

F-Secure Linux Security Administrator's Guide

Table of Contents

Chapter 1: Welcome	7
How the Product Works	8
Protection Against Malware	8
Host Intrusion Prevention System	8
Key Features and Benefits	9
Superior Protection against Viruses and Worms	9
Transparent to End-users	10
Protection of Critical System Files	10
Easy to Deploy and Administer	10
Extensive Alerting Options	10
 Chapter 2: Deployment	 11
Deployment on Multiple Stand-alone Linux Workstations	12
Deployment on Multiple Centrally Managed Linux Workstations	12
Central Deployment Using Image Files	12
 Chapter 3: Installation	 15
System Requirements	16
List of Used System Resources	17
Stand-alone Installation	19
Centrally Managed Installation	19
Upgrading.....	20
Upgrading from a Previous Product Version	20
Upgrading the Evaluation Version	22
Custom Installations.....	23
Preparing for Custom Installation.....	23
Unattended Installation	23

Installing Command Line Scanner Only	24
Using The Product With Samba Servers.....	25
Creating a Backup	26
Uninstallation	27

Chapter 4: Administering the Product29

Basics of Using F-Secure Policy Manager	30
Accessing the Web User Interface	30
Testing the Antivirus Protection	31

Chapter 5: Using the Product.....33

Summary.....	34
I Want to.....	34
Scanning for Viruses.....	37
What are Viruses and Other Malware?.....	37
Stopping Viruses and Other Malware.....	40
Methods of Protecting the Computer from Malware	42
Firewall Protection.....	50
What Is a Firewall?.....	50
What Are Security Profiles?.....	50
Firewall Rules.....	52
Firewall Settings.....	56
Integrity Checking	57
Known Files List	57
Software Installation Mode	59
Baseline.....	60
Rootkit Prevention	61
General Settings	62
Alerts	62
Automatic Updates	64
F-Secure Anti-Virus Proxies	66
About	66

Chapter 6: Troubleshooting.....	67
Installing Required Kernel Modules Manully	68
User Interface.....	68
F-Secure Policy Manager.....	70
Integrity Checking.....	70
Firewall.....	72
Virus Protection.....	73
Generic Issues.....	75
Appendix A: Command Line Tools.....	79
fsav	80
fsav-config	80
dbupdate	82
fsfwc	82
fsic	83
fsims	83
fsma	84
fssetlanguage	85
fschooser.....	85
Appendix B: Before You Install.....	87
64-bit Distributions	88
Distributions Using Prelink.....	88
Red Hat Enterprise Linux 3 and 4	89
Debian 3.1 and 4.0.....	90
SuSE	90
Turbolinux 10 and 11.....	91
Ubuntu 5.04, 5.10, 6.06, 7.04 and 7.10	91
Appendix C: List of Traps.....	93

Appendix D: Get More Help99

Welcome

Topics:

- [How the Product Works](#)
- [Key Features and Benefits](#)

Computer viruses are one of the most harmful threats to the security of data on computers. Viruses have increased in number from just a handful a few years ago to many thousands today. While some viruses are harmless pranks, other viruses can destroy data and pose a real threat.

The product provides an integrated, out-of-the-box ready security solution with a strong real-time antivirus and riskware protection and a host intrusion prevention (HIPS) functionality that provides protection against unauthorized connection attempts from network, unauthorized system modifications, userspace and kernel rootkits. The solution can be easily deployed and managed either using the web user interface or F-Secure Policy Manager.

F-Secure Policy Manager provides a tightly integrated infrastructure for defining and distributing security policies and monitoring the security of different applications from one central location.

How the Product Works

The product detects and prevents intrusions and protects against malware.

With the default settings, computers are protected right after the installation without any time spent configuring the product.

Protection Against Malware

The product protects the system against viruses and potentially malicious files.

When user downloads a file from the Internet, for example by clicking a link in an e-mail message, the file is scanned when the user tries to open it. If the file is infected, the product protects the system against the malware.

- *Real-time scanning* gives you continuous protection against viruses and riskware items as files are opened, copied, and downloaded from the Web. Real-time scanning functions transparently in the background, looking for viruses whenever you access files on the hard disk, diskettes, or network drives. If you try to access an infected file, the real-time protection automatically stops the virus from executing.
- When the real-time scanning has been configured to scan a limited set of files, the *manual scanning* can be used to scan the full system or you can use the scheduled scanning to scan the full system at regular intervals.
- *Automatic Updates* keep the virus definitions always up-to-date. The virus definition databases are updated automatically after the product has been installed. The virus definitions updates are signed by the F-Secure Anti-Virus Research Team.

Host Intrusion Prevention System

The Host Intrusion Prevention System (*HIPS*) detects any malicious activity on the host, protecting the system on many levels.

- *Integrity Checking* protects the system against unauthorized modifications. It is based on the concept of a known good configuration - the product should be installed before the computer is connected to the network to guarantee that the system is in a known good configuration.

You can create a baseline of the system files you want to protect and block modification attempts of protected files for all users.

- *The firewall* component is a stateful packet filtering firewall which is based on Netfilter and iptables. It protects computers against unauthorized connection attempts. You can use

predefined security profiles which are tailored for common use cases to select the traffic you want to allow and deny.

- If an attacker gains a shell access to the system and tries to add a user account to login to the system later, Host Intrusion Prevention System (*HIPS*) detects modified system files and alerts the administrator.
- If an attacker has gained an access to the system and tries to install a userspace rootkit by replacing various system utilities, *HIPS* detects modified system files and alerts the administrator.
- If an attacker has gained an access to the system and tries to install a kernel rootkit by loading a kernel module for example through `/sbin/insmod` or `/sbin/modprobe`, *HIPS* detects the attempt, prevents the unknown kernel module from loading and alerts the administrator.

If an attacker has gained an access to the system and tries to install a kernel rootkit by modifying the running kernel directly via `/dev/kmem`, *HIPS* detects the attempt, prevents write attempts and alerts the administrator.

Key Features and Benefits

The product offers superior protection against viruses and worms and is transparent to end-users.

Superior Protection against Viruses and Worms

The product scans files on any Linux-supported file system. This is the optimum solution for computers that run several different operating systems with a multi-boot utility.

- Scans files on any Linux-supported file system.
 - 👉 **Note:** The real-time scanning is not supported when using an NFS server, but other scan methods work.
- Superior detection rate with multiple scanning engines.
- A heuristic scanning engine can detect suspicious, potentially malicious files.
- The product can detect and categorize riskware items.
- The product can be configured so that the users cannot bypass the protection.
- Files are scanned for viruses when they are opened or closed and before they are executed.
- You can specify what files to scan, how to scan them, what action to take when malicious content is found and how to alert about the infections.
- Recursive scanning of archive files.
- Virus definition database updates are signed for security.

- Integrated firewall component with predefined security levels. Each security level comprises a set of rules that allow or deny network traffic based on the protocols used.

Transparent to End-users

The product works totally transparently to the end users.

- The product has an easy-to-use user interface.
- Virus definition databases are updated automatically without any need for end-user intervention.

Protection of Critical System Files

Critical information of system files is stored and automatically checked before access is allowed.

- The administrator can protect files against changes so that it is not possible to install, for example, a trojan version of a software.
- The administrator can define that all Linux kernel modules are verified before the modules are allowed to be loaded.
- An alert is sent to the administrator when a modified system file is found.

Easy to Deploy and Administer

The default settings apply in most systems and the product can be taken into use without any additional configuration.

- Security policies can be configured and distributed from one central location.

Extensive Alerting Options

The product has extensive monitoring and alerting functions that can be used to notify any administrator in the company network about any infected content that has been found.

- Alerts can be forwarded to F-Secure Policy Manager Console, e-mail and syslog.

Deployment

Topics:

- *Deployment on Multiple Stand-alone Linux Workstations*
- *Deployment on Multiple Centrally Managed Linux Workstations*
- *Central Deployment Using Image Files*

Deployment on Multiple Stand-alone Linux Workstations

Centrally Managed installation with F-Secure Policy Manager installed on a separate computer is recommended.

In centrally managed installation mode, F-Secure Policy Manager is used to manage Linux computers. The recommended deployment method is to delegate the installation responsibility to each user and then monitor the installation progress via F-Secure Policy Manager Console. After the installation on a host has completed, the host sends an autoregistration request to F-Secure Policy Manager. You can monitor with F-Secure Policy Manager Console which of the hosts have sent an autoregistration request.

When the company has multiple Linux computers deployed, but they are not managed centrally, users can install the software themselves.

In organizations with few Linux computers, the web user interface can be used to manage Linux workstations instead of F-Secure Policy Manager.

Deployment on Multiple Centrally Managed Linux Workstations

If computers are managed through an existing management framework, it can be used to push the product to computers.

When the company has multiple Linux computers deployed and they are managed through Red Hat network, Ximian Red Carpet, or similar, the software can be pushed to workstations using the existing management framework.

Central Deployment Using Image Files

When the company has a centralized IT department that install and maintains computers, the software can be installed centrally to all computers.

If you are going to install the product on several computers, you can create a disk image file that includes the product and use this image to replicate the software on the computers. Make sure that each computer on which the software is installed will create a new unique identification code.

Follow these steps to make sure that each computer uses a personalized Unique ID when a disk imaging software is used.

1. Install the system and all the software that should be in the image file, including the product.
2. Configure the product to use the correct F-Secure Policy Manager Server. However, do not import the host to F-Secure Policy Manager Console if the host has sent an autoregistration request to the F-Secure Policy Manager Server. Only hosts on which the image file will be installed should be imported.
3. Run the following command: `/etc/init.d/fsma clearuid`
The utility program resets the Unique ID in the product installation.
4. Shut down the computer and do not restart the computer before the image file has been created.
5. Create the disk image file.

A new Unique ID is created automatically when the system is restarted. This will happen individually on each computer where the image file is installed.

Computers will send autoregistration requests to F-Secure Policy Manager when they are restarted. These request can be processed as usual.

Installation

Topics:

- *System Requirements*
- *Stand-alone Installation*
- *Centrally Managed Installation*
- *Upgrading*
- *Custom Installations*
- *Creating a Backup*
- *Uninstallation*

System Requirements

A list of system requirements.

Operating system:

- Debian 4.0
- Red Hat Enterprise Linux 3, 4, 5
- SUSE Linux 9.0, 9.3, 10, 10.1
- openSUSE 10.2
- SUSE Linux Enterprise Desktop 10
- SUSE Linux Enterprise Server 9, 10
- Turbolinux 10
- Ubuntu 6.06 LTS (Dapper Drake), 7.10 (Gutsy Gibbon)

The following 64-bit (AMD64/EM64T) distributions are supported with 32-bit compatibility packages:


- Debian 4.0
- Red Hat Enterprise Linux 4, 5
- SUSE Linux Enterprise Desktop 10
- SUSE Linux Enterprise Server 9, 10
- SUSE Linux 10.1
- Turbolinux 10
- Ubuntu 7.10 (Gutsy Gibbon)

 **Note:**

F-Secure has tested the product extensively on the listed distributions. The command line installation mode should work on any Linux distribution that has glibc 2.3.2 or later and Linux kernel 2.4 or 2.6, but any product upgrades may not work on unsupported platforms.

You should report any issues that you may encounter with other distributions, but we cannot guarantee that they will be fixed.

Kernel version:	Linux kernel 2.4 or later (for 64-bit support, Linux kernel 2.6 or later)
Glibc version	Glibc 2.3.2 or later
Processor:	Intel x86, x86-64
Memory:	256 MB RAM or more
Disk space:	200 MB

 **Note:** Konqueror is not a supported browser with the local user interface. It is recommended to use Mozilla or Firefox browsers.

Note About Dazuko Version

The product needs the Dazuko kernel module for the real-time virus protection, integrity checking and rootkit protection. Dazuko is an open-source kernel module that provides an interface for the file access control. More information is at <http://www.dazuko.org>.

The product installs the Dazuko driver during the product installation.

The product has been tested extensively with the Dazuko version that is included with the product. Operation with other Dazuko versions or Linux distribution provided Dazuko versions is not supported or recommended.

List of Used System Resources

A summary of the system resources that the product uses.

Installed Files

All files installed by the product are in the following directories:

- /opt/f-secure
- /etc/opt/f-secure
- /var/opt/f-secure

In addition, the installation creates the following symlinks:

- /usr/bin/fsav -> /opt/f-secure/fssp/bin/fsav
- /usr/bin/fsic -> /opt/f-secure/fsav/bin/fsic
- /usr/bin/fsui -> /opt/f-secure/fsav/bin/fsui
- /usr/share/man/man1/fsav.1 -> /opt/f-secure/fssp/man/fsav.1
- /usr/share/man/man8/fsavd.8 -> /opt/f-secure/fssp/man/fsavd.8

Changed System Files

- `/etc/passwd`: Two new user accounts (fsma and fsaua) are created during the installation
- `/etc/group`: A new group (fsc) is created during the installation
- crontab of the root user: The virus definition database update command is added to the root crontab during the installation. Scheduled scanning tasks are added to the crontab when they are created.

Network Resources

When running, the product reserves the following IP ports:

Interface	Protocol	Port	Comment
lo	tcp	28005	Web User Interface internal communication port
lo	tcp	28078	PostgreSQL alert database
lo	tcp	28080	Local Web User Interface access
any	tcp	28082	Remote SSL Web User Interface access (if enabled)

Memory

The Web User Interface reserves over 200 MB of memory, but since the WebUI is not used all the time, the memory is usually swapped out. The other product components sum up to about 50 MB of memory, the on-access scanner uses the majority of it.

