

F-Secure Policy Manager

Administrator's Guide

Contents

Chapter 1: Introduction.....	7
1.1 System requirements.....	8
1.1.1 Policy Manager Server.....	8
1.1.2 Policy Manager Console.....	8
1.2 Main components.....	9
1.3 Features.....	10
1.4 Product registration.....	10
1.4.1 Upstream reporting.....	11
1.5 Basic terminology.....	11
1.6 Policy-based management.....	12
1.6.1 Management Information Base.....	12
 Chapter 2: Installing the product.....	 14
2.1 Installation steps.....	15
2.1.1 Download and run the installation package.....	15
2.1.2 Select components to install.....	15
2.1.3 Complete the migration wizard.....	16
2.1.4 Complete installation of the product.....	16
2.1.5 Run Policy Manager Console.....	16
2.2 Changing the web browser path.....	17
2.3 Uninstalling the product.....	17
 Chapter 3: Using Policy Manager Console.....	 18
3.1 Overview.....	19
3.2 Basic information and tasks.....	19
3.2.1 Logging in.....	19
3.2.2 Client Security management.....	20
3.2.3 Advanced mode user interface.....	21
3.2.4 Policy domain tree.....	21
3.2.5 Contents of the Advanced mode user interface.....	21
3.2.6 Messages pane.....	21
3.3 Managing domains and hosts.....	22
3.3.1 Adding policy domains.....	22
3.3.2 Adding hosts.....	22
3.4 Software distribution.....	25
3.4.1 Push installations.....	25
3.4.2 Policy-based installation.....	28
3.4.3 Local installation and updates with pre-configured packages.....	29
3.4.4 Local installation and Policy Manager.....	30
3.5 Managing policies.....	32

3.5.1 Settings.....	32
3.5.2 Discarding undistributed changes to settings.....	32
3.5.3 Restrictions.....	32
3.5.4 Configuring settings.....	32
3.5.5 Policy inheritance.....	33
3.6 Managing operations and tasks.....	33
3.7 Alerts.....	34
3.7.1 Viewing alerts and reports.....	34
3.7.2 Configuring alert forwarding.....	34
3.7.3 Forwarding alerts to syslog server.....	35
3.8 Reporting tool.....	35
3.8.1 Viewing and exporting a report.....	35
Chapter 4: Maintaining Policy Manager Server.....	37
4.1 Backing up & restoring Policy Manager data.....	38
4.2 Creating the backup.....	38
4.3 Restoring the backup.....	38
4.4 Exporting and importing signing keys.....	38
4.5 Replicating software using image files.....	39
Chapter 5: Updating virus definition databases.....	40
5.1 Automatic updates with Automatic Update Agent.....	41
5.1.1 How Automatic Update Agent works.....	41
5.1.2 The benefits of using Automatic Update Agent.....	41
5.2 Using Automatic Update Agent.....	42
5.2.1 Configuring Automatic Update Agent.....	42
5.2.2 How to read the log file.....	42
5.3 Forcing Automatic Update Agent to check for new updates immediately.....	44
5.4 Updating the databases manually.....	44
5.5 Troubleshooting.....	44
Chapter 6: Using the product on Linux.....	45
6.1 Overview.....	46
6.2 Installation.....	46
6.2.1 Install Automatic Update Agent and Policy Manager Server.....	47
6.2.2 Install Policy Manager Console.....	48
6.3 Uninstalling the product.....	49
6.4 Frequently asked questions.....	49
Chapter 7: Web Reporting.....	53
7.1 Generating and viewing reports.....	54
7.1.1 Generating a report.....	54
7.1.2 Scheduling reports.....	54
7.1.3 Creating a printable report.....	55
7.1.4 Automated report generation.....	55

7.2 Maintaining Web Reporting.....	55
7.3 Web Reporting error messages and troubleshooting.....	55
7.3.1 Error messages.....	55
7.3.2 Troubleshooting.....	56
7.3.3 Changing the Web Reporting port.....	56
Chapter 8: Policy Manager Proxy.....	57
8.1 Overview.....	58
Chapter 9: Anti-virus mode user interface.....	59
9.1 Settings inheritance.....	60
9.1.1 How settings inheritance is displayed on the user interface.....	60
9.1.2 Locking and unlocking all settings on a page at once.....	61
9.1.3 Settings inheritance in tables.....	61
Chapter 10: Configuring virus and spyware protection.....	62
10.1 Configuring automatic updates.....	63
10.1.1 Configuring automatic updates from Policy Manager Server.....	63
10.1.2 Configuring Policy Manager Proxy.....	63
10.1.3 Configuring clients to download updates from each other.....	64
10.2 Configuring real-time scanning.....	64
10.2.1 Enabling real-time scanning for the whole domain.....	64
10.2.2 Forcing all hosts to use real-time scanning.....	64
10.2.3 Excluding Microsoft Outlook's .pst file from real-time scanning.....	65
10.3 Configuring DeepGuard.....	65
10.3.1 DeepGuard settings.....	65
10.3.2 DeepGuard server queries.....	66
10.4 Configuring rootkit scanning.....	66
10.4.1 Launching a rootkit scan for the whole domain.....	66
10.5 Configuring e-mail scanning.....	67
10.5.1 Enabling e-mail scanning for incoming and outgoing e-mails.....	67
10.6 Configuring web traffic (HTTP) scanning.....	67
10.6.1 Enabling web traffic scanning for the whole domain.....	67
10.6.2 Excluding a web site from HTTP scanning.....	68
10.7 Configuring spyware scanning.....	68
10.7.1 Setting up spyware control for the whole domain.....	69
10.7.2 Launching spyware scanning in the whole domain.....	69
10.7.3 Allowing the use of a spyware or riskware component.....	70
10.8 Managing quarantined objects.....	70
10.8.1 Deleting quarantined objects.....	70
10.8.2 Releasing quarantined objects.....	70
10.9 Preventing users from changing settings.....	71
10.9.1 Setting all virus protection settings as final.....	71
10.10 Configuring alert sending.....	72
10.10.1 Setting Client Security to send virus alerts to an e-mail address.....	72
10.10.2 Disabling Client Security alert pop-ups.....	72

10.11 Monitoring viruses on the network.....	72
10.12 Testing your antivirus protection.....	73

Chapter 11: Configuring Internet Shield.....74

11.1 Configuring security levels and rules.....	75
11.1.1 Selecting an active security level for a workstation.....	75
11.1.2 Configuring a default security level for the managed hosts.....	75
11.1.3 Adding a new security level for a certain domain only.....	75
11.2 Configuring network quarantine.....	77
11.2.1 Turning network quarantine on in the whole domain.....	77
11.2.2 Fine-tuning network quarantine.....	77
11.3 Configuring rule alerts.....	77
11.3.1 Adding a new rule with alerting.....	78
11.4 Configuring application control.....	80
11.4.1 Setting up application control for the first time.....	80
11.4.2 Creating a rule for an unknown application on root level.....	81
11.4.3 Editing an existing application control rule.....	82
11.4.4 Turning off application control pop-ups.....	82
11.5 Using alerts to check that Internet Shield works.....	83
11.6 Configuring intrusion prevention.....	83
11.6.1 Configuring IPS for desktops and laptops.....	83

Chapter 12: Using Device Control.....85

12.1 Configuring Device Control.....	86
12.2 Blocking hardware devices.....	86
12.3 Granting access to specific devices.....	87
12.3.1 Finding hardware ID for a device.....	87

Chapter 13: Managing software updates.....88

13.1 Installing software updates automatically.....	89
13.2 Excluding software updates from automatic installation.....	89
13.3 Checking the status of software updates in your network.....	89
13.3.1 Installing missing software updates.....	89

Chapter 14: How to check that the network environment is protected.....91

14.1 Checking that all the hosts have the latest policy.....	92
14.2 Checking that the server has the latest virus definitions.....	92
14.3 Checking that the hosts have the latest virus definitions.....	92
14.4 Checking that there are no disconnected hosts.....	92
14.5 Viewing scanning reports.....	93
14.6 Viewing alerts.....	93
14.7 Creating a weekly infection report.....	94
14.8 Monitoring a possible network attack.....	94

Chapter 15: Upgrading managed software.....	95
15.1 Using policy-based installation.....	96
Chapter 16: Virus information.....	97
16.1 Malware information and tools on the F-Secure web pages.....	98
16.2 How to send a virus sample to F-Secure.....	98
16.2.1 How to package a virus sample.....	98
16.2.2 What should be sent.....	98
16.2.3 How to send the virus sample.....	99
16.3 What to do in case of a virus outbreak?.....	100
Chapter 17: Advanced features: virus and spyware protection....	102
17.1 Configuring scheduled scanning.....	103
17.2 Advanced DeepGuard settings.....	104
17.2.1 Letting an administrator allow or deny program events from other users.....	104
17.2.2 Allowing or denying events requested by a specific application automatically.....	104
17.3 Configuring Policy Manager Proxy.....	104
17.4 Excluding an application from the web traffic scanner.....	105
Chapter 18: Advanced features: Internet Shield.....	106
18.1 Managing Internet Shield properties remotely.....	107
18.1.1 Using packet logging.....	107
18.1.2 Using the trusted interface.....	107
18.1.3 Using packet filtering.....	107
18.2 Configuring security level autoselection.....	108
18.3 Troubleshooting connection problems.....	109
18.4 Adding new services.....	109
18.4.1 Creating a new Internet service based on the default HTTP.....	109
Chapter 19: Troubleshooting.....	112
19.1 Policy Manager Server and Policy Manager Console.....	113
19.2 Policy Manager Web Reporting.....	116
19.3 Policy distribution.....	116

Introduction

Topics:

- [*System requirements*](#)
- [*Main components*](#)
- [*Features*](#)
- [*Product registration*](#)
- [*Basic terminology*](#)
- [*Policy-based management*](#)

Policy Manager provides a scalable way to manage the security of numerous applications on multiple operating systems from one central location.

Policy Manager can be used for:

- defining and distributing security policies,
- installing application software to local and remote systems,
- monitoring the activities of all systems in the enterprise to ensure compliance with corporate policies and centralized control.

When the system has been set up, you can see status information from the entire managed domain in one single location. In this way it is very easy to make sure that the entire domain is protected, and to modify the protection settings when necessary. You can also restrict the users from making changes to the security settings, and be sure that the protection is always up-to-date.

1.1 System requirements

This section provides the system requirements for both Policy Manager Server and Policy Manager Console.

1.1.1 Policy Manager Server

In order to install Policy Manager Server, your system must meet the minimum requirements given here.

Operating system:	Microsoft Windows: <ul style="list-style-type: none"> • Microsoft Windows Server 2003 SP1 or higher (32-bit); Standard, Enterprise, Web Edition or Small Business Server editions • Windows Server 2003 SP1 or higher (64-bit); Standard or Enterprise editions • Windows Server 2008 SP1 (32-bit); Standard, Enterprise or Web Server editions • Windows Server 2008 SP1 (64-bit); Standard, Enterprise, Web Server, Small Business Server or Essential Business Server editions • Windows Server 2008 R2 with or without SP1; Standard, Enterprise or Web Server editions • Windows Server 2012; Essentials, Standard or Datacenter editions • Windows Server 2012 R2; Essentials, Standard or Datacenter editions
Processor:	P4 2Ghz or multi-core 3GHz CPU, depending on the operating system and the size of the managed environment.
Memory:	1 - 2 GB RAM, depending on the operating system and the size of the managed environment.
Disk space:	6 - 10 GB of free disk space, depending on the size of the managed environment.
Network:	100 Mbit network.
Browser:	<ul style="list-style-type: none"> • Firefox 3.6 or newer • Internet Explorer 7 or newer

1.1.2 Policy Manager Console

In order to install Policy Manager Console, your system must meet the minimum requirements given here.

Operating system:	Microsoft Windows: <ul style="list-style-type: none"> • Windows XP Professional (SP3) • Windows Vista (32-bit or 64-bit) with or without SP1; Business, Enterprise or Ultimate editions
-------------------	---

	<ul style="list-style-type: none"> • Windows 7 (32-bit or 64-bit) with or without SP1; Professional, Enterprise or Ultimate editions • Windows 8 (32-bit or 64-bit), any edition • Windows 8.1 (32-bit or 64-bit), any edition • Microsoft Windows Server 2003 SP1 or higher (32-bit); Standard, Enterprise, Web Edition or Small Business Server editions • Windows Server 2003 SP1 or higher (64-bit); Standard or Enterprise editions • Windows Server 2008 SP1 (32-bit); Standard, Enterprise or Web Server editions • Windows Server 2008 SP1 (64-bit); Standard, Enterprise, Web Server, Small Business Server or Essential Business Server editions • Windows Server 2008 R2 with or without SP1; Standard, Enterprise or Web Server editions • Windows Server 2012; Essentials, Standard or Datacenter editions • Windows Server 2012 R2; Essentials, Standard or Datacenter editions
Processor:	P4 2 GHz processor.
Memory:	512 MB - 1 GB of RAM, depending on the operating system and the size of the managed environment.
Disk space:	200 MB of free disk space.
Display:	Minimum 16-bit display with resolution of 1024x768 (32-bit color display with 1280x1024 or higher resolution recommended).
Network:	100 Mbit network.

1.2 Main components

The power of Policy Manager lies in the F-Secure management architecture, which provides high scalability for a distributed, mobile workforce.

Policy Manager Console Policy Manager Console provides a centralized management console for the security of the managed hosts in the network. It enables the administrator to organize the network into logical units for sharing policies. These policies are defined in Policy Manager Console and then distributed to the workstations through Policy Manager Server. Policy Manager Console is a *Java*-based application that can be run on several different platforms. It can be used to remotely install the Management Agent on other workstations without the need for local login scripts, restarting, or any intervention by the end user.

Policy Manager Console includes two different user interfaces:

- **Anti-virus mode** user interface that is optimized for managing Client Security and Anti-virus for Workstations.
- **Advanced mode** user interface that can be used for managing other F-Secure products.

Policy Manager Server	Policy Manager Server is the repository for policies and software packages distributed by the administrator, as well as status information and alerts sent by the managed hosts. Communication between Policy Manager Server and the managed hosts is accomplished through the standard <i>HTTP protocol</i> , which ensures trouble-free performance on both <i>LAN</i> and <i>WAN</i> .
Management Agent	Management Agent enforces the security policies set by the administrator on the managed hosts, and provides the end user with a user interface and other services. It handles all management functions on the local workstations and provides a common interface for all F-Secure applications, and operates within the policy-based management infrastructure.
Web Reporting	Web Reporting is an enterprise-wide, web-based graphical reporting system included in Policy Manager Server. With Web Reporting you can quickly create graphical reports based on historical trend data, and identify computers that are unprotected or vulnerable to virus outbreaks.
Update Server & Agent	Update Server & Agent are used for updating virus and spyware definitions on the managed hosts, and are included in Policy Manager Server. The Automatic Update Agent allows users to receive virus definition database updates and data content without interrupting their work to wait for files to download from the web. It downloads files automatically in the background using bandwidth not being used by other Internet applications. If Automatic Update Agent is always connected to the Internet, it will automatically receive new virus definition updates within about two hours after they have been published by F-Secure.

1.3 Features

Some of the main features of Policy Manager are described here.

Software distribution	<ul style="list-style-type: none"> • Installation of F-Secure products on hosts from one central location, and updating of executable files and data files, including virus definitions updates. • Updates can be provided in several ways: <ul style="list-style-type: none"> • From an F-Secure CD. • From the F-Secure web site to the customer. These can be automatically 'pushed' by Automatic Update Agent, or voluntarily 'pulled' from the F-Secure web site. • Policy Manager Console can be used to export pre-configured installation packages, which can also be delivered using third-party software, such as SMS and similar tools.
Configuration and policy management	<ul style="list-style-type: none"> • Centralized configuration of security policies. The policies are distributed from Policy Manager Server by the administrator to the user's workstation. Integrity of the policies is ensured through the use of digital signatures.
Event management	<ul style="list-style-type: none"> • Reporting to the Event Viewer (local and remote logs), e-mail, and report files and creation of event statistics.
Performance management	<ul style="list-style-type: none"> • Statistics and performance data handling and reporting.
Task management	<ul style="list-style-type: none"> • Management of virus scanning tasks and other operations.

1.4 Product registration

To use Policy Manager for other than evaluation purposes, you need to register your product.

To register your product, enter the customer number from your license certificate when you start up Policy Manager Console.

If you do not register your product, you can only use Policy Manager for a 30-day evaluation period.

The following questions and answers provide some more information about registering your installation of Policy Manager. You should also view the F-Secure license terms (http://www.f-secure.com/en_EMEA/estore/license-terms/) and privacy policy (http://www.f-secure.com/en_EMEA/privacy.html).

Where can I find my customer number for registering my product?

The customer number is printed on the license certificate that you get when buying F-Secure products.

Where can I get my customer number if I lose it?

Contact the F-Secure partner from whom you bought your F-Secure product.

What if I have several Policy Manager installations?

The number of installations is not limited; you can use the same customer number to register all of them.

What should I do if registration fails, saying that my customer number could not be validated?

Check your network configuration to make sure that Policy Manager Server is able to access the F-Secure registration server (<https://corp-reg.f-secure.com:443>).

What should I do if registration fails, saying that my customer number is invalid?

Check your license certificate to make sure that you entered the correct customer number. Otherwise, please contact your F-Secure partner to check your license agreement.

Who should I contact for help?

If registration issues persist, please contact your F-Secure partner or F-Secure support directly.

1.4.1 Upstream reporting

We collect data from registered products to help support and improve our products.

Why does F-Secure collect data?

We collect statistical information regarding the use of registered F-Secure products. This helps us improve our products, while also providing better service and support.

What information is sent?

We collect information that cannot be linked to the end user or the use of the computer. The collected information includes F-Secure product versions, operating system versions, the number of managed hosts and the number of disconnected hosts. The information is transferred in a secure and encrypted format.

Where is the information stored and who can access it?

The data is stored in F-Secure's highly secured data center, and only F-Secure's assigned representatives can access the data.

1.5 Basic terminology

Here you will find descriptions for some of the commonly used terms in this guide.

Host

Host refers to a computer that is centrally managed with Policy Manager.

Policy

A security policy is a set of well-defined rules that regulate how sensitive information and other resources are managed, protected, and distributed. The management architecture of F-Secure software uses policies that are centrally configured by the administrator for optimum control of security in a corporate environment.

The information flow between Policy Manager Console and the hosts is accomplished by transferring policy files.

Policy domain Policy domains are groups of hosts or subdomains that have a similar security policy.

Policy inheritance Policy inheritance simplifies the defining of a common policy. In Policy Manager Console, each policy domain automatically inherits the settings of its parent domain, allowing for easy and efficient management of large networks. The inherited settings may be overridden for individual hosts or domains. When a domain's inherited settings are changed, the changes are inherited by all of the domain's hosts and subdomains.

The policy can be further refined for subdomains or even individual hosts. The granularity of policy definitions can vary considerably among installations. Some administrators might want to define only a few different policies for large domains. Other administrators might attach policies directly to each host, achieving the finest granularity.

1.6 Policy-based management

A security policy is a set of well-defined rules that regulate how sensitive information and other resources are managed, protected, and distributed.

The management architecture of F-Secure software uses policies that are centrally configured by the administrator for optimum control of security in a corporate environment. Policy-based management implements many functions:

- Remotely controlling and monitoring the behavior of the products.
- Monitoring statistics provided by the products and the Management Agent.
- Remotely starting predefined operations.
- Transmission of alerts and notifications from the products to the system administrator.

The information flow between Policy Manager Console and the hosts is accomplished by transferring policy files. There are three kinds of policy files:

- *Default policy files* (.dpf)
- *Base policy files* (.bpf)
- *Incremental policy files* (.ipf)

The current settings of a product consist of all three policy file types:

Default policy files The default policy file contains the default values (the factory settings) for a single product that are installed by the setup. Default policies are used only on the host. If neither the base policy file nor the incremental policy file contains an entry for a variable, then the value is taken from the default policy file. New product versions get new versions of the default policy file.

Base policy files Base policy files contain the administrative settings and restrictions for all the variables for all F-Secure products on a specific host (with domain level policies, a group of hosts may share the same file). A base policy file is signed by Policy Manager Console, protecting the file against changes while it is passing through the network and while it is stored in the host's file system. These files are sent from Policy Manager Console to Policy Manager Server. The host periodically polls for new policies created by Policy Manager Console.

Incremental policy files Incremental policy files are used to store local changes to the base policy. Only changes that fall within the limits specified in the base policy are allowed. The incremental policy files are then periodically sent to Policy Manager Console so that current settings and statistics can be viewed by the administrator.






1.6.1 Management Information Base

The *Management Information Base (MIB)* is a hierarchical management data structure used in the *Simple Network Management Protocol (SNMP)*.

In Policy Manager, the MIB structure is used for defining the contents of the policy files. Each variable has an *Object Identifier (OID)* and a value that can be accessed using the *Policy API*. In addition to basic

SNMP MIB definitions, the F-Secure MIB concept includes many extensions that are needed for complete policy-based management.

The following categories are defined in a product's MIB:

Settings	Used to manage the workstation in the manner of an SNMP. The managed products must operate within the limits specified here.
Statistics	Delivers product statistics to Policy Manager Console.
Operations	Operations are handled with two policy variables: (1) a variable for transferring the operation identifier to the host, and (2) a variable for informing Policy Manager Console about the operations that were performed. The second variable is transferred using normal statistics; it acknowledges all previous operations at one time. A custom editor for editing operations is associated with the subtree; the editor hides the two variables.
Private	The management concept MIBs may also contain variables which the product stores for its internal use between sessions. This way, the product does not need to rely on external services such as Windows registry files.
Traps	<p>Traps are the messages (including alerts and events) that are sent to the local console, log file, remote administration process, etc. The following types of traps are sent by most F-Secure products:</p> <div> <div>  </div> <div>Info. Normal operating information from a host.</div> </div> <div> <div>  </div> <div>Warning. A warning from the host.</div> </div> <div> <div>  </div> <div>Error. A recoverable error on the host.</div> </div> <div> <div>  </div> <div>Fatal error. An unrecoverable error on the host.</div> </div> <div> <div>  </div> <div>Security alert. A security hazard on the host.</div> </div>

Installing the product

Topics:

- [*Installation steps*](#)
- [*Changing the web browser path*](#)
- [*Uninstalling the product*](#)

This section explains the steps required to install Policy Manager.

Here you will find instructions for installing the main product components; Policy Manager Server and Policy Manager Console.

2.1 Installation steps

Follow these steps in the order given here to install Policy Manager Server and Policy Manager Console on the same machine.

2.1.1 Download and run the installation package

The first stage in installing Policy Manager is to download and run the installation package.

To begin installing the product:


1. Download the installation package from www.f-secure.com/webclub.
You will find the file in the **Download** section of the **Policy Manager** page.
2. Double-click the executable file to begin installation.
Setup begins.
3. Select the installation language from the drop-down menu and click **Next** to continue.
4. Read the license agreement information, then select **I accept this agreement** and click **Next** to continue.

2.1.2 Select components to install

The next stage is to select the product components to install.

To continue installing the product:

1. Select the components to install and click **Next** to continue.
 - Select both Policy Manager Server and Policy Manager Console to install both components on the same machine.
 - Select Policy Manager Server if you want to install Policy Manager Console on a separate machine.
2. Choose the destination folder and then click **Next**.
It is recommended to use the default installation directory. If you want to install the product in a different directory, you can click **Browse** and select a new directory.


 **Note:** If you have Management Agent installed on the same machine, this window will not be shown.

3. Enter and confirm a password for your admin user account, then click **Next**.
Use this password to log in to Policy Manager Console with the user name `admin`.
4. Select the Policy Manager Server modules to enable:
 - The **Host** module is used for communication with the hosts. The default port is 80.
 - The **Administration** module is used for communication with Policy Manager Console. The default HTTPS port is 8080.

 **Note:** If you want to change the default port for communication, you will also need to include the new port number in the **Connections** URL when logging in to Policy Manager Console.

By default, access to the **Administration** module is restricted to the local machine.

- The **Web Reporting** module is used for communication with Web Reporting. Select whether it should be enabled. Web Reporting uses a local socket connection to the **Administration** module to fetch server data. The default HTTPS port is 8081.

 **Note:** Make sure that your firewall rules allow access to the ports used by Policy Manager Console and the hosts so that they can fetch policies and database updates.

5. Click **Next** to continue.

2.1.3 Complete the migration wizard



The migration wizard will open automatically during installation to allow you to import data from a previous installation of Policy Manager.

The migration wizard will only open when upgrading from a previous version of Policy Manager. If no previous Policy Manager data is detected, the wizard will not appear.

If the migration wizard does not appear, if it fails or if you want to import the migration data later, you can start the migration wizard at any time with the `<F-Secure>\Management Server 5\bin\fspms-migrator-launcher.exe` executable.

1. Enter the paths to your previous installation's communication directory and key-pair, then click **Next**.
2. Review the policy domain information shown, then click **Start**.
3. Wait until the data import is completed, then click **Close** to exit the wizard.

The migration wizard closes, and the installation wizard will appear again.

