F-Secure Client Security

Administrator's Guide

Contents

Chapter 1: Introduction....9

System requirements....10
Policy Manager Server....10
Policy Manager Console....10
Main components....12
Features....13
Product registration....14
Application management....15
Basic terminology....16

Chapter 2: Installing the product....17

Installation steps....18
Download and run the installation package....18
Select components to install....18
Complete installation of the product....19
Run Policy Manager Console....19
Changing the web browser path....21
Uninstalling the product....22

Chapter 3: Anti-virus mode user interface....23

Policy domains tab....24
Management tabs....25
Summary tab....25
Settings tab....27
Status tab....35
Alerts tab....37
Reports tab....37
Installation tab....38
Operations tab....38
The toolbar....39
Menu commands....40
Settings inheritance....42
How settings inheritance is displayed on the user interface....42
Locking and unlocking all settings on a page at once....43
Settings inheritance in tables....43

Chapter 4: Setting up the managed network....45

Logging in....46

Connection properties....46
Changing communication preferences....46
Managing domains and hosts....48
Adding policy domains....48
Adding hosts....49
Adding hosts in Windows domains....49
Importing autoregistered hosts....49
Push installations....51
Policy-based installation....53
Local installation and updates with pre-configured packages....55
Local installation and Policy Manager....58
System requirements....58
Uninstall other antivirus programs....58
Installation steps....59
Installing on an infected host....60
Checking that the management connections work....61

Chapter 5: Configuring virus and spyware protection....63

Configuring automatic updates....64
How do automatic updates work?....64
Automatic update settings....64
Configuring automatic updates from Policy Manager Server....64
Configuring Policy Manager Proxy....65
Configuring clients to download updates from each other....65
Configuring real-time scanning....67
Real-time scanning settings....67
Enabling real-time scanning for the whole domain....68
Forcing all hosts to use real-time scanning....69
Excluding Microsoft Outlooks's .pst file from real-time scanning....69
Configuring DeepGuard....70
DeepGuard settings....70
DeepGuard server queries....70
Configuring rootkit scanning (Blacklight)....72
Rootkit scanning settings....72
Launching a rootkit scan for the whole domain....72
Configuring e-mail scanning....73
E-mail scanning settings....73
Enabling e-mail scanning for incoming and outgoing e-mails....74
Configuring web traffic (HTTP) scanning....75
Web traffic scanning settings....75
Enabling web traffic scanning for the whole domain....75
Excluding a web site from HTTP scanning....75
Configuring spyware scanning....77
Spyware control settings....77

Setting up spyware control for the whole domain....78
Launching spyware scanning in the whole domain....79
Allowing the use of a spyware or riskware component....79
Managing quarantined objects....80
Deleting quarantined objects....80
Releasing quarantined objects....80
Preventing users from changing settings....82
Setting all virus protection settings as final....82
Configuring alert sending....83
Setting Client Security to send virus alerts to an e-mail address....83
Disabling Client Security alert pop-ups....83
Monitoring viruses on the network....84
Testing your antivirus protection....85

Chapter 6: Configuring Internet Shield....87

Global firewall security levels....88
Design principles for security levels....89
Configuring security levels and rules....90
Selecting an active security level for a workstation....90
Configuring a default security level for the managed hosts....90
Adding a new security level for a certain domain only....90
Configuring network quarantine....93
Network quarantine settings....93
Turning network quarantine on in the whole domain....93
Fine-tuning network quarantine....93
Configuring rule alerts....94
Adding a new rule with alerting....94
Configuring application control....97
Application control settings....97
Setting up application control for the first time....98
Creating a rule for an unknown application on root level....99
Editing an existing application control rule....100
Turning off application control pop-ups....100
Using alerts to check that Internet Shield works....102
Configuring intrusion prevention....103
Intrusion prevention settings....103
Configuring IPS for desktops and laptops....103

Chapter 7: How to check that the network environment is protected.105

Checking that all the hosts have the latest policy....106
Checking that the server has the latest virus definitions....107
Checking that the hosts have the latest virus definitions....108
Checking that there are no disconnected hosts....109
Viewing scanning reports....110