The memory consumption depends on the amount of file accesses on the system. If several users are logged in to the system and all of them access lots of files, the memory consumption grows.

CPU

The load on the processor depends on the amount of file accesses on the system, as the on-access scanner scans every file that is opened, closed and executed.

The CPU usage grows when many users are logged in to the system at the same time.

Some software products are designed to access many files and the on-access scanning can slow down these products noticeably.

Stand-alone Installation

The stand-alone installation mode is meant for evaluation use and for environments with few Linux computers where central administration with F-Secure Policy Manager is not necessary.

You must have a compiler and the kernel source installed. Read the distribution-specific instructions on the manual appendix on how to check that the required tools are installed.

You will need to install the product using an account with root privileges.

1. Copy the installation file to your hard disk. Use the following command to extract the installation file: `tar zxvf f-secure-linux-security-<version>.<build>.tgz`
2. Make sure that the installation file is executable: `chmod a+x f-secure-linux-security-<version>.<build>`
3. Run the following command to start the installation:
`./f-secure-linux-security-<version>.<build>`
4. The installation displays the license agreement. If you accept the agreement, answer `yes` press enter to continue.

The installation is complete.

Run `fsav-config` to configure the product if you need to change the default settings.

If you want to turn off certain features of the product completely, use `fschooser` to disable Web User Interface or firewall components and the [Summary](#) page in the Web User Interface to disable Integrity Protection and virus protection features.


Integrity Checking and Rootkit Protection features are off until you generate the baseline and a passphrase for it.

Centrally Managed Installation

In centrally managed mode, the product is installed locally, and it is managed with F-Secure Policy Manager that is installed on a separate computer. Centrally managed installation is the recommended installation mode when taking the product into use in a large network environment.

You must have a compiler and the kernel source installed. Read the distribution-specific instructions on the manual appendix on how to check that the required tools are installed.

You must have F-Secure Policy Manager installed on a separate computer before you install the product. For F-Secure Policy Manager Console installation instructions, see the F-Secure Policy Manager Administrator's Guide.

 **Note:** You cannot use the Anti-Virus mode of F-Secure Policy Manager Console to administer Linux products. Use the **Advanced** mode.

You will need to install the product using an account with root privileges.

1. Copy the installation file to your hard disk. Use the following command to extract the installation file: `tar zxvf f-secure-linux-security-<version>.<build>.tgz`
2. Make sure that the installation file is executable: `chmod a+x f-secure-linux-security-<version>.<build>`
3. Run the following command to start the installation:
`./f-secure-linux-security-<version>.<build>`
4. The installation displays the license agreement. If you accept the agreement, answer `yes` press enter to continue.

The installation is complete.

Run `fsav-config` to configure the product if you need to change the default settings.

If you want to turn off certain features of the product completely, use `fschooser` to disable Web User Interface or firewall components and the **Summary** page in the Web User Interface to disable Integrity Protection and virus protection features.

Integrity Checking and Rootkit Protection features are off until you generate the baseline and a passphrase for it.

Upgrading

You can upgrade the evaluation version or a previous product version without uninstalling the product.

Upgrading from a Previous Product Version

If you are running version F-Secure Linux Server Security 5.20 or later, you can install the product without uninstalling the previous version. If you have an earlier version, upgrade it to F-Secure Linux Server Security 5.20 first, or uninstall it before you install the latest version.

The uninstallation preserves all settings and the host identity, so you do not need to import the host to the F-Secure Policy Manager again. Note that the upgrade deletes all alerts generated with the earlier version.

Manual scanning, scheduled scanning and database update settings have changed in version 5.30 and later. If you have modified these settings before the upgrade, you have to make the same modifications again after the upgrade.

F-Secure Linux Client Security


You cannot upgrade any version of F-Secure Linux Client Security.


Uninstall the previous Client Security product before you install F-Secure Linux Security 7.

F-Secure Linux Server Security 5.5x and F-Secure Anti-Virus for Linux 4-series

Run the installation as usual to upgrade the product.

After the upgrade, you have to reboot the computer. The previous version of the kernel driver is incompatible with new real-time protection features and it is not running after the upgrade. The upgraded driver is loaded after the reboot.

 **Important:** In centrally managed installations, remember to upgrade the MIB in your F-Secure Policy Manager installation.

 **Note:** When you upgrade from F-Secure Linux Server Security 5.xx or earlier, the upgrade removes your previous keycode and the product is running in the evaluation version. Upgrade the evaluation version to full product version before using the product.

F-Secure Anti-Virus for Linux Servers version 4.65

The upgrade from version 4.65 is supported for the command-line installation only.

Upgrading from F-Secure Anti-Virus 4.65

You can upgrade version 4.65 to a command line only installation by running the installer normally.

Your old configuration file will be stored as `/opt/f-secure/fsav/migration/fsav4.conf`.

If you want to upgrade version 4.65 to the full version, uninstall the old version first and run the installer normally.

Uninstalling Earlier Version

The earlier version of the product can be uninstalled with the uninstallation command or by deleting program files and directories.

1. If you have version 5.x, run the following command from the command line to uninstall it:

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

2. If you have version 4.x, remove the following directories and files to uninstall it:

```
/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
```

Upgrading the Evaluation Version

The evaluation version of the product can be upgraded to the full, licensed version of the product.

If you evaluated a previous version of the product and the evaluation period has expired, uninstall the previous version first.


Follow these instructions if you want to upgrade the evaluation version to the full, licensed version of the product.

1. Open the Web User Interface.
2. Open the **About** page.
3. Enter the keycode to upgrade to the licensed version of the product. Enter the keycode in the format you received it, including the hyphens that separate sequences of letters and digits.

After you have entered the keycode, the evaluation version is upgraded to the full version.

To upgrade the evaluation version from the command line, run the following command:

```
/opt/f-secure/fsav/sbin/convert_to_full_installation.sh
```

-  **Note:** If the evaluation period of the current version of the product has expired before you upgrade to the full version, you have to restart the product after entering the keycode.

Custom Installations

If you do not want to install stand-alone or centrally managed product with the default options, you can do a custom install.

Preparing for Custom Installation

The RPM files can be extracted from the installation package if you need to create a custom installation package.

The product installation package is a self extracting package, which contains the software as RPMs. The RPM files can be extracted from the package as follows:

1. Type the following command: `./f-secure-linux-security-<version>.<build>
rpm`
2. Install RPM packages.
3. Run the following script: `/opt/f-secure/fsav/fsav-config`

Unattended Installation

In unattended installation mode, you can provide a set of default settings on the installer command line. This way, you can force the Integrity Checking baseline to be generated as a part of the installation process.

Use the following command line switch during the installation:

```
--auto MODE [fspms=FSPMSURL adminkey=/PATH/TO/ADMIN.PUB] lang=en|de|ja  
[no]remotewui [no]locallogin user=USER kernelverify|nokernelverify  
pass=PASSPHRASE keycode=KEYCODE
```

Where `MODE` is standalone for the standalone installation or managed for the centrally managed installation.

If `MODE` is managed, you have to provide the URL to F-Secure Policy Manager Server and the location of the administrator *public key*, for example:

```
fspms=http://fspms.company.com/ adminkey=/root/admin.pub
```

Use the following options in the command line:

<code>lang</code>	Select the language for the web user interface.
<code>remotewui</code>	Allow remote access to the web user interface.

noremotewui	Do not allow remote access to the web user interface.
nolocallogin	Allow local access to the web user interface without login.
locallogin	Require login for the local access to the web user interface.
user=USER	Specify the local account to use for the web user interface login.
kernelverify	Turn on the kernel module verification.
nokernelverify	Turn off the kernel module verification.
pass=PASS	Specify the passphrase for the baseline generation.
keycode=KEYCODE	Specify the keycode for license checks. If no keycode is provided, the product is installed in the evaluation mode.

For example, to install the product in standalone mode with English web user interface, with no remote access to user interface and not requiring login for local user interface access and not using kernel module verification:

```
./f-secure-linux-security-<version>.<build> --auto standalone lang=en
noremotewui nolocallogin nokernelverify
```

Installing Command Line Scanner Only

The command line only installation installs only the command line scanner and the automatic update agent.

The installation mode is designed for users migrating from F-Secure Anti-Virus for Linux 4.6x series and for users who do not need the real-time protection, integrity checking, web user interface or central management, for example users running AMaViS mail virus scanner.

Use the following command line when running the installer to install the command line scanner only version of the product:

```
./f-secure-linux-security-<version>.<build> --command-line-only
```

If you are running an earlier version and you want to upgrade to the latest version, but you want to install the command line scanner only, you have to uninstall the earlier version first.

Use the `/etc/opt/f-secure/fssp/fssp.conf` configuration file to configure the command line scanner only installation. See the file for detailed descriptions of the available settings.


Using The Product With Samba Servers

The product can protect the whole Samba server in addition to the data on shared directories.

All the protection features of the product are in use for Samba servers.

1. If you have F-Secure Anti-Virus for Samba Server installed, uninstall it before installing the product. Use the following command: `/opt/f-secure/fsav/bin/uninstall-fsav`
2. Follow the normal installation instructions.
The product protects samba shares after the installation, no additional setup is needed. After the installation, the firewall blocks incoming Windows Network share (Samba) access, so you have to change the firewall rules.
3. Change firewall rules to allow Samba traffic.
 - Use the Firewall Rule Wizard in the Web User interface.
 1. Open [I want to](#) page and click [Create a firewall rule](#).
 2. Select [Allow access to a service running on this machine](#).
 3. Select [Windows networking \(1\)](#).
 4. Finish the wizard.
 5. Run the wizard again and add another rule for [Windows networking \(2\)](#) service.
 - Use the Firewall Rule Editor in the Advanced Mode of the Web User interface.
 1. In Web User Interface, go to [Advanced Mode](#).
 2. Select [Firewall](#).
 3. On the [Firewall](#) page, select profile you want to use to the [Profile to edit](#) field.
 4. Click [Add rule](#).
 5. Enter, for example, `[myNetwork]` in the [Remote Host](#) field and add a short description for the rule.
 6. Select [Windows networking \(1\)](#) from the drop-down menu and click [Add service to this rule](#) to add it as a service.
 7. Select [Windows networking \(2\)](#) from the drop-down menu and click [Add service to this rule](#) to add it as a service.
 8. Use arrows on the right side of the table to move the rule above the deny rules in the firewall rules list.
 9. Click [Save](#) to take new rules in the use.
 - Use the Firewall Rule Editor in F-Secure Policy Manager Console.

1. In the advanced mode of F-Secure Policy Manager Console, select the host or policy domain that you want to administer.
2. Select **Linux Security 7.00** and open the **Firewall** tab.
3. In the **Rules** section, check that you have the security level you want to edit.
4. Click **Add Before**.
5. In the Rule Wizard, allow inbound traffic for the **Windows networking (1)**.
6. Run the Rule Wizard again to add **Windows networking (2)**.
7. Distribute the policy.

 **Note:** If the firewall rules have been edited locally, configure the setting as **Final** before you distribute the policy.

When you want to add new rules, you have to disable the firewall temporarily:

1. Change **Firewall protection** to **Disabled** or run the following command:
`/opt/f-secure/fsav/bin/fsfwc --mode bypass.`
2. Select the Security Level you want to edit and edit firewall rules as described.
3. Enable the firewall after you have finished in Web User Interface or run the following command:
`/opt/f-secure/fsav/bin/fsfwc --mode your_profile`, where `your_profile` is the profile edited (block, mobile, home, office, strict or normal).

Creating a Backup

You can backup and restore all product data.

To backup all relevant data, run the following commands:

```
# /etc/init.d/fsma stop
# /etc/init.d/fsaua stop
# tar cpsf <backup-filename>.tar /etc/init.d/fsma /etc/init.d/fsaua
  /etc/opt/f-secure /var/opt/f-secure /opt/f-secure
# /etc/init.d/fsaua start
# /etc/init.d/fsma start
```

To restore data from backup file, run the following commands:

```
# /etc/init.d/fsma stop
```

```
# /etc/init.d/fsaua stop
# cd /
# rm -rf /var/opt/f-secure
# tar xpsf <backup-filename>.tar
# /etc/init.d/fsaua start
# /etc/init.d/fsma start
```

Make sure that fsma and fsaua users and fsc group exist after the backup has been restored, for example by backing up also `/etc/passwd`, `/etc/shadow` and `/etc/group` files.

Uninstallation

You can uninstall the product with the `uninstall-fsav` command-line command.

Run the following script as root user to uninstall the product

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

The uninstall script does not remove configuration files. If you are sure that you do not need them any more, remove all files in the `/etc/opt/f-secure/fsma` path.

Chapter 4

Administering the Product


Topics:

- *Basics of Using F-Secure Policy Manager*
- *Accessing the Web User Interface*
- *Testing the Antivirus Protection*

Basics of Using F-Secure Policy Manager

In the centralized administration mode, F-Secure Policy Manager Console is used to change settings and view statistics of the F-Secure products.

If your corporate network utilizes F-Secure Policy Manager to configure and manage F-Secure products, you can add the product to the existing F-Secure Policy Manager environment.

 **Note:** You cannot use the Anti-Virus mode of F-Secure Policy Manager Console to administer Linux products. Use the **Advanced** mode.

Use the settings in the **F-Secure Linux Security** > **Settings** tabs to configure the product.

 **Note:** You can edit the settings under **F-Secure Security Platform for Linux**, **F-Secure Management Agent** and **F-Secure Automatic Update Agent** branches to change the behavior of the product as well.

For more information about F-Secure Policy Manager, see F-Secure Policy Manager Administrator's Guide.

Accessing the Web User Interface


You can access the Web User Interface from the system tray, or with a web address.