-  **Note:** The commdir data and signing keys from a previous version of Policy Manager will not be removed after upgrading, and can be used if you need to roll back to the previous version.
-  **Note:** Policy-based installation operations and the time period for considering hosts disconnected are not migrated when upgrading. You can set the time period in the **Tools > Server configuration** dialog box.

2.1.4 Complete installation of the product

The next stage is to complete the installation of the product.

1. Review the changes that setup is about to make, then click **Start** to start installing the selected components.
When completed, the setup shows whether all components were installed successfully.
2. Click **Finish** to complete the installation.
3. Restart your computer if you are prompted to do so.

2.1.5 Run Policy Manager Console

The last stage in setting up the product is to run Policy Manager Console for the first time.

To run Policy Manager Console for the first time:

1. Run Policy Manager Console by selecting **Start > Programs > F-Secure Policy Manager > F-Secure Policy Manager Console**.

When Policy Manager Console is run for the first time, you will be asked to register the product using your customer number. You can find your customer number in the license certificate provided with the product. If you do not register the product, you can use it normally for a 30-day evaluation period. When the evaluation period expires, you will not be able to connect to the server, but any client applications that you have installed will continue to work and your product setup will remain unchanged.

2. Click **Continue** to complete the setup process.

The setup wizard creates the user group `FSPM users`. The user who was logged in and ran the installer is automatically added to this group. To allow another user to run Policy Manager you must manually add this user to the `FSPM users` user group.

Policy Manager Console starts in **Anti-virus** mode, which is an optimized user interface for managing Client Security, Anti-virus for Workstations and Server Security. If you are going to use Policy Manager Console for managing any other F-Secure product, you should use the **Advanced mode** user interface. You can access it by selecting **View > Advanced mode** from the menu.

When setting up workstations, older versions of Client Security require the `admin.pub` key file (or access to it) for installation. You can get this key from the Policy Manager Server welcome page. In the latest version of Client Security, the installation packages are prepared in Policy Manager and include the key.

2.2 Changing the web browser path

Policy Manager Console acquires the file path to the default web browser during setup.

If you want to change the web browser path:

1. Select **Tools > Preferences** from the menu.
2. Select the **Locations** tab and enter the new file path.

2.3 Uninstalling the product

Follow these steps to uninstall Policy Manager components.

To uninstall any Policy Manager components:

1. Open the Windows **Start** menu and go to **Control Panel**.
2. Select **Add/Remove Programs**.
3. Select the component you want to uninstall (Policy Manager Console or Policy Manager Server), and click **Add/Remove**.
The F-Secure **Uninstall** dialog box appears.
4. Click **Start** to begin uninstallation.
5. When the uninstallation is complete, click **Close**.
6. Repeat the above steps if you want to uninstall other Policy Manager components.
7. When you have uninstalled the components, exit **Add/Remove Programs**.
8. It is recommended that you reboot your computer after the uninstallation.

Rebooting is necessary to clean up the files remaining on your computer after the uninstallation, and before the subsequent installations of the same F-Secure products.

Using Policy Manager Console

Topics:

- [*Overview*](#)
- [*Basic information and tasks*](#)
- [*Managing domains and hosts*](#)
- [*Software distribution*](#)
- [*Managing policies*](#)
- [*Managing operations and tasks*](#)
- [*Alerts*](#)
- [*Reporting tool*](#)

This section contains information about the Policy Manager Console component and how it is used.

Policy Manager Console is a remote management console for the most commonly used F-Secure security products, designed to provide a common platform for all of the security management functions required in a corporate network.

3.1 Overview

This section provides some general information about Policy Manager Console.

The conceptual world of Policy Manager Console consists of hosts that can be grouped within policy domains. Policies are host-oriented. Even in multi-user environments, all users of a specific host share common settings.

An administrator can create different security policies for each host, or create a single policy for many hosts. The policy can be distributed over a network to workstations, servers, and security gateways.

With Policy Manager Console, an administrator user can:

- Set the attribute values of managed products.
- Determine rights for users to view or modify attribute values that were remotely set by the administrator.
- Group the managed hosts under policy domains sharing common attribute values.
- Manage host and domain hierarchies easily.
- Generate signed policy definitions, which include attribute values and restrictions.
- Display status.
- Handle alerts.
- Handle F-Secure anti-virus scanning reports.
- Handle remote installations.
- View reports in HTML format, or export reports to various formats.

Policy Manager Console generates the policy definition, and displays status and alerts. Each managed host has a module (Management Agent) enforcing the policy on the host.

Read-only users can:

- View policies, statistics, operation status, version numbers of installed products, alerts and reports.
- Modify Policy Manager Console properties, because its installation is user-based and modifications cannot affect other users.

The user cannot do any of the following in read-only mode:

- Modify the domain structure or the properties of domains and hosts.
- Modify product settings.
- Perform operations.
- Install products.
- Save policy data.
- Distribute policies.
- Delete alerts or reports.

3.2 Basic information and tasks

The following sections describe the Policy Manager Console logon procedure, menu commands and basic tasks.

3.2.1 Logging in

When you start Policy Manager Console, the **Login** dialog box will open.



Tip: You can click **Options** to expand the dialog box to include more options.

The **Login** dialog box can be used to select defined connections. Each connection has individual preferences, which makes it easier to manage many servers with a single Policy Manager Console instance.

It is also possible to have multiple connections to a single server. After selecting the connection, enter your Policy Manager Console user name and password. The user name and password are specific for your Policy Manager user account, and are not linked to your network or network administrator password.

The password for the `admin` user is defined when installing the program, and other users (either with admin or read-only access) are created through Policy Manager Console.

The setup wizard creates the initial connection, which appears by default in the **Connections:** field. To add more connections, click **Add** or to edit an existing connection, click **Edit** (these options are available when the dialog box is expanded).

Connection properties

The connection properties are defined when adding a new connection or editing an existing one.

The link to the data repository is defined as the HTTPS URL of Policy Manager Server.

The **Display as** field specifies what the connection will be called in the **Connection:** field in the **Login** dialog box. If the **Name** field is left empty, the URL is displayed.

Adding new users

You can add or remove users with either admin or read-only access to Policy Manager.

1. Select **Tools > Users** from the menu.

The **Users** dialog box appears, with all current users listed.

2. Click **Add** to add a new user.
3. Enter a user name and password for the new user.
4. Select the domain access for the user.

You can give the user access to either a specific sub-domain only or **Root** access to all domains.

5. Select **Read-only access** if you want to limit the user's access, then click **OK**.

The new user will appear on the users list, and will now be able to access Policy Manager.



Note: Any user with full admin access will be able to delete any other user, but there must be at least one user with full, root-level admin access. Users with sub-domain access can only delete other users within the scope of their sub-domain. If a user account is deleted while that user is logged in, they will be logged out and prompted to log in the next time a connection to Policy Manager is required.



Note: The following operations are only available to users with full, root-level access:

- Product registration
- Creating and removing import rules
- Manually importing new hosts that are not matched by import rules
- Importing and removing product installation packages
- Importing and exporting signing keys
- Configuring the auto-removal policy for disconnected hosts
- Importing Active Directory structures

Changing your password

You can change the password for your user account when you are logged in to Policy Manager.

1. Select **Tools > Change password** from the menu.
2. Enter your new password in both fields, then click **OK**.
Your password is now changed.

3.2.2 Client Security management

When you first start Policy Manager Console, the **Anti-virus** mode user interface opens.

This mode is optimized for administering Client Security. Using the **Anti-virus** mode user interface you can complete most tasks for managing Client Security, Anti-virus for Workstations and Anti-virus for Windows Servers.

You should be able to complete most tasks with the **Anti-virus** mode user interface. However, particularly if you need to administer products other than Client Security, you will need to use the **Advanced mode** user interface.

3.2.3 Advanced mode user interface



To configure settings that are not available in **Anti-virus** mode, you need to change to the **Advanced mode** user interface.

To open the **Advanced mode** user interface, select **View > Advanced mode**.

3.2.4 Policy domain tree

You can perform actions for policy domains and hosts on the **Policy domain** tree.

On the **Policy domain** tree, you can do the following:

- Add a new policy domain (click the  icon, which is located on the toolbar). A new policy domain can be created only when a parent domain is selected.
- Add a new host (click the  icon).
- Find a host.
- View the properties of a domain or host. All hosts and domains should be given unambiguous names.
- Import new hosts.
- Autodiscover hosts from a Windows domain.
- Delete domains.
- Move hosts or domains, using cut and paste operations.
- Export a policy file.

After selecting a domain or host, you can access the above options from the **Edit** menu.

The domains referred to in the commands are not Windows NT or DNS domains. Policy domains are groups of hosts or subdomains that have a similar security policy.

3.2.5 Contents of the Advanced mode user interface

The function of the main application area in the **Advanced mode** user interface changes according to which tab is open.

- **Policy** tab: you can set the value of a policy variable. All modifications affect the selected policy domain or host. There are predefined settings available for each type of policy variable.
- **Status** tab: you can view settings, which are the local modifications reported by the host, and statistics.
- **Alerts** tab: when an alert is selected in the **Alerts** tab, details of the alert are displayed.
- **Scanning reports** tab: when a report is selected in the **Reports** tab, details of the report are displayed.
- **Installation** tab: you can view and edit installation information.

The traditional Policy Manager Console **MIB** tree contains all the settings/operations (policy) and local setting/statistics (status) in a product component specific **MIB** tree.

Using help

When you select an **MIB** tree node on the **Policy** tab, any available help text is displayed in the main application area.

3.2.6 Messages pane

Policy Manager Console logs messages in the **Messages** pane about different events.

Unlike the **Alerts** and **Scanning reports** tabs, **Messages** pane events are generated only by Policy Manager Console.

There are three categories of messages: **Information**, **Warnings**, and **Errors**. Each **Messages** view tab can contain messages of all three severities. You can delete a category in the displayed context menu

by right-clicking on a tab. By right-clicking on an individual message, a context menu is displayed with **Cut**, **Copy**, and **Delete** operations.

By default, messages are logged into both files in the message subdirectory of the local Policy Manager Console installation directory. Logs of the messages are kept both in English and the language you have set for Policy Manager Console. A separate log file is created for each message category (tab names in the **Messages** pane). You can use the **Preferences > Locations** page to specify the directory for the log file.

3.3 Managing domains and hosts

If you want to use different security policies for different types of hosts (laptops, desktops, servers), for users in different parts of the organization or users with different levels of computer knowledge, it is a good idea to plan the domain structure based on these criteria.

This makes it easier for you to manage the hosts later on. If you have designed the policy domain structure beforehand, you can import the hosts directly to that structure. If you want to get started quickly, you can also import all hosts to the root domain first, and create the domain structure later, when the need for that arises. The hosts can then be cut and pasted to the new domains.


All domains and hosts must have a unique name in this structure.

Another possibility is to create the different country offices as subdomains.

3.3.1 Adding policy domains

This topic describes how to add new policy domains.

To add a new policy domain:

1. Click  in the toolbar.
The new policy domain will be a subdomain of the selected parent domain.
2. Enter a name for the policy domain.
An icon for the domain will be created.

3.3.2 Adding hosts

This section describes different ways of adding hosts to a policy domain.

The main methods of adding hosts to your policy domain, depending on your operating system, are as follows:

- Import hosts directly from your Windows domain.
- Import hosts through autoregistration (requires that Management Agent is installed on the imported hosts). You can also use different criteria to import the autoregistered hosts into different sub-domains.
- Create hosts manually by using the **New host** command.

Importing hosts from an Active Directory structure

You can import a policy domain structure and hosts to Policy Manager from an Active Directory structure.

1. Select **Edit > Import Active Directory structure** from the menu.
The **Import Active Directory structure** wizard appears.
2. Enter the location of your Active Directory server and a user name and password that provide at least read access, then click **Next**.
3. Select the Active Directory domain, the containers you want to import and the target policy domain you want to import them to, then click **Next**.
Containers that include hosts will be highlighted.
4. Review the import rules, select which rules you want to create, then click **Start**.
The selected rules will be applied to the hosts from the Active Directory structure that send a request to be managed by Policy Manager.
5. Wait until the import operation is completed, then click **Close** to exit the wizard.

The hosts from Active Directory, along with any new items to the policy domain structure, will appear in Policy Manager.

Adding hosts in Windows domains

In a Windows domain, the most convenient method of adding hosts to your policy domain is by importing them through Intelligent Installation.

Note that this also installs Management Agent on the imported hosts. To import hosts from a windows domain:


1. Select the target domain.
2. Select **Edit > Autodiscover Windows hosts** from the menu.
After the Autodiscover operation is completed, the new host is automatically added to the **Policy domain** tree.

Importing new hosts

Another option for adding hosts in Policy Manager Console is to *import new hosts*.

You can do this only after Management Agent has been installed on the hosts and after the hosts have sent an autoregistration request. Management Agent will have to be installed from a CD-ROM, from a login script, or some other way.

To import new hosts:

1. Click  on the toolbar.
Alternatively:
 - Select **Edit > Import new hosts** from the menu.
 - Select **Import new hosts** from the **Installation** view.

When the operation is completed, the host is added to the domain tree. The new hosts can be imported to different domains based on different criteria, such as the hosts' IP or DNS address. The **New hosts** view offers a tabular view to the data which the host sends in the autoregistration message. This includes any custom properties that were included in the remote installation package during installation.

2. You can perform the following actions on the **New hosts** view:
 - You can sort messages according to the values of any column by clicking the corresponding table header.
 - You can change the column ordering by dragging and dropping the columns to the suitable locations, and column widths can be freely adjusted.
 - You can use the table context menu (click the right mouse button on the table header bar) to specify which properties are visible in the table.

Using import rules

You can define the import rules for new hosts on the **Import rules** tab in the **Import new hosts** window.

Import rules can be applied automatically to new hosts that connect to the server. This means that there is no need to run the import rules manually when new hosts connect to Policy Manager Server; the new hosts are added to the domain structure according to the existing import rules.

You can use the following as import criteria in the rules:


- WINS name, DNS name, custom properties
 - These support * (asterisk) as a wildcard. The * character can replace any number of characters. For example: `host_test*` or `*.example.com`.
 - Matching is not case-sensitive, so upper-case and lower-case characters are treated as the same character.
- IP address

- This supports exact IP address matching (for example: 192.1.2.3) and IP sub-domain matching (for example: 10.15.0.0/16).
1. You can hide and display columns in the table by using the right-click menu that opens when you right-click any column heading in the **Import rules** window.
Only the values in the currently visible columns are used as matching criteria when importing hosts to the policy domain. The values in the currently hidden columns are ignored.
 2. You can add new custom properties to be used as criteria when importing hosts.
One example of how to use the custom properties is to create separate installation packages for different organizational units, which should be grouped under unit-specific policy domains. In this case you could use the unit name as the custom property, and then create import rules that use the unit names as the import criteria. Note that custom property names that are hidden are remembered only until Policy Manager Console is closed. To add a new custom property:
 - a) Right-click a column heading and select **Add new custom property**.
The **New custom property** dialog opens.
 - b) Enter a name for the custom property, for example the unit name, then click **OK**.
The new custom property now appears in the table, and you can create new import rules in which it is used as import criteria.
 3. Create a new import rule:
 - a) Click **Add** on the **Import rules** tab.
The **Select target policy domain for rule** dialog opens displaying the existing domains and sub-domains.
 - b) Select the domain for which you want to create the rule and click **OK**.
 - c) Select the new row that was created and click the cell where you want to add a value.
 - d) Enter the value in the cell.
The import criteria is defined.
 - e) Select **Apply rules automatically when new hosts connect to the server** if you want the rules to be applied automatically for any new connected hosts.
This option is turned on for new installations of Policy Manager, and turned off for upgraded installations by default to emulate the behavior of the previous version.
 - When new hosts are imported, the rules are verified in top-down order, and the first matching rule is applied. You can change the order of the rules by clicking **Move down** or **Move up**.
 - If you want to create several rules for a domain, you can use the **Clone** option. Start by creating one rule for the domain. Then select the row and click **Clone**. Now you can edit the criteria on the new duplicated row.
 4. When you want to start the import operation, select the **New hosts** tab and click **Import**.
The import rules you have defined will be validated before importing starts.
After the hosts have been imported, you will see a summary dialog displaying the number of successfully imported hosts and the number of unsuccessful import operations. Note that an empty set of conditions is always treated as matching.

Creating hosts manually

This topic describes how to create hosts manually.

To create a host manually:

1. Select the target domain.
2. Select **Edit > New host** from the menu.
Alternatively:
 - Click  in the toolbar.
 - Press **Insert**.
3. Enter an identifier for the new host and click **OK**.
This operation is useful in the following cases:

- Learning and testing – you can try out a subset of Policy Manager Console features without actually installing any software in addition to Policy Manager Console.
- Defining policy in advance – you can define and generate a policy for a host before the software is installed on the host.
- Special cases – you can generate policies for hosts that will never access the server directly (that is, when it is not possible to import the host). For example, it is possible to generate base policy files for a computer that does not access the F-Secure Policy Manager Server. The base policy file must be transferred either manually or by using another external transport mechanism. To do this, select **Edit > Export policy file** from the menu.



Note: Hosts without Management Agent installed cannot be administered through Policy Manager Console because they have no means of fetching policies. Also, no status information will be available. Any changes made to the domain structure are implemented even though you exit Policy Manager Console without saving changes to the current policy data.

Handling disconnected hosts automatically

You can specify when hosts are considered disconnected, and also when disconnected hosts should be removed from the policy domain.

1. Select **Tools > Server configuration** from the menu.
2. Select **Hosts**.
3. Enter the number of days, after which the host status will be set to **Disconnected** in **Consider hosts disconnected after**.
4. Enter the number of days, after which disconnected hosts will be removed from the policy domain in **Remove disconnected hosts after**.
5. Click **OK** to close the dialog box.

3.4 Software distribution

Policy Manager offers multiple methods of installing and updating managed applications.

Shortcuts to all the installation-related features are gathered under the **Installation** tab.

3.4.1 Push installations

This section describes how to push installation packages to hosts.

The only difference between the **Autodiscover Windows hosts** and the **Push install to Windows hosts** features is how the target hosts are selected: Autodiscover browses the Windows domains and user can select the target hosts from a list of hosts, push install allows you to define the target hosts directly with IP addresses or host names. After the target hosts are selected, both push installation operations proceed the same way.



Note: Before you start to install F-Secure products on hosts, you should make sure there are no conflicting antivirus or firewall programs installed on them. You should also check that any firewalls do not block access to the target computer. Policy Manager uses TCP port 135 for remote procedure call (RPC) access, and ports 137 - 139 for network and file sharing access.

The push installation functionality is part of Policy Manager Console. This means that you can use push installations if you have Policy Manager Server running on a Linux machine and Policy Manager Console installed on a Windows machine. If you install Policy Manager Console on a Linux machine, push installation is not available.

Push installation works as follows:

1. Policy Manager Console uploads the installation package to the remote host's admin (**ADMIN\$**) share. This requires that file sharing is enabled on the remote host.
2. Policy Manager Console uses the remote procedure call (RPC) service to install and start the push installation service on the target computer with the appropriate parameters. The purpose of this service is to start the installer and to generate a file containing the installation results.

3. Installation progress is tracked by file. Policy Manager Console polls the `ADMIN$` share for the file that contains the installation results. Once the file is available, Policy Manager Console fetches the file, parses it and reports the result.

Autodiscover Windows hosts

Target hosts can be selected with the *Autodiscover* feature.

To select target hosts:

1. Select the target domain.
2. Select **Edit > Autodiscover Windows hosts** from the menu.

Alternatively, click the  button.

3. From the **NT domains** list, select one of the domains and click **Refresh**.

The host list is updated only when you click **Refresh**. Otherwise cached information is displayed for performance reasons. Before clicking **Refresh**, you can change the following options:

- **Hide already managed hosts**. Select this check box to show only those hosts, which do not have F-Secure applications installed.
- **Resolve hosts with all details (slower)**. With this selection, all details about the hosts are shown, such as the versions of the operating system and Management Agent.
- **Resolve host names and comments only (quicker)**. If all hosts are not shown in the detailed view or it takes too much time to retrieve the list, this selection can be used. Note, that sometimes it may take a while before **Master browser** can see a new host recently installed in the network.

4. Select the hosts to be installed.

Press the space bar to check selected host(s). Several hosts can be easily selected by holding down the shift key and doing one of the following:

- clicking the mouse on multiple host rows,
- dragging the mouse over several host rows,
- using the up or down arrow keys.

Alternatively, you can right-click your mouse. Use the host list's context menu to select:

- **Check** - checkmarks the selected host(s) (same as pressing the space bar).
- **Uncheck** - removes the checkmark from the selected host(s) (same as pressing the space bar).
- **Check all** - checkmarks all hosts in the selected Windows domain.
- **Uncheck all** - removes the checkmark from all hosts in the selected Windows domain.

5. Click **Install** to continue.

After you have selected your target hosts, you still need to push-install the applications to hosts.

Push install to Windows hosts

You can also select target hosts with the **Push install to Windows hosts** feature.

To select target hosts:

1. Select the target domain.
2. Select **Edit > Push install to Windows hosts** from the menu.

Alternatively, click the  button.

3. Enter the target host names of those hosts to which you want to push install, and click **Next** to continue.

You can click **Browse** to check the Management Agent version(s) on the host(s).

After you have selected your target hosts, you still need to push-install the applications to hosts.

Push install after target host selection

After selecting the target hosts, you have to push install the installation packages.

To push install the installation package(s) on the selected target hosts:

1. Select the installation package and click **Next** to continue.

You can import new installation packages on this page if necessary. The `Forced reinstallation` option is always turned on in all installation packages, so the application will be reinstalled if the host already has the same version number of the application installed.

2. Choose to accept the default policy, or specify which host or domain policy should be used as an anonymous policy, and click **Next** to continue.
3. Choose the user account and password for the push installation by selecting either **This account** (the current account) or **Another user**.



Note: Push installation requires administrator rights for the target machine during the installation. If the account you entered does not have administrator rights on one of the remote hosts, an **Access denied** error message will be indicated for that host, while installation will continue on the other hosts.

When you select **This account**, you will use the security rights of the account currently logged on. Use this option in the following cases:

- You are already logged in as domain administrator; or
- You are logged in as the local administrator with a password that matches the local administrator's password on the target host.

Another user: enter account and password. The administrator can enter any proper domain administrator account and password to easily complete the remote installation on selected hosts.

- When completing the installation to the trusted and non-trusted domains with a domain account, make sure you enter the account in the format `DOMAIN\ACCOUNT`.
- When using a local administrator account, use the format `ACCOUNT`. (Do not enter the host name as part of the account, otherwise the account is accepted only by the host in question.)



Note: When installing, if the administrator machine has open network connections to the target machine with another user account, the NT credential conflict error message **1219** appears. The solution in this case is to close the active connections before using the **Push installation** feature.

4. Review the installation summary.
5. To start the **Remote installation wizard**, click **Start**.

The **Remote installation wizard** will guide you through a series of dialog boxes in which you must answer some questions for the installation to take place. In the final dialog box, click **Finish**, and go to the next step.

Policy Manager installs Management Agent and the selected products on the hosts. During this process, the **Status** line will display the procedure in process. You can click **Cancel** at any time to stop the installation.

6. When the **Status** line displays finished, the process has finished and you can select in which domain the new hosts should be placed using the import settings.
7. Click **Finish**.

Policy Manager Console will place the new hosts in the domain that you selected, unless you specified another domain in this dialog. You can also choose not to place the hosts to any domain automatically. The new hosts will send autoregs and the hosts can be imported that way.

After a few minutes, the products that were installed will be listed.

8. To see this list, select the **Installation** tab (alternatively select the top domain on the **Policy domain** tree).

3.4.2 Policy-based installation

Installation operations on hosts that have Management Agent installed can be centrally managed through the policies in Policy Manager.

Policy-based installation creates and stores the operation-specific installation package, and writes an installation task to the base policy files (thus, policy distribution is required to start installations). Both base policy files and the installation package are signed by the management key-pair so that only genuine information is accepted by the hosts.

Management Agent on the hosts fetches the new policies from Policy Manager Server and discovers the installation task. Management Agent fetches the installation package specified in the task parameters from the server and starts the installation program.

When installation is complete, Management Agent sends the result of the installation operation in an incremental policy file to the server. The results of the new status information are then shown in Policy Manager Console .

Uninstallation uses these same delivery mechanisms. The results of the uninstallation will not be reported.

Using policy-based installation

Policy-based installation must be used on hosts that already have Management Agent installed.

You can use policy-based installation to perform installation operations on a selected domain or selected hosts. In addition to installing products, you can perform hotfix, upgrade, repair and uninstallation operations.

When the installation operation is completed successfully, you can leave the operation on the **Policy-based installations** table, so that the same installation operation will automatically be applied to any new hosts that are added to the corresponding domain.

To use policy-based installation:

1. Open the **Installation** tab.

On the **Installation** tab, **Policy-based installations** table shows the status of any current installation operations, and the **Installed products summary** table lists the products that are currently installed on managed hosts.