Viewing alerts....111
Creating a weekly infection report....112
Monitoring a possible network attack....113

Chapter 8: Upgrading software....115
Using the installation editor....116

Chapter 9: Local host operations....119
Scan manually....120
How to select the type of manual scan....120
Clean malware automatically....121
View the results of manual scan....121
Scan at set times....122
Schedule a scan....122
Cancel a scheduled scan....122
View the results of scheduled scan....123
Where to find firewall alerts and log files....124
View firewall alerts....124
View the action log....125
Monitor network traffic with packet logging....125
Connecting to Policy Manager and importing a policy file manually....128
Suspending downloads and updates....129
Allowing users to unload F-Secure products....130

Chapter 10: Virus information....131
Malware information and tools on the F-Secure web pages....132
How to send a virus sample to F-Secure....133
How to package a virus sample....133
What should be sent....133
How to send the virus sample....134
What to do in case of a virus outbreak?....136

Chapter 11: Setting up the Cisco NAC plugin....137
Installing the Cisco NAC plugin....138
Importing posture validation attribute definitions....139
Using attributes for the application posture token....140

Chapter 12: Advanced features: virus and spyware protection...141
Configuring scheduled scanning....142
Advanced DeepGuard settings....143
Notifying user on a deny event....143
Letting an administrator allow or deny program events from other users....143

Allowing or denying events requested by a specific application automatically.....143
Configuring Policy Manager Proxy.....145
Configuring automatic updates on hosts from Policy Manager Proxy.....146
Excluding an application from the web traffic scanner.....147

Chapter 13: Advanced features: Internet Shield.....149

Managing Internet Shield properties remotely.....150
Using packet logging.....150
Using the trusted interface.....150
Using packet filtering.....150
Configuring security level autoselection.....152
Troubleshooting connection problems.....153
Adding new services.....154
Creating a new Internet service based on the default HTTP.....154
Setting up dialup control.....156
Allowing and blocking phone numbers.....156
Using call logging.....156

Chapter 14: Modifying prodsett.ini.....159

Configurable prodsett.ini settings.....160

Chapter 15: E-mail scanning alert and error messages.....167

Alert and error messages.....168

Chapter 16: Products detected or removed during client installation.171

Product list.....172

Chapter

1

Introduction

Topics:

- *System requirements*
- *Main components*
- *Features*
- *Product registration*
- *Application management*
- *Basic terminology*

Policy Manager can be used for:

- defining security policies,
- 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.

System requirements

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

Policy Manager Server

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

Operating system:	Microsoft Windows: • 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; Standard, Enterprise or Web Server editions
Processor:	P4 2 GHz processor or faster. Managing more than 5000 hosts or using Web Reporting requires P4 3 GHz level processor or faster.
Memory:	512 MB RAM, 1 GB RAM recommended. Managing more than 5000 hosts or using Web Reporting requires 1 GB RAM.
Disk space:	5 GB of free hard disk space; 8 GB or more is recommended. The disk space requirements depend on the size of the installation. In addition to this it is recommended to allocate about 1 MB per host for alerts and policies. The actual disk space consumption per host is hard to anticipate, since it depends on how the policies are used and how many installation packages are stored.
Network:	10 Mbit network. Managing more than 5000 hosts requires a 100 Mbit network.

Policy Manager Console

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

Operating system:	Microsoft Windows: • Windows XP Professional (SP2 or higher) • Windows Vista (32-bit or 64-bit) with or without SP1; Business, Enterprise or Ultimate editions • Windows 7 (32-bit or 64-bit); Professional, Enterprise or Ultimate editions • 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; Standard, Enterprise or Web Server editions
Processor:	P4 2 GHz processor or faster. Managing more than 5000 hosts requires P4 3 GHz processor or faster.
Memory:	512 MB of RAM. Managing more than 5000 hosts requires 1 GB of memory.
Disk space:	200 MB of free hard disk space.
Display:	Minimum 16-bit display with resolution of 1024x768 (32-bit color display with 1280x1024 or higher resolution recommended).
Network:	10 Mbit network. Managing more than 5000 hosts requires a 100 Mbit network.