If you allow the remote access to the web user interface, you can access it with the following HTTPS address: `https://<host.domain>:28082/`. Follow these instructions to add the product icon to the system tray.

1. Install the product icon.
 - If you are using GNOME, follow these instructions:
 1. Right-click on the GNOME panel.
 2. Choose **Add Panel applet**.
 3. Select F-Secure Panel Applet from the list of installed GNOME panel applets.
 - If you are not using GNOME, enter `fsui` command from the command line.
2. Double-click the product icon in the system tray to open the Web User Interface.

After the product icon is installed to the system tray, you can access the Web User Interface with it.

It is possible to have both F-Secure Policy Manager and the Web User Interface in use at the same time.

 **Note:** The user can locally override the settings created with F-Secure Policy Manager unless the administrator has prevented this by selecting the **Final** checkbox in the F-Secure Policy Manager settings.

Testing the Antivirus Protection

To test whether the product operates correctly, you can use a special test file that is detected as a virus.

The EICAR (EICAR is the European Institute of Computer Anti-virus Research) standard antivirus test file is detected by several antivirus programs. The Eicar info page can be found at http://www.europe.f-secure.com/virus-info/eicar_test_file.shtml.

 **Tip:** You can use the EICAR test file to test your e-mail scanning as well.

1. Download or create the EICAR test file.
 - Download the EICAR test file from http://www.europe.f-secure.com/virus-info/eicar_test_file.shtml, or
 - Use any text editor to create the eicar.com file with the following single line in it:
`X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*`
2. Run the following command: `fsav eicar.com`

The product should detect the EICAR test file as a virus.

Chapter 5

Using the Product

Topics:

- *Summary*
- *Scanning for Viruses*
- *Firewall Protection*
- *Integrity Checking*
- *General Settings*

Summary

The summary page displays the product status and the latest reports.

The product status displays the protection status and any possible errors or malfunctions.

You can turn virus protection and integrity protection on and off and change the firewall protection level on the summary screen.

The report section offers guidance for any issues that may need your immediate attention.

I Want to...

You can configure the manual scan and firewall settings and check latest virus definition database updates from the [I want to...](#) page.

 **Note:** Click [Modify advanced settings...](#) to view and configure advanced settings.

Scanning The Computer Manually

You can scan the whole computer for malware manually with the Web User Interface.

When the product scans files, it must have at least read access to them. If you want the product to disinfect infected files, it must have write access to the files.

Check and edit the manual scanning settings before you start the manual scan.

1. To start the full computer scan, select [I want to...](#) in the basic user interface mode.
2. Click [Scan the computer for malware](#).

 **Note:** If you have the `nautilus-actions` package installed, scan actions are integrated into the right-click menu in GNOME file manager.

Creating Firewall Services and Rules

You can create new firewall services and rules if you want to allow traffic that is blocked or if you want to block specific net traffic. When you create or edit firewall rules, you should allow only the needed services and deny all the rest to minimize security risks.

To use the Firewall Wizard, go to [I want to...](#) and click [Create a firewall rule](#), follow the onscreen instructions and finish the wizard.

Follow these instructions to create a new service and rule in the advanced user interface:

1. Create a new service.
 - a) Select the **Network Services** in the **Advanced mode** menu.
 - b) Define a unique name for the service in the **Service Name** field.
 - c) Enter a descriptive comment in the **Description** field to distinguish this service from other services.
 - d) Select a protocol number for the service from the **Protocol** drop-down list.
If your service does not use ICMP, TCP or UDP protocol, select Numeric and type the protocol number in the field reserved for it.
 - e) If your service uses the TCP or UDP protocol, define **Initiator Ports** the service covers.
 - f) If your service uses TCP or UDP protocols, define **Responder Ports** the service covers.
 - g) Click **Add as a new service** to add the service to the Network services list.
 - h) Click **Save**.
The new service is saved to the service list.
2. Create a new rule for the service.
 - a) Select **Firewall Rules** in the **Advanced mode** menu to create a firewall rule that uses the service you have defined.
 - b) Select the profile where you want to add a new rule and click **Add new rule** to create a new rule.
 - c) Select **Accept** or **Deny** as a rule **Type** to choose whether the rule allows or denies the service.
 - d) Enter details about target addresses to the **Remote host** field. Enter the IP address and the subnet in bit net mask format.
For example: 192.168.88.0/29
You can use the following aliases as the target address:
 - [myNetwork] - The local-area network.
 - [myDNS] - All configured DNS servers.
 - e) Enter a descriptive comment in the **Description** field to distinguish this rule.
 - f) Select the new service you have created in the **Service** field and the direction when the rule applies.
 - in = all incoming traffic that comes to your computer from the Internet.
 - out = all outgoing traffic that originates from your computer.
 - g) Choose network interfaces to which the rule applies. Type network interfaces you want the rule to apply to the **Flag** field. The rule is applied to all network interfaces if you leave the **Flag** field empty.
For example, [if:eth0], [if:eth3].

- h) Click **Add Service to This Rule**.
The service is added to the new rule.
- i) If you do not want to add other services to the same rule, click **Add to Firewall Rules**.
Each rule must have at least one service. If the rule contains a new service, make sure you have saved the service list in the **Network Services** page.
The rule is added to the active set of rules on the **Firewall Rules** table.
- j) Click **Save** to save the new rule list.

Verify Baseline

You can verify the baseline manually to make sure that your system is safe and all baselined files are unmodified.

1. Enter your passphrase to verify the baseline.
2. Do not start any other integrity checking processes while the product verifies the baseline.

If an attacker has managed to gain a root access to the system and regenerated the baseline, the regenerated baseline does not match against your passphrase when you verify the baseline.

Automatic Updates

F-Secure Automatic Update Agent keeps the protection on your computer updated.

F-Secure Automatic Update Agent retrieves the latest updates to your computer when you are connected to the Internet.

Information about the latest virus definition database update can be found at:

<http://www.F-Secure.com/download-purchase/updates.shtml>

Software Installation Mode

Use the Software Installation Mode when you want to modify system files and programs.

Integrity Checking prevents unauthorized and unwanted modifications of system files and programs. When you update your operating system, apply a security update or install new versions of software, you need to modify files that Integrity Checking monitors.

When the Software Installation Mode is enabled, any process can load any kernel modules regardless whether they are in the baseline or not and any process can change any files in the baseline, whether those files are protected or not. The real-time scanning is still enabled and it alerts of any malware found during the installation.

When leaving the Software Installation Mode, the product updates the known files list with new files and generates the new baseline. If the integrity checking and the rootkit protection features have been enabled, they are turned back on after the new baseline is generated.

- 👉 **Important:** If you install software without the Software Installation Mode when Integrity Checking monitors updated files, you may be unable to install or use the new software. For example, Integrity Checking may prevent a kernel update from booting properly as new drivers are not in the baseline.

Baseline

Integrity Checking is set up by creating a baseline of the system files that you want to protect.

A default set of system files is added to the *Known Files List* during the installation. By default, *Kernel Module Verification* is enabled during the installation and the baseline is generated from the *Known Files List*. If you do not enable the *Kernel Module Verification* during the installation, you have to generate the baseline manually before Integrity Checking is enabled.

All files that are added to the baseline during the installation are set to **Allow** and **Alert** protection mode.

- 👉 **Note:** The default list of known files is generated upon installation, and contains the most important system files. The list of files differs between distributions. Run `/opt/f-secure/fsav/bin/fslistfiles` to retrieve the exact list of files.

Scanning for Viruses

The product stops *viruses* and other *malware*.

What are Viruses and Other Malware?

Malware are programs specifically designed to damage the computer, use the computer for illegal purposes without users knowledge or steal information from the computer.

Malware can:

- take control over the web browser,
- redirect the web search attempts,
- show unwanted advertising,
- keep track on the visited web sites,
- steal personal information such as your banking information,
- use the computer to send spam, and
- use the computer to attack other computers.

Malware programs can also cause the computer to become slow and unstable.

Viruses

A virus is usually a program that can attach itself to files and replicate itself repeatedly; they can alter and replace the contents of other files in a way that may damage the computer.

A *virus* is a program that is normally installed without users knowledge on the computer. Once there, the virus tries to replicate itself. The virus:

- uses some of the system resources
- may alter or damage files on the computer
- tries to use the computer to infect other computers
- may allow the computer to be used for illegal purposes.

Riskware

Riskware is not malware; it is not designed specifically to harm the computer, but it has security critical functions that may harm the computer if misused.

These programs perform some useful but potentially dangerous function. Examples of such programs are:

- programs for Instant messaging (like IRC, Internet relay chat),
- programs for transferring files over the Internet from one computer to another, or
- Internet phone programs (VoIP, *Voice Over Internet Protocol*).

If the program is identified as riskware but it is explicitly installed and correctly set it up, it is less likely to be harmful.

Riskware Types

Riskware categories and platforms.

List of categories

- Adware
- AVTool
- Client-IRC
- Client-SMTP
- CrackTool
- Dialer
- Downloader
- Effect
- FalseAlarm
- Joke
- Monitor

- NetTool
- Porn-Dialer
- Porn-Downloader
- Porn-Tool
- Proxy
- PSWTool
- RemoteAdmin
- RiskTool
- Server-FTP
- Server-Proxy
- Server-Telnet
- Server-Web
- Tool

List of platforms

- Apropos
- BAT
- Casino
- ClearSearch
- DOS
- DrWeb
- Dudu
- ESafe
- HTML
- Java
- JS
- Linux
- Lop
- Macro
- Maxifiles
- NAI
- NaviPromo
- NewDotNet
- Palm
- Perl
- PHP
- Searcher

- Solomon
- Symantec
- TrendMicro
- UNIX
- VBA
- VBS
- Win16
- Win32
- Wintol
- ZenoSearch

Rootkits

Rootkits are programs that make other *malware* difficult to find.

Rootkit programs subvert the control of the operating system from its legitimate functions. Usually, a rootkit tries to obscure its installation and prevent its removal by concealing running processes, files or system data from the operating system. In general, rootkits do this to hide malicious activity on the computer.

Protection Against Userspace Rootkits

If an attacker has gained an access to the system and tries to install a userspace rootkit by replacing various system utilities, *HIPS* detects modified system files and alerts the administrator.

Protection Against Kernel Rootkits

If an attacker has gained an access to the system and tries to install a kernel rootkit by loading a kernel module for example through `/sbin/insmod` or `/sbin/modprobe`, *HIPS* detects the attempt, prevents the unknown kernel module from loading and alerts the administrator.

If an attacker has gained an access to the system and tries to install a kernel rootkit by modifying the running kernel directly via `/dev/kmem`, *HIPS* detects the attempt, prevents write attempts and alerts the administrator.

Stopping Viruses and Other Malware

The product protects the computer from programs that may damage files, steal personal information or use it for illegal purposes.

By default, the product protects the computer from *malware* in real time in the background. The computer is protected from *malware* all the time.

The product can scan specified files and directories, any removable media (such as portable drives) and downloaded content automatically. The product guards the computer for any changes that may indicate *malware*.

How Does Real-time Scanning Protect Your Computer?

Real-time scanning protects the computer by scanning files when they are accessed and blocking access to files that contain *malware*.

Real-time scanning works as follows:

1. The computer tries to access a file.
2. The file is immediately scanned for *malware* before the computer is allowed access to the file.
3. If *malware* is found in the file, real-time scanning blocks access to the file so the *malware* cannot harm the computer.
4. Based on the real-time scanning settings, real-time scanning either renames, deletes or tries to disinfect the infected file.

Does Real-Time Scanning Affect the System Performance?

The amount of time and system resources that real-time scanning takes depends on the contents, location and type of the file.

Files that take a longer time to scan:

- Compressed files, such as .zip archives. Note that these files are not scanned by default.
- Files on network file systems.
- Large files.

Real-time scanning may slow down your computer when a lot of files are accessed at the same time.

Scanning The Computer Manually

You can scan the whole computer for malware manually with the Web User Interface.

When the product scans files, it must have at least read access to them. If you want the product to disinfect infected files, it must have write access to the files.

Check and edit the manual scanning settings before you start the manual scan.

1. To start the full computer scan, select **I want to...** in the basic user interface mode.
2. Click **Scan the computer for malware**.

 **Note:** If you have the `nautilus-actions` package installed, scan actions are integrated into the right-click menu in GNOME file manager.

Methods of Protecting the Computer from Malware

There are multiple methods of protecting the computer from *malware*; deciding which method to use depends on how powerful the computer is and how high a level of protection is needed.

Turning on all the virus protection features on can have a noticeable effect on the speed of the computer.

Scanning the Computer in Real Time

Real-time scanning scans for *malware* in real time so that the computer is always protected.

Action on Virus Infection

Select the primary and secondary action to take when a virus is found.

In the **I want to...** page in the web user interface, click **Modify advanced settings...** to view and configure advanced virus scanning settings.

1. Select the primary action to take when a virus is found. Choose one of the following actions:

- Select **Report and deny access** to display and alert about the found virus and block access to it. No other action is taken against the infected file. View **Alerts** to check security alerts.
- Select **Disinfect** to disinfect viruses. Note that some viruses cannot be disinfect. If the virus cannot be disinfect, the access to the infected file is still blocked.
- Select **Rename** to rename the infected file and remove its execute permissions. Renamed infected file stays on the computer, but it cannot cause any damage. The renamed file has `.virus` extension.
- Select **Delete** to delete the infected file.
- Select **Deny access** to block the access to the infected file without sending any alerts or reports.

By default, the primary action for infections is **Disinfect**.

2. Select the secondary action. The secondary action takes place if the primary action cannot be performed.

By default, the secondary action is **Rename**.