2. Click **Install** under the **Policy-based installations** table to start the remote installation wizard.

3. Complete the remote installation wizard with the necessary details.

The information entered in the remote installation wizard is used to prepare the customized package specific for this installation operation. The installation package will be then distributed to the selected domain or hosts once the policy is distributed.

Once the remote installation wizard is complete, the installation operation and status will appear on the **Policy-based installations** table as a new row.

4. Distribute the policy.

Once the installation operation is complete, the product name, version and number of hosts running the product are shown on the **Installed products summary** table.



Note: It may take a considerable length of time to carry out an installation operation. This may happen if an affected host is not currently connected to the network, or if the active installation operation requires a user to restart his host before the installation is completed. If the hosts are connected to the network and they send and receive policy files correctly, then there could be a real problem. The host may not be correctly acknowledging the installation operation. It is possible to remove the installation operation from the policy by clicking **Clear row** and then distributing the policy. This will cancel the installation operation. It is possible to stop the installation task in the selected domain and all subdomains by selecting the **Recursively cancel installation for subdomains and hosts** option in the confirmation dialog.

For other installation operations, for example upgrades or uninstallation, you can use the links next to the product on the **Installed products summary** table. These links will automatically appear whenever the installation packages necessary for the corresponding action are available. The options are: **hotfix**, **upgrade**, **repair** and **uninstall**.

If the link for the operation you want to run is not shown on the **Installed products summary** table, you can click either **Install** or **Uninstall**, depending on the operation you want to run, under the **Policy-based installations** table and check if the required package is available there. However, if for example the product does not support remote uninstallation, there will not be an option for uninstallation.

When uninstalling Management Agent, no statistical information will be sent stating that the uninstallation was successful, because Management Agent has been removed and is unable to send any information. For example, if uninstalling F-Secure Anti-Virus and Management Agent:

1. Uninstall F-Secure Anti-Virus
2. Wait for Policy Manager Console to report the success or failure of the uninstallation.
3. If F-Secure Anti-Virus was uninstalled successfully, uninstall Management Agent.
4. If uninstallation of Management Agent is unsuccessful, Policy Manager Console will display a statistical report of the failure. Success cannot be reported, but is evident from ceased communication, and the final report for Management Agent will state `in progress....`

3.4.3 Local installation and updates with pre-configured packages

You can export pre-configured packages in MSI (Microsoft Installer) or JAR format.

The MSI packages can be distributed, for example, using Windows Group Policy in an Active Directory environment.

The procedure for exporting is the same in both formats, and is explained below. You can select the file format for the customized package in the **Export installation package** dialog box.

Using the customized remote installation package

There are two ways of using the login script on Windows platforms: by using a customized MSI package or a customized remote installation JAR package.

To use a customized installation package:

1. Run Policy Manager Console.
2. Select **Tools > Installation packages** from the menu.
This will open the **Installation packages** dialog box.
3. Select the installation package that contains the products you want to install, and click **Export**.
4. Specify the file format, MSI or JAR, and the location where you want to save the customized installation package, then click **Export**.
5. Specify the file location where you want to save the customized installation package and click **Save**.
6. Select the products you want to install and click **Next** to continue.
7. Choose to accept the default policy, or specify which host or domain policy should be used as an anonymous policy, then click **Next** to continue.
8. Review the summary and click **Start** to continue to the installation wizard.

Policy Manager Console displays the **Remote installation wizards** that collect all necessary setup information for the selected products. It is possible to include any number of custom properties in the installation package. A host will add these custom properties to the message it sends to the Policy Manager after local installation. These customer-specific properties will appear together with the standard host identification properties in the **New hosts** view. The custom property name will be the column name, and the value will be presented as a cell value.

One example of how to utilize custom properties is to create a separate installation package for different organizational units, which should be grouped under unit-specific policy domains. The property name could be `Unit` and the value is different in each installation package. Now hosts from each unit can be distinguished in the new hosts view, and using the column sorting and multiple selection all the hosts from one unit can be imported to their target domain. Note that the target domain can be changed directly from the **New hosts** view, and after that the hosts from another unit can be imported to their target domain.

9. When you reach the last wizard page, click **Finish** to continue.
10. You can also install an exported JAR to the hosts by running the `ilaunchr.exe` tool.

The `ilaunchr.exe` tool is located in the Policy Manager Console installation directory under the `...\Administrator\Bin` directory. To do this:

- a) Copy `ilaunchr.exe` and the exported JAR to a location where the login script can access them.
- b) Enter the command: `ilaunchr <package name>.jar` where `<package name>` is replaced by the actual name of the JAR package being installed.

When the installation runs, the user will see a dialog displaying the installation progress. If a restart is required after the installation, the user is prompted to restart the computer as defined when the installation package was exported. If you want the installation to run in silent mode, enter the command in format: `ilaunchr <package name>.jar /Q`. Also in this case the user may be prompted to restart the computer after the installation, and if a fatal error occurs during the installation, a message is displayed.

ILAUNCHR has the following command line parameters:

`/U` — Unattended. No messages are displayed, even when a fatal error occurs.

`/F` — Forced installation. Completes the installation even if Management Agent is already installed.

Enter `ILAUNCHR /?` on the command line to display complete help.

When installing on Windows XP and newer you can also use the following parameters:

- `/user:domain\username` (variation: `/user:username`) — Specifies the user account and the domain name. The domain name can be optionally left out.
- `/password:secret` (variation: `/password:"secret with spaces"`) — Specifies the password of the user account.

The `ilaunchr` functionality stays the same if neither of these two parameters is given. If only one of the parameters is given, `ilaunchr` returns an error code. If both parameters are given, `ilaunchr` starts the **Setup** program. An example of the command:

```
ILaunchr <jar file> /user:domain\user_name /password:secret_word
```

3.4.4 Local installation and Policy Manager

Local installation is recommended if you need to install Client Security locally on a workstation that is otherwise centrally managed by Policy Manager.

You must have Policy Manager already installed before you can continue with the installation.

System requirements

Read the following before starting to use the product.

The recommended requirements for installing and using the product on your computer are:

System requirements

Processor:	<ul style="list-style-type: none"> On Windows Vista and Windows 7: Intel Pentium 4 2 GHz or higher On Windows XP: Intel Pentium III 1 GHz or higher
Operating system:	<ul style="list-style-type: none"> Windows 7 32-bit and 64-bit Windows Vista 32-bit and 64-bit Windows XP SP3
Memory:	<ul style="list-style-type: none"> On Windows Vista and Windows 7: 1 GB of RAM or more On Windows XP: 512 MB of RAM or more
Disk space:	800 MB free hard disk space
Display:	<ul style="list-style-type: none"> On Windows Vista and Windows 7: 16 bit or more (65000 colors) On Windows XP: 16 bit, 65000 colors or more

Internet connection: Required to validate your subscription and receive updates

Uninstall other antivirus programs

Before you begin installing Client Security, you should remove any other antivirus programs currently installed on the workstations.

To uninstall other antivirus programs:

1. Select the currently installed programs in the **Start > Settings > Control Panel > Add/Remove Programs** dialog.
2. Remove any related components.
Some programs may have several related components, which may need to be uninstalled separately. If you encounter problems, refer to the user documentation for the currently installed antivirus program.
3. Restart your computer.

Installation steps

The package used for local installation is created in Policy Manager.

To install the product:

1. Run Policy Manager Console.
2. Select **Tools > Installation packages** from the menu.
This will open the **Installation packages** dialog box.
3. Select the installation package that contains the products you want to install, and click **Export**.
4. Specify the file format, MSI or JAR, and the location where you want to save the customized installation package, then click **Export**.
5. Specify the file location where you want to save the customized installation package and click **Save**.
6. Select the products you want to install and click **Next** to continue.
7. Choose to accept the default policy, or specify which host or domain policy should be used as an anonymous policy, then click **Next** to continue.
8. Review the summary and click **Start** to continue to the installation wizard.

Policy Manager Console displays the **Remote installation wizards** that collect all necessary setup information for the selected products. It is possible to include any number of custom properties in the installation package. A host will add these custom properties to the message it sends to the Policy Manager after local installation. These customer-specific properties will appear together with the standard host identification properties in the **New hosts** view. The custom property name will be the column name, and the value will be presented as a cell value.

One example of how to utilize custom properties is to create a separate installation package for different organizational units, which should be grouped under unit-specific policy domains. The property name could be `Unit` and the value is different in each installation package. Now hosts from each unit can be distinguished in the new hosts view, and using the column sorting and multiple selection all the hosts from one unit can be imported to their target domain. Note that the target domain can be changed directly from the **New hosts** view, and after that the hosts from another unit can be imported to their target domain.

9. When you reach the last wizard page, click **Finish** to continue.
10. Copy the installation package to the workstation where you want to install Client Security.
11. Run the installation package.


The computer restarts automatically. To restart immediately, select **Restart now**.

After the restart, the product tries to connect to the Internet to validate your subscription and download updates. Make sure that you are connected to the Internet. Downloading these major updates may take some time. When the updates have been downloaded, the protection is up to date. The latest updates ensure the best protection.

3.5 Managing policies

This section describes how to configure and distribute policies.

Several users can be logged in and make changes to the policies at the same time. Any changes made by users are automatically saved to their own personal workspace, so there is no need to save the changes manually. Changes made by any user will only be visible to other users and take effect when the user distributes the policy changes.

 **Note:** There is no conflict resolution for policy changes made by different users; the last distributed changes will override any previous changes to the policy variables.

When policy changes are distributed, the policy files are generated automatically for each host on request. This means that there is no need to redistribute the policy when you change the domain structure, for example by adding new hosts, or after you upgrade the managed software on existing hosts.

3.5.1 Settings

To configure settings, browse the policy tree and change the values of the policy variables.

A policy variable may have a pre-defined default value. The default values behave as if they were inherited from above the root domain. That is, they appear to be inherited values even if the top (root) domain is selected. Default values can be overridden just like any other value.

Values on the selected policy domain level are color-coded as follows:

- Black – changed values on the selected policy domain or host level.
- Gray – inherited values.
- Red – invalid values.
- Dimmed red – inherited invalid values.

3.5.2 Discarding undistributed changes to settings

You can undo any changes to settings that have not yet been applied.

Select **File > Discard policy changes** from the menu.

The settings will revert to what they were when the policy was last distributed. If the changes have already been distributed, you need to manually revert the changes and redistribute the policy.

3.5.3 Restrictions

Using restrictions, an administrator can restrict access to any policy variable from the user.

Policy variables that are set to **Disallow user changes** always forces the setting: the policy variable overrides any local host value, and the end user cannot change the value as long as the **Disallow user changes** restriction is set.


3.5.4 Configuring settings

Settings are changed by modifying the policy variables.

To configure settings:

1. Browse the policy tree.
2. Change the values of the policy variables.
3. Distribute the policies:

After you have finished configuring the domains and hosts, you must distribute the new configurations to the hosts. To do this:

- Click  in the toolbar.
- Select **File > Distribute** from the menu.
- Press CTRL + D.

Once you distribute the changes, the updated policies are saved to the database, where F-Secure software on the hosts will automatically check for updates.



Note: No changes will take effect before you have distributed the policy and the host has fetched it. This also applies to operations, because they are implemented using the policy-based mechanism.

3.5.5 Policy inheritance

In Policy Manager Console, each policy domain automatically inherits the settings of its parent domain, allowing for easy and efficient management of large networks.

The inherited settings may be overridden for individual hosts or domains. When a domain's inherited settings are changed, the changes are inherited by all of the domain's hosts and subdomains. Any overridden setting can be made inherited again by using the **Clear** operation. Because the setting is deleted from the currently selected policy domain or host, the setting is replaced by the setting in the parent domain.

Policy inheritance simplifies the defining of a common policy. The policy can be further refined for subdomains or even individual hosts. The granularity of policy definitions can vary considerably among installations. Some administrators might want to define only a few different policies for large domains. Other administrators might attach policies directly to each host, achieving the finest granularity.

Combining these strategies achieves the best of both worlds. Some products could inherit their policies from large domains, while other products could inherit their policies from subdomains or even get host-specific policies.

If policy changes are implemented at multiple levels of the policy domain hierarchy, tracking changes can become a challenging task. One convenient way is to use the **Show domain values** operation to see what changes have been made to one specific policy setting.

If the subdomain or host values need to be reset to the current domain values, the **Force value** operation can be used to clean the sub-domain and host values.



Tip: You can also use the **Reporting tool** to create **Inheritance reports** that show where inherited settings have been overridden.

Index inheritance in tables

When you clear a row in a table using the **Clear row** button, the selected row is emptied; the result depends on the types of default rows defined in the parent domains and in MIB as default rows.

- If a row exists that has the same index values as the cleared row, it will be re-inherited.
- If a row that has the same index values as the cleared row does not exist, the emptied row will remain empty after the Clear row operation.



Note: The row can be inherited from a parent domain, or from a MIB (a definition of the settings and containing the default values for all settings) as a default row. The MIB can be considered a "domain above the root domain" in relation to leaf value or row inheritance. MIB defaults are inherited to subdomains unless overridden at a domain level. To override an inherited row, define a row with the same index column values. MIB defaults are obtained based on the product version installed on hosts. For a domain, the values from the newest product version are used.

3.6 Managing operations and tasks

You can perform various product-specific operations through Policy Manager Console.

To launch an operation from Policy Manager Console:

1. Select one of the actions from the **Operations** tab.

You can also see available operations in the **Advanced mode** view, under the selected product's **Operations** branch on the **Policy** tab.

2. Click **Start** to start the selected operation.

3. The operation begins on the host as soon as you have distributed the new policy and the host has fetched the policy file.

You can click **Cancel** at any time to undo the operation.

3.7 Alerts

This section describes how to view alerts and reports, and how to configure alert forwarding.






3.7.1 Viewing alerts and reports

The hosts can send alerts and reports if there has been a problem with a program or an operation.

When an alert is received, the  button will light up. To view the alerts:

1. Click .

The **Alerts** tab will open. All alerts received will be displayed in the following format:

Ack	Click the Ack button to acknowledge an alert. If all the alerts are acknowledged, the Ack button will be dimmed.		
Severity	The problem's severity. Each severity level has its own icon:		
		Info	Normal operating information from a host.
		Warning	A warning from the host.
		Error	Recoverable error on the host.
		Fatal error	Unrecoverable error on the host.
		Security alert	Security hazard on the host.
Date/Time	Date and time of the alert.		
Description	Description of the problem.		
Host/User	Name of the host/user.		
Product	The F-Secure product that sent the alert.		

When an alert is selected from the list, more specific information about the alert will be displayed. F-Secure anti-virus scanning alerts may have an attached report, which will also be displayed.

2. To view reports, click on the **Scanning reports** tab, or select **Product view** > **Messages** from the menu.

The **Scanning reports** tab has the same structure as the **Alerts** tab. **Alerts** tables and **Scanning reports** tables can be sorted by clicking on the column heading.

3.7.2 Configuring alert forwarding

You can configure alerts by editing the **Alert forwarding** table, which is located under **F-Secure Management Agent** > **Settings** > **Alerting** > **Alert Forwarding**.

The same table can also be found in the Management Agent product view in the **Alert Forwarding** tab.

To configure alert forwarding:

1. Select **F-Secure Management Agent** > **Settings** > **Alerting** > **Alert Forwarding** from the menu.
2. Specify where alerts are sent according to severity level.

The target can be Policy Manager Console, the local user interface, an alert agent (such as the **Event viewer**, a log file, or SMTP), or a management extension.


The **Alert forwarding** table has its own set of default values.

Information alerts and warning-level alerts are, by default, not sent to Policy Manager Console or displayed to the user. These lower-priority alerts and notifications can provide very useful information for troubleshooting, but if these alerts are enabled, the number of transmitted alerts will increase substantially. If you have a large domain structure, specifying strict alert-forwarding rules at the root domain level could flood Policy Manager Console with too many alerts.

3. Configure the alert target further, if necessary, by setting the policy variables under target-specific branches.
For example **Settings > Alerting > F-Secure Policy Manager Console > Retry send interval** specifies how often a host will attempt to send alerts to Policy Manager Console when previous attempts have failed.

3.7.3 Forwarding alerts to syslog server

You can set Policy Manager to forward alerts to a third-party syslog server.

 **Note:** Currently, UDP is the only transport protocol supported.

To configure alert forwarding:

1. Select **Tools > Server configuration** from the menu.
2. Click **Syslog**.
3. Select **Forward alerts to syslog** and enter the server address.
By default, alerts are forwarded to syslog using UDP port number 514. If you want to use a different port, enter the port number after the server address, for example, `example.com:8080`.
4. Click **OK**.

3.8 Reporting tool

The **Reporting tool** allows users to view and export reports of Policy Manager Console managed data.

The viewing and exporting functionality provides a way to examine the data of several hosts/domains at the same time.

3.8.1 Viewing and exporting a report

You can view and export reports using the **Reporting tool**.

To use the **Reporting tool**:

1. Select **Tools > Reporting...** from the menu.
Alternatively:
 - Launch the **Reporting tool** from the context menu in the main application area.
 The **Reporting tool** opens.
2. Select the domains and/or hosts you want to include in the report.
 - Select **Recursive** if you want all hosts under the selected domains to be included in the report.
3. Select the report type.
4. Select the products to include in the report, if necessary.
5. Select report type-dependent configurations for the currently selected report, if necessary.
6. View or export the report:
 - Click **View** in the bottom pane to generate the report and view it in HTML format with your default web browser. If no default web browser has been defined, a dialog box appears prompting you to define your web browser.

- Click **Export** in the bottom pane to generate the report and save it as a file. The file path and report format are defined in the **File save** dialog box that appears after clicking **Export**.

Maintaining Policy Manager Server

Topics:

- [*Backing up & restoring Policy Manager data*](#)
- [*Creating the backup*](#)
- [*Restoring the backup*](#)
- [*Exporting and importing signing keys*](#)
- [*Replicating software using image files*](#)


This section contains topics on how to ensure the reliable running of Policy Manager Server.

Here you will find details on how to backup and restore console data in Policy Manager Server.

4.1 Backing up & restoring Policy Manager data

Policy Manager Server can be maintained by routinely backing up the data on the server in case it needs to be restored.

It is highly recommended that you back up the most important management information regularly. The domain and policy data, as well as the signing keys, are all stored in the H2 database.

 **Note:** Before backing up the data, you will need to stop the Policy Manager Server service.

You can also export the signing keys in use on your installation of Policy Manager Server to a network location, from where they can be imported again if necessary.

If you want to save the Policy Manager Console preferences, back up the `lib\Administrator.properties` file from the local installation directory.

 **Note:** The `Administrator.properties` file is created during the first run of Policy Manager Console and contains session related information such as window size or the server URL.

4.2 Creating the backup

Here you will find how to create a backup of the policy data and domain structure.

1. Stop the Policy Manager Server service.
2. Backup the `<F-Secure installation folder>\Management Server 5\data\h2db` directory.
3. Restart the Policy Manager Server service.
4. Reopen the Policy Manager Console management sessions.

4.3 Restoring the backup

In the event of lost Policy Manager data, you can restore the most recently backed up data.

To restore backed up Policy Manager data:

1. Stop the Policy Manager Server service.
2. Copy the backup of the `<F-Secure installation folder>\Management Server 5\data\h2db` directory to its correct location.
3. Restart the Policy Manager Server service.
4. Reopen the Policy Manager Console management sessions.

4.4 Exporting and importing signing keys

You can export your signing keys to an external location or import existing signing keys to replace the ones generated during installation.

You may need to export the signing keys, for example if you use several installations of Policy Manager to manage a large environment, but want to use the same signing keys across the whole environment.

1. Select **Tools > Server configuration** from the menu.
2. Select **Keys**.

To export your current signing keys:

- a) Click **Export**.
- b) Select the target folder or network location for the exported keys, then click **Save**.
- c) Enter and confirm a passphrase for the exported private key, then click **OK**.

To import existing signing keys to replace those currently in use:

- a) Click **Replace**.
- b) Browse to the location of the keys you want to import, then click **OK**.

c) Enter the passphrase for the imported signing keys, then click **OK**.

A notification will appear to confirm that the signing keys were successfully exported or replaced.

3. Click **OK** to close the **Server configuration** dialog box.

4.5 Replicating software using image files

If you use image files to distribute product installations, you need to make sure that there are no unique ID conflicts.

Anti-virus may be included when software is replicated using disk image files. Every product installation does, however, contain a unique identification code (Unique ID) that is used by Policy Manager. Several computers may attempt to use the same Unique ID if disk image software is used to install new computers. This situation will prevent Policy Manager from functioning properly.

Please follow these steps to make sure that each computer uses a personalized Unique ID even if disk imaging software has been used:

1. Install the system and all the software that should be in the image file, including Anti-virus.
2. Configure Anti-virus to use the correct Policy Manager Server.



Note: Do not import the host to Policy Manager Console if the host has sent an autoregistration request to Policy Manager Server. Only hosts to where the image file will be installed should be imported.

3. Run the `fsmutil resetuid` command from the command prompt.

This utility is typically located in the `C:\Program Files\F-Secure\Common` directory (the directory may be different if you are using a localized version of Windows or if you have specified a non-default installation path).

4. Shut down the computer.



Note: Do not restart the computer at this stage.

5. Create the disk image file.

The utility program resets the Unique ID in the Anti-virus installation. A new Unique ID is created automatically when the system is restarted. This will happen individually on each machine where the image file is installed. These machines will send autoregistration requests to Policy Manager and the request can be processed normally.

Updating virus definition databases

Topics:

- [*Automatic updates with Automatic Update Agent*](#)
- [*Using Automatic Update Agent*](#)
- [*Forcing Automatic Update Agent to check for new updates immediately*](#)
- [*Updating the databases manually*](#)
- [*Troubleshooting*](#)

This section covers how to keep the virus definition databases up to date.

Virus definition databases must be kept up to date to ensure proper protection against the latest threats.

5.1 Automatic updates with Automatic Update Agent

With Automatic Update Agent, you are able to receive automatic updates and informative content without interrupting your work to wait for files to download from the Web.

Automatic Update Agent downloads files automatically in the background using bandwidth not being used by other Internet applications, so users can always be sure they will have the latest updates without having to search the Internet.

If Automatic Update Agent is always connected to the Internet, it will automatically receive new automatic updates within about two hours after they have been published by F-Secure. Any possible delays will depend on when a connection to the Internet is available.

Automatic Update Agent is used to update centrally managed F-Secure products. By default the agent also downloads virus news. Downloading news can be disabled if so desired. You may install and use Automatic Update Agent in conjunction with licensed Anti-virus and security products.

5.1.1 How Automatic Update Agent works

Automatic Update Agent polls the server regularly to see whether there is new content available, which it then automatically downloads.

When the Automatic Update Agent service is started, it connects to the F-Secure update server. The agent will keep polling the server regularly to see whether there is new content available. Any new content will be automatically downloaded. The polling interval is set on the server side and cannot be adjusted from the client side.

In Policy Manager 6.0 and onwards, the Automatic Update Agent installed with F-Secure products tries to download the automatic updates from the configured update sources in the following order:

1. If there are Policy Manager proxies in use in the company network, the client tries to connect to Policy Manager Server through each Policy Manager proxy in turn.
2. If the client is configured to use HTTP proxy, it tries to download the updates through the HTTP proxy from Policy Manager Server.
3. Next the client tries to download the updates directly from Policy Manager Server.
4. If there are Policy Manager proxies in use in the company network, the client tries to connect to the F-Secure update server through each Policy Manager proxy in turn.
5. If the client is configured to use HTTP proxy, it tries to download the updates through the HTTP proxy from the F-Secure update server.
6. After that the client tries to download the updates directly from the F-Secure update server.

5.1.2 The benefits of using Automatic Update Agent

Automatic Update Agent downloads updates automatically, and also saves bandwidth.

Optimized downloads of virus definition updates

Automatic Update Agent detects when the virus definition database has been changed. It uses sophisticated byte-level algorithms to download only the changes instead of whole files or the whole database. Changes are typically only a small fraction of the complete update, and this enables dial-up users with slow modems to get the daily updates conveniently, saving significant amounts of bandwidth for fixed-connection users as well.

Resumable data transfers

Automatic Update Agent downloads content over multiple sessions. If the download is interrupted, Automatic Update Agent saves what was downloaded and continues to download the rest of the file next time you connect.

Automated updates


You don't have to look for the updates and manually download them. With Automatic Update Agent, you will automatically get the virus definition updates when they have been published by F-Secure.

5.2 Using Automatic Update Agent

You can configure the Automatic Update Agent by editing the `fsaua.cfg` configuration file.

5.2.1 Configuring Automatic Update Agent

With Policy Manager 7.0 and onwards, the Automatic Update Agent installed with Policy Manager is configured by editing the `fsaua.cfg` configuration file.

 **Important:** These configuration instructions apply only to the Automatic Update Agent installed with Policy Manager Server. You should only edit the settings mentioned below. Do not edit the other settings in the configuration file.