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 *HTTP protocol*, which ensures trouble-free performance on both *LAN* and *WAN*.

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.

Features

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

Software distribution

- 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:
  - 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

- 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

- Reporting to the Event Viewer (local and remote logs), e-mail, and report files and creation of event statistics.

Performance management

- Statistics and performance data handling and reporting.

Task management

- Management of virus scanning tasks and other operations.

Product registration

You have the option of providing F-Secure with information regarding the use of Policy Manager by registering your product.

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*).

Why does F-Secure collect data?

In order to improve our service, we collect statistical information regarding the use of F-Secure products. To help F-Secure provide better service and support, you can allow us to link this information to your contact information. To allow this, please enter the customer number from your license certificate during the installation of Policy Manager.

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.

What do I benefit from submitting information to F-Secure?

When you contact our support, we can provide a solution to your problem more quickly based on the information collected. In addition, with this information we can further develop our product and services to match the needs of our customers even better.

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 employees can access the data.

Application management

Policy Manager includes various components to manage applications within your network.

Management Agent

The Management Agent enforces the security policies set by the administrator on the managed hosts. It acts as a central configuration component on the hosts, and for example, interprets the policy files, sends autoregistration requests and host status information to Policy Manager, and performs policy-based installations.

Cisco Network Admission Control (NAC) Support

F-Secure Corporation participates in the *Network Admission Control* (*NAC*) collaboration led by Cisco Systems®. The Cisco NAC can be used to restrict the network access of hosts that have too old virus definition databases, or the antivirus or firewall module disabled.

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.

Chapter

2

Installing the product

Topics:

- *Installation steps*
- *Changing the web browser path*
- *Uninstalling the product*

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

Installation steps

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

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.

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 your customer number and then click **Next**.
   You can find your customer number in the license certificate provided with the product.
4. If setup does not detect any previous installation of Policy Manager, it asks you to confirm if a previous installation of the product exists:
   - If a previous version has been installed, select **I have an existing F-Secure Policy Manager installation**. Enter the communication directory path of the installed Policy Manager. The contents of this directory will be copied under `<server installation directory>\commdir\` (communication directory under the Policy Manager Server installation directory), and this will be the directory that Policy Manager Server will use as a repository. You can use the previous `commdir` as a backup, or you can delete it once you have verified that Policy Manager Server is correctly installed.
   - If no previous version has been installed, select **I do not have an existing F-Secure Policy Manager**. This will not require an existing `commdir`, and will create an empty `commdir` in the default location (under `<F-Secure Policy Manager 5 installation directory>\commdir`).
5. Click **Next** to continue.
6. Select whether you want to keep the existing settings or change them:

Note: This dialog is displayed only if a previous installation of Policy Manager Server was detected on the computer.

- By default the setup keeps the existing settings. Select this option if you have manually updated the Policy Manager Server configuration. This option automatically keeps the existing administration, host and web reporting ports.
- If you want to change the ports from the previous installation, select **Change settings**. This option overwrites the edited configuration and restores the default settings.

7. Click **Next** to continue.
8. 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 HTTP port is 8080.

     Note: If you want to change the default port for communication, you will also need to change the **HTTP Port Number** setting in Policy Manager Console.

     By default, access to the **Administration** module is restricted to the local machine. This is the most secure way to use the product. When using a connection over a network, please consider securing the communication with F-Secure SSH.
   - 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 port is 8081.

     By default, access to Web Reporting is allowed also from other computers. If you want to allow access only from this computer, select **Restrict access to the local machine**.
9. Click **Next** to continue.
10. Select the product installation package(s) to install from the list of available packages, then click **Next** to continue.

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.

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 Console** ➤ **F-Secure Policy Manager Console**.