After configuring the virus infection actions, configure how alerts and reports are handled in the **Alerts** page.

Suspected Files

Select the primary and secondary actions to take when heuristics scanning engine finds a suspected file.

In the **I want to...** page in the web user interface, click **Modify advanced settings...** to view and configure advanced virus scanning settings.

1. Select the primary action to take when heuristics scanning engine finds a suspected file. Choose one of the following actions:
 - Select **Report and deny access** to display and alert about the suspected file and block access to it. No other action is taken. View **Alerts** to check security alerts.
 - Select **Rename** to renames the suspected file and remove its execute permissions. Renamed suspected file stays on the computer, but it cannot cause any damage. The renamed file has `.suspected` extension.
 - Select **Delete** to delete the suspected file.
 - Select **Deny access** to block the access to the suspected file without sending any alerts or reports.

By default, the primary action for suspected files is **Report only**.

2. Select the secondary action. The secondary action takes place if the primary action cannot be performed. By default, the secondary action is **Deny access**.

After configuring the suspected file settings, configure how alerts and reports are handled in the **Alerts** page.


Select What to Scan

Specify files and directories that you want to scan for malware.

In the **I want to...** page in the web user interface, click **Modify advanced settings...** to view and configure advanced virus scanning settings.

1. Specify **Files and directories excluded from scanning** to define files and directories which are excluded from the virus scan. Type each directory on a new line, only one directory per line.


If scanning a certain directory takes a long time and you know that no user can create or copy an infected file in it, or you get false alarms during the scan, you can exclude the directory from the virus scan.

 **Tip:** The list can also contain files if you want to exclude specific files from the scan.


2. If you do not want to scan any other files for viruses except executables, turn **Scan only executables** on. Clear the check box to scan all specified files for viruses.

 **Note:** If [Scan on open](#) and [Scan on execute](#) are turned off, nothing is scanned even if [Scan only executables](#) is enabled.


3. Define [Whitelisted executables](#) which may access any files. The virus scan does not block any file accesses from whitelisted executables.

 **Note:** Be sure that you can trust the executable file that you add as a whitelisted application. It is recommended to limit the file access for whitelisted applications. Whitelisting an application is always a potential security risk and should be used with caution.

4. If you want to use the whitelist setting with *Integrity Checking*, turn on [Whitelisted executables must match baseline](#) to require that whitelisted executables are unmodified in the *known files list*. If this setting is enabled and the executable cannot be found in the integrity checking baseline, it is not whitelisted.

 **Note:** If you have defined whitelisted applications, it is highly recommended to turn on this option.

5. If you want to scan files every time they are opened, turn on [Scan when opening a file](#).
6. If you want to scan files every time they are closed, turn on [Scan when closing a file](#).
7. If you want to scan files every time when they are run, turn on [Scan when running an executable](#).


 **Note:** Only regular files on mounted filesystems can be scanned. Special files, such as CD-ROM or DAT devices (*/dev/st0*, */dev/hda* and such), cannot be scanned unless they are mounted as filesystems, or files are extracted on a filesystem from the tape first.

Archive Scanning

The archive scanning can scan files inside compressed ZIP, ARJ, LZH, RAR, CAB, TAR, BZ2, GZ, JAR and TGZ archives.

In the [I want to...](#) page in the Web User Interface, click [Modify advanced settings...](#) to view and configure advanced virus scanning settings.

1. Turn on [Scan inside archives](#) if you want to scan files inside archives.

 **Note:** When the archive scanning is enabled, some e-mail clients may stop processing further e-mails when an infected e-mail is opened.

2. In [Maximum number of nested archives](#), set the number of levels in nested archives the product scans. Nested archives are archives inside other archives.

3. Select how to treat password protected archives. Password protected archives cannot be scanned for viruses.
 - Turn on **Treat password protected archives as safe** to allow access to password protected archives. The user who opens the password protected archive should have an up-to-date virus protection on the computer if password protected archives are treated as safe.
 - Turn off **Treat password protected archives as safe** to deny users from accessing the archive.
4. If you want the archive scan to stop immediately when it finds an infected file, turn on **Stop on first infection inside an archive** to stop scanning the archive. If the setting is turned off, the product scans the whole archive.

Riskware Scanning

Select the primary and secondary action to take when riskware is found.

In the **I want to...** page in the web user interface, click **Modify advanced settings...** to view and configure advanced virus scanning settings.

1. Select the primary action to take when riskware is found. Choose one of the following actions:
 - Select **Report and deny access** to display and alert about the found riskware and block access to it. No other action is taken against the infected file. View **Alerts** to check security alerts. (Not available during the manual scanning.)
 - Select **Rename** to rename the riskware file and remove its execute permissions. Renamed file stays on the computer, but it cannot cause any damage. The renamed file has `.riskware` extension.
 - Select **Delete** to delete the riskware file.
 - Select **Deny access** to block the access to the riskware file without sending any alerts or reports. (Not available during the manual scanning.)
 - Select **Report only**.

By default, the primary action for infections is **Report only**.

2. Select the secondary action. The secondary action takes place if the primary action cannot be performed.
By default, the secondary action is **Deny access**.
3. In the **Excluded Riskware** field, specify riskware types that the product should not scan. Use the following format to specify riskware you want to exclude and separate each entry with a semicolon (;) `Category.Platform.Family` where category, platform or family can be * wildcard.
For example, `Client-IRC.*.*` excludes all riskware entries in the Client-IRC category.

After configuring the risware scanning settings, configure how alerts and reports are handled in the [Alerts](#) page.

Scanning the Computer Manually

You can scan the computer for viruses manually to make sure that specified files or every possible file is checked for viruses.

Action on Virus Infection During Manual Scan

Select the primary and secondary action to take when a virus is found during the manual scan.

In the [I want to...](#) page in the web user interface, click [Modify advanced settings...](#) to view and configure advanced virus scanning settings.

1. Select the primary action to take when a virus is found. Choose one of the following actions:

- Select [Disinfect](#) to disinfect viruses. Note that some viruses cannot be disinfected. If the virus cannot be disinfected, the access to the infected file is still blocked.
- Select [Rename](#) to rename the infected file and remove its execute permissions. Renamed infected file stays on the computer, but it cannot cause any damage. The renamed file has `.virus` extension.
- Select [Delete](#) to delete the infected file.

By default, the primary action for infections is [Disinfect](#).

2. Select the secondary action. The secondary action takes place if the primary action cannot be performed.

By default, the secondary action is [Rename](#).

After configuring the virus infection actions, configure how alerts and reports are handled in the [Alerts](#) page.

Suspected Files Found During the Manual Scan

Select the primary and secondary actions to take when heuristics scanning engine finds a suspected file during the manual scan.

In the [I want to...](#) page in the web user interface, click [Modify advanced settings...](#) to view and configure advanced virus scanning settings.

1. Select the primary action to take when heuristics scanning engine finds a suspected file. Choose one of the following actions:

- Select [Rename](#) to renames the suspected file and remove its execute permissions. Renamed suspected file stays on the computer, but it cannot cause any damage. The renamed file has `.suspected` extension.
- Select [Delete](#) to delete the suspected file.

By default, the primary action for suspected files is **Report only**.

2. Select the secondary action. The secondary action takes place if the primary action cannot be performed.

After configuring the suspected file settings, configure how alerts and reports are handled in the **Alerts** page.


Select What to Scan During the Manual Scan

Specify files and directories that you want to scan for malware when you run a manual scan.

In the **I want to...** page in the web user interface, click **Modify advanced settings...** to view and configure advanced virus scanning settings.

1. In **Scan files** setting, select whether you want to scan all files during the manual scan or files with specified extensions.
If you select to scan **Only files with specified extensions**, **Included extensions** field opens. Specify file extensions you want to be scanned, separate each extension with a comma (.).
2. Specify **Files and directories excluded from scanning** to define files and directories which are excluded from the virus scan. Type each directory on a new line, only one directory per line.


If scanning a certain directory takes a long time and you know that no user can create or copy an infected file in it, or you get false alarms during the scan, you can exclude the directory from the virus scan.

 **Tip:** The list can also contain files if you want to exclude specific files from the scan.

3. If you do not want to scan any other files for viruses except executables, turn **Scan only executables** on. Clear the check box to scan all specified files for viruses.

 **Note:** If **Scan on open** and **Scan on execute** are turned off, nothing is scanned even if **Scan only executables** is enabled.

4. If you do not want the manual scan to change the last access time of the file when it is scanned, select the **Preserve access times** check box.

 **Note:** Only regular files on mounted filesystems can be scanned. Special files, such as CD-ROM or DAT devices (`/dev/st0`, `/dev/hda` and such), cannot be scanned unless they are mounted as filesystems, or files are extracted on a filesystem from the tape first.

Archive Scanning

The archive scanning can scan files inside compressed ZIP, ARJ, LZH, RAR, CAB, TAR, BZ2, GZ, JAR and TGZ archives.

In the **I want to...** page in the Web User Interface, click **Modify advanced settings...** to view and configure advanced virus scanning settings.

1. Turn on **Scan inside archives** if you want to scan files inside archives.
 -  **Note:** When the archive scanning is enabled, some e-mail clients may stop processing further e-mails when an infected e-mail is opened.
2. In **Maximum number of nested archives**, set the number of levels in nested archives the product scans. Nested archives are archives inside other archives.
3. Select how to treat password protected archives. Password protected archives cannot be scanned for viruses.
 - Turn on **Treat password protected archives as safe** to allow access to password protected archives. The user who opens the password protected archive should have an up-to-date virus protection on the computer if password protected archives are treated as safe.
 - Turn off **Treat password protected archives as safe** to deny users from accessing the archive.
4. If you want the archive scan to stop immediately when it finds an infected file, turn on **Stop on first infection inside an archive** to stop scanning the archive. If the setting is turned off, the product scans the whole archive.

Riskware Found During the Manual Scan

Select the primary and secondary action to take when riskware is found during the manual scan.

In the **I want to...** page in the web user interface, click **Modify advanced settings...** to view and configure advanced virus scanning settings.

1. Select the primary action to take when riskware is found. Choose one of the following actions:
 - Select **Rename** to rename the riskware file and remove its execute permissions. Renamed file stays on the computer, but it cannot cause any damage. The renamed file has `.riskware` extension.
 - Select **Delete** to delete the riskware file.
 - Select **Report only**.

By default, the primary action for infections is **Report only**.

2. Select the secondary action. The secondary action takes place if the primary action cannot be performed.
3. In the **Excluded Riskware** field, specify riskware types that the product should not scan.

Use the following format to specify riskware you want to exclude and separate each entry with a semicolon (;) `Category.Platform.Family` where category, platform or family can be * wildcard.

For example, `Client-IRC.*.*` excludes all riskware entries in the Client-IRC category.

After configuring the riskware scanning settings, configure how alerts and reports are handled in the [Alerts](#) page.

Scanning the Computer at Set Times

You can use scheduled scanning to scan the computer for *malware* at regular intervals, for example daily, weekly or monthly.

Creating a Scheduled Scanning Task

Create scheduled scanning tasks to scan the computer for *malware* at regular intervals.

In the [I want to...](#) page in the web user interface, click [Modify advanced settings...](#) to view and configure advanced virus scanning settings.

Note that the scheduled scanning tasks use the [Manual Scanning](#) settings. To set the scanning schedule, follow these instructions:

1. Click [Add a new task](#).
2. Set the date and time when the scheduled scan should start.
Settings are defined the same way as regular crontab entries. For example:
 - To perform the task each sunday at 4 am:
Minute: 0, Hour: 4, Day of the Month: *, Month: *, Day of the Week: sun
 - To perform the task every day at 5:30 am:
Minute: 30, Hour: 5, Day of the Month: *, Month: *, Day of the Week: *
3. Add directories that should be scanned to the [Directories to scan](#) box. Add one directory per line.
4. Click [Save task](#) to add the scheduled scanning task into the schedule.

A scheduled scan can take several hours, so it is a good idea to run it when the system is idle, for example during the night. Another alternative is to configure several scheduled scan tasks, and to scan only some directories at one time.

Configure how alerts and reports are handled in the [Alerts](#) page.

Firewall Protection

The firewall protects the computer against unsafe Internet traffic as well as against attacks originating from inside the local-area network.

The product:

- Protects against intruders who try to access the computer without a permission. They may, for example, try to steal personal information, such as files, passwords or credit card numbers.
- Provides protection against information theft as unauthorized access attempts can be prohibited and detected.

The firewall keeps the computer protected after the product is installed automatically.

What Is a Firewall?

The *firewall* protects the computer by allowing safe Internet traffic and blocking unsafe traffic.

Typically, the *firewall* allows all traffic from your computer to the Internet, but blocks all traffic from the Internet to your computer unless you specifically allow it. By blocking the inbound traffic, the firewall protects your computer against *malicious software*, such as *worms*, and prevents intruders from accessing your computer.

The computer is protected with the predefined *firewall* settings. Usually, you do not have to change them. However, you may have to change the settings, if you use a very strict *security level*, or if you have added your own *firewall rules* or services.




Caution: Do not turn the *firewall* off. If you do, the computer is vulnerable to all network attacks.

What Are Security Profiles?

Firewall *security profiles* define the level of protection on the computer.

Each *security profile* has a predefined set of *firewall rules*, which define the type of traffic that is allowed to or denied from your computer. To some levels you can also add rules that you have created yourself.

The following table contains a list of the security profiles available in the product and the type of traffic each of them either allow or deny.

