Installing F-Secure® Anti-Virus (FSAV)

Last update: 26 Apr 2013

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

Table of Contents

FSAV 4.x, 5.x and 7.x End of Life
FSAV 8.x and FSLS 7.x End of Life
Windows Servers
Windows Workstations
Linux Servers
Recommended FSAV versions for LISTSERV 15.0 and following
Special Considerations for Windows Workstations
F-Secure Hotfixes Recommended
Windows Installation
Linux Installation

FSAV 4.x, 5.x, and 7.x End of Life

L-Soft can no longer guarantee an uninterrupted virus signature update path for older versions of FSAV (7.x and older), which have been at end-of-life for more than a year. We therefore *strongly recommend* that sites running LISTSERV versions prior to 15.0 should upgrade to the latest supported version of LISTSERV (currently 16.0-2011a), so that they can also install the latest version of FSAV.

Because the 7.x and older versions are no longer supported in any way by F-Secure, we have removed installation instructions for them from this document.

FSAV 8.x and FSLS 7.x End of Life

F-Secure has recently announced that FSAV 8 for Windows and FSLS 7 for Linux have reached End of Life. This means that there will be no further updates for either package, meaning that LISTSERV sites depending on them should strongly consider upgrading to the latest supported version. This document contains information for installing both FSAV 9 for Windows and FSLS 9 for Linux.

The table below indicates the Web sites for F-Secure downloads.

Windows Servers (2003/2008/2012)
NOTICE: Use of FSAV 9.20 and later requires, at minimum, LISTSERV version 15.0. LISTSERV version 16.0-2011a or later is recommended*. **FSSS 9.20 will not install on Windows 2012 Server. Use FSSS 10.00 instead.** **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 15.0 and later:

F-Secure Server Security 10.00 for Windows Servers (2003/2008/2012, including R2)
ftp://ftp.lsoft.com/f-secure/ss1000-435-rtm.exe (see below for hotfixes)

F-Secure Server Security 9.20 for Windows Servers (2003/2008, including R2)
ftp://ftp.lsoft.com/f-secure/ess920.exe (see below for hotfixes)

Please note that L-Soft does *not* provide licenses for the sister product F-Secure Email and Server Security. We are licensed only for F-Secure Server Security, 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 10.00 for Windows Servers reported as F-Secure Anti-Virus 9.50 in the output of a LISTSERV "release" command. This is NOT a LISTSERV bug -- LISTSERV is repeating what FSAV tells it. To ensure that FSAV 10.00 is installed, right-click the "F" shield icon in the system tray and click "About". It should report "F-Secure Server Security 10.00 build 435" and "F-Secure Anti-Virus 9.50 build 19153" (or possibly later builds depending on the kit).

Note: At the time this document was revised, F-Secure Server Security 9.20 for Windows Servers reported as F-Secure Anti-Virus 9.30 in the output of a LISTSERV "release" command. This is NOT a LISTSERV bug -- LISTSERV is repeating what FSAV tells it. To ensure that FSAV 9.20 is installed, right-click the "F" shield icon in the system tray and click "About". It should report "F-Secure Server Security 9.20 build 682" and "F-Secure Anti-Virus 9.30 build 18060" (or possibly later builds depending on the kit).

Manuals:
F-Secure E-Mail and Server Security for Windows Servers

We recommend upgrading LISTSERV to at least version 16.0-2011a because of an incompatibility introduced in the 9.x versions of the F-Secure products. The incompatibility may result in occasional spurious reports from LISTSERV of out-of-date anti-virus signatures. **We have taken account of this incompatibility in LISTSERV version 16.0-2011a. To ensure that you have at least LISTSERV version 16.0-2011a, issue a SHOW LICENSE to your LISTSERV server. The build date reported should be 28 Oct 2011 or later.*

Windows Workstations (XP, Vista, Windows 7)

NOTICE: Use of FSAV 9.32 and later requires, at minimum, LISTSERV version 15.0. LISTSERV version 16.0-2011a or later is 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 .