   When Policy Manager Console is run for the first time, the **Console Setup Wizard** collects the information needed to create an initial connection to the server. The first page of the Policy Manager Console setup wizard summarizes the installation process.
2. Click **Next** to continue.
3. Select your user mode according to your needs:

- **Administrator mode** - enables all administrator features.
- **Read-only mode** - allows you to view administrator data, but no changes can be made. If you select **Read-only mode**, you will not be able to administer hosts. To change to **Administrator mode**, you will need the `admin.pub` and `admin.prv` administration keys.

4. Click **Next** to continue.
5. Enter the address of the Policy Manager Server that is used for communicating with the managed hosts, then click **Next** to continue.
6. Enter the path where the administrator's public key and private key files will be stored.

   By default, key files are stored in the Policy Manager Console installation directory: `Program Files\F-Secure\Administrator`.
7. Click **Next** to continue.

   Note: If the key-pair does not already exist, it will be created later in the setup process.
8. Move your mouse cursor around in the window to initialize the random seed used by the management key-pair generator.

   Using the path of the mouse movement ensures that the seed number for the key-pair generation algorithm has enough random variation.

   When the progress indicator has reached 100%, the **Passphrase** dialog box will open automatically.
9. Enter a passphrase, which will secure your private management key.
10. Re-enter your passphrase in the **Confirm passphrase** field and click **Next**.
11. Click **Finish** to complete the setup process.
    Policy Manager Console will generate the management key-pair. After the key-pair is generated, Policy Manager Console will start.

    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 Anti-virus for Windows Servers. 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, you must provide them with a copy of the `admin.pub` key file (or access to it). If you install the F-Secure products on the workstations remotely with Policy Manager, a copy of the `admin.pub` key file is installed automatically on them. However, if you run the setup from a CD, you must transfer a copy of the `admin.pub` key file manually to the workstations. The best and most secure method is to copy the `admin.pub` file to a diskette and use this diskette for workstation installations. Alternatively, you can put the `admin.pub` file in a directory that can be accessed by all hosts that will be installed with remotely managed F-Secure products.

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.

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.

Chapter

3

Anti-virus mode user interface

Topics:

- *Policy domains tab*
- *Management tabs*
- *The toolbar*
- *Menu commands*
- *Settings inheritance*

This section provides a reference of the settings available on the various pages of the **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**, **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.

Policy domains tab

You can perform actions for policy domains and hosts within the **Policy domains** tab.

In the **Policy domains** tab, you can do the following:

- Add a new policy domain by clicking 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 by clicking the icon.
- Find a host.
- View the properties of a domain or host. All hosts and domains should be given unambiguous names.
- Import autoregistered hosts.
- Autodiscover hosts from a Windows domain.
- Delete hosts or 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 or by right-clicking the selected host or domain. The **Autodiscover** and **Import autoregistered hosts** operations are also available on the **Installation** tab.

Note: 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.

Management tabs

This section describes the management tabs (**Summary**, **Settings**, **Status**, **Alerts**, **Reports**, **Installation** and **Operations**), and the different pages on each of these tabs.

Summary tab

The **Summary** tab is designed to display the most important information concerning the selected domain(s) or host(s) at a glance.

When a domain is selected, the **Summary** tab displays information about the whole domain. When a single host is selected, you can see more detailed information concerning the host.

If some of the settings displayed on the **Summary** tab require your immediate attention or action, an icon is displayed beside the setting. The icons can be interpreted as follows:

	Warns of an error situation that requires your action. The error cannot be fixed automatically. The icon is displayed, for example, when the latest policies have not been distributed, or when virus definitions on hosts are outdated.
	Warns of a situation that may require your action. This does not create security problems yet, but it may lead to a security problem later on if the problem is not fixed now. The icon is displayed, for example, when there are disconnected hosts.

The information displayed on the **Summary** tab depends on what is selected in the **Policy domains** tab:

- When a domain is selected, the **Summary** tab displays information divided into the following sections: **Policy Manager**, **Domain**, **Virus Protection for Workstations**, and **Internet Shield**.
- When a host is selected, the sections are: **Policy Manager**, **Host**, **Virus Protection** and **Internet Shield**.

Summary tab when a domain is selected

The information described here is displayed on the **Summary** tab when a domain is selected on the **Policy domains** tab.