To configure Automatic Update Agent:

1. Open the `fsaua.cfg` configuration file located in `C:\Program Files\F-Secure\FSAUA\program\fsaua.cfg`.
2. Specify HTTP proxies:

The `http_proxies` directive controls which HTTP proxies are used by Automatic Update Agent. Use the following format:

```
http_proxies=[http://] [[domain\]user[:passwd]@]<address>[:port]
[, [http://] [[domain\]user[:passwd]@]<address>[:port]]
```


Examples:

```
http_proxies=http://proxy1:8080/,http://backup_proxy:8880/,
http://domain\username:usernamepassword@ntlmproxy.domain.com:80
```

3. Specify the polling interval:

The `poll_interval` directive specifies how often Automatic Update Agent checks for new updates. The default is 1800 seconds, which is half an hour.

```
poll_interval=1800
```

 **Note:** If the minimum polling interval defined on the F-Secure update server is, for example, 2 hours, the settings in Automatic Update Agent configuration file cannot override that limitation.

4. Save and close the file.
5. For the changes to take effect, you need to stop and restart the **fsaua** service.

To do this, enter the following commands on the command line:

```
net stop fsaua
net start fsaua
```

5.2.2 How to read the log file

The `fsaua.log` file is used to store messages generated by Automatic Update Agent.

Some of the messages provide information about normal operations, such as startup and shutdown. Other messages indicate errors.

The `fsaua.log` file is located in `C:\Program Files\F-Secure\FSAUA\program`.

Every message in the log contains the following information:

- The date and time the message was generated.

```
[ 3988]Thu Oct 26 12:40:39 2006(3): Downloaded
'F-Secure Anti-Virus Update 2006-10-26_04' -
'DFUpdates' version '1161851933' from
```

```
fsbwsrvr.f-secure.com, 12445450 bytes (download
size 3853577)
```

- A brief explanation of what happened. When an update is downloaded, the update name and version are shown.

```
[ 3988]Thu Oct 26 12:40:39 2006(3): Downloaded
'F-Secure Anti-Virus Update 2006-10-26_04' -
'DFUpdates' version '1161851933' from
fsbwsrvr.f-secure.com, 12445450 bytes (download
size 3853577)
```

- For updates, the message also shows the update source and the size of the download.

```
[ 3988]Thu Oct 26 12:40:39 2006(3): Downloaded
'F-Secure Anti-Virus Update 2006-10-26_04' -
'DFUpdates' version '1161851933' from
fsbwsrvr.f-secure.com, 12445450 bytes (download
size 3853577)
```

Messages in fsaua.log

Below are examples of some messages that you can find in the log file.

Message	Meaning
Update check completed successfully	The connection to the update source was successful.
Update check completed successfully. No updates are available.	The connection to the update source was successful, but there was nothing new to download.
Downloaded 'F-Secure Anti-Virus Update 2006-10-26_04' - 'DFUpdates' version '1161851933' from fsbwsrvr.f-secure.com, 12445450 bytes (download size 3853577)	The connection was successful and some files were downloaded.
Installation of 'F-Secure Anti-Virus Update 2006-10-26_04' : Success	The files were successfully placed into the destination directory (and the existing files were removed). Note that Automatic Update Agent is not able to display whether the new files have been taken into use by the host(s) or not.
Update check failed. There was an error connecting fsbwsrvr.f-secure.com (DNS lookup failure)	An error message indicating that the update check failed.

How to check from the log that everything works?

When everything works the way it should, the last installation result for each downloaded update should be shown as **Success**. For example:

```
Installation of 'F-Secure Anti-Virus Update 2006-10-26_04' : Success
```

You can also see a summary of the virus, spyware and DeepGuard update statuses on the server on the **Summary** tab in Policy Manager Console.

To check the update status on a centrally managed host, go to the **Status > Overall Protection** page in Policy Manager Console.

5.3 Forcing Automatic Update Agent to check for new updates immediately

If you need to force Automatic Update Agent to check for new updates immediately, you can do so in the Automatic Update Agent interface.

To do this:

1. Select **Start > Programs > F-Secure Policy Manager > F-Secure Automatic Update Agent** to open the Automatic Update Agent application interface.
2. Click **Check now** to check if any updates are currently available.
The **Communication** line will indicate the current update status.

5.4 Updating the databases manually

If your computer is not connected to the Internet, you can update the databases manually.

1. Connect to http://www.f-secure.com/en/web/labs_global/removal-tools/-/carousel/view/140 from another computer.
2. Download the update tool listed in the steps for manually updating the databases.
3. Transfer the update tool to your computer, for example by using a memory stick or other removable media, and run it.

5.5 Troubleshooting

Below are some examples of problems that may be logged as error messages in the `fsaua.log` file.

Problem	Reason	Solution
There was a DNS lookup failure, or connection failed, was lost or refused.	Network problems	Check that the network is configured correctly.
Proxy Authentication failed.	The password entered for HTTP proxy is incorrect.	Check and correct the HTTP proxy password in the <code>http_proxies</code> directive in the <code>fsaua.cfg</code> file.
The disk is full or there was an IO error.	There is not enough free disk space on the drive where the destination directory is located.	Free some disk space to enable the update.
There was a server error or an unspecified error.	Unknown	-

Using the product on Linux

Topics:

- [Overview](#)
- [Installation](#)
- [Uninstalling the product](#)
- [Frequently asked questions](#)

Policy Manager can also be installed on Linux.

Policy Manager works the same way on Linux as on Windows, although some functionality is not available, and the installation procedure is different.

6.1 Overview

Here you will find some general information about using and installing the product on Linux.

Differences between Windows and Linux

Services not available when Policy Manager Console is running on Linux:

- Push installation features,
- Windows installer package (MSI) export,
- Autodiscovery of workstations on the network.

Supported distributions

Policy Manager supports many of the Linux distributions based on the Debian package management (DEB) system and on the Redhat Package Management (RPM) system. Both 32-bit and 64-bit versions of the distributions are supported.

Supported distribution	Packaging system
Red Hat Enterprise Linux 5 and 6	RPM
CentOS 6	RPM
SUSE Linux Enterprise Server 10 and 11	RPM
SUSE Linux Enterprise Desktop 11	RPM
openSUSE 12	RPM
Debian GNU Linux 6 and 7.2 (Wheezy)	DEB
Ubuntu 10.04, 12.04, 14.04	DEB

6.2 Installation

Policy Manager is installed in three parts.

The product components must be installed in the following order:

1. Automatic Update Agent
2. Policy Manager Server
3. Policy Manager Console

Policy Manager Server and Automatic Update Agent must be installed on the same computer.

Policy Manager Console can be installed on the same or a separate computer.



Note: When upgrading from a previous version of Policy Manager where Web Reporting has been installed, you must first uninstall Web Reporting before upgrading Policy Manager Server.



Note: For more details on the installation process and on upgrading from a previous version of Policy Manager, see the release notes.

Installation notes

Red Hat and Suse distributions:

- Some platforms require the `libstdc++` compatibility library. Install the following packages before installing Policy Manager Server:
 - For Red Hat Enterprise Linux 5 and 6, install the `compat-libstdc++-33` package.
 - For 32-bit openSuse 11, install the `libstdc++33` package.

- For 64-bit openSuse 11, install the `libstdc++33` and `libstdc++33-32bit` packages.
- When installing Policy Manager Server and Policy Manager Console on a 64-bit platform, you need to use the 64-bit version of the installation packages.

Debian and Ubuntu distributions:

- Policy Manager Server requires the `libstdc++` compatibility library. Install the `libstdc++5` package before installing Policy Manager Server. If installation was not completed because the compatibility library was not found, install the library and then use the `apt-get install -f` command to complete installing the product.
- When installing Policy Manager Server and Policy Manager Console on a 64-bit platform, you need to use the 64-bit version of the installation packages. In addition:
 - Install the `ia32-libs` package with runtime libraries for the ia32/i386 architecture before installing Policy Manager Server.
 - Install the Automatic Update Agent package with the `--force-architecture` option specified.

6.2.1 Install Automatic Update Agent and Policy Manager Server

The first step is to install F-Secure Automatic Update Agent and Policy Manager Server.

1. Log in as `root`.

If you are installing the product on an Ubuntu distribution, you should log in as a normal user that has been added to `/etc/sudoers`.

2. Open a terminal.

3. To install, enter the following commands:

Distribution type	Command
Debian-based distributions	<pre>dpkg -i f-secure-automatic-update-agent_<version_number>.<build number>_i386.deb dpkg -i f-secure-policy-manager-server_<version_number>.<build number>_i386.deb</pre>
RPM-based distributions	<pre>rpm -i f-secure-automatic-update-agent-<version_number>.<build number>-1.i386.rpm rpm -i f-secure-policy-manager-server-<version_number>.<build number>-1.i386.rpm</pre>
Ubuntu distributions	<pre>sudo dpkg -i f-secure-automatic-update-agent_<version_number>.<build number>_i386.deb sudo dpkg -i f-secure-policy-manager-server_<version_number>.<build number>_i386.deb</pre>

4. To configure, type `/opt/f-secure/fspms/bin/fspms-config` and answer the questions.

For Ubuntu distributions, type `sudo /opt/f-secure/fspms/bin/fspms-config`.

Press Enter to choose the default setting (shown in square brackets).

5. Log in as a normal user and enter the following commands to check the status of the components:

- `/etc/init.d/fsaua status`
- `/etc/init.d/fspms status`

Alternatively, you can open your browser and go to the following URLs:

- <http://localhost> - Policy Manager Server status
- <http://localhost/B> - Automatic Update Server status
- <http://localhost:8081> - Web Reporting status

Once the configuration script is finished, Automatic Update Agent and Policy Manager Server are running and will start automatically whenever the computer is restarted.

6.2.2 Install Policy Manager Console

Next, you need to install Policy Manager Console.

1. Log in as `root`.

If you are installing the product on an Ubuntu distribution, you should log in as a normal user that has been added to `/etc/sudoers`.

2. Open a terminal.

3. To install type:

Distribution type	Command
Debian-based distributions	<pre>dpkg -i f-secure-policy-manager-console_<version_number>.<build number>_i386.deb</pre>
RPM-based distributions	<pre>rpm -i f-secure-policy-manager-console-<version_number>.<build number>-1.i386.rpm</pre>
Ubuntu distributions	<pre>sudo dpkg -i f-secure-policy-manager-console_<version_number>.<build number>_i386.deb</pre>

Policy Manager Console is installed to `/opt/f-secure/fspmc/`. A new user group called `fspmc` is created automatically.

4. Add users to the `fspmc` user group.

This needs to be done before they can run Policy Manager Console:

- a) Check which groups the user belongs to:

```
groups <user id>
```

For example, if the user is Tom:

```
groups Tom
```

- b) Add this user to the `fspmc` group:

```
/usr/sbin/usermod -G fspmc,<groups the user belongs to now (as comma
separated list)> <user id>
```

For example, if Tom belongs to the groups `normal_users` and `administrators` the command is:

```
/usr/sbin/usermod -G fspmc,normal_users,administrators Tom
```



Note: The comma separated group list will replace whatever groups the user previously belonged to.

5. Select Policy Manager Console from the F-Secure submenu in the **Programs** menu.

You can also start Policy Manager Console from the command line by entering `sg fspmc -c /opt/f-secure/fspmc/fspmc`.

The first time Policy Manager Console is started, you will be prompted to answer a few questions to complete the configuration. These questions are the same as for the Windows version.

6.3 Uninstalling the product

To uninstall Policy Manager on Linux, you must uninstall the components in a set order.

You must uninstall the three components in this order:

1. Policy Manager Server
2. Automatic Update Agent
3. Policy Manager Console

1. Log in as `root`.

If the product is installed on an Ubuntu distribution, you should log in as a normal user that has been added to `/etc/sudoers`.

2. Open a terminal.

3. Enter the following commands in the given order:

Distribution type	Command
Debian-based distributions	<ol style="list-style-type: none"> 1. <code>dpkg -r f-secure-policy-manager-server</code> 2. <code>dpkg -r f-secure-automatic-update-agent</code> 3. <code>dpkg -r f-secure-policy-manager-console</code>
RPM-based distributions	<ol style="list-style-type: none"> 1. <code>rpm -e f-secure-policy-manager-server</code> 2. <code>rpm -e f-secure-automatic-update-agent</code> 3. <code>rpm -e f-secure-policy-manager-console</code>
Ubuntu distributions	<ol style="list-style-type: none"> 1. <code>sudo dpkg -r f-secure-policy-manager-server</code> 2. <code>sudo dpkg -r f-secure-automatic-update-agent</code> 3. <code>sudo dpkg -r f-secure-policy-manager-console</code>



Note: To prevent accidentally deleting irreproducible data created by Policy Manager components, for example log files, MIB files, the domain tree, policies, configuration files and preferences, the uninstallation process will not remove the directories listed below. Do not delete keys that may be needed in the future. If you want to completely remove the product, log in as `root` and enter the following commands:

```
rm -rf /var/opt/f-secure/fspms
rm -rf /var/opt/f-secure/fsaus
rm -rf /etc/opt/f-secure/fspms
rm -rf /etc/opt/f-secure/fsaus
rm -rf /opt/f-secure/fspmc
```

6.4 Frequently asked questions

You can find answers to common problems here.

Question	Answer
Where are the log files and configuration files located in the Linux version?	<p>You can list all files and their places by entering the following commands as a normal user:</p> <ul style="list-style-type: none"> • RPM-based distributions: <code>rpm -ql f-secure-<component_name></code>. • Debian-based distributions: <code>dpkg -L f-secure-<component_name></code>. <p>You will find the log files in the following locations:</p>

Question	Answer
	<ul style="list-style-type: none"> • Policy Manager Console: <code>/opt/f-secure/fspmc/lib/Administrator.error.log</code> • Automatic Update Agent logs runtime errors, warnings and other information via <code>syslog</code>, which is typically in <code>/var/log/messages</code> • Policy Manager Server: <code>/var/opt/f-secure/fspms/logs</code> and <code>/var/opt/f-secure/fsaus/log</code>. <p>You will find the configuration files in the following locations:</p> <ul style="list-style-type: none"> • Policy Manager Console: <code>/opt/f-secure/fspmc/lib/Administrator.properties</code> • Automatic Update Agent: <code>/etc/opt/f-secure/fsaua/fsaua_config</code> • Policy Manager Server: <code>/etc/opt/f-secure/fspms/fspms.conf</code>.
Why are the files located so unusually?	<p>All files for Policy Manager have their own location according to the File Hierarchy Standard. For more information on FHS, go to http://www.pathname.com/fhs/.</p>
Why doesn't Policy Manager Server start?	<p>Make sure you have run the configuration script: <code>/opt/f-secure/fspms/bin/fspms-config</code>.</p> <p>You can also check that the ports configured for Policy Manager Server are active by logging in as <code>root</code> and running the <code>netstat -lnpt</code> command.</p>
How can I start, stop, restart or check the status of Policy Manager components?	<p>Automatic Update Agent: <code>/etc/init.d/fsaua {start stop restart status}</code></p> <p>Policy Manager Server: <code>/etc/init.d/fspms {start stop restart status}</code></p>
How can I specify an HTTP proxy?	<p>You can run the configuration script <code>/opt/f-secure/fsaua/bin/fsaua-config</code> or edit the configuration file manually. The directive is <code>http_proxies=http://address:port/</code>.</p> <p>Remember to restart Automatic Update Agent in order to take the new settings into use.</p>
How can I change the default ports (80 and 8080) in which Policy Manager Server listens for requests?	<p>These ports are configured with the configuration script: <code>/opt/f-secure/fspms/bin/fspms-config</code>.</p>
How can I change the default port (8081) in which Web Reporting listens for requests?	<p>The Web Reporting port is configured with the Policy Manager Server configuration script: <code>/opt/f-secure/fspms/bin/fspms-config</code>.</p>

Question	Answer
Can I set up my own schedule for updating F-Secure virus definitions?	<p>Yes. Automatic updates are achieved by using the operating system's own scheduling daemon, <code>cron</code>. Just edit or add your own scheduling entry to the <code>/etc/crontab</code> file.</p> <p>For example, to schedule virus definitions updates for every 10 minutes, add this line to <code>/etc/crontab</code>:</p> <pre>*/10 * * * * fspms /opt/f-secure/fspms/bin/fsavupd</pre> <p>For more on configuring automatic updates using <code>cron</code>, see <code>man cron</code> and <code>man 5 crontab</code>. In most of the cases you can configure the scheduled updating of F-Secure virus definitions with the <code>/opt/f-secure/fspms/bin/fspms-config</code> command.</p>
How can I update F-Secure virus definitions manually?	<p>Log in as an <code>fspms</code> user and run the updating tool by typing:</p> <pre>sudo -u fspms /opt/f-secure/fspms/bin/fsavupd --debug</pre> <p>The optional <code>--debug</code> flag forces more verbose diagnostic messages.</p>
How can I publish F-Secure virus definitions manually from the latest <code>fsdbupdate</code> package?	<p>Download the latest <code>fsdbupdate.run</code> tool from http://download.f-secure.com/latest/fsdbupdate.run. Log in as <code>root</code> and run this tool:</p> <pre>./fsdbupdate.run</pre> <p>This will update all databases in Automatic Update Agent. After this, you need to publish these updates to the Update Server and Policy Manager Server by either having <code>fsavupd</code> scheduled in <code>crontab</code> or by manually running the <code>fsavupd</code> command:</p> <pre>sudo -u fspms /opt/f-secure/fspms/bin/fsavupd</pre>
Is there any diagnostic tool I can use?	<p>Yes. Please use <code>fsdiag</code> to collect information about your system and related packages. When logged in as <code>root</code>, run:</p> <pre>/opt/f-secure/fspms/bin/fsdiag</pre> <p>All relevant information will be stored into the <code>fsdiag.tar.gz</code> archive located in the current directory. You can then send that file to F-Secure Customer Support by request.</p>
I get the warning <code>...Another Automatic Update Server was found...</code> during startup. What should I do?	<p>1. Check if another Automatic Update Server is running and still using the TCP sockets:</p> <pre>netstat -anp grep bwserver</pre>

Question	Answer
	<pre>ps axuww grep bwserver</pre> <p>2. Stop the other Automatic Update Server by running:</p> <pre>kill `pidof bwserver`</pre> <pre>kill -9 `pidof bwserver`</pre> <p>3. Restart Policy Manager Server:</p> <pre>/etc/init.d/fspms stop</pre> <pre>rm -f /var/lock/subsys/fsaus</pre> <pre>/var/run/fsaus.pid</pre> <pre>/etc/init.d/fspms start</pre>
<p>How can I install software to remote hosts from Policy Manager Console on Linux?</p>	<p>You can export installation packages to JAR files and use the <code>ilaunchr.exe</code> tool to install software on hosts, for example by using logon scripts. Please follow the process defined in the manual. You will find the <code>ilaunchr.exe</code> tool in the <code>/opt/f-secure/fspmc/bin</code> directory.</p>
<p>How can I configure Policy Manager for use in large environments?</p>	<ul style="list-style-type: none"> • Increase the Incoming packages polling interval and Outgoing packages update interval values to 30 - 60 minutes in Policy Manager Console. • Use Policy Manager Proxy installation(s) to minimize the load on Policy Manager Server caused by serving database updates to clients.

Web Reporting

Topics:

- [*Generating and viewing reports*](#)
- [*Maintaining Web Reporting*](#)
- [*Web Reporting error messages and troubleshooting*](#)

Web Reporting is a graphical reporting system included in Policy Manager Server.


The detailed graphical reports in Web Reporting allow you to identify computers that are unprotected or vulnerable to virus outbreaks. With Web Reporting, you can quickly create graphical reports based on historical trend data using a web-based interface. You can produce a wide range of useful reports and queries from Client Security alerts and status information sent by Management Agent to Policy Manager Server. You can export the reports into HTML.

In order to view the reports generated by Web Reporting, your computer must have an Internet browser, for example Internet Explorer or Mozilla Firefox.

7.1 Generating and viewing reports

The general types of reports you can generate include, for example, bar and pie graphs of the current security situation, trend reports and detailed list reports.

To view the exact reports and report templates available, select one of the pages (**Virus Protection summary**, **Internet Shield summary**, **Alerts**, **Installed software** and **Host properties**) in the Web Reporting user interface.

 **Note:** Web Reporting uses a HTTPS connection and requires authentication to access reports. Use your Policy Manager Console user name and password to access Web Reporting.

7.1.1 Generating a report

With Web Reporting, you can quickly create graphical reports based on historical trend data using a web-based interface.

You can generate a web report as follows:

1. Open the Web Reporting main page.
2. Enter the name or IP address of the Policy Manager Server followed by the Web Reporting port (separated by a colon) in your browser.
For example, `fspms.example.com:8081`.
Alternatively, if you are accessing Web Reporting locally, you can access Web Reporting from the **Start** menu: **Start > F-Secure Policy Manager Server > Web Reporting**.
3. Wait until the Web Reporting page opens.
In large environments this can take a lot of time.
When the Web Reporting page opens, it displays a default report for the currently selected report category. **Root** is selected by default in the **Policy domains** tree.
4. To view a new report, first select the domain, subdomain or host for which you want to generate the report.
5. Select a report category (**Virus Protection summary**, **Internet Shield summary**, **Alerts**, **Installed software** and **Host properties**) and the exact report to be generated.
6. Wait until the report is displayed in the lower part of the main window.

7.1.2 Scheduling reports


You can configure Web Reporting to send regular reports by e-mail to one or more recipients.

To send the reports by e-mail, you need to enter the mail server details in Policy Manager Console. To do this:

1. Select **Tools > Server configuration** and click the **Mail** tab.
2. Enter the mail server address and authentication information.
3. Enter the address that you want to display as the sender in the report e-mails. This does not have to be a valid e-mail address.
4. Click **OK**.

To configure the report scheduling:

1. On the Web Reporting main page, select **Scheduled reporting**.
2. On the policy domain tree, select the domain that you want to use for the reports.

 **Note:** You cannot schedule reports for individual hosts, only for domains. You can use the root domain if you want the reports to cover all configured domains.

3. In the **Recipient e-mails** field, enter the e-mail addresses that should receive the reports.
Use semi-colons to separate multiple addresses.
4. Choose whether to send the reports daily, weekly or monthly.

a) If you want to send the reports on a weekly basis, select the weekday.

If you choose to send the reports on a monthly basis, the reports for each month are automatically sent on the first day of the following month.

5. Select which reports you want to send.

The listed recipients will receive the selected reports in HTML format according to your settings.

If you want to check that the report e-mails are delivered correctly, click **Send reports now**.

7.1.3 Creating a printable report

You can also print a generated report.

To get a printable version of the page:

1. Click the **Printable version** link in the upper right corner of the page.

This opens a new browser window with the contents of the main frame in printable format.

2. Print the page with your browser's normal print functionality.

You can also save the report for later use with your browser's **Save as** or **Save page as** options. You should make sure that the **Save** option used saves the complete web page, including images:

- If you are using Microsoft Internet Explorer, select **File > Save** from the menu. When the **Save Web Page** window opens, select **Web Page, complete** from the **Save as Type** drop-down menu.
- If you are using Mozilla, select **File > Save Page As** from the menu.

7.1.4 Automated report generation

You can also save the URL of a printable report to generate automated reports.


When using automated report generation, you do not have to select the report category, report type or policy domain which you want to monitor separately the next time you want to generate the same report, because this information is already included in the report-specific URL address.

You have two possibilities:

- Generate a printable report that includes the selections you want to monitor, and then add a link to that report on your computer (desktop, bookmarks or some other location). The next time you access Web Reporting through this link, the report is regenerated and will contain the latest data.
- You can also save the report you have generated so that you can compare the current situation with the reports you will generate in the future. First generate a printable version of the page and then save the whole page in a browser. This will always show the 'old' report.

7.2 Maintaining Web Reporting

This section covers the most common Web Reporting maintenance tasks.

-  **Note:** Web Reporting is turned on and off during the installation of Policy Manager Server. Restricting access to the local machine is also set during installation. You can turn Web Reporting on or off through the registry or by reinstalling Policy Manager Server.

All Web Reporting data is stored in the H2 database used by Policy Manager Server, so whenever you back up that database, the Web Reporting data is also backed up.

7.3 Web Reporting error messages and troubleshooting

This section covers Web Reporting error messages and Web Reporting database troubleshooting.

7.3.1 Error messages

Common error messages that you may encounter when using Web Reporting are listed here.

- Browser error message: **The connection was refused when attempting to contact <location>**

Your browser could not contact Policy Manager Server at all. The link you have might point to the wrong machine or to the wrong port, Policy Manager Server is not installed on that machine, or the Policy Manager Server service is not running. Check all of these in this order. A firewall may also prevent the connection.

- Error message: **Web Reporting lost its database connection, this may require restarting the Policy Manager Server service.**

If Web Reporting cannot contact the database, you should restart the Policy Manager Server service. If this does not help, you may wish to reinstall Policy Manager Server, keeping the existing database.

7.3.2 Troubleshooting

In general, if Web Reporting does not work, you should try the steps listed here.

Try these steps in the following order:

1. Reload the page.
2. If the problem is caused by all processes not having started yet, wait for a while, and then try to reload the page.
You can also reduce the startup time by deleting unnecessary alerts.
3. Restart the Web Reporting service.
4. Restart Policy Manager Server.
5. Restart the computer.
6. Re-install Policy Manager Server, keeping the existing configuration.
7. If all else fails, reset the Web Reporting database or restore it from a backup copy.