Security profile	Description
Block All	Blocks all network traffic (excluding loopback).
Server	<p>Allows only IP configuration via DHCP, DNS lookups and ssh protocol out and in.</p> <p> Important: The server profile has to be customized before it can be taken into use.</p>
Mobile	Allows normal web browsing and file retrievals (HTTP, HTTPS, FTP), as well as e-mail and Usenet news traffic. Encryption programs, such as VPN and SSH are also allowed. Everything else is denied. Local rules can be added after the malware probes detection.
Home	Allows all outbound TCP traffic and FTP file retrievals. Everything else is denied. Local rules can be added to enable new network functionality.
Office	Allows all outbound TCP traffic and FTP file retrievals. Everything else is denied by default. With this profile, a firewall should exist between 0.0.0.0/0 and the host.
Strict	Allows outbound web browsing, e-mail and News traffic, encrypted communication, FTP file transfers and remote updates. Everything else is denied.
Normal	Allows all outbound traffic, and denies some specific inbound services.
Disabled	Allows all inbound and outbound network traffic.

How are security profiles related to firewall rules and services?

A *security profile* consists of several *firewall rules*. A *firewall rule* consists of several *firewall services*. Services are defined by the *protocols* and *ports* they use.

For example, the **Normal** security profile has a firewall rule called **Web browsing**. This rule allows you to browse the web. The rule includes the

services that are needed for web browsing, such as the [HyperText Transfer Protocol \(HTTP\)](#) service. This service uses the TCP *and port* number 80.

Changing the Firewall Protection Level

Firewall protection levels allow you to instantly change your firewall rule set.

1. Open [I want to...](#) page in the Web User Interface
2. Select the level you want to use in the [Firewall Protection](#).

Editing Security Profile

Different security profiles can be assigned and edited to suit different users' needs.


Each security profile has a set of pre-configured firewall rules.

1. Select the firewall profile you want to edit. You can change the current security profile from the [Summary](#) page.

The current security profile is displayed on the top of the [Firewall Rules](#) page.

2. The list of rules displays the currently used ruleset. To edit the ruleset:

- Clear the [Enabled](#) checkbox to disable the rule temporarily.
- Use up and down arrows to change the order of rules in the ruleset.

 **Note:** Changing the order of the rules may affect all the other rules you have created.

- Click [X](#) to delete the rule permanently.
- To edit a rule, select it from the list of rules. The selected rule is displayed in the [Edit Rule](#) pane below the list of rules.

3. If the profile contains more than 10 rules, use [<<](#), [<](#), [>](#) and [>>](#) arrows to browse rules.

Firewall Rules

Firewall rules define what kind of Internet traffic is allowed or blocked.

Each *security level* has a predefined set of *firewall rules*, which you cannot change. The selected security level affects the priority which your own rules receive in relation to the predefined rules.

A *firewall rule* can be applied to traffic from the Internet to your computer (inbound), or from your computer to the Internet (outbound). A rule can also be applied to both directions at the same time.

A *firewall rule* consists of *firewall services*, which specify the type of traffic and the *ports* that this type of traffic uses. For example, a rule called **Web browsing** has a service called **HTTP**, which uses the TCP and *port* number 80.

Firewall rules also define whether firewall *alert* pop-ups are shown to you about the traffic that matches the *firewall rules*.

When do you have to add a new *firewall rule*?

You may have to add a new firewall rule if you want to allow traffic that is blocked or if you want to block specific Internet traffic.

By adding all the services that the program or device needs to the same rule, you can easily:

- turn the rule on or off later, or
- remove the rule if you uninstall the program or remove the device.

You also have to add a new rule if you have denied certain type of traffic but you want to allow it to certain IP addresses. In this case, you already have a general "deny" *firewall rule*. To allow the traffic to certain IP addresses, you have to create a more specific "allow" rule.

Firewall Services

Firewall services define the type of traffic to which a *firewall rule* applies.

Network services, such as web browsing, *file sharing* or *remote console access*, are examples of these firewall services.

A service uses a certain *protocol* and *port*. For example, the HTTP service uses the TCP *protocol* and the *port* number 80.

A firewall service uses two kinds of ports:

- *Initiator port*: the *port* on the computer that starts the connection.
- *Responder port*: the *port* on the computer where the connection ends.

Whether the *port* on the computer is an *initiator port* or *responder port* depends on the direction of the traffic:

- If the *firewall service* is for outbound traffic, the *initiator port* is the *port* on your own computer. The *responder port* is then the *port* on a remote computer.
- If the *firewall service* is for inbound traffic, the *initiator port* is the *port* on a remote computer. The *responder port* is then the *port* on your own computer.

The *responder ports* are typically mentioned in the software documentation. The *initiator port* can usually be any *port* higher than 1023. However, for some games you may also have to define specific *initiator ports*. In this case, they are also mentioned in the software documentation.

If you create a new *firewall rule*, you have several predefined services that you can add to the rule. You can also create and add your own services if the service that you need is not on the services list.

Creating Firewall Services and Rules

You can create new firewall services and rules if you want to allow traffic that is blocked or if you want to block specific net traffic. When you create or edit firewall rules, you should allow only the needed services and deny all the rest to minimize security risks.

To use the Firewall Wizard, go to **I want to...** and click **Create a firewall rule**, follow the onscreen instructions and finish the wizard.

Follow these instructions to create a new service and rule in the advanced user interface:

1. Create a new service.
 - a) Select the **Network Services** in the **Advanced mode** menu.
 - b) Define a unique name for the service in the **Service Name** field.
 - c) Enter a descriptive comment in the **Description** field to distinguish this service from other services.
 - d) Select a protocol number for the service from the **Protocol** drop-down list.
If your service does not use ICMP, TCP or UDP protocol, select Numeric and type the protocol number in the field reserved for it.
 - e) If your service uses the TCP or UDP protocol, define **Initiator Ports** the service covers.
 - f) If your service uses TCP or UDP protocols, define **Responder Ports** the service covers.
 - g) Click **Add as a new service** to add the service to the Network services list.
 - h) Click **Save**.
The new service is saved to the service list.
2. Create a new rule for the service.
 - a) Select **Firewall Rules** in the **Advanced mode** menu to create a firewall rule that uses the service you have defined.
 - b) Select the profile where you want to add a new rule and click **Add new rule** to create a new rule.
 - c) Select **Accept** or **Deny** as a rule **Type** to choose whether the rule allows or denies the service.
 - d) Enter details about target addresses to the **Remote host** field. Enter the IP address and the subnet in bit net mask format.
For example: 192.168.88.0/29

You can use the following aliases as the target address:

- [myNetwork] - The local-area network.
 - [myDNS] - All configured DNS servers.
- e) Enter a descriptive comment in the **Description** field to distinguish this rule.
- f) Select the new service you have created in the **Service** field and the direction when the rule applies.
- in = all incoming traffic that comes to your computer from the Internet.
 - out = all outgoing traffic that originates from your computer.
- g) Choose network interfaces to which the rule applies. Type network interfaces you want the rule to apply to the **Flag** field. The rule is applied to all network interfaces if you leave the **Flag** field empty.
For example, [if:eth0], [if:eth3].
- h) Click **Add Service to This Rule**.
The service is added to the new rule.
- i) If you do not want to add other services to the same rule, click **Add to Firewall Rules**.
Each rule must have at least one service. If the rule contains a new service, make sure you have saved the service list in the **Network Services** page.
The rule is added to the active set of rules on the **Firewall Rules** table.
- j) Click **Save** to save the new rule list.

How Does the Priority Order of *Firewall Rules* Work?

Firewall rules have a priority order that determines the order in which the rules are applied to network traffic.

Firewall rules are shown as a list on the **Rules** page. The *rules* are applied from top to bottom, and the first rule that matches the traffic overrides all the other rules below. The main principle is to allow only the needed traffic and block the rest. Therefore, the last rule of a *security level* is the **Deny rest** rule. It blocks all the traffic that the rules above it do not specifically allow.

An example of how the priority order works

Following examples clarify how you can control which rules are applied to a specific network traffic by changing the order of firewall rules.

- You have added a rule that denies all outbound *FTP* traffic. Above the rule in the rules list, you add another rule that allows an *FTP* connection to your Internet Service Provider's IP address. This rule allows you to create an *FTP* connection to that IP address.

- You have added a rule that allows you to create an *FTP* connection to your Internet Service Provider's IP address. Above the rule in the rules list, you add another rule that denies all *FTP* traffic. This rule prevents you from creating an *FTP* connection to your Internet Service Provider's IP address (or any other IP address).

Firewall Settings

On the **Settings** tab, you can select network packet logging settings and configure trusted network interfaces.

Logging Unhandled Network Packets

You can log unhandled network packets in problem solving situations.

By default, you do not need to log unhandled network packets.

1. Open the Web User Interface.
2. Select the **Advanced** check box turn on the advanced mode.
3. Go to **Firewall Protection** ► **General** .
4. Check the **Log all unhandled network packets** check box to log all network packets that do not match to any firewall rules.

All network packets that do not match any firewall rules are logged using syslog (may vary depending on the Linux distribution you use).

Editing Trusted Network Interfaces

Firewall rules apply to all network interfaces on the host. All interfaces on the trusted list have a pass-by rule that accepts all traffic.

1. Open the Web User Interface.
2. Select the **Advanced** check box turn on the advanced mode.
3. Go to **Firewall Protection** ► **General** .
4. Add network interfaces to the **Trusted network interfaces** list and separate each entry with a comma.

All traffic to trusted network interfaces is allowed.

Integrity Checking

Integrity Checking protects important system files against unauthorized modifications.

You can use Integrity Checking to block any modification attempts to protected files, regardless of file system permissions.


Use Integrity Checking Wizards on the [I want to...](#) page to generate and verify the file system baseline. The file system baseline guards your computer against unauthorized file changes. For more integrity checking options, configure settings in the [Advanced](#) mode.

Integrity Checking works by comparing files on the disk to the baseline, which is a cryptographically signed list of file properties. Integrity Checking can be configured to send alerts to the administrator about modification attempts of the monitored files.

Known Files List

The *Known Files List* contains all files that the product monitors and protects.

The baseline is created from the *Known Files List* by reading the properties of the files in the list and cryptographically signing the result. Integrity Checking compares this result to real-time file accesses.

 **Note:** The *Known Files List* in the Web User Interface shows only the baseline status that is currently stored in the product. To view the actual, up-to-date file system status, use the Verify baseline operation in Web User Interface or run the fsic command line utility.

Using the Known Files List Search


Use search filters to select files you want to view in the *Known Files List*.

1. Select files you want to view in the known files list.
 - Select **Modified and new** to display all files that have been modified or added to the baseline.
 - Select **Modified** to display all files that have been modified.
 - Select **New** to display all files that have been added to the baseline.
 - Select **Unmodified** to display all baselined files that have not been modified.
 - Select **All** to display all files in the known files list.
2. If you want to limit the search by the filename, enter any part of the filename of the monitored file you want to view in the known files list to the **Filename** field.

3. Click **Search**.
The *Known Files List* displays search results.
4. View the search results.

Option	Description
Filename	Displays the name of the file.
Detection time	Displays the time when a modification was detected.
Detected modifier	Displays the filename of the process that modified the file.
Action	Displays whether the product allows or denies modifications to the file.
Alert	Displays whether the product sends an alert when the file is modified.
Protection	Displays whether the file is monitored or protected. Protected files cannot be modified while monitored files are only monitored and can be modified.

5. Select the action you want to perform:
 - To regenerate the baseline, select new and modified files you want to baseline and click **Regenerate baseline for highlighted files**.
 - If you want to remove files from the baseline, click files to select them and click **Remove highlighted files** to stop monitoring the selected files.


 **Note:** Integrity Checking does not protect new or modified files before you regenerate the baseline. If you add files to the *Known Files List* or files have been modified, regenerate the baseline to protect those files.

Adding Files to the Known Files List


You can add files to known files list to protect them from unwanted modifications.

1. Enter the filename of the file you want to monitor to the **Filename** field. If you want to add more than one file, separate each filename with a space.
2. Select the protection method you want to use.
 - Select **Monitor** to only monitor the file. Monitored file may be modified.

- Select **Protect** to deny all modifications of the file. The protected file can be opened but it cannot be changed.
3. Select whether you want to prevent the access to the modified file.
 - Select **Allow** to allow the access to the modified file when it is executed or opened.
 - Select **Deny** to deny the access to the modified file. Modified files cannot be opened or executed.
 4. If you want to ignore changes to some attributes of the file, select one or more of the **Ignored Attributes** checkboxes:
 - Mode: Changes to file permissions are ignored
 - User: Changes to file ownership are ignored
 - Group: Changes to file group are ignored
 - Size: Changes to file size are ignored
 - Modification time: Changes to file modification time are ignored
 - Hash: Changes to the content of the file are ignored

 **Note:** Ignoring only the hash attribute is not usually desirable, since modifying file contents usually changes the modification time and size as well.
 5. Click **Add to known files** to add the entry to the *Known Files List*.

Integrity checking does not protect new or modified files before you regenerate the baseline. Regenerate the baseline to protect files you have added.

 **Note:** You can add a single file or multiple files to the baseline at the same time.


Software Installation Mode

Use the Software Installation Mode when you want to modify system files and programs.

Integrity Checking prevents unauthorized and unwanted modifications of system files and programs. When you update your operating system, apply a security update or install new versions of software, you need to modify files that Integrity Checking monitors.

When the Software Installation Mode is enabled, any process can load any kernel modules regardless whether they are in the baseline or not and any process can change any files in the baseline, whether those files are protected or not. The real-time scanning is still enabled and it alerts of any malware found during the installation.

When leaving the Software Installation Mode, the product updates the known files list with new files and generates the new baseline. If the integrity checking and the rootkit protection features have been enabled, they are turned back on after the new baseline is generated.