Policy Manager

In the **Policy Manager** section you can:

- See the current **Policy** distribution status (**Saved**/**Unsaved**, **Distributed**/**Undistributed**), and when necessary, save the policy data and distribute the new policies to hosts.
- See the status of the virus definitions on the server.
- See the status of the spyware definitions on the server.
- See the status of **DeepGuard** updates on the server.
- See the number of new autoregistered hosts. If there are new hosts, you can add them to the domain by clicking **Add these hosts to a domain...**.
- Autodiscover hosts from a Windows domain by clicking **Autodiscover Windows hosts...**.

Domain

In the **Domain** section you can:

- See the number of hosts that have the latest policy and access a summary of their latest policy update by clicking **View hosts's latest policy update...**. This takes you to the **Status** tab and **Centralized management** page.
- See the number of disconnected hosts. You can also access a detailed list displaying the hosts' connection status by clicking **View disconnected hosts...**, which takes you to the **Status** tab and **Centralized management** page.
- See a summary of new alerts. If you want to get more detailed information on the alerts, you can click on **View alerts by severity...** link to access the **Alerts** tab.

  The severity of the alerts is indicated by the following icons:

Icon	Reference	Description
	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.

Virus Protection for Workstations

In the **Virus Protection for Workstations** section you can:

- See how many hosts in the domain have **Virus Protection** installed.
- See how many hosts in the domain have **Real-time scanning** enabled. If you want to see which hosts have it enabled and which do not, click **View hosts' overall protection...** to access more detailed information on the **Status** tab and **Overall protection** page.
- See how many infections have been found in the domain. If you want to see host specific infection information, click **View hosts' infection status...** to access the **Status** tab and **Overall protection** page.
- See how many of the hosts have the latest virus definitions and whether the virus definitions on some hosts are recent or outdated.
  - **Recent** means that the virus definitions are not the latest ones.
  - **Outdated** means that the virus definitions are older than the configured time limit.

    Note: If you have F-Secure Anti-Virus 5.40 installed on some hosts, the virus definitions version on these hosts is displayed as **Unknown**.

  If you need to update the virus definitions on some hosts, click **Update virus definitions...**, which takes you to the **Operations** tab.

Internet Shield

In the **Internet Shield** section you can:

- See how many hosts in the domain have Internet Shield installed.
- See what is the most common latest attack and what percentage of the domain has been affected. If you want to get more detailed information on the latest attacks, you can click **View Internet Shield Status...** to access the **Status** tab and **Internet Shield** page.

Summary tab when a host is selected

When a host is selected in the **Policy domains** tab, the **Summary** tab displays more detailed information in the **Host** section.

Host

In the **Host** section you can:

- See the name of the selected host displayed beside **Computer identity**. You can also access more detailed information on the host by clicking **View host properties...**. This takes you to the **Status** tab and **Host properties** page.
- See what is the active protocol (HTTP or file sharing), the address of the Policy Manager Server the host is connected to and the date and time of the last connection.
- See whether the policy file the host is using is the latest one or not.
- See whether the host is disconnected or not.
- See a summary of new alerts. If you want to get more detailed information on the alerts, click on **View alerts by severity...** to access the **Alerts** tab.

Virus Protection for Workstations

In addition to the information displayed when a domain is selected, the **Virus Protection for Workstations** section also displays the version number of the virus definitions.

Internet Shield

In addition to the information displayed when a domain is selected, the **Internet Shield** section also displays the currently selected Internet Shield security level for the host.

Settings tab

The **Settings** tab contains 12 different pages that are used for configuring the components of Client Security, which are described briefly in this section.