DOCUMENTED RESTRICTION: With the release of FSAV version 9, F-Secure no longer supports real-time scanning of compressed archives in FSAV for Windows Workstations. This means that sites running LISTSERV on a Windows Workstation platform (e.g., Windows XP) will not be able to prevent compressed files containing malicious payloads from being distributed if using FSAV 9 for anti-virus scanning. **Please see below for a discussion of alternatives.**

Installation kits:

For use with LISTSERV 15.0 and later:
FSAV 9.32 for Windows Workstations
ftp://ftp.lsoft.com/F-Secure/fsav4wks9.32.rtm.exe (see below for hotfixes)

Manuals:
Getting Started Guide

Admin Guide

We recommend upgrading LISTSERV to at least version 16.0-2011a because of an incompatibility introduced in the 9.x versions of the F-Secure products. The incompatibility may result in occasional spurious reports from LISTSERV of out-of-date anti-virus signatures.* ***We have taken account of this incompatibility in LISTSERV version 16.0-2011a.* *To ensure that you have at least LISTSERV version 16.0-2011a, issue a SHOW LICENSE to your LISTSERV server. The build date reported should be 28 Oct 2011 or later.*

Linux-x86 and Linux-x64:

NOTICE: Use of F-Secure Linux Security 9.32 and later requires, at minimum, LISTSERV version 15.0. LISTSERV version 16.0-2011a or later is recommended*.

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

Installation kits:
For use with LISTSERV 15.0 and later:
F-Secure Linux Security (FSLS) 9.13
ftp://ftp.lsoft.com/f-secure/f-secure-linux-security-9.13.1893.tar.gz

Manuals:
F-Secure Linux Security 9.0x documentation:
Admin guide
Manual

We recommend upgrading LISTSERV to at least version 16.0-2011a because of an incompatibility introduced in the 9.x versions of the F-Secure products. The incompatibility may result in occasional spurious reports from LISTSERV of out-of-date anti-virus signatures.* ***We have taken account of this incompatibility in LISTSERV version 16.0-2011a.* *To ensure that you have at least LISTSERV version 16.0-2011a, issue a SHOW LICENSE to your LISTSERV server. The build date reported should be 28 Oct 2011 or later.*

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

- For Windows Server 2003/2003 R2/2008/2008 R2 Server: version 9.20
- For Windows XP/Vista/7: version 9.32

(For workstation systems, the minimum requirement is Windows XP with Service Pack 3. Windows 2000 is no longer supported. XP is supported in 32-bit only; Vista and Windows 7 are supported in either 32-bit or 64-bit.)

- For Linux: F-Secure Linux Security (FSLS) version 9.13

Recommended FSAV versions for LISTSERV 15.0 and following

- L-Soft strongly recommends that all such Windows LISTSERV sites running on a Server version of Windows upgrade to at least F-Secure Server Security version 9.20 with all hotfixes for that version released to date.

- L-Soft strongly recommends that all such Linux-x86 and Linux-x86_64 LISTSERV sites upgrade to F-Secure Linux Security version 9.13, build 1893 with all hotfixes for that version released to date.

The FSAV for Windows Servers or FSAV for Linux Servers license key provided by L-Soft is for a single stand-alone server only. If you wish to run the Enterprise edition of F-Secure Anti-Virus, this can be purchased separately, directly from F-Secure, and it will still work with LISTSERV.

The FSAV for Windows Servers 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, Windows Vista, or Windows XP). If you are affected by this, please contact your sales representative for an FSAV for Windows Workstations key.

The FSAV 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 Anti-Virus or purchase a separate key from F-Secure.

Special Considerations For Windows Workstations

With the release of FSAV version 9, F-Secure no longer supports real-time scanning of compressed archives in FSAV for Windows Workstations. This means that sites running LISTSERV on a Windows Workstation platform (e.g., Windows XP) will not be able to prevent compressed files containing malicious payloads from being distributed if using FSAV 9 for anti-virus scanning.

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

- Continue to run LISTSERV with FSAV 8 for Windows Workstations, with the understanding that updates for FSAV 8 ceased when FSAV 8 reached end-of-life on 31 December 2011.
- Run LISTSERV with FSAV 9 for Windows Workstations, with the understanding that compressed archives that MAY contain malicious content WILL NOT be scanned prior to distribution.
- 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 both Windows and Linux can be downloaded from the F-Secure WebClub product page for the particular product in question. **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 Anti-Virus Installation Instructions for Windows Servers

The following is a quick summary of steps to install F-Secure Anti-Virus (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 and run the kit.
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 Anti-Virus 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 9.30* and *DeepGuard 3.00* should be checked.

If you are installing F-Secure Anti-Virus for Windows Workstations, be aware that in step 5 you may also see an option to install *Microsoft NAP plug-in 1.00.* The plug-in is described at this F-Secure link, and is for use in environments where Microsoft Network Access Protection support is available. The plug-in is not required for LISTSERV but may be required by your local Windows security policy. Please check with your network administrators regarding whether or not to install the plug-in. L-Soft cannot assist you with this.