 **Important:** If you install software without the Software Installation Mode when Integrity Checking monitors updated files, you may be unable to install or use the new software. For example, Integrity Checking may prevent a kernel update from booting properly as new drivers are not in the baseline.

Turning on the Software Installation Mode

Turn on the Software Installation Mode when you want to update or modify protected files.

To access the Software Installation Mode, follow these instructions.

1. Open the Web User Interface.
2. Go to [I want to...](#) page.
3. Click [Install software](#).
The Software Installation Mode wizard opens.

The Software Installation Mode wizard guides you through the software installation and updates the baseline with new software that you install on your system.


You can also use `fsims` command line tool to use the Software Installation Mode from the shell.

Baseline

Integrity Checking is set up by creating a baseline of the system files that you want to protect.

A default set of system files is added to the *Known Files List* during the installation. By default, *Kernel Module Verification* is enabled during the installation and the baseline is generated from the *Known Files List*. If you do not enable the *Kernel Module Verification* during the installation, you have to generate the baseline manually before Integrity Checking is enabled.



All files that are added to the baseline during the installation are set to [Allow](#) and [Alert](#) protection mode.

 **Note:** The default list of known files is generated upon installation, and contains the most important system files. The list of files differs between distributions. Run `/opt/f-secure/fsav/bin/fslistfiles` to retrieve the exact list of files.

Baseline Passphrase

The baseline has to be signed to prevent anyone from modifying the protected files.

The product verifies the baseline and the system integrity cryptographically. A cryptographic algorithm is applied to the baseline contents and the passphrase to generate a signature (a HMAC signature) of the baselined information.

-  **Important:** You must take great care not to forget the passphrase used as it cannot be recovered and the baseline cannot be verified against tampering without using the same passphrase.
-  **Note:** All administrators who know the passphrase can regenerate the baseline, so sharing the passphrase should be limited.

Verify Baseline

You can verify the baseline manually to make sure that your system is safe and all baselined files are unmodified.

1. Enter your passphrase to verify the baseline.
2. Do not start any other integrity checking processes while the product verifies the baseline.

If an attacker has managed to gain a root access to the system and regenerated the baseline, the regenerated baseline does not match against your passphrase when you verify the baseline.

Rootkit Prevention

When the Integrity Checking is enabled, the product can prevent rootkits.

Hackers can use rootkits to gain access to the system and obtain administrator-level access to the computer and the network.

Configuring Rootkit Prevention

When Integrity Checking is on, the product can prevent rootkit infiltrations.

In the [I want to...](#) page in the web user interface, click [Modify advanced settings...](#) to view and configure Integrity Checking settings.

1. Turn [Kernel module verification](#) on or off.
The kernel module verification protects the system against rootkits by preventing unknown kernel modules from loading. When the kernel module verification is on, only those kernel modules that are listed in the known files list and which have not been modified can be loaded. If the kernel module verification is set to [Report only](#), the product sends an alert when an unknown or modified kernel module is loaded but does not prevent it from loading.
2. Turn [Write protect kernel memory](#) on or off.

Kernel memory write-protection protects the `/dev/kmem` file against write attempts. A running kernel cannot be directly modified through the device. If the write protection is set to **Report only**, the product sends an alert when it detects a write attempt to `/dev/kmem` file, but it does not prevent the write operation.

3. Specify **Allowed kernel module loaders**.
Specified programs are allowed to load kernel modules when the kernel module verification is on. By default, the list contains the most common module loaders. If the Linux system you use uses some other module loaders, add them to the list. Type each entry on a new line, only one entry per line.

General Settings

In general settings, you can configure alerting and automatic virus definition database updates and view the product information.

Alerts

On the Alerts page, you can read and delete alert messages.

Alert Severity Levels

Alerts are divided into severity levels.

Severity Level	Syslog priority	Description
Informational	info	Normal operating information from the host.
Warning	warning	A warning from the host. For example, an error when trying to read a file.
Error	err	Recoverable error on the host. For example, the virus definition database update is older than the previously accepted version.


Severity Level	Syslog priority	Description
Fatal Error	emerg	Unrecoverable error on the host that requires attention from the administrator. For example, a process fails to start or loading a kernel module fails.
Security alert	alert	A security alert on the host. For example, a virus-alert. The alert includes information of the infection and the performed operation.

Processing Alerts

You can search and delete specific alerts from hosts.

To find the alert message you want to view, follow these instructions:

1. Select the Status of security alerts you want to view.
 - Select **All** to view All alerts.
 - Select **Unread** to view new alerts.
 - Select **Read** to view alerts you have already viewed.
2. Select the **Severity** of security alerts you want to view.
3. You can delete or mark multiple messages as read simultaneously.
 - Click alerts to highlight them and click **Mark highlighted as read** to flag them as read.
 - Click **Delete highlighted** to delete all highlighted alerts.

 **Note:** You can delete or mark multiple messages as read simultaneously. Select how old and which alert severity messages you want to edit and click Perform action to delete or mark selected messages as read.

Configuring Alerts

Change **Communications** settings to configure where alerts are sent.

In the centrally managed installation mode, make sure that the URL of the F-Secure Policy Manager Server address is correct in the **Server Address** field. Use **Upload Policy Manager Server Certificate** field to enter the location of the `admin.pub` key. This is the key that you created during F-Secure Policy Manager Console Installation


1. In **Alert Level**, specify where an alert is sent according to its severity level. You can send an alert to any of the following:
 - **E-mail to** - Enter the e-mail address where the alert is sent as an e-mail.
 - **Local** - Alert is displayed in the Web User Interface.
 - **Syslog** - Alert is written to the system log. The syslog facility is LOG_DAEMON and alert priority varies.
 - **Policy Manager** - Alert is sent to F-Secure Policy Manager.

 **Note:** F-Secure Panel Applet in the GNOME system tray displays local alerts as pop-ups.

2. Specify **E-mail Settings**.

The e-mail settings are used for all alert messages that have been configured to send e-mail alerts.

- a) Enter the address of the SMTP server in the **Server Address** field. You can use either the DNS-name or IP-address of the SMTP server. The server port is always 25 and it cannot be changed.

 **Note:** If the mail server is not running or the network is down, it is possible that some e-mail alerts are lost. To prevent this, configure a local mail server to port 25 and use it for relaying e-mail alerts.

- b) Enter the full e-mail address (sender@example.com) that you want to use as a sender of the alert in the e-mail message to the **From** field.
- c) Enter the e-mail alert message subject. Use %DESCRIPTION% as the subject to display a short description of the alert in the subject line to the **Subject** field.

Automatic Updates

F-Secure Automatic Update Agent keeps the protection on your computer updated.

F-Secure Automatic Update Agent retrieves the latest updates to your computer when you are connected to the Internet.

Information about the latest virus definition database update can be found at:

<http://www.F-Secure.com/download-purchase/updates.shtml>

Configuring Automatic Updates Options

Configure automatic updates if you use proxy services and you want to control how the product retrieves virus definition updates automatically.

1. Check the **Updates enabled** check box to enable automatic virus definition updates. By default automatic updates are enabled.
2. Configure F-Secure Policy Manager Proxies.

The **Policy Manager Proxies** list displays a list of virus definition database update sources and F-Secure Policy Manager proxies. If no update servers are configured, the product retrieves the latest virus definition updates from F-Secure Update Server automatically.

- a) To add a new address to the list, enter the url to the **PM Proxy address** field.
- b) Define the priority level of the new address.

The priority numbers define the order in which the host tries to connect servers. Virus definition updates are downloaded from the primary sources first, secondary update sources can be used as a backup.

The product connects to the source with the smallest priority number first (1). If the connection to that source fails, it tries to connect to the source with the next smallest number (2) until the connection succeeds.

- c) Click **Add PM Proxy** to add the new entry to the list.

3. Configure HTTP Proxy if you need to use proxy to access the Internet.

- a) Check the **Use HTTP Proxy** check box to use an HTTP proxy server to download database updates.
- b) Enter the HTTP proxy server address in the **HTTP Proxy Address** field. Use the following format: `http://[username:password@]host[:port]`
For example: `http://user:password@example.com:8080`

4. Configure periodic updates.

- a) Define (in minutes) how often the product checks the virus definition database update sources for new updates in the **Automatic updates interval** field.
- b) Define (in minutes) the failover time to connect to specified update servers in the **Intermediate server failover time** field.


If the product cannot connect to update servers during the specified time, it retrieves the latest virus definition updates from F-Secure Update Server if **Allow fetching updates from F-Secure Update Server** is enabled.

- c) Check the **Allow fetching updates from F-Secure Update Server** check box to enable the product to download virus definition updates from F-Secure Update Server when it cannot connect to specified update servers.
 - d) Select whether a virus scan should be launched automatically after the virus definitions have been updated. The virus scan scans all local files and directories and it can take a long time. The scan uses the manual scanning settings. By default, the scan is not launched automatically.
5. Configure reminders.
- a) If the virus definition databases have not been updated in a while, the product can be set to send a reminder. To enable reminders, check the **Send reminders** check box.
The severity of the reminder is security alert.
The database age field appears.
 - b) Specify the age of the virus definition databases when they are considered old (3-30 days, the default value is 7 days). An alert is sent as a reminder when the database is older than the specified age.

F-Secure Anti-Virus Proxies

F-Secure Anti-Virus Proxy offers a solution to bandwidth problems in distributed installations of the product by significantly reducing load on networks with slow connections.


When you use F-Secure Anti-Virus Proxy as an updates source, F-Secure products can be configured to retrieve virus definition database updates from a local update repository rather than from the central F-Secure Policy Manager Server.

 **Note:** For information about how to install and configure F-Secure Anti-Virus Proxy, see chapter F-Secure Anti-Virus Proxy in F-Secure Policy Manager Administrator's Guide.

About

The About page in the Web User Interface displays the license terms, the product version number and the database version.

If you are using the evaluation version of the product, you can enter the keycode in the About page to upgrade the product to the fully licensed version.

 **Note:** If the evaluation period has expired before you upgrade to the full version, you have to restart the product after entering the keycode.

Troubleshooting

Topics:

- *Installing Required Kernel Modules Manully*
- *User Interface*
- *F-Secure Policy Manager*
- *Integrity Checking*
- *Firewall*
- *Virus Protection*
- *Generic Issues*

Installing Required Kernel Modules Manully

You may need to install required kernel modules manually if you forgot to use Software Installation Mode and the system is not working properly or in large installations when some hosts do not include development tools or kernel source.

Make sure that the running kernel version is the same as the version of the kernel sources installed. The kernel configuration must also be the same. On some distributions, such as older SUSE distributions, you may need to go to `/usr/src/linux` and run the following commands before the kernel sources match the installed kernel: `make cloneconfig` `make modules_prepare`


Follow the instructions below to install required kernel modules:

Run the following command as the root user:

```
/opt/f-secure/fsav/bin/fsav-compile-drivers
```

If the summary page in the user interface does not show any errors, the product is working correctly.

`fsav-compile-drivers` is a shell script that configures and compiles the Dazuko driver automatically for your system and for the product. For more information on the Dazuko driver, visit www.dazuko.org.

 **Note:** You can download the Dazuko driver from www.dazuko.org and use it with the product, but it is not recommended. The product has been extensively tested only with the Dazuko version that ships with the product, which is installed in `/opt/f-secure/fsav/dazuko.tar.gz`.

If your Linux distribution has a preinstalled Dazuko, it cannot be used as Dazuko depends on the included patches and configuration options, which are likely different in the preinstalled Dazuko. Uninstall the preinstalled Dazuko or make sure that it is not run during the system startup and follow the installation instructions above to install Dazuko with all required patches and configuration options.

User Interface

Troubleshooting issues with the Web User Interface.

I cannot log in to the Web User Interface. What can I do?

On some distributions, you have to comment (add a hash sign (#) at the beginning of the line) the following line in `/etc/pam.d/login`:

```
# auth requisite pam_securetty.so
```

The F-icon has a red cross over it, what does it mean?

When the F-icon in the system tray or in GNOME Panel Applet has a red cross over it, the product has encountered an error. Open the Web User Interface to see a detailed report about the issue.

To fix the problem, try to restart the product. Run the following command:

```
/etc/init.d/fsma restart
```

How can I get the F-icon visible in the system tray?

You may need to logout and login again to get the F-icon in your systray. If you are using GNOME Desktop, make sure you have a notification area in your GNOME Panel and follow these instructions:

1. Right-click on the GNOME panel.
2. Choose **Add Panel applet**.
3. Select F-Secure Panel Applet from the list of installed GNOME panel applets.

How do I enable the debug log for the web user interface?

Change `/opt/f-secure/fsav/tomcat/bin/catalina.sh` from:

```
#CATALINA_OUT="$LOGS_BASE"/catalina.out
CATALINA_OUT=/dev/null
```

to:

```
CATALINA_OUT="$LOGS_BASE"/catalina.out
#CATALINA_OUT=/dev/null
```


The logfile is in `/var/opt/f-secure/fsav/tomcat/catalina.out`.

F-Secure Policy Manager

Troubleshooting issues with F-Secure Policy Manager

How can I use F-Secure Linux Security with F-Secure Policy Manager 6.0x for Linux?

F-Secure Policy Manager Server has to be configured to retrieve new riskware and spyware databases for the product.

 **Note:** These instructions apply to F-Secure Policy Manager Server 6.0x for Linux only, the product is not compatible with other Linux or Windows F-Secure Policy Manager Server versions.

Add a line to the `/etc/opt/f-secure/fspms/fspms-fsauasc.conf` file by running the following command:

```
echo "avpe=republish" >> /etc/opt/f-secure/fspms/fspms-fsauasc.conf
```

My network stopped working after I upgraded the product, how can I fix this?

