Installing F-Secure® Server Security (FSSS)

Last update: 22 Feb 2018

Please see also the LISTSERV/F-Secure FAQ for further information.

Table of Contents

Supported F-Secure Anti-Virus Versions

L-Soft can no longer guarantee an uninterrupted virus signature update path for versions of F-Secure Anti-Virus or F-Secure Server Security which are older than those described in this document. We therefore *strongly recommend* that sites running LISTSERV versions prior to LISTSERV 16.0-2017a should upgrade to the latest supported version of LISTSERV (currently 16.0-2017a), so that they can also install the latest version of FSAV.

The following F-Secure Anti-Virus versions are supported by LISTSERV 16.0-2017a and later.

Windows Servers (2008 R2, 2012/2012 R2, 2016)

NOTICE: Use of F-Secure Server Security Standard 12.12 and later requires, at minimum, LISTSERV version 16.0-2014b. LISTSERV version 16.0-2017a or later is STRONGLY RECOMMENDED*.

Issue a SHOW VERSION command to LISTSERV to ascertain your product level BEFORE upgrading or installing FSAV. The current LISTSERV for Windows kit can be downloaded at http://www.lsoft.com/download/listserv.asp#windows .

Installation kits:

For use with LISTSERV 16.0-2017a and later:

F-Secure Server Security 12.12 for Windows Servers (2008 R2, 2012/2012 R2, 2016)
https://ftp.lsoft.com/f-secure/fsss-12.12.104.exe (see below for hotfixes)

Please note that L-Soft does *not* provide licenses for the sister product F-Secure Email and Server Security, nor do we provide licenses for any "premium" version of the F-Secure software. We are licensed only for **F-Secure Server Security Standard**, which is all that is needed with LISTSERV. If downloading the product directly from F-Secure's WebClub, please be aware of the difference and be sure to download the correct kit.

Note: At the time this document was revised, F-Secure Server Security 12.12 for Windows Servers reported as F-Secure Anti-Virus 9.52 in the output of a LISTSERV "release" command. This is NOT a LISTSERV bug -- LISTSERV is repeating what FSAV tells it. To ensure that FSSS 12.12 is installed, right-click the "F" shield icon in the system tray and click "About". It should report "F-Secure Server Security 12.12 build 104" .

Manuals:
F-Secure E-Mail and Server Security Administrator's Guide

We recommend upgrading LISTSERV to at least version 16.0-2017a (the current released version) because of an incompatibility with earlier versions of LISTSERV that is present in current versions of the F-Secure products. The incompatibility may result in display errors when F-Secure reports a virus.* ***We have taken account of this incompatibility in LISTSERV version 16.0-2017a and later.* *To ensure that you have at least LISTSERV version 16.0-2017a, issue a SHOW LICENSE to your LISTSERV server. The build date reported should be 28 Feb 2017 or later.*

It should be noted that earlier versions of LISTSERV do not support, or do not completely support, the DMARC anti-spam standards currently in place with many large ISPs world-wide. For this reason also, ***we strongly recommend*** *upgrading older versions of LISTSERV to the latest generally-available version, at time of writing, 16.0-2017a.*

Windows Workstations (Windows 7 and later)

Unfortunately, F-Secure does not provide a standalone kit for F-Secure Client Security (the Workstation version of their business-class anti-virus suite). This makes it impossible for L-Soft to provide F-Secure kits for Windows Workstation class operating systems (7, 8.x, 10, and so forth).

For more information on alternatives, please see below at "Special Considerations for Windows Workstations".

In order to use LISTSERV®'s Anti-Virus features, F-Secure® Server Security must be installed on the same server as LISTSERV. If you already have F-Secure Server Security installed on the server, you should make sure that you are running the version supported by LISTSERV:

- For Windows Server 2008/2012/2016 Server (including R2 versions): version 12.12
- For Windows XP/Vista/7: Please see Special Considerations for Windows Workstations, below.

Recommended FSSS versions for LISTSERV 15.0 and following

- L-Soft strongly recommends that all LISTSERV sites running on a Server version of Windows upgrade to at least F-Secure Server Security version 12.12 with all hotfixes for that version released to date.

The F-Secure Server Security license key normally provided by L-Soft is for the server version of F-Secure Anti-Virus. The server version will not install on a workstation version of Windows (that is, Windows 7, 8, 8.1, 10, Windows Vista, or Windows XP). If you are affected by this, please see below.

The FSSS key provided by L-Soft is valid only as long as your paid maintenance contract for LISTSERV is up-to-date. If you discontinue LISTSERV maintenance, you must uninstall F-Secure Server Security, or purchase a separate key directly from F-Secure.

Special Considerations For Windows Workstations

Starting with the release of F-Secure Client Security version 10, F-Secure no longer provided a standalone installation kit for its workstation OS anti-virus product. As noted above, this means that L-Soft can no longer provide an F-Secure Client Security installation kit.

Sites running LISTSERV 15.0 or later under a Windows Workstation variant such as Windows 7 or Windows 10 have the following options:

- Run LISTSERV with an antivirus product from another vendor that supports real-time scanning of compressed archives, by using the FOREIGN_ANTI_VIRUS site configuration parameter.

- Migrate the installation to a Windows Server platform.

F-Secure Hotfixes Recommended

Given our own experience and that of customers who have reported problems to support, L-Soft strongly recommends that all currently-available hotfixes for FSAV be installed.