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"
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 Anti-Virus 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. Double-click on the F-Secure logo in the Windows Taskbar to bring up the F-Secure Settings and Statistics applet.
  2. Select F-Secure Anti-Virus and press the “Properties…” button.
  3. Go to the “Real-time protection” tab.
  4. Make sure “Enable protection” is checked, and select an action to take on infected files (preferably other than “Report only”).
  5. Under “Scanning Options” select “Files with these extensions” and enter “EXE” in the data entry box.
  6. 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.

F-Secure Linux Security Installation Instructions for Linux Servers

L-Soft is pleased to offer its Linux customers the ability to integrate F-Secure Linux Security (FSLS) 9.13 into their LISTSERV 15.0 or later environment.

Please be aware that L-Soft provides a license for the "command-line" version of F-Secure Linux Security. The "command-line" version does not include the real-time protection, integrity checking, web user interface or central management features provided in the full version. This version is designed specifically for users migrating from the F-Secure Anti-Virus 4.6x series or for users who do not need the additional functions.

Before starting to install FSLS 9.13, make sure that you have your FSLS installation key from your sales representative. The FSLS key is normally sent with your LISTSERV LAK(s) but may be obtained separately if you have not previously received it.

Please note that the support department does not have access to, nor can it provide, either LISTSERV LAKs or FSLS keys.

IMPORTANT: Required LISTSERV Version

F-Secure Linux Security 9.13 and later works with LISTSERV 15.0 and later.

THIS IS AN ABSOLUTE REQUIREMENT. FSLS 9.10 WILL NOT WORK WITH LISTSERV VERSIONS THAT REPORT AS BEING EARLIER THAN VERSION 15.0.

F-Secure Linux Security 9.13 is fully certified to work with LISTSERV 15.0 and later.

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

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

Upgrading from an earlier version of FSAV or FSLS

FSLS 7.x versions previously supported with LISTSERV may be upgraded directly with the FSLS 9.13 installer.

FSAV 5.x for Linux was never supported with LISTSERV. However, if for some reason you have this version of FSAV installed, you can uninstall it before upgrading to FSLS 9.13 by running the command

```
/opt/f-secure/fsav/bin/uninstall-fsav
```

from the command line.

FSAV 4.x versions previously supported with LISTSERV *cannot* be upgraded with the FSLS 9.13 kit. The earlier version must be uninstalled before making a new installation of FSLS 9.13. To uninstall FSAV 4.x, remove the following directories and files:

/opt/f-secure/fsav/
/var/opt/f-secure/fsav/
/etc/opt/f-secure/fsav/
/usr/bin/fsav
/usr/share/man/man1/fsav.1
/usr/share/man/man5/fsav.conf.5
/usr/share/man/man5/fsavd.conf.5
/usr/share/man/man8/dbupdate.8
/usr/share/man/man8/fsavd.8
/usr/share/man/man8/fsavschedule.8

If it exists, also delete the hourly cron job that runs dbupdate. It is no longer needed with FSAV 9.

For 64-bit Linux versions

If installing F-Secure Linux Security 9.13 under a 64-bit Linux operating system, please be aware that you must also install the Linux 32-bit compatibility packages appropriate for your Linux distribution. This is because FSLS 9.13 is a 32-bit application and, as such, will not be able to use 64-bit common libraries.

In some cases 32-bit compatibility packages may be installed by default. Should you have any question about the 32-bit compatibility packages, please contact your OS vendor. ***L-Soft is unable to assist in the installation of these packages.***

Please read F-Secure's pre-installation checklist for 64-bit systems before installing.

Installing F-Secure Linux Security

1. Login as (or 'su' to) 'root' and download the FSLS installation kit from the URL indicated in the table above. We recommend creating a scratch directory somewhere in your filesystem and downloading the file to that location.

Note that you can download FSLS 9.13 directly from the F-Secure website, but the manufacturer's kit does *not* include the L-Soft-supplied fsavd-config.sh file used in step 9.

2. Expand the downloaded archive:

```
zcat f-secure-linux-security-9.13.1893.tar.gz | tar xvf -
```

This leaves the following files in the directory `f-secure-linux-security-9.13.1893` :

```
fsavd-config.sh
fsav_linux_900_mib-signed.jar
f-secure-daemon-api-sdk.tgz
f-secure-linux-security-9.13.1893
f-secure-linux-security-9.13.1893-release-notes.txt
```

The file called `f-secure-linux-security-9.13.1893` should have execute permission. (If it does not, chmod it appropriately.)

3. Execute (still as root) the following command:

```
./f-secure-linux-security-9.13.1893 --command-line-only
```

It is very important that the `--command-line-only` flag be appended to this command! If it is not, you will install an evaluation copy of the full version of the product, for which you are not licensed. You will then have to uninstall the product and reinstall it in command-line mode.