You have to upgrade the MIB file in your F-Secure Policy Manager installation, otherwise the upgraded product uses the Server firewall profile, which blocks virtually all traffic.

Integrity Checking

Troubleshooting issues with the integrity checking feature.

Symlinks are not working for Integrity Checking or Rootkit Protection, what can I do?

You may be denied to load a kernel module if the file containing the kernel module is a symlink and the real file where the symlink points to is not in the Integrity Checking baseline. The same applies if `modprobe` or `insmod` utilities (the module loaders) use files or libraries which are symlinks and the file where the symlink points to is not in the baseline.

For example, `modprobe` uses `/lib/libz.so.1`, which is really a symlink to a real file `/lib/libz.so.1.2.2`. The symlink is in the baseline but the real file is not. In this case, `modprobe` is not allowed to run as it tried to open a file that is not in the baseline.

You should never add only symlinks to the baseline, you should always add both the symlink and the real file where the symlink points.

I forgot to use Software Installation Mode and my system is not working properly. What can I do?

Create a new baseline. Execute the following commands:

```
/opt/f-secure/fsav/bin/fslistfiles | fsic --add -  
fsic --baseline
```

Can I update the Linux kernel when I use Integrity Checking?

Use the Software Installation Mode. After you have updated the kernel, disable the Software Installation Mode to restore the normal protection level.

There are too many modified files to update with the user interface.

Create a new baseline. Execute the following commands:

```
/opt/f-secure/fsav/bin/fslistfiles | fsic --add -  
fsic --baseline
```

The Integrity Checking page in the user interface does not display all entries. How can I fix this?

If you have many (over 10000) files in the baseline, you may have to adjust the memory settings of the Java Virtual Machine view all entries in the baseline.

1. Edit `/opt/f-secure/fsav/tomcat/bin/catalina.sh` file. Replace:

```
JAVA_OPTS=-Djava.library.path=/opt/f-secure/fsav/tomcat/shaj
```

with

```
JAVA_OPTS="-Djava.library.path=/opt/f-secure/fsav/tomcat/shaj  
-Xmx256M"
```

- Restart the product to take new settings into use:

```
/etc/init.d/fsma restart
```

Do I have to use the same passphrase every time I generate the baseline?

No, you have to verify the baseline using the same passphrase that was used when the baseline was generated, but you do not have to use the same passphrase again when you generate the baseline again.

Firewall

Troubleshooting issues with the firewall.

After installing the product, users cannot access samba shares on my computer, how can I fix this?

The Office firewall profile contains a rule that allows Windows Networking but that rule is disabled by default. Enable the rule to allow accesses to samba shares.

After installing the product, I cannot browse local area network domains and workgroups (SMB). How can I fix this?

You need to add a rule to the firewall that allows browsing Windows shares on your local area network. Follow these instructions:

- Go to **Firewall** ► **Network Services** page in the Web User Interface advanced mode.
- Click **Add new service**.
- Create the following service:
 - Service Name:** Windows Networking Local Browsing
 - Protocol:** UDP
 - Initiator ports:** 137-138
 - Responder:** >1023
 - Description:** SMB LAN browsing
- Click Add as a new service and **Save**.
- Go to the firewall menu and click **Firewall Rules**.

6. Click **Add new rule**.
7. Create the following rule:
 - **Type:** ACCEPT
 - **Remote Host:** [myNetwork]
 - **Description:** Windows Networking Local Browsing
 - **Service** (select box): Windows Networking Local Browsing
 - **Direction:** in
8. Click **Add Service to this Rule** and **Add to Firewall Rules**. The new rule should be visible at the bottom of the firewall rule list. If you cannot see the rule, click **>>** to move to the end of the list.
9. Click on the up arrow next to the new rule to move the rule above any "Deny rest" rule.
10. Click **Save** to save your new rule set and apply new firewall rules.

Your SMB LAN browsing should work now.

How can I set up firewall rules to access NFS servers?

You need to allow the following network traffic through the firewall:

- portmapper (tcp and udp port 111)
- nfsd (tcp and udp 2049)
- mountd (variable port from portmapper)

Mountd is needed only when the NFS share is mounted. After the mount is completed, all traffic is to the nfsd.

As the mountd port is not always the same, follow these instructions to mount NFS shares:

- Either turn off the firewall, mount (or umount) the NFS share and turn on the firewall again, or
- on the NFS server, start mountd with the `--port PORT` option, which forces mountd to use a fixed port number instead of a random port.
- Then, create a firewall rule that allows udp and tcp traffic to that port number.

Virus Protection

Troubleshooting issues with the virus protection feature.

How do I enable the debug log for real-time virus scanner?

In Policy Manager Console, go to **Product** ► **Settings** ► **Advanced** and set **fsoasd log level** to **Debug**.

In standalone installation, run the following command:

```
/opt/f-secure/fsma/bin/ctest s 44.1.100.11 9
```

The log file is in `/var/opt/f-secure/fsav/fsoasd.log`.

How can I use an HTTP proxy server to downloading database updates?

In Policy Manager Console, go to **F-Secure Automatic Update Agent** ► **Settings** ► **Communications** ► **HTTP Settings** ► **User-defined proxy settings** and set **Address** to: `http://[[user][:pass]@]proxyhost[:port]`.

In Web User Interface, use the setting in the **Automatic Updates** page in the advanced mode.

Does the real-time scan work on NFS server?

If the product is installed on NFS server, the real-time scan does not scan files automatically when a client accesses a file on the server.

How do I disable the real-time virus scan temporarily?

During some administrative tasks (for example, backup or restore) you may want to temporarily disable all virus scanning in the background.

Run the following commands to disable the virus scan and integrity checking:

```
/opt/f-secure/fsma/bin/ctest s 45.1.40.10 0
```

```
/opt/f-secure/fsma/bin/ctest s 45.1.70.10 0
```

To enable real-time scan and integrity checking again, run the following commands:

```
/opt/f-secure/fsma/bin/ctest s 45.1.40.10 1
```

```
/opt/f-secure/fsma/bin/ctest s 45.1.70.10 1
```

Does the real-time scan scan files when they are renamed or linked?

The real-time scan can scan files every time they are opened, closed or executed. It does not scan them when you rename or create or remove a link to a file.

Generic Issues

Generic troubleshooting issues with the product.

How can I clean an interrupted installation?

If the product installation is interrupted, you may have to remove the product components manually.

1. List all installed rpm packages:

```
rpm -qa | grep f-secure  
rpm -qa | grep fsav
```

2. Remove installed packages. Run the following command for each installed package:

```
rpm -e --noscripts <package_name>
```

3. Remove all of the product installation directories:

```
rm -rf /var/opt/f-secure/fsav  
rm -rf /var/opt/f-secure/fsma  
rm -rf /etc/opt/f-secure/fsav  
rm -rf /etc/opt/f-secure/fsma  
rm -rf /opt/f-secure/fsav
```

```
rm -rf /opt/f-secure/fsma
```

System is very slow. What is causing this?

The real-time virus scan and Integrity Checking can slow down the system.

1. Use basic Linux tools (top and vmstat) to check what is slowing down the system.
2. Make sure that you are using the dazuko version that is shipped with the product.
3. If a file that is accessed often is time-consuming to scan, consider adding it to the excluded list.
4. If you are using the centralized administration mode, make sure that the DNS queries return addresses quickly or use IP addresses with F-Secure Policy Manager.

The product is unable to contact the database, how can I fix this?

Sometimes, after a hard reset for example, the product may be unable to contact the database. Follow these instructions to resolve the issue:

1. As root, remove the database PID file:

```
rm /var/opt/f-secure/fsav/pgsql/data/postmaster.pid
```

2. As root, restart the product:

```
/etc/init.d/fsma restart
```

I get reports that "F-Secure Status Daemon is not running", how can I start it?

Sometimes, after a hard reset for example, F-Secure Status Daemon may fail to start. Restart the product to solve the issue:

```
/etc/init.d/fsma restart
```

Alternatively, you may start F-Secure Status Daemon manually:

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

I need to compile kernel drivers manually, how do I do that?

You may need to compile kernel drivers that the product need manually, if

- you did not have compilers and other required tools installed during the installation,
- you did not have kernel headers or sources installed during the installation, or
- you have upgraded the kernel and you need to compile drivers for the new kernel.

To compile and install drivers, run the following command:

```
/opt/f-secure/fsav/bin/fsav-compile-drivers
```


Command Line Tools

Topics:

- *fsav*
- *fsav-config*
- *dbupdate*
- *fsfwc*
- *fsic*
- *fsims*
- *fsma*
- *fssetlanguage*
- *fschooser*

For more information on command line tools and options, see man pages.

fsav

`fsav` is a program that scans files for viruses and other malicious code.

`fsav` scans specified targets (files or directories) and reports any malicious code it detects. Optionally, `fsav` disinfects, renames or deletes infected files.

Follow these instructions to scan files from the shell:


- To scan all default file types on all local disks, type: `fsav /`
- To scan all files in a directory and its subdirectories, enter the directory name. For example:
`fsav mydirectory`
- To scan a single file, enter the file name (without wildcards). For example: `fsav myfile.exe`

Recursive scan detects mounted network file system subdirectories and does not scan network file systems. Scanning a network file system from the client would create unnecessary load on the network and it is much slower than scanning the local file system.

If you want to scan the network file system, run `fsav /` on the server.

If you cannot run `fsav` on the server, you can scan the network file system from the client by explicitly specifying mounted network file system directories on the `fsav` command line.

For example, if an NFS file system is mounted in `/mnt/server1`, scan it with the following command: `fsav /mnt/server1`

 **Note:** Only regular files on mounted filesystems can be scanned. Special files, such as CD-ROM or DAT devices (`/dev/st0`, `/dev/hda` and such), cannot be scanned unless they are mounted as filesystems, or files are extracted on a filesystem from the tape first.

For more information on command line options, see the `fsav` man pages or type: `fsav --help`

fsav-config

`fsav-config` tool creates the initial product configuration.

If you install the product using RPM packages, you have to use the `fsav-config` command line tool.

1. Use the following command to create the initial product configuration:

```
/opt/f-secure/fsav/fsav-config
```

The script will display some questions. The default value is shown in brackets after the question. Press `ENTER` to select the default value.

2. Select the language you want to use in the Web User Interface.

```
Select language to use in Web User Interface
[1] English (default)
[2] Japanese
[3] German
```

3. Enter the keycode to set up the full, licensed version of the product. Enter the keycode in the format you received it, including the hyphens that separate sequences of letters and digits. If you want to evaluate the product and do not have a keycode, press `ENTER`.
4. Select between the stand-alone and centrally managed installation.
 - a) In the centrally managed installation, enter the address of the F-Secure Policy Manager Server.

```
Address of F-Secure Policy Manager Server:
[http://localhost/]:
```

- b) In the centrally managed installation, enter the location of the `admin.pub` key. This is the key that you created during F-Secure Policy Manager Console Installation.
5. Select whether you want to allow remote accesses to the Web User Interface.


```
Allow remote access to the web user interface? [no]
```

6. Select whether the Web User Interface can be opened from the localhost without a login.

```
Allow connections from localhost to the web user interface
without login? [yes]
```

7. Enter the user name who is allowed to use the Web User Interface.

```
Please enter the user name who is allowed to use the web user
interface.
```

-  **Note:** The user name is a local Linux account. You have to create the account if it does not exist yet. Do not use the root account for this purpose.

8. Select whether you want add currently installed kernel modules to the Integrity Checker known files list and generate the baseline.

```
Would you like to enable Linux kernel module verification
[yes]?
```

9. Enter the baseline passphrase.

```
Please insert passphrase for HMAC creation (max 80
characters)
```

dbupdate

`dbupdate` is a shell script for updating F-Secure Anti-Virus virus definition databases.

Before you can update virus definition databases manually, you have to disable the periodic database update.

Follow these instructions to update virus definition databases manually from the command line:

1. Download the `fsdbupdate.run` file from:
<http://download.f-secure.com/latest/fsdbupdate.run>
`fsdbupdate.run` is a self-extracting file that stops the automatic update agent daemon, updates databases and restarts the automatic update agent.
2. Run the following command as root user: `dbupdate fsdbupdate.run`
 where `fsdbupdate.run` is the absolute or relative path to the `fsdbupdate.run` file.

For more information on command line options, see the `dbupdate` man pages or type: `dbupdate --help`

fsfwc

`fsfwc` is a command line tool for setting firewall security levels.

Use the following command to change the current security profile:

```
/opt/f-secure/fsav/bin/fsfwc --mode {block, mobile, home, office,
strict, normal, bypass}
```

fsic

You can create the baseline, add files to the baseline and verify the baseline with the `fsic` command line tool.

1. To create the baseline, follow these instructions:
 - a) Run the `fsic` tool with the `--baseline` option: `fsic --baseline`
 - b) Enter a passphrase to create the signature.
A new baseline has been created.
2. To add files to the baseline, follow these instructions:
 - a) Run the `fsic` tool with the `--add`, `--alert` and `--protect` options:

```
/opt/f-secure/fsav/bin/fsic --add --alert=yes --protect=yes
/etc/passwd /etc/shadow
```
 - b) Recalculate the baseline. The baseline update progress is displayed during the process, and you are prompted to select whether to include the new files in the baseline:

```
/opt/f-secure/fsav/bin/fsic --baseline
```
 - c) Enter a passphrase to create the signature.
In this example, the product is also configured to send an alert about unauthorized modification attempts of the protected files.
3. To verify the baseline:
 - a) Run the command: `/opt/f-secure/fsav/bin/fsic`
 - b) Enter the passphrase that you used when you created the baseline.
The product validates files and displays whether the files are intact.

fsims

You can use `fsims` command to use the Software Installation Mode from the shell.