7.3.3 Changing the Web Reporting port

The recommended method for changing the Web Reporting port is to re-run the Policy Manager setup, and change the Web Reporting port there.

You can also change the Web Reporting port by editing the `HKEY_LOCAL_MACHINE\SOFTWARE\Data Fellows\F-Secure\Management Server 5` registry key:

1. Stop Policy Manager Server.
2. Open the `HKEY_LOCAL_MACHINE\SOFTWARE\Data Fellows\F-Secure\Management Server 5` registry key.
3. Edit the `WRPortNum` value and enter the new port number.
Make sure **Decimal** is selected as the **Base** option when entering the new port number.
4. Start Policy Manager Server.

If there is a port conflict, Policy Manager Server will not start, and an error message will be printed in the log file. In this case you should try another, unused port.

Policy Manager Proxy

Topics:

- [Overview](#)

This section provides a brief introduction to Policy Manager Proxy.

In this section, you will find some basic information regarding Policy Manager Proxy.

8.1 Overview

Policy Manager Proxy offers a solution to bandwidth problems in distributed installations of Client Security by significantly reducing load on networks with slow connections.

Policy Manager Proxy caches virus definition database updates retrieved from Policy Manager Server or F-Secure Update Server, and resides in the same remote network as the hosts that use it as a database distribution point. There should be one Policy Manager Proxy in every network that is behind slow network lines. Policy Manager Proxy retrieves virus definition database updates directly from the F-Secure distribution server, and hosts running Anti-virus fetch the updates locally from Policy Manager Proxy. Workstations in the remote offices communicate also with the Policy Manager Server in the main office, but this communication is restricted to remote policy management, status monitoring, and alerting.

Anti-virus mode user interface

Topics:

- [Settings inheritance](#)

This section introduces the Policy Manager **Anti-virus mode** user interface.



Note: Policy Manager also includes another user interface, the **Advanced mode** user interface. It is used to manage products other than Client Security and Anti-virus for Workstations. It is also used when you need to change advanced Client Security settings. You can switch between the modes by selecting **Advanced mode** or **Anti-virus mode** in the **View** menu.

The main components of the **Anti-virus mode** user interface are:

- The **Policy domains** tab that displays the structure of the managed policy domains.
- The management tabs: **Summary**, **Settings**, **Status**, **Alerts**, **Scanning reports**, **Installation** and **Operations** that can be used for configuring and monitoring Client Security installed on hosts as well as for carrying out operations.
- The **Message** view at the bottom of the window that displays informative messages from Policy Manager, for example, when the virus definitions on the server have been updated.

9.1 Settings inheritance





This section explains how settings inheritance works and how inherited settings and settings that have been redefined on the current level are displayed in the user interface.

The settings in Policy Manager Console can either be inherited from a higher level in the policy domain structure, or they may have been changed on the current level. When a locally redefined setting is cleared (by clicking the **Clear** link displayed beside it), the value from a higher domain level or the default value of the setting is re-inherited.

When necessary, setting changes can be disallowed, which means that the users are not allowed to change them. Disallowing user changes always forces the policy: the policy variable overrides any local host value, and the end user cannot change the value as long as the **Disallow user changes** restriction is set. If the settings have not been restricted, users are allowed to change them.

9.1.1 How settings inheritance is displayed on the user interface

The inherited settings and settings that have been redefined on the current level are displayed in a different way on the Policy Manager user interface.

Not inherited	Inherited	Description
		A closed lock means that users cannot change the setting, because user changes have been disallowed. If the lock symbol is blue, the setting has been redefined on the current level. If the lock symbol is grey, the setting is inherited.
		An open lock symbol means that users are allowed to change the setting at the current level. If the lock symbol is blue, the setting has been redefined on the current level. If the lock symbol is grey, the setting is inherited.
Clear		If Clear is displayed beside a setting, it means that the setting has been redefined on the current level and that it can be cleared. When the setting is cleared, the default or inherited value is restored. If nothing is displayed beside a setting, it means that the setting is inherited.
Text boxes		Inherited values are displayed as dimmed (with grey text). Settings that are not inherited are displayed as black text on a white background.

Not inherited	Inherited	Description
Check boxes		Inherited values are displayed as dimmed on a grey background. Values that are not inherited are displayed on a white background.

9.1.2 Locking and unlocking all settings on a page at once

You can choose to lock or unlock all of the settings on a page.

The following links can be used to lock and unlock all settings on a page:

Allow user changes	Unlocks all the settings that have a lock symbol displayed beside them on the current page. After this the users can change these settings.
Disallow user changes	Locks all the settings that have a lock symbol displayed beside them on the current page. After this the users cannot change these settings.
Clear all...	Clears all the settings that have been redefined on the current page and restores the default or inherited values.

9.1.3 Settings inheritance in tables

Settings inheritance is also displayed on tables within the settings pages.

The **Firewall security levels** table and the **Firewall services** table are so-called global tables, which means that all computers in the domain have the same values. However, different subdomains and different hosts may have different security levels enabled.

In tables the default values derived from MIBs are displayed as grey. The values that have been edited on the current level are displayed as black.

Configuring virus and spyware protection

Topics:

- [*Configuring automatic updates*](#)
- [*Configuring real-time scanning*](#)
- [*Configuring DeepGuard*](#)
- [*Configuring rootkit scanning*](#)
- [*Configuring e-mail scanning*](#)
- [*Configuring web traffic \(HTTP\) scanning*](#)
- [*Configuring spyware scanning*](#)
- [*Managing quarantined objects*](#)
- [*Preventing users from changing settings*](#)
- [*Configuring alert sending*](#)
- [*Monitoring viruses on the network*](#)
- [*Testing your antivirus protection*](#)

Virus and spyware protection in Client Security consists of automatic updates, manual scanning, scheduled scanning, real-time scanning, spyware scanning, DeepGuard, rootkit scanning, e-mail scanning and browsing protection.

Virus and spyware protection keeps computers protected against file viruses, spyware, riskware, rootkits and viruses that are spreading by e-mail attachments and in web traffic.

Automatic updates guarantee that virus and spyware protection is always up-to-date. Once you have set up virus and spyware protection and the automatic updates by distributing the settings in a security policy, you can be sure that the managed network is protected. You can also monitor the scanning results and other information the managed hosts send back to Policy Manager Console.

When a virus is found on a computer, one of the following actions will be taken:

- the infected file is disinfected,
- the infected file is renamed,
- the infected file is deleted,
- the infected file is quarantined,
- the user is prompted to decide what action to take with the infected file,
- the infected file or attachment (in e-mail scanning) is reported only, or
- the infected attachment (in e-mail scanning) is either disinfected, removed or blocked.

10.1 Configuring automatic updates


This section explains the different configuration settings available for automatic updates in Policy Manager, and gives some practical configuration examples for hosts with different protection needs.

By following these instructions you can always keep the virus and spyware definitions on hosts up-to-date, and choose the best update source based on user needs.

10.1.1 Configuring automatic updates from Policy Manager Server


When centralized management is used, all hosts can fetch their virus and spyware definition updates from Policy Manager Server.

This is configured as follows:

1. Select **Root** on the **Policy domains** tab.
2. Go to the **Settings** tab and select the **Automatic updates** page.
3. Make sure that **Enable automatic updates** is selected.
4. Make sure that the polling interval defined in **Interval for polling updates from F-Secure Policy Manager** is suitable for your environment.
5. If you want to use HTTP proxies, check that the **Use HTTP proxy** and **HTTP proxy address settings** are suitable for your environment.
6. If you want to enable the system to use Policy Manager Server or the F-Secure update server as a fall back when no Policy Manager Proxy can be accessed, select **Allow falling back to Policy Manager Server if Policy Manager Proxies are inaccessible** or **Allow falling back to F-Secure update server if Policy Manager Proxies are inaccessible** correspondingly.
7. If you want to restrict users from changing these settings, click the lock symbol beside the settings.
8. Click  to distribute the policy.

10.1.2 Configuring Policy Manager Proxy

If the different offices of a company have their own Policy Manager Proxy in use, it is often a good idea to configure the laptops that the user takes from one office to another to use a Policy Manager Proxy as the updates source.

 **Note:** Policy Manager Proxy is a new product, and not to be confused with F-Secure Anti-Virus Proxy.

In this configuration example, it is assumed that the laptops have been imported to one subdomain on the **Policy domains** tab, and that the different offices of the company have their own Policy Manager Proxy, and all of them will be included on the list of Policy Manager Proxy servers.

1. Select the subdomain where you want to use the Policy Manager Proxy on the **Policy domains** tab.
2. Go to the **Settings** tab and select the **Automatic updates** page.
3. Make sure that **Enable automatic updates** is selected.
4. Click **Add** to add new servers to the list of available proxy servers.
This opens the **Policy Manager Proxy server properties** window.
5. Enter a priority number for the Policy Manager Proxy in the **Priority** text box.
The priority numbers are used to define the order in which the hosts try to connect to the Policy Manager Proxy. Use, for example, 10 for the Policy Manager Proxy in the office where the host is normally located, and 20, 30 and so on for the other proxies.
6. Enter the URL of the Policy Manager Proxy server in the **Address** text box, then click **OK**.
7. Repeat the above steps to add the other servers to the list.
8. When you have added all proxies to the list, check that they are in the correct order.
If necessary, you can modify their order by altering the priority numbers.
9. If you want to restrict users from changing these settings, click the lock symbols beside the settings.

10. Click  to distribute the policy.



Note: End users can also add a Policy Manager Proxy to the list in the local user interface, and the host uses a combination of these two lists when downloading virus and spyware definitions updates. A Policy Manager Proxy added by an end user is tried before those added by the administrator.

10.1.3 Configuring clients to download updates from each other

You can configure Automatic Update Agent so that updates are downloaded from each other in addition to any existing servers or proxies.

This feature is known as neighborcast. Updates may be downloaded from the following sources:

- A Policy Manager Server
- A Policy Manager Proxy
- An HTTP proxy
- An F-Secure update server
- Another Automatic Update Agent (for example Client Security) with neighborcast enabled.

To enable neighborcast:

1. Select the target domain.
2. Select the **Settings** tab and the **Automatic updates** page.
 - a) To set clients in the selected domain to download updates from other clients, select **Enable Neighborcast client**.
 - b) To set clients in the selected domain to serve updates to other clients, select **Enable Neighborcast server**.
3. To change the port used for neighborcast, enter the new port number in **Neighborcast port**.


10.2 Configuring real-time scanning

Real-time scanning keeps the computer protected all the time, as it is scanning files when they are accessed, opened or closed.

It runs in the background, which means that once it has been set up, it is basically transparent to the user.

10.2.1 Enabling real-time scanning for the whole domain


In this example, real-time scanning is enabled for the whole domain.

1. Select **Root** on the **Policy domains** tab.
2. Go to the **Settings** tab and select the **Real-time scanning** page.
3. Select the **Real-time scanning enabled** check box.
4. Select **Files with these extensions** from the **Files to scan**: drop-down list.
5. Select the action to take when an infected file is found from the **File scanning: Action on infection** drop-down list.
6. Check that the other settings on this page are suitable for your system, and modify them if necessary.
7. Click  to distribute the policy.

10.2.2 Forcing all hosts to use real-time scanning

In this example, real-time scanning is configured so that users cannot disable it; this ensures that all hosts stay protected in any circumstances.


1. Select **Root** on the **Policy domains** tab.
2. Go to the **Settings** tab and select the **Real-time scanning** page.
3. Select the **Real-time scanning enabled** check box.
4. Select **Files with these extensions** from the **Files to scan**: drop-down list.

5. Select the action to take when an infected file is found from the **Custom action on infection** drop-down list.
Alternatively, select **Decide action on infection automatically** to let the product automatically decide what action to take.
6. Check that the other settings on this page are suitable for your system, and modify them if necessary.
7. Click **Disallow user changes** to restrict users from disabling real-time scanning on their computers. Now a closed lock symbol is displayed beside all settings on this page.
8. Click  to distribute the policy.

10.2.3 Excluding Microsoft Outlook's .pst file from real-time scanning

If you have set real-time scanning to scan all files, you might want to exclude Microsoft Outlook's .PST file from the scanning in order not to slow down the system unnecessarily, as PST files are typically very large and take a long time to scan.

The .PST file is excluded from scanning for the whole domain as follows:

1. Select **Root** on the **Policy domains** tab.
2. Go to the **Settings** tab and select the **Real-time scanning** page.
3. Select the **Enable excluded extensions** check box.
4. Enter the extension `PST` in the **Excluded extensions** text box.
Note that the extension should be added without the preceding `.` (dot).
5. If you want to restrict users from changing the settings, click the lock symbol beside the settings.
6. Click  to distribute the policy.

10.3 Configuring DeepGuard

DeepGuard is a host-based intrusion prevention system that analyzes the behavior of files and programs.

DeepGuard can be used to block intrusive ad pop-ups and to protect important system settings, as well as Internet Explorer settings against unwanted changes.

If an application tries to perform a potentially dangerous action, it will be checked for trust. Safe applications are allowed to operate, while actions by unsafe applications are blocked.

When DeepGuard is turned on, you can configure application control in such a way that it asks users what to do only in those cases when DeepGuard does not trust an application.

10.3.1 DeepGuard settings

The settings for DeepGuard, which are displayed on the **Settings > Real-time scanning** page, are described here.

To turn DeepGuard on, select **Enable DeepGuard**.

You can select what to do when a system modification attempt is detected. The following actions are available:

Action	Definition
Always ask permission	DeepGuard asks the users whether they want to allow or block all monitored actions, even when DeepGuard identifies the application as safe.
Ask when case is unclear	DeepGuard asks the users whether they want to allow or block monitored actions only when DeepGuard cannot identify the application as safe or unsafe (default option).

Action	Definition
Automatic: Do not ask	DeepGuard blocks unsafe applications and allows safe applications automatically without asking the user any questions.

If you encounter problems with legitimate programs being blocked by DeepGuard, you can try to clear **Use advanced process monitoring**. For maximal protection, DeepGuard temporarily modifies running programs. Because of this advanced process monitoring, some programs may fail. This happens to programs that check their own integrity.

10.3.2 DeepGuard server queries

DeepGuard server queries provide up-to-date information for detecting malicious programs, and also reduce the number of false positives detected.

Select **Use server queries to improve detection accuracy** to check the F-Secure servers when DeepGuard detects an unknown application. We recommend that you enable server queries for two reasons:

- A computer with server queries enabled has a higher level of protection. There is less time between discovery of a new security threat and protection from that threat.
- A computer with server queries enabled generates noticeably fewer dialogs asking if an unknown process should be allowed to run or not. The user has less chance of making a decision that could compromise the security of their computer. The user is also disturbed from their work less.

What should I know about server queries?

Server queries require access to the Internet to work. If your network allows access only through an HTTP proxy, set the Automatic Update Agent HTTP proxy setting to your proxy server's address to make sure server queries work.

10.4 Configuring rootkit scanning

Rootkit scanning can be used to scan for files and drives hidden by rootkits.

Rootkits are typically used to hide malicious software, such as spyware, from users, system tools and traditional antivirus scanners. The items hidden by rootkits are often infected with viruses, worms or trojans.

10.4.1 Launching a rootkit scan for the whole domain

In this example, a rootkit scan is launched for the whole domain.

1. Select **Root** on the **Policy domains** tab.
2. Go to the **Settings** tab and select the **Manual scanning** page.
3. In the **Rootkit scanning** section, make sure that **Enable rootkit scanning** is selected.
4. Select the **Report suspicious items after full computer check** check box.
5. Check that the other settings on this page are suitable, and modify them if necessary.
6. Go to the **Operations** tab, and click the **Scan for viruses and spyware** button.



Note: You have to distribute the policy for the operation to start.

7. Click to distribute the policy.

After the scanning operation on the local hosts has finished, you can see if any rootkits were detected from **Scan reports** on the **Scanning reports** tab.

10.5 Configuring e-mail scanning


E-mail scanning can be used to keep both inbound and outbound e-mails protected against viruses.

Enabling it for outbound e-mails also ensures that you do not accidentally send out infected e-mail attachments. This section describes the e-mail scanning settings and also presents a practical configuration example.

E-mail scanning scans all POP, IMAP and SMTP traffic. If SSL protocol is used, all attachments received through SSL are also scanned as they are stored to the local e-mail cache. All files sent out are also scanned by real-time scanning.

10.5.1 Enabling e-mail scanning for incoming and outgoing e-mails

In this example, e-mail scanning is enabled for both incoming and outgoing e-mails.

1. Select **Root** on the **Policy domains** tab.
2. Go to the **Settings** tab and select the **E-mail scanning** page.
3. Configure incoming e-mail scanning:
 - a) Select **Enable incoming e-mail scanning**.
 - b) Select the action to take from the **Action on incoming infected attachment** drop-down list.
 - c) Select the action take from the **Action on scanning failure** drop-down list.
 - d) Select the action to take from the **Action on malformed message parts** drop-down list.
4. Configure outgoing e-mail scanning:
 - a) Select **Enable outgoing e-mail scanning**.
 - b) Select the action to take from the **Action on outgoing infected attachment** drop-down list.
 - c) Select the action take from the **Action on scanning failure** drop-down list.
 - d) Select the action to take from the **Action on malformed message parts** drop-down list.
5. Check the **General settings**.
Check that the other settings on this page are suitable for your system, and modify them if necessary.
6. Click  to distribute the policy.

10.6 Configuring web traffic (HTTP) scanning


Web traffic scanning can be used to protect the computer against viruses in HTTP traffic.

When enabled, web traffic scanning scans HTML files, image files, downloaded applications or executable files and other types of downloaded files. It removes viruses automatically from the downloads. You can also enable a notification flyer that is shown to the end-user every time web traffic scanning has blocked viruses in web traffic and downloads.

This section describes the web traffic scanning settings and also presents some practical configuration examples.

10.6.1 Enabling web traffic scanning for the whole domain

In this example, HTTP scanning is enabled for the whole domain.

1. Select **Root** on the **Policy domains** tab.
2. Go to the **Settings** tab and select the **HTTP scanning** page.
3. Select the **Enable HTTP scanning** check box.
4. Make sure that the **Action on infection** is set to **Block**.
5. Make sure that the **Action on scanning failure** is set to **Block**.
6. Check that the other settings on this page are suitable for your system, and modify them if necessary.
7. Click  to distribute the policy.

10.6.2 Excluding a web site from HTTP scanning

You can exclude a web site or certain web pages from HTTP scanning by defining them in the **Trusted sites** table.

Excluding a web site might be a good idea, for example, if the site contains unrecognizable streaming content, which may cause the user to experience unwanted delays (see download time-out setting).


In this configuration example, one whole domain (www.example.com) and a sub-directory from another domain (www.example2.com/news) are excluded from HTTP scanning.

1. Select **Root** on the **Policy domains** tab.
2. Go to the **Settings** tab and select the **Web traffic scanning** page.
3. Exclude a domain from HTTP scanning:

To exclude an entire domain from HTTP scanning, enter the URL of the domain in the **Trusted sites** table as follows:

 - a) Click the **Add** button under the **Trusted sites** table.
This creates a new line in the table.
 - b) Click on the line you just created so that it becomes active, and enter `http://*.example.com/*`.
This excludes all the sub-domains.
 - c) Click the **Add** button under the **Trusted sites** table.
This creates another new line in the table.
 - d) Click on the line you just created so that it becomes active, and enter `http://example.com/*`.
This excludes the second-level domain.
4. Exclude a sub-directory from HTTP scanning:

To exclude a sub-directory from HTTP scanning, enter the URL of the domain with the directory path in the **Trusted sites** table as follows:

 - a) Click the **Add** button under the **Trusted sites** table.
This creates a new line in the table.
 - b) Click on the line you just created so that it becomes active, and enter `http://www.example2.com/news/*`.
5. Click  to distribute the policy.

10.7 Configuring spyware scanning

Spyware scanning protects the hosts against different types of spyware, such as data miners, monitoring tools and dialers.

In centrally managed mode, spyware scanning can be set, for example, to report the spyware items found on hosts to the administrator or to quarantine all found spyware items automatically. It is also possible to allow the use of certain spyware applications by specifying them as allowed spyware on the Spyware Control page.

A note about cleaning spyware and riskware

Spyware is a gray area between a fully legitimate application and a virus/trojan. Some spyware may be necessary to run ordinary applications, while most spyware is just malware and should not be allowed to run even once. By default, spyware scanning is configured to allow all spyware to run. You can check whether you need to allow some spyware to run on your network before you tighten the security and prevent all new spyware from executing.

Spyware scanning also detects and reports riskware. Riskware is any program that does not intentionally cause harm but can be dangerous if misused, especially if set up incorrectly. Examples of such programs are chat programs (IRC), or file transfer programs.

10.7.1 Setting up spyware control for the whole domain

This example explains how to set up spyware control in such a way that it is transparent to the end-users and that it protects them against spyware and tracking cookies.

When you are setting up spyware control for the first time, you should first use a small test environment that consists of hosts that have the applications normally used in your company installed on them. At this phase you can also allow certain applications, if that is necessary. After the testing phase you can distribute the policy to the whole managed domain.

Spyware control also detects riskware. Riskware is any program that does not intentionally cause harm but can be dangerous if misused, especially if set up incorrectly. Examples of such programs are chat programs (IRC), or file transfer programs. If you want to allow the use of these programs in the managed domain, you should include them in the test environment and allow their use when you are checking and configuring rules for the applications in **Spyware and riskware reported by hosts** table.

1. Create a test domain and enable spyware scanning:

- a) Create a test environment with a few computers that have the programs normally used in your company installed.
- b) Import these hosts to the centrally managed domain.
- c) Go to the **Settings** tab and select the **Real-time scanning** page.
- d) Make sure that **Real-time scanning enabled** is selected.

Alternatively, you can launch a manual spyware scan on the hosts.

- e) Click  to save and distribute the policy.

2. Check the reported spyware and riskware:

A list of the spyware and riskware found during the scanning is displayed in the **Spyware and riskware reported by hosts** table. This table is shown on the **Spyware control** page.

- a) Check the list of reported spyware and riskware.
- b) If there are applications that are needed in your organization, select the application in the table and click **Exclude application**.

A dialog asking you to confirm the action is opened.

- c) Check the information displayed in the dialog, and if you are sure you want to allow the spyware or riskware to run on the host or domain, click **OK**.

The selected application will be moved into the **Applications excluded from spyware scanning** table.

3. If you want to make sure that users cannot allow any spyware or riskware to run on their computers, set **Allow users to define the allowed spyware items is set to **Not allowed**.**

4. Check that the manual scanning settings are valid for the managed domain.

- 5. Click  to distribute the policy.**

10.7.2 Launching spyware scanning in the whole domain

In this example, a manual scan is launched in the whole domain.

This will partially clean out the **Spyware and riskware reported by hosts** table.

1. Select **Root on the **Policy domains** tab.**

2. As the manual scanning task also includes manual virus scanning, check the settings on the **Manual scanning page, and modify them if necessary.**

3. Go to the **Operations tab, and click the **Scan for viruses and spyware** button.**




Note: You have to distribute the policy for the operation to start.

- 4. Click  to distribute the policy.**

10.7.3 Allowing the use of a spyware or riskware component


In this example, the use of a spyware or riskware component that was found during the spyware scanning is allowed for one host.

1. On the **Policy domains** tab, select the host for which you want to allow the use of spyware or riskware.
2. Go to the **Settings** tab and select the **Spyware control** page.
3. Select the spyware component you want to allow on the **Spyware and riskware reported by hosts** table, and click **Exclude application**.
A dialog asking you to confirm the action opens.
4. Check the information displayed in the dialog, and if you are sure you want to allow the application to run on the host or domain, click **OK**.
The selected application will be moved to the **Applications excluded from spyware scanning** table.
5. Click  to distribute the policy.

10.8 Managing quarantined objects


Quarantine management gives you the possibility to process objects that have been quarantined on host machines in a centralized manner.

All infected files and spyware or riskware that have been quarantined on host machines are displayed on the **Settings > Quarantine management** page. From there, you can either release the objects from quarantine, or delete them.

 **Note:** Quarantine management should be used primarily for troubleshooting purposes. For example, if a business-critical application is considered riskware and it has not yet been included in the virus definition database, you can use quarantine management to allow it to be used. Such cases are relatively rare, and once new virus definition updates that treat the application as normal are available, the problem should be fixed automatically.

10.8.1 Deleting quarantined objects

Infected files, spyware or riskware that have been quarantined on hosts can be removed from quarantine, in which case they are deleted from the host machine.

1. Select the target domain.
2. Go to the **Settings** tab and select the **Quarantine management** page.
3. Select the quarantined object you want to delete on the **Quarantined objects** table, and click **Delete**.
The object is moved to the **Actions to perform on quarantined objects** table, with **Delete** given as the **Action** for the object.
4. Click  to distribute the policy.

10.8.2 Releasing quarantined objects


Infected files, spyware or riskware that have been quarantined on hosts can be released from quarantine, in which case they are allowed on the host machines and can be accessed and run normally.

