibility with F-Secure Policy Manager

The product can be installed on the same computer with F-Secure Policy Manager version 9.00. However, the installation order is important: F-Secure Policy Manager 9.00 **must** be installed first and F-Secure Anti-Virus for Windows Servers 9.00 only after that. Installing the products in different order will result to a non-working environment.

Older versions than 9.00 of F-Secure Policy Manager are not supported and cannot be used to manage the product, even if it is installed on a separate computer. Managing F-Secure Anti-Virus for Windows Servers 9.0 with earlier F-Secure Policy Manager version will prevent the virus definition updates from working.

5.2 Compatibility with F-Secure Anti-Virus for Microsoft Exchange

F-Secure Anti-Virus for Windows Servers 9.00 can be installed on the same server with F-Secure Anti-Virus for Microsoft Exchange 9.00. These two products can be installed in any order.

Note: F-Secure Anti-Virus for Windows Servers 9.00 does not coexist with F-Secure Anti-Virus for Microsoft Exchange 8.00 or older. It is recommended to use F-Secure Anti-Virus for Windows Servers 8.01 with older versions of F-Secure Anti-Virus for Microsoft Exchange on the same server.

As F-Secure Anti-Virus for Windows Servers 9.00 scans all the files that are accessed on the server in real-time, the scan would interfere with any operation of an e-mail scanning product, unless those files were excluded from the real-time scan. During the installation, F-Secure Anti-Virus for Windows Servers 9.00 is configured to exclude from the real-time scan all folders that F-Secure Anti-Virus for Microsoft Exchange uses.

If F-Secure Anti-Virus for Microsoft Exchange configuration is changed after you install F-Secure Anti-Virus for Windows Servers 9.00 - for example, the location of the quarantine folder is changed - you need to reconfigure F-Secure Anti-Virus for Windows Servers 9.00 to exclude the correct folder from the real-time scan.

To update the configuration, follow these instructions:

1. Log on to the server with an account that has administration privileges.
2. Go to the installation directory of F-Secure Anti-Virus for Windows Servers 9.00. By default, this directory is in:
C:\Program Files\F-Secure\Anti-Virus (or in 64-bit servers: *C:\Program Files (x86)\F-Secure\Anti-Virus*).
3. Run the *cssecx.exe* program. This program detects the new configuration and updates the excluded folders list for F-Secure Anti-Virus for Windows Servers 9.00. The program does not require any user input after you run it.
Note: If you want to see the list of folders that will be excluded from the scan, run the *cssecx.exe* program from the command line (cmd.exe).

5.3 Compatibility with F-Secure Internet Gatekeeper (Windows)

F-Secure Anti-Virus for Windows Servers 9.00 does not coexist with any Windows version of F-Secure Internet Gatekeeper. If you are using F-Secure Internet Gatekeeper, you need to install F-Secure Anti-Virus for Windows Servers 8.01 on the same server if local server protection is required.

6. Known issues

6.1 Installation and uninstallation

Upgrade installation may require server restart [57103]

When the product is installed as an upgrade of the previous release, you may need to restart the server, as some files of the previous version may be locked during the installation.

If you upgrade the product remotely with F-Secure Policy Manager, the server may not restart automatically if the server restart has been disabled. You need to restart the server after the installation to make sure that all upgraded components are activated. In cases like these, F-Secure Management Agent service may remain stopped until the server is restarted. Although it is possible to start the service manually, it is not recommended, as the service may still be using some components of the previous product version.

Some files installed under "F-Secure" folder regardless of installation path [53259]

If you change the product installation folder to something other than the default folder, some files are still installed under the F-Secure folder in the Program Files (a directory tree ... \Program Files\F-Secure\common\custom is created during the installation).

F-Secure tray icon is not launched automatically after the remote installation from Policy Manager Console [65721]

To solve this, open the *Common* directory in F-Secure Anti-Virus for Windows Servers 9.00 installation directory (by default, *C:\Program Files\F-Secure\Common* or in 64-bit servers, *C:\Program Files (x86)\F-Secure\Common*), and start *fsm32.exe* manually.

Admin.pub cannot be located with Browse button during installation [69882]

When installing the product on Windows Server Core platform, the Browse button in the setup wizard is not functioning due to lack of the common Windows dialog. As the workaround, the path to the admin.pub file can be specified manually.