Follow these instructions to install new software:

1. Use the following command to enable Software Installation Mode:

```
/opt/f-secure/fsav/bin/fsims on
```
2. Install the new software.
3. Disable the Software Installation Mode to restore the normal protection level:

```
/opt/f-secure/fsav/bin/fsims off
```

fsma

You can use `fsma` command to check the status of the product modules.

Run the following command: `/etc/init.d/fsma status`

Module	Process	Description
F-Secure Alert Database Handler Daemon	<code>/opt/f-secure/fsav/sbin/fsadhhd</code>	Stores alerts to a local database. Alerts can be viewed with the web user interface.
F-Secure FSAV Policy Manager Daemon	<code>/opt/f-secure/fsav/bin/fsavpmd</code>	Handles all F-Secure Policy Manager Console operations (for example, Scan all hard disks now, Update database now, Reset statistics)
F-Secure Firewall Daemon	<code>/opt/f-secure/fsav/bin/fsfwd.run</code>	The interface between F-Secure Management Agent and the iptables/netfilter firewall.
F-Secure FSAV License Alerter	<code>/opt/f-secure/fsav/libexec/fslmalerter</code>	Checks and informs how many days are left in the evaluation period when the product is installed in the evaluation mode.
F-Secure FSAV On-Access Scanner Daemon	<code>/opt/f-secure/fsav/sbin/fsoasd</code>	Provides all real-time protection features: real-time virus scanning, real-time integrity checking and rootkit protection.
F-Secure FSAV Status Daemon	<code>/opt/f-secure/fsav/bin/fstatusd</code>	Checks the current status of every component keeps desktop panel applications and web user interface up-to-date.

Module	Process	Description
F-Secure FSAV Web UI	<code>/opt/f-secure/fsav/tomcat/bin/catalina.sh start</code>	Handles the web user interface.
F-Secure FSAV PostgreSQL daemon	<code>/opt/f-secure/common/postgresql/bin/startup.sh</code>	Stores alerts that can be viewed with the web user interface.

fssetlanguage

You can use the `fssetlanguage` tool to change the Web User Interface language.

Use the following command to set the language:

```
/opt/f-secure/fsav/bin/fssetlanguage <language>
```

Where language is:


- en - english
- ja - japanese
- de - german

fschooser

With `fschooser`, you can turn certain product features on or off.

You can turn off some product components that you do not need or if you do not have enough system resources to run them.

1. Run the following command: `/opt/f-secure/fsav/sbin/fschooser`.
The screen lists security components of the product.
2. Follow the on-screen instructions to turn components on or off.
Firewall - ENABLED, press f+RET to toggle
Web User Interface - ENABLED, press w+RET to toggle
3. Press RETURN to accept your selection.

 **Note:** Press `ctrl+C` to cancel your changes.

Before You Install

Topics:

- [64-bit Distributions](#)
- [Distributions Using Prelink](#)
- [Red Hat Enterprise Linux 3 and 4](#)
- [Debian 3.1 and 4.0](#)
- [SuSE](#)
- [Turbolinux 10 and 11](#)
- [Ubuntu 5.04, 5.10, 6.06, 7.04 and 7.10](#)



Note: Some distributions run `prelink` periodically from `cron` to make linked libraries run faster. Run this manually if it is not run automatically before you activate the Integrity Checker.

64-bit Distributions

Some 64-bit distributions do not install 32-bit compatibility libraries by default. Make sure that these libraries are installed.

The name of the compatibility library package may vary, see the documentation of the distribution you use for the package name for 32-bit compatibility libraries.

On 64-bit Ubuntu, install `ia32-libs`.

Distributions Using Prelink

Prelinking can reduce the startup time of binaries, but it conflicts with the Integrity Checker in the product.

You should disable automatic prelink runs from cron. On Asianux, edit `/etc/sysconfig/prelink` and change the line: `PRELINKING=yes` to `PRELINKING=no` and run `/etc/cron.daily/prelink` before you install the product.

Some distributions, like Asianux, run `prelink` periodically from `cron` to reduce the startup time of binaries which use dynamic libraries. Prelinking modifies binaries and dynamic libraries on the disk, which conflicts with the purpose of the Integrity Checker, which detects modifications to system files.


If you have already installed F-Secure Linux Security, follow these instructions:

1. Run `/opt/f-secure/fsav/bin/fsims on` from the command line to turn on the software installation mode.
In the software installation mode, the product allows modifications to system files.
2. Edit `/etc/sysconfig/prelink` and change the line: `PRELINKING=yes` to `PRELINKING=no`.
3. Run `/etc/cron.daily/prelink`.
4. Running `/opt/f-secure/fsav/bin/fsims off` from the command line to turn off the software installation mode.

When the software installation mode is turned off, the state of system files is stored in the Integrity Checker baseline.

To use prelinking, you have to turn on the software installation mode before prelinking and turn it off when prelinking is finished. This allows the prelink to make the changes in system files in a controlled way. For example:

```
# /opt/f-secure/fsav/bin/fsims on
# prelink -a
# /opt/f-secure/fsav/bin/fsims off
```

 **Note:** This operation cannot be automated easily - Turning off the software installation mode creates a new baseline, which needs to be signed with a passphrase that the administrator has to enter.

Red Hat Enterprise Linux 3 and 4

Follow these instructions to install the product on a server running Red Hat Enterprise Linux 3 or 4 AS.

1. Install the following RPM packages from Red Hat Enterprise Linux CDs. (The packages for RHEL 3 can be found on RHEL 3 disc 3.)
 - Use the command: `rpm -ivh <rpm files>`
 - Use [Applications](#) ► [System Settings](#) ► [Add/Remove Applications](#)
 - Use `up2date`

a) Make sure you have all the following RPM packages installed:

 - `gcc`
 - `glibc-devel`
 - `glibc-headers`
 - `glibc-kernheaders`

b) Make sure you have at least one of the following RPM packages installed (Use the `uname -r` command to see the current kernel version information):

RHEL 3:

 - `kernel-source`

RHEL 4:

 - `kernel-devel`
 - `kernel-hugemem-devel`

- `kernel-smp-devel`
- c) The system tray applet requires the following RPM packages:
- `kdelibs`
 - `compat-libstdc++`
2. Install the product normally.

Debian 3.1 and 4.0

Follow these instructions to install the product on a computer running either Debian 3.1 or 4.0.

1. Install a compiler, kernel headers and RPM before you install the product.
 - a) `sudo apt-get install gcc rpm make libc6-dev`
 - b) Debian 3.1: `sudo apt-get install kernel-headers-`uname -r | cut -d- -f 1-``
 - c) Debian 4.0: `sudo apt-get install linux-headers-`uname -r``
2. If you want to use the system tray applet, run the following command: `sudo apt-get install kde-core`
3. Install the product normally.

SuSE

Follow these instructions to install the product on a computer running SuSE version 9.1, 9.2, 9.3, 10.0 or 10.1.

1. Before you install the product, make sure that `kernel-source`, `make` and `gcc` packages are installed. Use YaST or another setup tool.
2. Install the product normally.

Turbolinux 10 and 11

Turbolinux kernel sources may not be configured and so they cannot be used to compile kernel drivers.

Turbolinux kernel sources may not be configured and so they cannot be used to compile kernel drivers. To fix this, follow these instructions:

- Turbolinux 10:

run the following command in the kernel source tree: `make oldconfig`

- Turbolinux 11:

Run these commands in the command line:

```
cd /usr/src/linux-2. major.minor
./SetupKernelSource.sh architecture
```

where *major.minor* is the kernel version number and *architecture* is either *i686*, *i686smp64G* or *x86_64*.

Ubuntu 5.04, 5.10, 6.06, 7.04 and 7.10

Follow these instructions to install the product on a computer running Ubuntu 6.06 or 7.10.

1. Install a compiler, kernel headers and RPM before you install the product.

- Ubuntu 6.06:

1. `sudo apt-get install gcc rpm make libc6-dev`

2. `sudo apt-get install linux-headers-`uname -r``

3. If you are using Ubuntu 5.10, make sure that `gcc-3.4` package is installed.

4. If you want to use the system tray applet, run the following command: `sudo apt-get install kdelibs libstdc++5`

- Ubuntu 7.10: `sudo apt-get install rpm libc6-dev patch`

2. If you want to enable logins to the Web User Interface, comment (add a hash sign (#) at the beginning of the line) the following line in `/etc/pam.d/login`:

```
auth requisite pam_securetty.so
```

3. Install the product normally.

List of Traps

Integrity Checking

The list of FSIC traps:

Trap Number	Severity	Description
710	Security alert	Integrity checking baseline generated at host
711	Security alert	Integrity checking baseline verification failed. Baseline has been compromised or the passphrase used to verify the baseline is incorrect
730	Security alert	File failed integrity check
799	Error	Could not save the baseline entries to policy

Policy Manager

The list of FSAVPMD traps. All other alerts that are possibly sent from perl script are sent with ERROR level.

Trap Number	Severity	Description
50	Informational	Scan started
51	Informational	Scan finished

Trap Number	Severity	Description
60	Informational	Database update started
61	Informational	Database update finished
100	Security alert	On-Access Virus Alert
150	Informational	Process started
151	Informational	Process stopped
152	Fatal error	Process crashed
153	Fatal error	Process failed to start
158	Informational	F-Secure Anti-Virus Linux Security started
159	Informational	F-Secure Anti-Virus Linux Security stopped
170	Security alert	Evaluation period expired
171	Informational	Evaluation version
200	Security alert	Virus Alert
201	Security alert	Virus Alert: Disinfected
202	Security alert	Virus Alert: File deleted
203	Security alert	Virus Alert: File renamed
204	Security alert	Virus Alert: Not disinfected
205	Security alert	Virus Alert: Action failed
206	Security alert	Virus Alert: Custom action executed
207	Security alert	Virus Alert: Scan aborted
322	Informational	Database update files received successfully
500	Informational	Virus definition database integrity verified successfully
999	Informational	Debug output

Virus Definition Database Verification

The list of DAAS traps.

Trap Number	Severity	Description
506	Warning	Extra files were detected in the database update package
512	Warning	The package has been modified
513	Warning	Bad or missing manifest file
514	Warning	Bad or missing manifest file certificate
515	Warning	The virus definition database update is older than the previously accepted one
516	Warning	The manifest file does not have a matching certificate
518	Warning	Bad or missing F-Secure Corporation certificate
519	Warning	Bad or missing certificate from virus definition database publisher
520	Warning	No certificate from the publisher matches the manifest file certificate
521	Warning	The certificate in the package has not been issued by F-Secure Corporation
522	Warning	The publisher's certificate was not valid when the database update was published
523	Warning	The publisher's certificate in the package does not express the right to publish database updates
530	Warning	The publisher's certificate in the package had been revoked when the database update was published

Trap Number	Severity	Description
531	Warning	The publisher's certificate in the package has been revoked with high severity
535	Warning	Bad or missing revocation file
550	Warning	There was not enough memory to complete the operation
551	Warning	A file I/O error occurred during the operation
552	Warning	Unsupported database type

DBTool

The list of DBTool traps.

Trap Number	Severity	Description
4	Error	File was not found
308	Error	Cannot open file
309	Error	File is encrypted
310	Error	Scanning of a file could not be completed at this time
311	Error	Cannot write to file
323	Error	Virus definition database file is invalid
324	Error	Virus definition database file is invalid. The integrity check failed for the database file.

Firewall

The list of firewall daemon traps.

Trap Number	Severity	Description
153	Fatal error	Process failed to start
801	Informational	Firewall enabled
802	Error	Firewall disabled
803	Error	Could not set firewall rules
804	Informational	Firewall rules updated

Anti-virus

The list of on-access scanner traps

Trap Number	Severity	Description
150	Informational	Process started
153	Fatal error	Process failed to start
200	Security alert	Virus Alert
201	Security alert	Virus Alert: Disinfected
202	Security alert	Virus Alert: File deleted
203	Security alert	Virus Alert: File renamed
205	Security alert	Virus Alert: Action failed
220	Security alert	Riskware Alert
221	Security alert	Riskware Alert: Disinfected
222	Security alert	Riskware Alert: File deleted
223	Security alert	Riskware Alert: File renamed
225	Security alert	Riskware Alert: Action failed
301	Error	Scanning Error
309	Error	File Encrypted
318	Error	Scanning Aborted
600	Security alert	Real-time protection fatal error

Trap Number	Severity	Description
700	Security alert	Integrity checking fatal error
720	Security alert	Integrity checking hash calculation failed
721	Security alert	Integrity checking file attribute check failed
730	Security alert	Integrity checked file compromised
731	Security alert	Integrity checker prevented a modification attempt to a protected file
733	Security alert	Kernel module loader tried to open unbaselined file
734	Security alert	Kernel module loader tried to open compromised file
735	Security alert	Unknown kernel module loader detected
736	Security alert	Kernel protected from modification
741	Security alert	Kernel modified

Appendix D

Get More Help

The `fsdiag` report, which is generated by the F-Secure Diagnostics Tool, contains vital information from your system. The information is needed by our support engineers so that they can solve your problem. After you run `fsdiag`, the `fsdiag.tar.gz` report file is created on the current directory.

The report contains information about F-Secure products, as well as operating system logs and system settings. The collected data is essential for problem solving and troubleshooting. In some cases this information might be considered confidential. Please note that the data collected will only be stored locally.

Go to <http://support.f-secure.com> to see more troubleshooting information and for instructions on how to contact our technical support team.