1. Select the target domain.
2. Create an exclusion rule for the object.
Exclusion rules are required to make sure that the object will not be quarantined again in future. If the object is listed as a virus or infected file:
 - a) Go to the **Settings > Quarantine management** page and copy the object's file path.
 - b) Go to the **Settings > Real-time scanning** page.
 - c) Right-click **Enable excluded objects** and select **Locate in advanced mode** from the context menu.
This will open the **Advanced mode** user interface.
 - d) On the **Policy** tab, select **Excluded Objects**.
 - e) Click **Add** and enter the file path for the quarantined object.

- f) Select **View > Anti-virus mode** from the menu to return to the **Anti-virus mode** user interface, and make sure that **Enable excluded objects** is selected on the **Settings > Real-time scanning** page.

If the object is spyware or riskware:

- a) Go to the **Settings > Spyware control** page.
- b) Select the object you want to allow on the **Spyware and riskware reported by hosts** table and click **Exclude application**.
A dialog asking you to confirm the action opens, after which the selected application will be moved to the **Applications excluded from spyware scanning** table.

3. Go to the **Settings** tab and select the **Quarantine management** page.
4. Select the quarantined object you want to allow on the **Quarantined objects** table, and click **Release**.
The object is moved to the **Actions to perform on quarantined objects** table, with **Release** given as the **Action** for the object.
5. Click  to distribute the policy.

10.9 Preventing users from changing settings


If you want to make sure that the users cannot change some or any of the virus protection settings, you can make these settings final.

There are different possibilities for doing this:

- If you want to prevent users from changing a certain setting, click on the lock symbol beside it.
- When you are on one of the pages on the **Settings** tab, you can set all the settings on the page final at once by clicking **Disallow user changes**. This page-specific shortcut affects only the settings that have an attached lock symbol and it operates all lock symbols on the page at once.
- If you want to make all settings for both virus protection and Internet Shield final, go to the **Settings** tab and **Centralized management** page, and click **Do not allow users to change any settings....**
This operation also makes the **Advanced mode** settings final.

10.9.1 Setting all virus protection settings as final

In this example, all the virus protection settings are set as final.

1. Select **Root** on the **Policy domains** tab.
2. Go to the **Settings** tab and select the **Automatic updates** page.
3. Check that all the settings on this page are defined as they should be.
4. Click **Disallow user changes**.
All settings on this page are now marked as final.
5. Select the **Real-time scanning** page.
6. Check that all the settings on this page are defined as they should be.
7. Click **Disallow user changes**.
8. Select the **Manual scanning** page.
9. Check that all the settings on this page are defined as they should be.
10. Click **Disallow user changes**.
11. Select the **E-mail scanning** page.
12. Check that all the settings on this page are defined as they should be.
13. Click **Disallow user changes**.
14. Click  to distribute the policy.

10.10 Configuring alert sending

This section describes how to configure the product to send Client Security virus alerts to an e-mail address and how to disable the alert pop-ups.

It is a good idea to have all virus alerts sent to administrators by e-mail to ensure that they are informed of any potential outbreaks as quickly as possible.

10.10.1 Setting Client Security to send virus alerts to an e-mail address

In this example, all the security alerts that the managed Client Security clients generate are forwarded to an e-mail address.

1. Select **Root** on the **Policy domains** tab.

2. Go to the **Settings** tab and select the **Alert sending** page.

3. Set up **E-mail alert sending**:

If e-mail alert sending has not been set up before, you can do it now, as follows:

a) Enter the address of the SMTP server in the **E-mail server address (SMTP)** field.

Use the following format:

`<host>[:<port>]` where `host` is the DNS name or IP address of the SMTP server, and `port` is the SMTP server port number.

b) Enter the sender's address for e-mail alert messages in the **E-mail sender address (From):** field.

c) Enter the e-mail alert message subject in the **E-mail subject:** field.

Refer to the MIB help text for a list of possible parameters to use in the message subject.

4. Set up **Alert forwarding**:

The **Alert forwarding** table is used to configure where different types of alerts are forwarded.

a) Select the **E-mail** check box on the **Security alert** row.

This opens the **E-mail recipient addresses (To)** dialog box.

b) Select **Use the same address for all products**, and enter the e-mail address in the field that is activated.

If you want the alerts to be sent to several e-mail addresses, separate them by commas.

c) When finished, click **OK**.

5. Click  to distribute the policy.

10.10.2 Disabling Client Security alert pop-ups

In this example, Client Security alerting is configured so that no alert pop-ups are displayed to users.

1. Select **Root** on the **Policy domains** tab.

2. Go to the **Settings** tab and select the **Alert sending** page.

3. Clear the check boxes for all products in the **Local user interface** column.

4. Click  to distribute the policy.

10.11 Monitoring viruses on the network

Policy Manager offers different ways and levels of detail for monitoring infections on your network.

The best way to monitor whether there are viruses on the network is to check the **Virus protection** section of the **Summary** tab. If it displays new infections, you can access more detailed information by clicking **View hosts' infection status....** It takes you to the **Status** tab and **Virus protection** page, where you can see details of each host's infection status.

You can also check the **Alerts** and **Scanning reports** tabs to see the scanning reports from different hosts.

10.12 Testing your antivirus protection

To test that Client Security operates correctly, you can use a special test file that is detected by Client Security as though it were a virus.

This file, known as the EICAR Standard Anti-Virus Test File, is also detected by several other antivirus programs. You can also use the EICAR test file to test your e-mail scanning. EICAR is the European Institute of Computer Anti-virus Research. The Eicar info page can be found at

<http://www.f-secure.com/v-descs/eicar.shtml>.

You can test your antivirus protection as follows:

1. You can download the EICAR test file from <http://www.f-secure.com/v-descs/eicar.shtml>.

Alternatively, use any text editor to create the file with the following single line in it:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

2. Save this file to any name with a .com extension, for example EICAR.COM.

Make sure that you save the file in the standard MS-DOS ASCII format. Note also that the third character of the extension is an upper-case O, not numeral 0.

3. Now you can use this file to see what it looks like when Client Security detects a virus.

Naturally, the file is not a virus. When executed without any virus protection, EICAR.COM displays the text EICAR-STANDARD-ANTIVIRUS-TEST-FILE! and exits.

Configuring Internet Shield

Topics:

- [*Configuring security levels and rules*](#)
- [*Configuring network quarantine*](#)
- [*Configuring rule alerts*](#)
- [*Configuring application control*](#)
- [*Using alerts to check that Internet Shield works*](#)
- [*Configuring intrusion prevention*](#)

This section provides an overview of Internet Shield and how you can configure it to suit your network.

Internet Shield protects the computers against unauthorized access from the Internet as well as against attacks originating from inside the LAN.

Internet Shield provides protection against information theft, because unauthorized access attempts can be prohibited and detected. It also protects the users against malicious applications and provides a possibility to control network usage and prohibit the use of bandwidth consuming applications.

The firewall component included in the Internet Shield can be used to restrict traffic based on the protocols used. Application control is designed to prevent malicious programs from sending information out of the computer. It can be used to further restrict the traffic based on the applications, the IP addresses and the ports used. The intrusion prevention system stops the malicious packets aimed at open ports in the host.


Internet Shield contains seven predefined security levels, and each of them have a set of pre-configured firewall rules associated with them. Different security levels can be assigned to different users based on, for example, company security policy, user mobility, location and user experience.

11.1 Configuring security levels and rules

This section explains how you can set and select the security levels based on the users' needs.

In the practical configuration examples it is assumed that the managed hosts have been imported into a domain structure where, for example, laptops and desktops are located in their own subdomains.


When enabling a certain security levels for a domain, you should check that the security level is appropriate for that domain. Different domains can have different security levels enabled.

 **Important:** When you change a security level on a host, click the lock symbol next to the setting to make sure that the new security level will be taken into use.


11.1.1 Selecting an active security level for a workstation

In this example, the **Office** security level is set as the active security level for the workstations in the `Desktops/Eng.` subdomain.

To change the Internet Shield security level for the `Desktops/Eng.` subdomain, do as follows:

1. Select the **Desktops/Eng.** subdomain on the **Policy domains** tab.
2. Go to the **Settings** tab and select the **Firewall security levels** page.
You can see the default security level that is currently applied to the policy in the **Internet Shield security level at host** drop-down list.
3. Select **Office** from the **Internet Shield security level at host** drop-down list.
4. To restrict users from changing the setting, click the lock symbol beside it.
5. Click  to distribute the policy.


You can verify that the new security level change has become effective by going to the **Status** tab and selecting the **Overall protection** page.

 **Note:** If the selected security level cannot be used for some reason, the default security level is used instead. The current default security level can be seen in the **Global security levels** table on the **Firewall security levels** page.

11.1.2 Configuring a default security level for the managed hosts

Default security level is a global setting, and it is used only if the otherwise selected security level is disabled.

In this example, the **Office** security level is configured as default for all the hosts in the domain.

1. Select the **Laptops/Eng.** domain on the **Policy domains** tab.
2. Go to the **Settings** tab and select the **Firewall security levels** page.
3. On the **Firewall security levels** table, click the **Default** radio button on the **Office** row.
Policy Manager prompts you to confirm the security level change for all managed hosts.
4. Click **OK**.
5. Click  to distribute the policy.

11.1.3 Adding a new security level for a certain domain only

In this example, a new security level with two associated rules is created.


The new security level is added only for one subdomain and the hosts are forced to use the new security level. This subdomain contains computers that are used only for Internet browsing, and are not connected to the company LAN.

To add a new security level for a certain domain only, you first have to disable that security level on root level, and then enable it again on the appropriate lower level.

Create the new security level

The first step in adding a new security level is to create the new security level.

This is done as follows:

1. Select **Root** on the **Policy domains** tab.
2. Go to the **Settings** tab and select the **Firewall security levels** page.
3. Click **Add** to add a new security level.
This opens the **Security level - Description** dialog box.
4. Enter a name for the new security level, for example, `BrowserSecurity`.
You can also include a description in the **Description:** text box.
5. Click **Finish**.
6. Click  to distribute the policy.

Create rules for the new security level

The next step is to create rules for the new security level.


The associated rules for the new security level are created as follows:

1. Go to the **Firewall rules** page.
2. Select the **BrowserSecurity** Internet Shield security level you just created.
The **Firewall rules** table is empty when this security level is selected, because there are no associated rules yet.
3. Click **Add before** to add a rule that allows outbound HTTP traffic as the first one on the list.
This opens the **Firewall rule** wizard.
4. Complete the **Firewall rule** wizard:
 - a) On the **Rule type** page select **Allow** as the rule type.
 - b) On the **Remote hosts** page select **Any remote host** to apply the rule to all Internet connections.
 - c) On the **Services** page select **HTTP** in the **Service** column to apply the rule to HTTP traffic.
 - d) On the **Services** page select **=>** in the **Direction** column to apply the rule to outbound connections only.
 - e) On the **Advanced settings** page you can accept the default values.
 - f) Verify the new rule on the **Summary** page.
You can also add a descriptive comment for the rule; for example, `Allow outbound HTTP traffic for browsing..`
 - g) Click **Finish**.
5. Click **Add after** to add a rule that denies all other traffic both ways as the last one on the list.
6. Complete the **Firewall rule** wizard:
 - a) On the **Rule type** page select **Deny** as the rule type.
 - b) On the **Remote hosts** page select **Any remote host** to apply the rule to all connections.
 - c) On the **Services** page select **All traffic** in the **Service** column to apply the rule to all traffic.
 - d) On the **Services** page select **Both** in the **Direction** column to apply the rule to inbound and outbound connections.
 - e) On the **Advanced settings** page you can accept the default values.
 - f) Verify the new rule on the **Summary** page.
You can also add a descriptive comment for the rule. For example, `Deny rest.`
 - g) Click **Finish**.

Take the new security level into use

The next step is to take the new security level into use.

To take the new security level into use only in the selected subdomain(s), you first have to turn it off on root level and then turn it on on a lower level in the policy domain hierarchy. This is done as follows:

1. Select **Root** on the **Policy domains** tab.
2. Go to the **Firewall security levels** page.
3. Turn off the **BrowserSecurity** security level by clearing the **Enabled** check box beside it on the **Firewall security levels** table.
4. On the **Policy domains** tab, select the subdomain where you want to use this security level.
5. Turn on the **BrowserSecurity** security level by selecting the **Enabled** check box beside it on the **Firewall security levels** table.
6. Set the new security level as the active security level by selecting it from the **Internet Shield security level at host** drop-down list.
7. Click  to distribute the policy.

11.2 Configuring network quarantine


Network quarantine is an Internet Shield feature that makes it possible to restrict the network access of hosts that have very old virus definitions and/or that have real-time scanning turned off.

The normal access rights of such hosts are automatically restored once the virus definitions are updated and/or real-time scanning is turned on again.

This section describes the network quarantine settings and contains an example of how to enable the network quarantine feature in the managed domain. There is also a short description of how to configure the network quarantine security level by adding new firewall rules.

11.2.1 Turning network quarantine on in the whole domain

You can enable network quarantine for the whole domain by following the steps given here.

1. Select **Root** on the **Policy domains** tab.
2. Go to the **Settings** tab and select the **Firewall security levels** page.
3. Select **Enable network quarantine**.
4. Specify the **Virus definitions age to activate network quarantine**.
5. If you want to restrict the host from accessing the network when real-time scanning is turned off, select **Activate network quarantine on host if real-time scanning is disabled**.
6. Click  to distribute the policy.

11.2.2 Fine-tuning network quarantine

Network quarantine is implemented by forcing hosts to the **Network quarantine** security level, which has a restricted set of firewall rules.

You can add new **Allow** rules to the firewall rules in the **Network quarantine** security level to allow additional network access to hosts in network quarantine. You should not restrict access further as this may cause hosts to lose network connectivity.

11.3 Configuring rule alerts

Internet Shield rule alerts can be used to get notifications if certain types of malware try to access the computers.

It is possible to issue an alert every time a rule is hit or when illegal datagrams are received, which makes it easy to see what kind of traffic is going on in your system.

Proper alerting can only be done by having proper granularity in the security level: have one rule for each type of alert you want. Designing alerting based on broad rules will generate a lot of alerts, and any important information might be lost in large volumes of useless noise.

11.3.1 Adding a new rule with alerting

In this example, a **Deny** rule with alerting is created for inbound ICMP traffic for a certain subdomain, so that an alert is issued when somebody tries to ping the computer.

At the end of this example the rule is tested by pinging one of the computers in the subdomain. This example also describes the different selections you can make when creating new rules with the **Firewall rules** wizard.

Select the rule type and denied service

The first step is to select the rule type and define the denied service.

To do this:

1. Select the subdomain for which you want to create the rule on the **Policy domains** tab.
2. Go to the **Settings** tab and select the **Firewall rules** page.
3. Select the Internet Shield security level for which you want to add the new rule from the **Internet Shield security level being edited** drop-down menu.
Now all the rules that have been defined for this Internet Shield security level are displayed on the table.
4. Click **Add before** to add the new rule as the first one on the list.
This opens the **Firewall rule** wizard.
5. Select **Deny** to deny the inbound ICMP connections.
6. Specify affected hosts.

Choose whether to apply this rule to all connections or to selected connections only. You can either:

- Check the **Any remote host** option to apply the rule to all Internet connections,
- Check the **All hosts on locally connected networks** option to apply the rule to all connections from the local network,
- Check the **Specified remote hosts** option to apply the rule to an IP address, a range of IP addresses or DNS addresses. When this option is selected, you can specify the addresses in the text field below. If you want to enter several addresses or address ranges in the field, separate them by spaces.

For this rule, select **Any remote host**.

7. Choose the denied service and direction for the rule.

Select the service for which this rule will apply, from the list of available services. If you want the rule to apply to all services, select **All** from the top of the list. You can select as many individual services as you want in this window.

For the chosen services, select the direction in which the rule will apply by clicking on the arrow in the **Direction** column. Repeated clicks cycle between the available choices. See the table below for examples.

Direction	Explanation
<=>	The service will be allowed/denied to/from your computer in both directions.
<=	The service will be allowed/denied if coming from the defined remote hosts or networks to your computer.
=>	The service will be allowed/denied if going from your computer to the defined remote hosts or networks.

For this rule, select:

- **ICMP** from the **Service** drop-down list
- **<=** from the **Direction** column.

Define the advanced options

The next step is to define the advanced options for the rule.

To do this:

1. Define whether the rule is applied only when a dial-up link is open by selecting or clearing the check box.
 - a) Define whether the rule is applied only when a dial-up link is open by selecting or clearing the check box.
 - b) Select the alert type in the **Send alert** drop-down list.
For this rule select **Security alert**.
 - c) Select the alert trap to be sent in the **Alert trap** drop-down list.
 - d) Enter a descriptive comment for the alert in the **Alert comment:** field.
 - e) You can accept the default values for the rest of the fields in this window.
2. Select the alert type in the **Send alert** drop-down list.
3. Select the alert trap to be sent in the **Alert trap** drop-down list.
For this rule select **Network event: inbound service denied**.
4. Enter a descriptive comment for the alert in the **Alert comment:** field.
This comment is displayed in the Client Security local user interface.
5. You can accept the default values for the rest of the fields in this window.
6. Review and accept the rule.
You can review your rule now. You can also add a descriptive comment for the rule to help you understand the rule when it is displayed in the **Firewall rules** table. If you need to make any changes to the rule, click **Back** through the rule.
7. If you are satisfied with your new rule, click **Finish**.
Your new rule will be added to the top of the list in the active set of rules on the **Firewall rules** page.

Configure alert forwarding

The next step is to configure alert forwarding for the rule.


To do this:

1. Go to the **Settings** tab and select the **Alert sending** window.
2. In the **Alert forwarding** section make sure that the security alerts are forwarded to Policy Manager Console.
3. If necessary, select the **Security alert** check box in the **Policy Manager Console** column.

Apply and test the new rule

The last step is to take the new rule into use and test it.

To do this:

1. Make sure that you have the correct subdomain selected on the **Policy domains** tab.
2. Select the **Firewall security levels** page on the **Settings** tab.
3. Set the security level for which you created the rule as the active security level by selecting it from the **Internet Shield Security level at host** drop-down list.
4. Click  to distribute the policy.
5. Test the rule you created.
You can test the rule you just created by pinging one of the managed hosts in the subdomain from a computer outside of that domain. When you have done this, you can check that the rule works as follows:
 - a) Select the subdomain for which you created the rule on the **Policy domains** tab.
 - b) Go to the **Summary** tab, and check if any new security alerts are displayed for the domain.
 - c) To see the alert details, click **View alerts by severity**....

This takes you to the **Alerts** tab that displays a detailed list of security alerts.

11.4 Configuring application control

Application control allows for safe browsing and is an excellent defence against malicious computer programs.

Application control is also an excellent tool for fighting trojans and other network malware as it does not allow them to send any information to the network.

Application control rules can be used to define more specific restrictions to network traffic, on top of the restrictions defined in firewall rules. The application permissions cannot be used to allow traffic that has been denied by static firewall rules. However, if you have allowed some network traffic in the static rules, you can use application control to decide whether an application can be allowed to take advantage of the rules or not. In other words, you can create a rule that allows traffic and limit the use of that rule with application control.

When application control is centrally managed, the administrator can decide which programs that access the network can be used in the workstations. In this way it is possible to prevent the use of programs that are against the company security policy, and to monitor which programs the end users really are using.

The basic idea when configuring application control is to allow the necessary applications and deny the rest.

How application control and DeepGuard work together

When application control detects an outbound connection attempt, and when it is set to prompt the user to decide whether to allow or deny the connection, you can set application control to check from DeepGuard whether the connection should be allowed. This reduces the amount of application control pop-ups shown to users.

An example:


1. If there is a rule for the application that tries to open an outbound connection in the **Application Rules for Known Applications** table, application control allows or denies the connection attempt based on this rule.
2. If there is no rule for the application in the **Application Rules for Known Applications** table, application control allows or denies the connection attempt based on the currently defined **Default action for client applications**.
3. If the currently specified default action is **Prompt for user decision**, and if the **Do not prompt for applications that DeepGuard has identified** setting is turned on, application control checks from DeepGuard whether it should allow the outbound connection. If DeepGuard now identifies the application, the end user is not prompted for decision, and the outbound connection is allowed.
4. If DeepGuard did not identify the application, the user is prompted to decide whether to allow or deny the connection.

11.4.1 Setting up application control for the first time

When you are setting up application control for the first time, you should use a small test environment to create the list of allowed applications, which contains the standard applications that are used in the company.

The list of allowed applications is distributed in a policy to the whole managed domain. This is done as follows:

1. Create a list of known applications:
 - a) Create a test environment with, for example, two computers, that have the programs normally used in your company installed.
 - b) Import these hosts to the centrally managed domain.
 - c) Select **Report** from the **Send notifications for new applications** drop-down list, so that the new applications will appear on the **Unknown applications reported by hosts** list.
 - d) Define the allow rules for these applications.

- e) When you have existing rules for all the necessary applications, this set of rules can be distributed as a policy to the entire managed domain.
2. Configure the basic application control settings that will be used when application control is running:
 - a) Select the default action to take when an unknown application tries to make an outbound connection from the **Default action for client applications** drop-down list.
 - b) Select the default action to take when an unknown application tries to make an inbound connection **Default action for server applications** drop-down list.
 - c) Set the new applications to be reported to the administrator by selecting **Report new unknown applications**.
This way you can see what kind of applications the end users are trying to launch, and you can define new rules for them if necessary.
 - d) Define whether the default messages are displayed to users when an unknown application tries to make an inbound or an outbound connection by selecting or clearing the **Show default messages for unknown applications** check box.
3. Verify the settings and take them into use.
Application control can be enabled for the whole domain as follows:
 - a) Select **Root** on the **Policy domains** tab.
 - b) Select the **Firewall security levels** page on the **Settings** tab, and make sure that **Enable application control** is selected.
 - c) Click  to save and distribute the policy.

11.4.2 Creating a rule for an unknown application on root level

In this example, a rule will be created to deny the use of Internet Explorer 4.

In this case it is assumed that the program already appears on the **Unknown applications reported by hosts** list.


1. Select the application(s) for the rule:
 - a) Go to the **Settings** tab and select the **Application control** page.
 - b) Select **Internet Explorer 4.01** in the **Unknown applications reported by hosts** table.
 - c) Click **Create rule(s)** to start the application control rule wizard.
2. Select application rule type:
 - a) Select **Deny** as the action to take when the application acts as a client and tries to make an outbound connection.
 - b) Select **Deny** as the action to take when the application acts as a server and an inbound connection attempt is made.
3. Select the message shown to users:
 - a) Select whether a message is shown to users when a connection attempt is made.
The options are: **No message**, **Default message** or **Customized message**.
If you selected **Default message**, you can check what the currently defined default messages are by clicking **Define default messages...**
 - b) If you selected **Customized message**, the customized message text box is activated and you can enter the message there.
In this case you could use a customized message, for example: The use of Internet Explorer 4 is prohibited by company security policy. Please use some other browser instead.
4. Select the rule target:
 - a) Select the domain or host that the rule affects from the domains and hosts displayed in the window.
If the target host or domain already has a rule defined for any of the applications affected by the rule, you are prompted to select whether to proceed and overwrite the existing rule at the host.
In this example select **Root**.
 - b) When the rule is ready, click **Finish**.

The new rule is now displayed in the **Application rules for known applications** table. The **Unknown applications reported by hosts** table has been refreshed.

5. Click  to distribute the policy.


11.4.3 Editing an existing application control rule

In this example, the rule created earlier is edited to allow the use of Internet Explorer 4 temporarily for testing purposes in a subdomain called `Engineering/Testing`.

1. Select the rule to be edited:
 - a) Go to the **Settings** tab and select the **Application control** page.
 - b) Select the rule which you want to edit in **Application rules for known applications**.
 - c) Click **Edit** to start the application control rule wizard.
2. Edit the application rule type:
 - a) Select the action to take when the application acts as a client and tries to make an outbound connection.
In this case select **Allow** for **Act as client (out)**.
 - b) Select the action to take when the application acts as a server and an inbound connection attempt is made.
3. Select the message shown to users.
Select whether a message is shown to users when a connection attempt is made.
4. Select the new rule target:
 - a) Select the domain or host that the rule affects.
In this case select **Engineering/Testing**.
If the target host or domain already has a rule for any of the applications affected by the rule, you are prompted to select whether to proceed and overwrite the existing rule at the host.
 - b) When the rule is ready, click **Finish**.
The modified rule is now displayed in the **Application rules for known applications** table. It is a copy of the original rule with the changes you just made.
5. Click  to distribute the policy.

11.4.4 Turning off application control pop-ups

When you want to configure application control in such a way that it is totally transparent to the end users, all pop-ups have to be turned off.


1. Select **Root** on the **Policy domains** tab.
2. Go to the **Settings** tab and select the **Application control** page.
On this page select:
 - **Allow** from the **Default action for server applications** drop-down list.
 - **Allow** from the **Default action for client applications** drop-down list.
3. When creating any application control rules with the **Application control rule** wizard, select:
 - Either **Allow** or **Deny** as the action on incoming and outgoing connection attempts in the **Application rule type** dialog box.
 - **No message** in the **Message shown to users** dialog box.
4. Click  to distribute the policy.