If available, hotfixes for Windows can be downloaded from the F-Secure WebClub product page for F-Secure Server Security. **Please check the F-Secure website regularly for any hotfixes that may be provided.**

When downloading F-Secure hotfixes for Windows, be sure to choose the ones for standalone environments. These are the ones with the .fsfix extension.

F-Secure Server Security Installation Instructions for Windows Servers

The following is a quick summary of steps to install F-Secure Server Security (from the stand-alone kit). If you need further clarification, please consult the manuals cited in the table above.

1. Download the appropriate installation kit (it will be an installer executable with the extension .exe) for your platform (see table above).
2. CD into the scratch directory where you have downloaded the executable, and run it.
3. When prompted for a key, enter the F-Secure key that you received from your L-Soft sales representative. If you did not receive an F-Secure Server Security key along with your LISTSERV LAK, please contact your L-Soft sales representative.
4. When prompted for the Administration Method, choose *Stand-alone Installation*.
5. When prompted to “Choose Products to Install”, *Virus & Spy Protection xx.xx* and *DeepGuard x.xx* should be checked.

IMPORTANT: Required LISTSERV Version

F-Secure Server Security 12.x and later works with LISTSERV 15.0 and later. However, we strongly recommend upgrading any older installation of LISTSERV with the current generally-available version, which at time of writing was LISTSERV 16.0-2017a.

THIS IS AN ABSOLUTE REQUIREMENT. FSSS 12.x WILL NOT WORK AT ALL WITH LISTSERV VERSIONS THAT REPORT AS BEING EARLIER THAN VERSION 15.0, AND MAY NOT UPDATE ANTI-VIRUS SIGNATURES PROPERLY WITH VERSIONS EARLIER THAN VERSION 16.0-2017a.

Please visit the LISTSERV documentation page to read the LISTSERV release notes.

Please visit the LISTSERV product download page to download the current LISTSERV kit.

Using and Configuring the F-Secure Web Console

F-Secure Server Security is managed via a web console, which opened by either clicking Start/All Programs/F-Secure Server Security/F-Secure Server Security Web Console, or by browsing locally to https://127.0.0.1:25023 . Login is with the same userid and password as you used to log into Windows. (If you are logging in as a domain account, you must specify the domain, e.g., `\mydomain\myuserid` .)

The web console will require a local certificate to be generated and installed. Please see section *2.2.1 Logging in for the First Time* in the F-Secure E-mail and Server Security Administrator's Guide for details on how to install the certificate.

Recommended F-Secure Settings under Windows

1. Real Time protection enabled (mandatory)
2. Action: "Delete Automatically" (strongly recommended)
3. Scanning Options: "Files with these extensions" (and accept the default)
4. Scan inside compressed files: "checked"
5. LISTSERV and/or LSMTP spool directories MUST be exempted from scanning.
6. *.mail, *.mai or *.job files MUST be exempted from scanning. (Technically speaking, if you apply point 5, you should not have to explicitly exempt any LISTSERV or LSMTP file types.)

7. We do not recommend (nor do F-Secure recommend) that the "Scanning Options" box titled "All files" be checked. This can lead to serious performance degradation and is strongly discouraged.

Performance Considerations under Windows

F-Secure Server Security running on Windows provides an option for “real-time protection”. This means that F-Secure will automatically check any file matching the criteria configured. The “real-time protection” settings that are set by default should work for most installations.

However please note that L-Soft does STRONGLY recommend that you change the "Action to take on infected files" to "Delete Automatically".

Otherwise, the “out-of-the-box” settings enable protection for all file extensions that are known to be susceptible to viruses, on all directories on the server. As long as your LISTSERV maintenance is up-to-date, you are entitled to protect the entire server on which LISTSERV resides, not just LISTSERV itself, using the FSAV key provided by L-Soft. Therefore, there is no need to change the settings, other than noted above.

If you do decide to change the real-time protection settings, please keep the following in mind:

- Requesting scanning for “All Files” may result in a noticeable drop in performance.

  If you have real-time scanning enabled for “All Files”, without specifying exceptions, then every file written on the server will be checked for viruses. This has the potential to slow down the server in a situation where many files are written continuously. In particular, an active LISTSERV site tends to create many files containing incoming LISTSERV “jobs” and outgoing mail. To avoid performance problems, avoid enabling automatic scanning of all files on the server.

- *At a minimum*, you should keep real-time scanning on for the EXE extension on the LISTSERV directory tree.
  To do this, follow these steps:

  1. Open the F-Secure Server Security Web Console.
  2. Choose “Real-time Scanning” from the sidebar, under "Server Protection".
  3. Make sure “Enable protection” is checked[1], and select an action to take on infected files. To select a custom action, you must uncheck the "Decide action automatically" box and then choose one of the actions in the drop-down boxes.
  4. Under “Scanning Options” select “Files with these extensions” and enter “EXE” in the data entry box.
  5. Press the “OK” button to save the settings.

- Some performance benefits may be found by excluding “immune” folders from the real-time scanning.

  You may want to exclude certain folders that will never contain any files that are prone to infection, for example folders that only contain text files. To exclude folders: in the “Real-time protection” applet, under “Scanning options” check the box for “Exclude objects (files, folders)”, then press the “Select…” button. Next, select those folders that do not need to be scanned. LISTSERV’s archive directories, for example, should never contain infected files unless there are people or processes external to LISTSERV that use those directories for other purposes.

[1] In FSSS 12, this is actually a clickable green or grey dot to the right of the page title, green being "ON" and grey being "OFF".