4. The installation script will first ask you to view and accept the F-Secure license agreement.

```
[home]root:~/f-secure-linux-security-9.13.1893# ./f-secure-linux-security-
9.10.886 --command-line-only
F-Secure Linux Security installation
Copyright (c) 1999-2008 F-Secure Corporation. All Rights Reserved.

Preparing...



You must accept following F-Secure license agreement
to install F-Secure Linux Security.
Press enter to view license agreement.
```

Simply press enter and then use the space bar to page down. At the end of the license agreement you will be asked:

```
Do you accept this license agreement?
```

Type "y" or "Y" or some form of "yes" to continue.

After accepting the license agreement, the product will install and create a default configuration.

```
The license agreement text is available at /opt/f-secure/fsav/LICENSE.
```

```
Installing RPM packages, please wait...

Running configuration
.....
```

You will then be asked to provide the F-Secure license key (and please note that the key shown is only for illustration; it is not a valid key). Type in the key and then hit return.

```
Keycode for F-Secure Linux Security
To install the licensed version of the product, please enter the keycode you
have received with your purchase or press enter to install the fully functional
30-day evaluation version.
keycode: 1234-5678-90AB-CDEF-GHIJ
```

5. The remainder of the installation looks like the following.

```
Keycode accepted.
Configuring

F-Secure Security Platform
F-Secure Virus Description Database Update

Copyright (c) 1999-2008 F-Secure Corporation. All Rights Reserved.

Databases updated successfully.
Database version: 2011-03-10_08

Configuring...

Note: The Virus Definition Databases are now being updated to the newest
versions in the background. You can check the date of the current the
databases by typing 'fsav --version'.


[home]root:~/f-secure-linux-security-9.13.1893#
```

6. Unlike previous F-Secure versions, there is no need to install a cron entry to update the virus signatures. An F-Secure automatic update agent is provided as part of the installation and will download the new signatures in the background as they become available.

7. **After installation, there are two minor change that MUST be made to the default FSLS configuration.** The default behavior of FSLS is first to try to disinfect, and then to try to rename the file upon detection. Because LISTSERV expects the anti-virus scanner only to report when it detects a virus, and not otherwise change or delete the file, this behavior must be changed. The change is made by opening the FSLS configuration file, normally found at `/etc/opt/f-secure/fssp/fssp.conf`, in a text editor, and changing the values of two variables in the file as follows:

   `odsFilePrimaryActionOnInfection 1`

   `odsFileSecondaryActionOnInfection 0`

   Then save the file.

Please note carefully that this element of the installation is required. If you skip it, FSLS will end up disinfecting or renaming infected files, and LISTSERV will not receive the return code that tells it to reject the message. There is no need for FSLS to delete or rename the file. LISTSERV itself will delete the file when it receives the correct return code.

8. After restarting LISTSERV, you should see an entry similar to the following in the log:

```
12 Aug 2012 09:54:03 F-Secure Anti-Virus 9.13 activated, explicit file scan.
```

9. Finally, run (as 'root') the fsavd-config.sh script (provided by L-Soft) which installs a modified 'fsavd' daemon startup script into `/etc/init.d` , registers it as a system "service", and starts it. This script allows you to ensure that the fsavd daemon starts when your machine is rebooted, and that it runs under the 'listserv' UID. This is required in order for LISTSERV to be able to "see" FSAV when it starts up.

   Note that you may have to issue the shell command `chmod u+x fsavd-config.sh` to make the shell script executable.

   If you downloaded FSLS 9.13 from the F-Secure website, you will not have this file. It can be downloaded from ftp://ftp.lsoft.com/f-secure/tools/fsavd-config.sh if needed.

   fsavd-config.sh makes one change to the fsavd startup script, altering

   ```
   fsavuser=fsav
   ```

   to

   ```
   fsavuser=listserv
   ```

   Please note carefully that this element of the installation is *required*. If you skip it, LISTSERV will not see FSAV at startup and LISTSERV's AV scanning feature will be disabled. It should be noted that this will NOT affect how fsavd reacts to requests from other users. F-Secure normally recommend that the fsavd daemon should run under a non-priviledged UID to begin with.

   If you have installed LISTSERV to start under a different UID (not common), you will have to manually change the fsavuser= line in `/etc/init.d/fsavd` to the correct UID value and then stop and restart the 'fsavd' daemon. You can stop and restart the daemon from the shell prompt with "/sbin/service fsavd restart".