11.5 Using alerts to check that Internet Shield works

In normal use you should not get any alerts from Internet Shield; if you suddenly start to receive a lot of alerts it means that there is either a configuration mistake or then there is a problem.

When configuring alerting you should also remember that you should have one rule for each type of alert you want. Designing alerting based on broad rules will generate a lot of alerts, and any important information might be lost in large volumes of useless alerts.

You can also create special rules that you can use for testing that Internet Shield works. In this example a rule that allows the use of ping is created. If this rule includes alerting, it can be used for testing that the alerting works.

1. Go to **Settings** tab and select the **Firewall rules** page.
2. Select the security level you want to use for testing purposes.
3. To start the creation of the new rule, click **Add before**.
This starts the **Firewall rule** wizard.
4. Select **Allow** on the **Rule type** page.
5. Select **Any remote host** on the **Remote hosts** page.
6. On the **Services** page, select **Ping** from the **Service** drop-down list, and **Both** from the **Directions** drop-down list.
7. On the **Advanced options** page, select the following options:
 - **Security alert** from the **Send alert** drop-down list
 - **Network event: Potentially dangerous service allowed** from the **Alert trap** drop-down list
 - You can also enter a comment for the alert in the **Alert comment** field.
8. On the **Summary** page you can verify that the rule is correct and enter a descriptive comment for the rule.
9. Click  to distribute the policy.
10. You can now test the rule by pinging one of the managed hosts and checking that an alert is created and displayed on the **Alerts** tab.

11.6 Configuring intrusion prevention

Intrusion prevention monitors inbound traffic and tries to find intrusion attempts.


Intrusion prevention (IPS) can also be used to monitor viruses that try to attack computers in the LAN. Intrusion prevention analyses the payload (the contents) and the header information of an IP packet, and compares this information with the known attack patterns. If the information is similar or identical to one of the known attack patterns, intrusion prevention creates an alert and takes the action it has been configured to take.

11.6.1 Configuring IPS for desktops and laptops

In this example, the IPS is enabled for all the desktops and laptops in two subdomains.

It is assumed that desktops and laptops are located in their own subdomains, *Desktops/Eng* and *Laptops/Eng*. It is assumed that the desktops are also protected by the company firewall, and therefore the alert performance level selected for them is lower. The laptops are regularly connected to networks that cannot be considered safe, and therefore the alert performance level selected for them is higher.

1. Configuring IPS for desktops:
 - a) Select the **Desktops/Eng** subdomain on the **Policy domains** tab.
 - b) Go to the **Settings** tab and select the **Firewall security levels** page.
 - c) Select the **Enable intrusion prevention** check box.
 - d) Select **Log without dropping** from the **Action on malicious packet:** drop-down list.
 - e) Select **Warning** from the **Alert severity:** drop-down list.
 - f) Select **25%** from the **Detection sensitivity:** drop-down list.

2. Configuring IPS for laptops:
 - a) Select the **Laptops/Eng** subdomain on the **Policy domains** tab.
 - b) Go to the **Settings** tab and select the **Firewall security levels** page.
 - c) Select the **Enable intrusion prevention** check box.
 - d) Select **Log without dropping** from the **Action on malicious packet:** drop-down list.
 - e) Select **Warning** from the **Centralized alert severity:** drop-down list.
 - f) Select **100%** from the **Alert and performance level:** drop-down list.
3. Click  to distribute the policy.

Using Device Control

Topics:

- [*Configuring Device Control*](#)
- [*Blocking hardware devices*](#)
- [*Granting access to specific devices*](#)

Device Control blocks certain hardware devices to protect the network.

Device Control prevents malware from spreading to the network from external devices such as USB storage devices and DVD/CD-ROM drives. When a blocked device is plugged in to the client computer, Device Control turns it off to prevent access to it.



Note: Device Control is provided with Client Security 9.30.

12.1 Configuring Device Control

Device Control can be configured with F-Secure Policy Manager.

Follow these instructions to configure Device Control.

1. To open Device Control settings, go to **F-Secure Device Control > Settings** branch.
2. To turn on Device Control, select **Enabled** in **Device Control Enabled**.
3. In **Notify Administrator**, select the type of alert that is sent for the administrator when a device is blocked.
4. The **Hardware Devices** table contains device blocking rules. Devices can be identified by the following IDs (from specific to general):

Option	Description
Device ID	Any single device has only one device ID.
Hardware ID	A device can have multiple hardware IDs.
Compatible ID	General device IDs for same kind of devices.
Class	A single GUID of device interface class. Every device has only one class, which is a registry key under HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class where the device information is stored.

A device that has **Access Level** set to **Blocked** cannot be accessed, when the rule is set as active. The most specific rule is used to determine the access level for a device.

12.2 Blocking hardware devices

You can block the access to devices with predefined rules.

By default, rules do not block any devices. To block devices, follow these instructions:

1. Go to **F-Secure Device Control > Settings > Devices > Hardware Devices**.
2. Set **Access Level** to **Blocked** to block any of the following devices:

- USB mass storage devices
- Wireless devices
- DVD/CD-ROM drives
- Windows CE ActiveSync devices
- Floppy drives
- Modems
- COM & LPT ports (does not control the device, but the port itself)
- Printers
- Smart Card readers
- Imaging devices (cameras and scanners)
- IEEE 1394 Bus host controllers
- IrDA devices
- Bluetooth devices



Note: Some USB Wi-Fi adapters do not use the `USB\Class_E0` hardware id and need a custom rule to work with Device Control.

12.3 Granting access to specific devices

You can set rules to allow a specific device while all other devices of same class are blocked.

You need to know the hardware ID of the device that you want to allow before you can create a rule that grants full access to the device.

To add an exception to a rule, follow these instructions:

1. Get Hardware ID of device that you want to allow.
The hardware ID has to be more specific than the ID which is used to block the device.
2. Go to **F-Secure Device Control > Settings > Devices > Hardware Devices**.
3. Add a new rule to the Hardware Devices table with the ID of the device.
4. Set **Access Level** to **Full access** to allow the use of the device.
5. Set **Active** to **Yes** for the new rule.

12.3.1 Finding hardware ID for a device

You can find the hardware ID of the device in multiple ways. You can use this ID with blocking rules.

Follow these instructions to find the hardware ID either with F-Secure Policy Manager or Windows Device Manager.

1. Open F-Secure Policy Manager and go to **F-Secure Device Control > Statistics**.
Use **Hardware IDs**, **Compatible IDs** and **Device Class** columns to find the ID of the device that has been blocked.
2. If you cannot find the ID using the statistics or the device has not been blocked yet, open **Windows Device Manager** in the client computer.
3. Find the device which ID you want to know in the list of devices.
4. Right-click the device and select **Properties**.
5. Go to **Details** tab.
6. Select one of the following IDs from the drop-down menu and write down its value:
 - Hardware IDs
 - Compatible IDs
 - Device class guid

Managing software updates

Topics:

- [*Installing software updates automatically*](#)
- [*Excluding software updates from automatic installation*](#)
- [*Checking the status of software updates in your network*](#)

You can manage and install software updates for the computers in your network.


It is important to have the latest software updates installed on the workstations in your network, because many updates fix security vulnerabilities in installed products.

You can configure Policy Manager to automatically install security updates to computers. You can also check the status of software updates and install missing software updates manually when needed.

13.1 Installing software updates automatically

You can configure Policy Manager to automatically install security updates for software to computers in your network.

To turn on automatic installation of security updates:

1. Select the target domain.
2. Select the **Settings** tab and the **Software Updater** page.
3. Select **Enable Software Updater**.
4. Under **Automatic installation**, select the security update categories and schedule that you want to use.
5. Click  to distribute the policy.

13.2 Excluding software updates from automatic installation

You can enter the name and bulletin ID for any software that you do not want Software Updater to update automatically.

Exclusion is based on the update installation status reported by managed hosts. When a host starts installing missing updates, it checks for any excluded updates and reports that they were not installed due to exclusion by the administrator. This also means that excluded updates do not immediately disappear from the list on the **Software updates** tab, because the hosts only report the installation status once they attempt to install the missing update.

To exclude software updates from automatic installation:

1. Select the target domain.
2. Under **Exclude software from automatic installation**, click **Add**.
3. Enter the details for the update that you want to exclude.

You can enter both the name of the software and the bulletin ID for the specific update. The software name can include a product name and a service pack name. For example "windows sp3" will match all windows updates related to SP3. If you use the bulletin ID for excluding updates, only updates matching the exact bulletin ID will be excluded.

4. Click  to distribute the policy.

Any updates for software matching the entered text or bulletin ID is now excluded from automatic installation. You can click **View** in the **Matching updates** column to see a list of the updates currently found for the entered software.

13.3 Checking the status of software updates in your network

On the **Software updates** page, you can check the status of software updates in your network.

The **Software updates** page provides a list of updates for the software in use within your network. Each entry on the list includes the software in question, category, ID and description for the update, as well as the update status if a single host is selected. If you select a domain or multiple hosts, you can click **View hosts** to see the update status. From this page, you can check which computers are missing selected updates, and also install the missing updates to those computers.



Tip: In the Advanced mode, you can turn off reporting for missing service packs and updates that are not security-related.

13.3.1 Installing missing software updates

You can install missing software updates manually.

To install the missing software updates:

1. Select the target domain.

2. On the **Software updates** page, select the updates that you want to install.
3. Click **Install**.

How to check that the network environment is protected

Topics:

- *[Checking that all the hosts have the latest policy](#)*
- *[Checking that the server has the latest virus definitions](#)*
- *[Checking that the hosts have the latest virus definitions](#)*
- *[Checking that there are no disconnected hosts](#)*
- *[Viewing scanning reports](#)*
- *[Viewing alerts](#)*
- *[Creating a weekly infection report](#)*
- *[Monitoring a possible network attack](#)*

This section contains a list of things you can check to make sure that the network environment is protected.

As part of the monitoring and system administration processes, you can regularly perform the tasks listed here to ensure that your network environment is protected.

14.1 Checking that all the hosts have the latest policy

You can ensure that all hosts have the correct settings by checking that they have the latest policy.

1. Select **Root** on the **Policy domains** tab.
2. Go to the **Summary** tab and check how many hosts of the entire domain have the latest policy.
3. If all hosts do not have the latest policy, click **View hosts' latest policy update....**
This takes you to the **Status** tab and **Centralized management** page.
4. On the **Centralized management** page, check which of the hosts do not have the latest policy.
You can also see the possible reasons for this; for example, the host is disconnected or there has been a fatal error on the host.

14.2 Checking that the server has the latest virus definitions

You should check that the virus definitions are up to date on the server.

1. Select **Root** on the **Policy domains** tab.
2. Go to the **Summary** tab and check that the virus definitions on the server are the latest available.

14.3 Checking that the hosts have the latest virus definitions

You should regularly check that the virus definitions are up to date on all hosts within the domain.

1. Select **Root** on the **Policy domains** tab.
2. Go to the **Summary** tab and check what is displayed in the **Virus Protection for Workstations** section beside **Virus definitions**.
3. If the virus definitions on some hosts are outdated, there are two alternatives:
 - You can select the **Status** tab and the **Overall protection** page to see which hosts do not have the latest virus definitions. Then select these hosts in the **Policy domains** tab, go to the **Operations** tab and click **Update virus definitions**. This orders the selected hosts to fetch new virus definitions at once.
 - Alternatively, click the **Update virus definitions** link. This takes you to the **Operations** tab. Once on the **Operations** tab, click **Update virus definitions**. This orders all hosts to fetch new virus definitions at once.

14.4 Checking that there are no disconnected hosts

You can ensure that all hosts are getting the latest updates by checking that there are no disconnected hosts.

1. Select **Root** on the **Policy domains** tab.
2. Go to the **Summary** tab and check what is displayed in the **Domain** section beside **Disconnected hosts**.
3. If there are disconnected hosts, click **View disconnected hosts....**
This takes you to the **Status** tab and **Centralized management** page.
4. Check which of the hosts are disconnected and the possible reasons for this.



Note: You can define the time after which a host is considered disconnected. Select **Tools > Server configuration** from the menu, then select the **Hosts** tab. You will see the currently defined time for when hosts are considered disconnected.

14.5 Viewing scanning reports

You can view the scanning reports from hosts to check if there have been any problems.

If you want to see a scanning report from certain hosts, do as follows:

1. Select the hosts in the **Policy domains** tab.
2. Go to the **Scanning reports** tab.
The scanning information from the selected hosts is displayed in the **Scanning reports** table.
3. Select a single host by clicking on a row in the table.
The associated scanning report from that host is now displayed in the report view in the lower part of the window.

14.6 Viewing alerts

If there has been a problem with a program or with an operation, the hosts can send alerts and reports about it.






It is a good idea to check regularly that there are no new alerts, and also to acknowledge (and delete) the alerts that you have already handled.

When an alert is received, the  button will light up. To view the alerts:

1. Click .

Alternatively, you can click **View alert summary...** on the **Summary** tab.

The **Alerts** tab will open. All alerts received will be displayed in the following format:

Ack	Click the Ack button to acknowledge an alert. If all of the alerts are acknowledged, the Ack button will be dimmed.		
Severity	The problem's severity. Each severity level has its own icon:		
		Info	Normal operating information from a host.
		Warning	A warning from the host.
		Error	Recoverable error on the host.
		Fatal error	Unrecoverable error on the host.
		Security alert	Security hazard on the host.
Date/Time	Date and time of the alert.		
Description	Description of the problem.		
Host/User	Name of the host/user.		
Product	The F-Secure product that sent the alert.		

When an alert is selected from the list, the **Alert view** under the alerts table displays more specific information about the alert.

2. You can use the **Ack** button to mark the alerts that you have seen and are planning to troubleshoot.
3. The alert summary displayed on the **Summary** tab is not automatically refreshed, so you can click **Refresh alert summary** to refresh the alert view.

14.7 Creating a weekly infection report

You can use the Web Reporting tool to create a weekly infection report, as well as other reports to be generated at regular intervals.

Web Reporting is a web-based tool with which you can generate a wide range of graphical reports from Client Security alerts and status information.

14.8 Monitoring a possible network attack

If you suspect that there is a network attack going on in the local network, you can monitor it by following these steps.

1. Select **Root** on the **Policy domains** tab.
2. Go to the **Summary** tab.
3. Check what is displayed beside **Most common recent attack**.
4. If there has been an attack, you can access more detailed information by clicking **View Internet Shield status....**

This takes you to the **Status** tab and **Internet Shield** page, where you can see detailed information on the latest attacks on different hosts.

Upgrading managed software

Topics:

- [*Using policy-based installation*](#)

This section describes how to upgrade software using the installation editor.

You can remotely upgrade F-Secure anti-virus software already installed on hosts by using the **Installation editor**. The editor creates policy-based installation tasks that each host in the target domain will carry out after the next policy update.



Note: It is also possible to upgrade Client Security by using any other installation scheme.

15.1 Using policy-based installation

Policy-based installation must be used on hosts that already have Management Agent installed.

You can use policy-based installation to perform installation operations on a selected domain or selected hosts. In addition to installing products, you can perform hotfix, upgrade, repair and uninstallation operations.

When the installation operation is completed successfully, you can leave the operation on the **Policy-based installations** table, so that the same installation operation will automatically be applied to any new hosts that are added to the corresponding domain.

To use policy-based installation:

1. Open the **Installation** tab.
On the **Installation** tab, **Policy-based installations** table shows the status of any current installation operations, and the **Installed products summary** table lists the products that are currently installed on managed hosts.
2. Click **Install** under the **Policy-based installations** table to start the remote installation wizard.
3. Complete the remote installation wizard with the necessary details.
The information entered in the remote installation wizard is used to prepare the customized package specific for this installation operation. The installation package will be then distributed to the selected domain or hosts once the policy is distributed.
Once the remote installation wizard is complete, the installation operation and status will appear on the **Policy-based installations** table as a new row.
4. Distribute the policy.
Once the installation operation is complete, the product name, version and number of hosts running the product are shown on the **Installed products summary** table.



Note: It may take a considerable length of time to carry out an installation operation. This may happen if an affected host is not currently connected to the network, or if the active installation operation requires a user to restart his host before the installation is completed. If the hosts are connected to the network and they send and receive policy files correctly, then there could be a real problem. The host may not be correctly acknowledging the installation operation. It is possible to remove the installation operation from the policy by clicking **Clear row** and then distributing the policy. This will cancel the installation operation. It is possible to stop the installation task in the selected domain and all subdomains by selecting the **Recursively cancel installation for subdomains and hosts** option in the confirmation dialog.

For other installation operations, for example upgrades or uninstallation, you can use the links next to the product on the **Installed products summary** table. These links will automatically appear whenever the installation packages necessary for the corresponding action are available. The options are: **hotfix**, **upgrade**, **repair** and **uninstall**.

If the link for the operation you want to run is not shown on the **Installed products summary** table, you can click either **Install** or **Uninstall**, depending on the operation you want to run, under the **Policy-based installations** table and check if the required package is available there. However, if for example the product does not support remote uninstallation, there will not be an option for uninstallation.

When uninstalling Management Agent, no statistical information will be sent stating that the uninstallation was successful, because Management Agent has been removed and is unable to send any information. For example, if uninstalling F-Secure Anti-Virus and Management Agent:

1. Uninstall F-Secure Anti-Virus
2. Wait for Policy Manager Console to report the success or failure of the uninstallation.
3. If F-Secure Anti-Virus was uninstalled successfully, uninstall Management Agent.
4. If uninstallation of Management Agent is unsuccessful, Policy Manager Console will display a statistical report of the failure. Success cannot be reported, but is evident from ceased communication, and the final report for Management Agent will state `in progress...`

Virus information

Topics:

- [*Malware information and tools on the F-Secure web pages*](#)
- [*How to send a virus sample to F-Secure*](#)
- [*What to do in case of a virus outbreak?*](#)

This section contains useful general information about viruses and virus handling.

This section provides information on where to find out about viruses and how to handle viruses you encounter.

16.1 Malware information and tools on the F-Secure web pages

You can find a list of sources of information about malware and useful tools on the F-Secure web site.

For information of the latest security threats you can check these sources:

- The F-Secure blog: <http://www.f-secure.com/weblog/>
- A list of vulnerabilities in common software is here: <http://www.f-secure.com/vulnerabilities/>
- The latest threats are also delivered to your desktop through Client Security as F-Secure news.

Before sending us a sample you may consider trying our **RescueCD**. This is a tool that starts its own operating system and so can find some malware that cannot be found from within Windows. You can find it, as well as other tools, from the Security Center: http://www.f-secure.com/security_center/.

Instructions on how to use the **RescueCD** are included in the downloaded file.

16.2 How to send a virus sample to F-Secure

This section covers information on sending a virus sample to the F-Secure Security Lab.



Note: This section is for advanced users.

Please send detailed descriptions of the problem, symptoms or any questions you have in English whenever possible.

Our usual response time is less than a day. Complicated cases may take a longer time to investigate. If you do not get a reply from us within a few business days, please re-submit your sample.

16.2.1 How to package a virus sample

All files should be sent in ZIP archive only.

To package the virus samples you can download a trial version of WinZip at <http://www.winzip.com/>. A free InfoZIP utility is also available at <http://www.info-zip.org/pub/infozip/>.

All ZIP packages should be named using only English letters and/or numbers. You can use long file names.

To be sure that we receive the ZIP archive, protect the ZIP file with the password `infected`. Otherwise any malware sample you attempt to send to us may be removed by an intermediary server as a safety measure. However, password-protected (encrypted) archives cannot be scanned and should be assumed to be safe. You can find more instructions on how to package a virus sample here: <http://support.f-secure.com/enu/home/virusproblem/samples/index.shtml>.

16.2.2 What should be sent

Here you will find what files and details to send, as viruses are not all of the same type, so they cannot all be sent in one specific way.

The following lists what to send according to the virus types:

1. Trojan or other standalone malware (malicious programs):

If you are sending a sample of a suspected standalone malware (worm, backdoor, trojan, dropper), specify the location of the file on the infected system and the way it was started (registry, `.ini` files, `Autoexec.bat`, etc.). A description of the source of the file is also useful.

2. A false alarm from one of our antivirus products:

If you receive a missed or incorrect detection, or a false alarm with Client Security, try to send us the following:

- the file in question,
- the Client Security version number,
- the last virus definition updates date,

- a description of the system configuration,
- a description of how to reproduce the problem, and
- the Client Security scanning report file. For instructions on how to save the file see: <http://support.f-secure.com/enu/home/virusproblem/samples/index.shtml>.

3. A new virus or trojan:

If you think an unknown infection is in the computer system and an antivirus program does not find anything, please send us:

- If you are running Windows XP, the **msinfo32** report. To create the report:
 1. Select **Start > Run....**
 2. Type `msinfo32` and click **OK**.
 3. While viewing the **System Summary** node select **File > Save**.
- Some Windows configuration files (`WIN.INI`, `SYSTEM.INI`) and DOS configuration files (`Autoexec.bat`, `Config.sys`).
- A full or partial export from a system registry (this can be done with the **Regedit** utility that all Windows versions have).
- the contents of the `\Start Menu\Programs\Startup\` folder.

4. Virus that infects executable files:

Try to get different infected files from your system. Usually 3-5 different samples are enough. If possible, add clean copies of the same files as well (taken from backups). To do this, use two directories in your zip file, for example:

```
ORIGINAL\APPEND.EXE
ORIGINAL\COMMAND.COM
INFECTED\APPEND.EXE
INFECTED\COMMAND.COM
```

5. Macro virus:

Send an infected copy of the `NORMAL.DOT` file (the global template) in addition to the infected `DOC` files. With Excel viruses, send the `PERSONAL.XLS` file, if it exists, in addition to the infected `XLS` files. If the macro virus also infected other types of files, send a sample of every file type.

6. Boot sector virus:

If an infection is on a hard drive, use the **GetMBR** utility to collect boot sector samples. When the script is finished send us the `mbr.dmp` file in the way described in this chapter. **GetMBR** can be downloaded from our ftp site: <ftp://ftp.f-secure.com/anti-virus/tools/getmbr.zip>.

7. An infection or a false alarm on a CD:

If an infection or false alarm is on a CD, you can send the CD to our office in Finland.

Please include a description of the problem, and a printed Client Security report, if possible. We will return your CD if it has no infection.

16.2.3 How to send the virus sample

Here you will find details of the different ways you can send us virus samples.

There are three methods to send us samples:

- The most common is to use our sample submission webform. This webform guides you to give us all the information we need to process a sample. You can find the webform at: <http://www.f-secure.com/samples>.
- If the sample is larger than 5Mb in size, you must upload the sample to our ftp site at: <ftp://ftp.f-secure.com/incoming/>.
- If the sample is on some physical media, for example a CD, DVD or USB drive, you can send the physical media to us at:

Security Labs
 F-Secure Corporation
 Tammasaarenkatu 7
 PL 24
 00181 Helsinki
 Finland

16.3 What to do in case of a virus outbreak?

You can use this checklist of what you should do and remember in case there is a virus outbreak in the company network.

1. Disconnect the infected computer from the network immediately.
 If the infection keeps spreading, the whole network should be taken down without delay. All outgoing traffic should be blocked. Employees must be instructed to report suspicious activities on their computers immediately.
2. Try to identify whether it is a real infection or a possible false alarm.
 Scan the computer with the latest version of Client Security with the latest virus definitions updates. If the infection is identified exactly, go to the next step. If the infection is identified as possible new virus, could be an image of a boot sector virus and so on, send a sample together with the Client Security scan report through the **Submit Malware Sample** web tool at: <http://www.f-secure.com/samples>.
3. If it is a known infection, go to the F-Secure virus information pages and get a description of the malware.
 Download disinfection tools (if available) and print disinfection instructions. In case disinfection assistance is needed, contact Support through our support web page: <http://support.f-secure.com>.
 If you need urgent assistance, please point it out in your message.
4. If it is a new virus, try to locate a sample and send it to F-Secure Security Labs through the sample submission webform at: <http://www.f-secure.com/samples>.
 Provide as much information about the problem as possible. It is important to know how many computers are affected with the virus.
5. If a computer is infected with malware that spreads in the local network, it is recommended to take down the network until all infected computers are disinfected.
 The network can be taken into use only after all computers are cleaned because a single infected machine can re-infect the whole network within minutes.
6. Wait for a report from the Security Labs, and follow the provided disinfection instructions carefully.
 It is advised to backup any important data from the infected computer before disinfecting it. This backup should not be taken using the network; use external backup devices instead. Back up only data files, not executable files. If there is a need to restore the backup later, all restored files should be checked for infection.
7. When provided with a disinfection solution, test it on one computer first. If it works, it can be applied to all infected computers.
 Scan the cleaned computers with Client Security and the latest virus definitions updates to ensure that no infected files are left.
8. Re-enable the network only after every single infected computer is cleaned.
 If the malware contained backdoors or data stealing capabilities, it is strongly recommended to change passwords and logins for all network resources.
9. Inform the employees about the outbreak and warn them against running unknown attachments and visiting suspicious Internet sites.