6.2 Automatic updates

Aquarius engine is not downloaded in some cases after upgrade from 8.00/8.01 [67819]

If the *Real-time Scanning* status on *Summary* page of Web Console is *Partially loaded* after all updates have been installed, this may indicate that Aquarius engine was not downloaded or installed properly. Reinstall the product to solve this issue.

Engine database dates are shown as 0-00-00 in the Plug-ins table [66561]

The database dates for Blacklight and/or USS engines may be shown as 0-00-00 in the Plug-ins table in F-Secure Anti-Virus statistics even though the latest database updates are installed. The problem is being investigated and planned to be fixed through automatic database updates.

6.3 Virus & Spy Protection

Real-time scanning may malfunction after installation [70488]

This may happen if the product doesn't receive database updates right after installation. Please make sure that the product can receive updates from F-Secure database update server or from the Policy Manager Server (if the product is installed in the centralized administration mode.)

Scanning big folders doesn't disinfect found malware if scanning is interrupted [68901]

When a manual scan task started from the Web Console is interrupted, the admin-defined actions may not take place for found malware or spyware items. You will need to run the manual scanning again and wait until it is completed.

"Hosts" file protection fails after installation [67246]

The *Hosts* file is not protected when the product is installed in the centralized mode until the server is rebooted after the installation.

Excluded folders for which a backup snapshot is created, are no longer excluded [67235]

This problem is going to be fixed with the upcoming scanning platform update and it will be possible to exclude snapshot directories by making exclusion entries with wildcards.

Quarantined files are not restored with original file attributes [67794, 67800]

The advanced file attributes (as compression or encryption) as well as symbolic link information are not preserved when a file is placed to the quarantine. Therefore, when the file is restored from the quarantine, it doesn't get all original attributes back. If the file had originally any of the advanced file attributes set, you need to restore them manually after restoring the file from quarantine.

6.4 Web Console

Manual Scanning doesn't allow to scan mapped network drives/shares [70572]

Since the Web Console logs in the user without loading the full user profile, it is not possible to scan a network drive or share from the manual scanning page. You can still scan network drives/shares with "Virus and spyware scanning" menu from F-Secure icon in the system tray or with the "Scan Folder for Viruses" menu from Windows Explorer.

Internet Explorer 8 may show the security warning on the login page [70956]

After the existing session has expired, the Web Console returns to the login page automatically. When it happens, Internet Explorer 8 may show the security warning about content that may be delivered using non-secure connection. You can ignore this warning.

6.5 Other

Compatibility with F-Secure Anti-Virus for Microsoft Exchange: most of the services are stopped after uninstallation of one product [68345]

If you uninstall either one of the products from the server where you had both products installed, the uninstallation does not ask you to reboot the computer, but most of F-Secure services are stopped,

including F-Secure Management Agent. It is recommended to reboot the server after uninstallation.

Entering full license key does not activate On Access Scanning and On Demand Scanning immediately [70470]

When your evaluation version of the product is expired and you enter the full license key, on-access and on-demand scanning may not be activated immediately and thus not provide full server protection. It may take up to half an hour before the product gets fully functional. In order to speed up the license activation process, you can restart FSGKHS service or reboot the server.

7. Contact information and feedback

Please report any technical issues through the F-Secure support web site: <http://www.f-secure.com/>. You can also consult the product forum available at: <http://forum.f-secure.com/>.

Before sending us a problem report, please run F-Secure Support Tool, *FSDiag.exe*, on each of the hosts running F-Secure Anti-Virus for Windows Server. This utility gathers basic information about hardware, operating system, network configuration and installed F-Secure and third-party software. You can run the F-Secure Support Tool from the Web Console as follows:

Log in to the Web Console.

Type <https://127.0.0.1:25023/fsdiag/> in the address field of the browser. (If you are accessing the server remotely, use the real IP address of the server instead of 127.0.0.1).

F-Secure Support Tool starts automatically and the dialog displays the data collection progress.

When the tool has finished collecting the data, click **Report** to download and save the collected data

You can also run the FSDiag.exe utility under the F-Secure\Common folder. The tool generates a file called FSDiag.tar.gz.

8. F-Secure license terms

F-Secure license terms are included in the software. You must read and accept them before you can install and use the software.