Check the security settings of installed software on workstations. Make sure that e-mail scanners and firewalls function correctly on servers. Client Security should receive updates automatically, however it is recommended to periodically check that these automatic updates are working correctly.

- 10.** Warn your partners about the outbreak and recommend them to scan their computers with Client Security and the latest virus definitions updates to make sure that an infection did not leave your network.

Advanced features: virus and spyware protection

Topics:

- [*Configuring scheduled scanning*](#)
- [*Advanced DeepGuard settings*](#)
- [*Configuring Policy Manager Proxy*](#)
- [*Excluding an application from the web traffic scanner*](#)

Here you will find information on advanced virus and spyware protection features.

This section contains instructions for some advanced virus protection administration tasks, such as configuring scheduled scanning from the **Advanced mode** user interface and configuring the anti-virus proxy.

17.1 Configuring scheduled scanning

A scheduled scanning task can be added from the **Advanced mode** user interface.

In this example, a scheduled scanning task is added in a policy for the whole policy domain. The scan is to be run weekly, every Monday at 8 p.m, starting from August 25, 2009.

1. Select **View > Advanced mode** from the menu.
The **Advanced mode** user interface opens.
2. Select **Root** on the **Policy domains** tab.
3. On the **Policy** tab, select **F-Secure > F-Secure Anti-Virus > Settings > Scheduler > Scheduled tasks**.

The currently set scheduled tasks are displayed on the **Scheduled tasks** table. Now you can add scheduled scanning as a new task.

4. Click **Add**.
This adds a new row to the **Scheduled tasks** table.
5. Click the **Name** cell on the row you just created and then click **Edit**.
6. The **Name** cell is now activated and you can enter a name for the new task.

For example, `Scheduled scanning for all hosts`.

7. Next click the **Scheduling parameters** cell, and then click **Edit**.

8. Now you can enter the parameters for the scheduled scan.

A scheduled scan that is to be run weekly, every Monday starting at 8 p.m, from August 25, 2009 onwards, is configured as follows: `/t20:00 /b2009-08-25 /rweekly`



Note: When the **Scheduling parameters** cell is selected, the parameters that you can use and their formats are displayed as a help text in the **Messages** pane (below the **Scheduled tasks** table).

9. Select the task type by clicking the **Task type** cell and then clicking **Edit**.
10. From the drop-down list that opens select **Scan local drives**.
The scanning task is now ready for distribution.

11. Click  to distribute the policy.

Running scheduled scans on specific weekdays and days of the month:

When you are configuring a weekly scheduled scan, you can also define specific weekdays when the scan is to be run. Similarly, when you are configuring a monthly scheduled scan, you can define specific days of the month when the scan is to be run. For both of these, you can use the `/Snn` parameter:

- For weekly scheduled scans you can use `/rweekly` together with parameters `/s1 - /s7`. `/s1` means Monday and `/s7` means Sunday.

For example, `/t18:00 /rweekly /s2 /s5` means that the scan is run every Tuesday and Friday at 6 p.m.

- For monthly scheduled scans you can use `/rmonthly` together with parameters `/s1 - /s31`.

For example, `/t18:00 /rmonthly /s5 /s20` means that the scan is run on the 5th and 20th of each month at 6 p.m.




Note: Weekly scheduled scans are automatically also run on each Monday. Monthly scheduled scans are automatically also run on the first day of each month.

17.2 Advanced DeepGuard settings

This section covers the advanced settings relating to DeepGuard.

17.2.1 Letting an administrator allow or deny program events from other users

You can allow a user with administrator rights to allow or deny event caused by an application started by another user.

1. Select **View > Advanced mode** from the menu.
The **Advanced mode** user interface opens.
2. Select **Root** on the **Policy domains** tab.
3. On the **Policy** tab, select **F-Secure > F-Secure DeepGuard > Settings > Local administrator control**.
4. Select **All processes**.
5. Click  to distribute the policy.

17.2.2 Allowing or denying events requested by a specific application automatically


You can choose to allow all events for a safe application or deny all events for an application that should not be used.

1. First you must calculate the SHA-1 hash identifier for the application.

There are free SHA-1 calculators available on the Internet. You can use for example, the Microsoft File Checksum Integrity Verifier. This tool is available from: <http://support.microsoft.com/kb/841290>.



Note: A SHA-1 hash uniquely identifies the sequence of instructions that define a program. If a new version of the program is made available, you must repeat this process as the new program will have a different SHA-1 hash.

2. When you have the SHA-1 identifier hash, select **View > Advanced mode** from the menu.
The **Advanced mode** user interface opens.
3. Select **Root** on the **Policy domains** tab.
4. On the **Policy** tab, select **F-Secure > F-Secure DeepGuard > Settings > Applications**.
5. Click **Add** to add a new rule.
6. Double-click the **SHA-1 hash** cell for the new entry and paste the SHA-1 hash into the empty cell.
7. Double click the **Notes** cell for the new entry and enter a note.
You should use this note as a reminder which application the SHA-1 hash identifies.
8. Double-click the **Trusted** cell for the new entry:
 - Select **Yes** to allow all events for the application.
 - Select **No** to deny all events for the application.
9. Double-click the **Enabled** cell for the new entry.
10. Select **Yes** to enable to the rule.
11. Click  to distribute the policy.

The application rule cannot be over-ridden locally by the user.

17.3 Configuring Policy Manager Proxy

Policy Manager offers a solution to bandwidth problems in distributed installations by significantly reducing load on networks with slow connections.

Policy Manager Proxy caches automatic updates retrieved from the central F-Secure update server or the corporate Policy Manager Server, and it resides in the same remote network as the hosts that use it

as a database distribution point. There should be one Policy Manager Proxy in every network that is behind slow network lines.

Hosts running Client Security or Anti-virus for Workstations fetch virus definition updates through Policy Manager Proxy. Policy Manager Proxy contacts Policy Manager Server and the F-Secure distribution server when needed.

Workstations in remote offices also communicate with the Policy Manager Server in the main office, but this communication is restricted to remote policy management, status monitoring, and alerting. Since the heavy database update traffic is redirected through the Policy Manager Proxy in the same local network, the network connection between managed workstations and Policy Manager Server has a substantially lighter load.



Note: For more information on installing and configuring Policy Manager Proxy, see the Policy Manager Proxy Administrator's Guide.

17.4 Excluding an application from the web traffic scanner

If web traffic scanning causes problems with a program that is common in your organization you can exclude this application from the web traffic scanner.

1. Select **View > Advanced mode** from the menu.
2. On the **Policy** tab select **F-Secure Client Security > Settings > Select protocol scanner > Trusted applications > List of trusted processes**.
3. Enter the name of the process to exclude from the web traffic scanner.

To enter more than one process, type a comma between the name of each process. Do not enter any whitespace between the process names.



Tip: In Windows you can learn the process name of an application by using the Windows task explorer.

For example to exclude the applications notepad and skype from the web traffic scanner you should enter `notepad.exe, skype.exe`.

4. Click  to distribute the policy.

Advanced features: Internet Shield

Topics:

- [*Managing Internet Shield properties remotely*](#)
- [*Configuring security level autoselection*](#)
- [*Troubleshooting connection problems*](#)
- [*Adding new services*](#)

Here you will find information on advanced Internet Shield features.

This section covers some advanced Internet Shield features and also contains some troubleshooting information.


18.1 Managing Internet Shield properties remotely

This section describes how you can manage Internet Shield properties remotely.


18.1.1 Using packet logging

Packet logging is a very useful debugging tool to find out what is happening on the local network.

Packet logging is also a powerful tool that can be abused by the end user to eavesdrop on the activities of other users on the LAN, and this means that in some corporate environments the administrator needs to disable the packet logging.

1. Select **View > Advanced mode** from the menu.
The **Advanced mode** user interface opens.
2. Select **Root** on the **Policy domains** tab.
3. Select **F-Secure Internet Shield > Settings > Packet logging > Active**.
This variable shows the status of the packet logging; **Disabled** means that it is not running, and **Enabled** that it is currently running on the host.
4. To turn off logging completely, make sure that it is set to **Disabled**, and select **Disallow user changes**.
5. Click  to distribute the policy.

To later undo this change, select **Allow user changes** and distribute the new policy.


 **Note:** Use this with caution, as for example setting the variable to **Enabled** for the whole domain would start a logging session on every affected host.

18.1.2 Using the trusted interface

The trusted interface mechanism is used to allow use of the firewalled host as a connection-sharing server.

Firewall rules are not applied to traffic going through the trusted interface. If it is used wrongly it can open up the host to any kind of attack from the network, so it is a good security precaution to turn this mechanism off if it is not absolutely needed.

The trusted interface is turned on as follows:


1. Select **View > Advanced mode** from the menu.
The **Advanced mode** user interface opens.
2. Select the subdomain where you want to enable the trusted interface in the **Policy domains** tree.
3. On the **Policy** tab, select **F-Secure Internet Shield > Settings > Firewall engine > Allow trusted interface**.
4. Select **Enabled** to turn on the trusted interface for the currently selected subdomain.
This allows the end-users in the subdomain to configure a network interface as the trusted interface.
5. Click  to distribute the policy.

18.1.3 Using packet filtering

This is one of the basic security mechanisms in the firewall; it filters all the IP network traffic based on information in the protocol headers of each packet.

Packet filtering can be turned on or off from the **Advanced** tab in the **Network protection** settings. Turning it off is sometimes needed for testing purposes, but will endanger the security. Because of this, most corporate environments should make sure that the packet filtering is always on.

1. Select **View > Advanced mode** from the menu.
The **Advanced mode** user interface opens.
2. Select **Root** on the **Policy domains** tab.
3. On the **Policy** tab, select **F-Secure Internet Shield > Settings > Firewall engine > Firewall engine enabled**.

4. To make sure packet filtering is always turned on, set this variable to **Yes** and select **Disallow user changes**.
5. Click  to distribute the policy.

18.2 Configuring security level autoselection


In this example, security level autoselection is configured for a subdomain that contains only laptops in such a way that when the computers are connected to company LAN, the **Office** security level is used; when a dialup connection is used, the security level is changed to **Mobile**.

Before you start, you should know the DNS server IP address and the default gateway's address, as they are needed for defining the security level autoselection criteria. You can find out these addresses by issuing the `ipconfig -all` command in the command prompt.

1. Select **View > Advanced mode** from the menu.
The **Advanced mode** user interface opens.
2. Select the subdomain on the **Policy domains** tree.
3. On the **Policy** tab, select **F-Secure > F-Secure Internet Shield > Settings > Security level > Autoselect mode**.
4. Make sure that security level autoselection is turned on.
To turn on security level autoselection, select **User can change** or **Admin full control** from the **Autoselect mode** drop-down list.
5. Go to the **Autoselect** page and click **Add** to add the first security level, in this example **Office**.
6. You can enter the data in the cells by selecting a cell and clicking **Edit**.

For the **Office** security level you should add the following data:

- **Priority:** The rules are checked in the order defined by the priority numbers, starting from the smallest number.
- **Security level:** Enter the ID (composed of number and name) of the security level here; for example: 40office.
- **Method 1:** Select **DNS server IP address** from the drop-down list.
- **Argument 1:** Enter the IP address of your local DNS server here; for example: 10.128.129.1.
- **Method 2:** Select **Default Gateway IP address** from the drop-down list.
- **Argument 2:** Enter the IP address of you default gateway; for example: 10.128.130.1.

 **Note:** You can only use one argument, for example one IP address, in the **Argument** field. If there are several default gateways in use in your company, and you want to use all of them in the security level autoselection, you can create a separate rule for each of them in the table.

The first security level is now ready.

7. Click **Add** to add the second security level, in this example **Mobile**.
8. Enter the data in the cells by selecting a cell and clicking **Edit**.

For the **Mobile** security level you should add the following data:

- **Priority:** The rules are checked in the order defined by the priority numbers, starting from the smallest number.
- **Security level:** Enter the ID of the security level here; for example: 20mobile.
- **Method 1:** Select **Dialup** from the drop-down list.
- **Argument 1:** You can leave this empty.
- **Method 2:** Select **Always** from the drop-down list.
- **Argument 2:** You can leave this empty.

The configuration is now ready.

9. Click  to distribute the policy.

18.3 Troubleshooting connection problems

If there are connection problems, for example a host cannot access the Internet, and you suspect that Internet Shield might cause these problems, you can use the steps given here as a check list.

1. Check that the computer is properly connected.
2. Check that the problem is not in the network cable.
3. Check that ethernet is up and working properly.
4. Check that the DHCP address is valid.

You can do this by giving the command `ipconfig` in the command prompt.

5. Next you should ping the default gateway.

If you do not know the address, you can find it out by issuing the command `ipconfig -all` in the command prompt. Then ping the default gateway to see if it responds.

6. If normal Internet browsing does not work, you can try to ping a DNS server:

- Run `nslookup` to make sure that the DNS service is running.
- You can also try to ping a known web address to make sure that the computer at the other end is not down.

7. Next you should check whether something in the centrally managed domain has been changed; is there a new policy in use and does this policy contain some settings that might cause these problems?

- Check from firewall rules that outbound HTTP connections are allowed.
- Check from the local application control that the IP address the user tries to connect to has not accidentally been added to the list of denied addresses.

8. If nothing else helps, unload F-Secure products or set the Internet Shield to allow all mode.

If even this does not help, it is likely that the problem is in routing or in some other component in the computer the user is trying to connect to.

18.4 Adding new services

Service, short for network service, means a service that is available on the network, e.g. file sharing, remote console access, or web browsing.

Services are most often described by what protocol and port they use.

18.4.1 Creating a new Internet service based on the default HTTP

In this example, it is assumed that there is a web server running on a computer, and the web server is configured to use a non-standard web port.

Normally a web server would serve TCP/IP port 80, but in this example it has been configured to serve port 8000. To enable connections to this server from the workstations you will have to create a new service. The standard HTTP service does not work here because we are not using the standard HTTP port any more. This new service is `HTTP port 8000` and it is based on the default `HTTP` service.

1. Select the subdomain for which you want to create the new service in the **Policy domains** tab.
2. Go to the **Settings** tab and open the **Firewall services** page.

This page contains the **Firewall services** table.

3. Click the **Add** button to start the **Firewall services** wizard.

4. Enter a service name:

- a) Define a unique name for the service in the **Service name** field; you cannot have two services with the same name.

For example, `HTTP port 8000`.

- b) Enter a descriptive comment for the service in the **Service comment** field.

The comment will be displayed on the **Firewall services** table.

5. Select an IP protocol number:

a) Select a protocol number for this service from the **Protocol** drop-down list.

It contains the most commonly used protocols (TCP, UDP, ICMP). If your service uses any other protocol, refer to the table below and enter the respective number.

In this example, select **TCP (6)** from the **IP-protocol number:** drop-down list.

Protocol name	Protocol number	Full name
ICMP	1	Internet Control Message Protocol
IGMP	2	Internet Group Management Protocol
IPIP	4	IPIP Tunnels (IP in IP)
TCP	6	Transmission Control Protocol
EGP	8	Exterior Gateway Protocol
PUP	12	Xerox PUP routing protocol
UDP	17	User Datagram Protocol
IDP	22	Xerox NS Internet Datagram Protocol
IPV6	41	IP Version 6 encapsulation in IP version 4
RSVP	46	Resource Reservation Protocol
GRE	47	Cisco Generic Routing Encapsulation (GRE) Tunnel
ESP	50	Encapsulation Security Payload protocol
AH	51	Authentication Header protocol
PIM	103	Protocol Independent Multicast
COMP	108	Compression Header protocol
RAW	255	Raw IP packets

6. Select the initiator ports:

If your service uses the TCP or UDP protocol, you need to define the initiator ports the service covers. The format for entering the ports and port ranges is as follows:

- `>port`: all ports higher than `port`
- `>=port`: all ports equal and higher than `port`
- `<port`: all ports lower than `port`
- `<=port`: all ports equal and lower than `port`
- `port`: only the `port`
- `minport-maxport`: `minport` and `maxport` plus all ports between them (notice that there are no spaces on either side of the dash).

You can define comma-separated combinations of these items. For example ports 10, 11, 12, 100, 101, 200 and over 1023 can be defined as `10-12, 100-101, 200, >1023`.

In this example, define the initiator port as `>1023`.

7. Select responder ports:

If your service uses the TCP or UDP protocol, you need to define the responder ports the service covers.

In this example, define the responder port as 8000.

8. Select a classification number for the service from the drop down list.

You can accept the default value.

9. Select whether any extra filtering is to be applied for the traffic allowed by the service you are creating, in addition to the normal packet and stateful filtering.

In this example you can accept the default, **Disabled**.



Note: When the service uses TCP protocol, and you do not have application control enabled, you can select **Active mode FTP** from the **Extra filtering** drop-down menu. **Active mode FTP** requires special handling from the firewall, as the information about the port that should be opened for the connection is included in the transferred data.

10. You can review your rule now.

If you need to make any changes to the rule, click **Back** through the rule.

11. Click **Finish** to close the rule wizard.

The rule you just created is now displayed on the **Firewall rules** table.

12. Take the new rule into use:

To take this new service into use you will have to create a new Internet Shield rule that allows the use of the **HTTP 8000** firewall service in the currently used Internet Shield security level. In this case you can select the new service on the **Rule wizard > Service** page and you do not have to define any alerts on the **Rule Wizard > Advanced options** page.

Troubleshooting

Topics:

- [*Policy Manager Server and Policy Manager Console*](#)
- [*Policy Manager Web Reporting*](#)
- [*Policy distribution*](#)


This section contains troubleshooting information and frequently asked questions about Policy Manager.


If you encounter problems when using the product, you can find possible solutions in this section.

19.1 Policy Manager Server and Policy Manager Console

Issues regarding Policy Manager Server and Policy Manager Console are described here.

Question	Answer
Why doesn't Policy Manager Server start?	<p>Runtime errors, warnings and other information can be found in the files:</p> <pre><F-Secure>\Management Server 5\logs\fspms-webapp-errors.log and <F-Secure>\Management Server 5\logs\fspms-service.log</pre> <p>Check that the access rights (properties/security/permissions) includes the Local Service user account. If Local Service is not listed as an authorized user, add the user manually, and set the access rights to Full Control. Propagate the access rights to the Management Server 5 directory (by default C:\Program Files\F-Secure\Management Server 5) and all its subdirectories. After these changes, restart the Policy Manager Server service or reboot the computer.</p> <p>The Local Service account is the Windows system account, and the Policy Manager Server service is started under this user account. With normal installation, the directory access rights for the Management Server 5 directory are automatically set correctly. If the directory is copied by hand or, for example, restored from backup, the access rights might be deleted. In this case execute the steps described in the previous paragraph.</p>
Where are the log files and configuration files located for Policy Manager Server?	<p>The log files are located in:</p> <pre><F-Secure>\Management Server 5\logs</pre> <p>The configuration files are in:</p> <pre><F-Secure>\Management Server 5\conf</pre>
Where are the Policy Manager Console log files located?	<p>The log file is:</p> <pre><F-Secure>\Administrator\lib\administrator.error.log</pre> <p>Policy changes applied with the Distribute policy operation are logged to:</p> <pre>fspms-policy-audit.log</pre>
The migration wizard didn't start up during installation. Can I run it separately outside installation?	<p>You can start the migration wizard by running this executable:</p> <pre><F-Secure>\Management Server 5\bin\fspms-migrator-launcher.exe</pre>

Question	Answer
I have lost the admin password. Can I retrieve or reset the password?	<p>If you have lost the password for the <code>admin</code> user, or if the account was accidentally deleted, you can reset the user account with the following tool:</p> <pre data-bbox="837 342 1433 369"><F-Secure>\bin\reset-admin-account.bat</pre> <p> Note: You need to stop Policy Manager Server manually before running the reset tool.</p>
How can the server role change stop Policy Manager Server from working?	<p>The Domain Controller server and Member/Standalone server use different types of accounts: domain accounts on Domain Controller and local accounts on Member server. Because Policy Manager Server uses its own account to run, this account becomes invalid with the role change.</p> <p>The easiest way to restore Policy Manager Server after a server role change is to re-install Policy Manager Server with the Keep existing settings option selected. This will recreate the Policy Manager Server account and reset all file access rights to the correct ones.</p>
How can Windows security hardening stop Policy Manager Server from working?	<p>Access rights restrictions, especially restrictions under the <code>%SystemRoot%</code> directory (<code>c:\windows</code> or <code>c:\winnt</code>) can stop Policy Manager Server from starting, as its own account (Local Service) needs to be able to read the network related DLL and SYS files.</p> <p>You must allow the Local Service account to 'read' the following directories:</p> <pre data-bbox="837 1308 1305 1435">%SystemRoot% %SystemRoot%\system32 %SystemRoot%\system32\drivers</pre> <p>Some service restrictions can also prevent the Policy Manager Server service from starting. For more information on these please consult the Microsoft Windows Server documentation.</p>
Why does Policy Manager Console lose the connection to Policy Manager Server?	<p>If Policy Manager Console is run on a separate computer from Policy Manager Server, then the connection may be affected by network problems. There have been numerous reports where, for example, a network switch change caused loss-of-connection problems between Policy Manager Console and Policy Manager Server. Usually these problems are fixed by updating the network drivers to the latest version in the affected machines or by reconfiguring the new switch and the network cards on the Policy Manager Console and Policy Manager Server machines.</p>

Question	Answer
	<p>If Policy Manager Console is installed on the same computer as Policy Manager Server, then there is a risk that Policy Manager Server could be under such a heavy network load that it does not have any free network connections available. Policy Manager Console and all hosts are competing for the same network resources.</p> <p>Possible solutions are to increase the polling intervals of hosts, to change the Windows networking timeouts shorter, or to increase the number of Windows networking ports.</p> <p>Useful Windows networking settings are:</p> <pre>HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\MaxUserPort (maximum number of network ports, default = 5000)</pre> <pre>HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpTimedWaitDelay (time to wait before closing inactive network connection, default = 240 seconds).</pre> <p>The <code>netstat -an</code> command can be used to check whether there are too many connection open to the server.</p>
<p>How can I change the ports where the server listens for requests?</p>	<p>By default, the Policy Manager Server admin module (the component that handles requests coming from Policy Manager Console) listens in port 8080, and the Policy Manager Server host module (the component that handles requests from workstations) listens in port 80. These can be changed during installation.</p> <p>If you need to change the port numbers after installation:</p> <ol style="list-style-type: none"> 1. Stop Policy Manager Server. 2. Open the <code>HKEY_LOCAL_MACHINE\SOFTWARE\Data Fellows\F-Secure\Management Server</code> registry key. 3. Edit the <code>AdminPortNum</code> (admin module) and <code>HttpPortNum</code> (host module) values and enter the new port numbers. <p>Make sure Decimal is selected as the Base option when entering the new port number.</p> 4. Start Policy Manager Server. <p> Caution: If you have workstations already configured to access Policy Manager Server (through the Policy Manager Server host module) you should not change the Policy Manager Server host port where agents communicate, since you might reach a state where the workstations will not be able to contact the server.</p>

19.2 Policy Manager Web Reporting

The locations of log and configuration files are given here.

Question	Answer
Where are the log files and configuration files located for Web Reporting?	<p>The log files are located in:</p> <pre><F-Secure>\Management Server 5\Web Reporting\logs</pre> <p>The configuration files are in:</p> <p>The <code>HKEY_LOCAL_MACHINE\SOFTWARE\Data Fellows\F-Secure\Management Server 5</code> registry key</p> <p>See also the Policy Manager Server configuration files:</p> <pre><F-Secure>\Management Server 5\conf</pre>

19.3 Policy distribution

You will find information on common error messages relating to policy distribution here.

Question	Answer
When distributing a policy, Policy Manager Console shows an error message about an invalid policy value. What should I do?	See below for information on error messages you may see during policy distribution, and for the reasons and solutions.

Error message	Reason	Solution
"<setting name>" has value out of restriction	Reason 1:	Divide the hosts into subdomains so that it is possible to set the new value for hosts with the new software installed, and to use some older policy values for other hosts. To do this:
"<setting name>" has invalid restriction	The value selected from a choice list is not among the choices on a sub-domain or host, too high or low values are specified as range restriction boundaries, or an empty choice list is specified.	1. Group the hosts into subdomains based on the installed product version. For example, group hosts that have Client Security 6.x installed into one sub-domain, and hosts that have Client Security 7.x installed into another domain.
"<setting name>" has invalid value: "<value>"	When a domain includes hosts that have different product versions installed, the MIB settings from the newest product version are used for editing the policy values. As result, policy distribution may fail on hosts that have older versions of the software installed, because the older versions do not support the new policy settings or values.	2. Set most of the settings on the root domain and create a sub-domains for exceptions. This is a good solution if you have only a few hosts with the older software versions installed.

Error message	Reason	Solution
	Reason 2: You entered an integer value that is outside of the range restrictions.	
"<setting name>" is required but undefined	The setting is required but it is currently empty.	Enter a value or apply the Clear operation to re-inherit the value from parent domain or MIB. If the value is empty on several domain levels, you may need to apply the Clear operation several times.