Context menu on settings pages

By right-clicking any setting on a **Settings** tab page you can access a context menu that contains the following options:

Clear	This option clears a setting that has been redefined on the current level.
Force value	The **Force value** menu item is available only when a policy domain is selected. You can use this command to enforce the current domain setting to be active also in all subdomains and hosts. In practice, this operation clears the corresponding setting in all subdomains and hosts below the current domain, enabling the inheritance of the current value to all subdomains and hosts. Use this menu entry cautiously: all values defined in the subdomains or hosts under the selected domain are discarded, and cannot be restored.
Show domain values	The **Show domain values** menu item is available only when a policy domain is selected. You can use this command to view a list of all policy domains and hosts below the selected policy domain, together with the value of the selected field. Click any domain or host name to quickly select the domain or host on the **Policy domains** tab. It is possible to open more than one **Domain value** dialog simultaneously.
Locate in advanced mode	This option is for advanced users. It takes you to the **Advanced mode** user interface and selects the setting there.

Automatic updates

The **Automatic Updates** page is divided into two sections; **Automatic Updates** and **Neighborcast**.

Automatic Updates

In the **Automatic Updates** section you can:

- Enable or disable automatic updates. Note that deselecting this setting disables all ways for the host to get automatic updates.
- Specify the time interval for polling updates from Policy Manager Server.
- See a list of Policy Manager Proxy servers. You can also add new servers on the list, delete servers from the list and edit their addresses and priorities.
- Select whether an HTTP proxy can be used and specify the HTTP proxy address.
- Select whether clients should download updates from each other in addition to any servers or proxies.

Neighborcast

Neighborcast allows clients to download updates from each other as well as from any available servers or proxies. In this section you can:

- Set a client to serve updates to other clients.
- Set a client to download updates from other clients serving updates.
- Choose the port to use.

Real-time scanning

The settings displayed on this page affect the real-time scanning of hosts in the selected domain.

Unless otherwise stated, the settings listed on this page are valid for all Client Security versions. To view and configure the settings that are no longer valid for Client Security 9 or higher and Anti-virus for Windows Servers 9 or higher, but that are valid for older product versions, click **Settings for older clients (7.x, 8.x)...**.

General

In this section you can turn real-time scanning on or off.

File Scanning

In this section you can:

- Select which files will be scanned and define the included extensions.
- Select whether certain extensions will be excluded from the scan and define what they are.
- Select whether the users can exclude objects from real-time scanning.
- Select whether network drives are included in real-time scanning.
- Define the action to take automatically when an infected file is found (for Client Security 9 or higher and Anti-virus for Windows Servers 9 or higher).
- Turn protection of the "Hosts" file on or off.
- Select whether tracking cookies are included in the scan.

DeepGuard

In this section you can:

- Turn DeepGuard on or off.
- Select the action to take when a system modification attempt is detected.
- Select whether to query a remote server to improve detection accuracy.
- Turn advanced process monitoring on or off.

Manual scanning

The settings displayed on this page affect the scans that are run manually by the host users.

Manual File Scanning

In this section, the following options are available for selecting what to scan:

- Select which files will be scanned and define the included extensions.
  - **All files**: All files will be scanned, regardless of their file extension. Forcing this option is not recommended because it might slow down system performance considerably.
  - **Files with these extensions**: Files with specified extensions will be scanned. To specify files that have no extension, type `.`. You can use the wildcard `?` to represent any letter. Enter each file extension separated by a space.
- Select whether to scan inside compressed files. Select this check box to scan inside compressed `ZIP`, `ARJ`, `LZH`, `RAR`, `CAB`, `TAR`, `BZ2`, `GZ`, `JAR` and `TGZ` files. Scanning inside large compressed files might use a lot of system resources and slow down the system.
- Select whether certain extensions will be excluded from the scan and define what they are. You can specify whether some files will not be scanned, and enter the extensions that will be excluded from scanning in the **Excluded extensions** field.
- Select whether the users can exclude objects from real-time scanning. When **Enable excluded objects** is selected, the users can specify individual files or folders that will not be scanned.
- From the **Action on infection** drop-down list, you can select the action Client Security will take when an infected file is detected. Choose one of the following actions:

Action	Definition
Ask after scan	Starts the **Disinfection Wizard** when an infected file is detected.
Disinfect automatically	Disinfects the file automatically when a virus is detected.
Rename automatically	Renames the file automatically when a virus is detected.
Delete automatically	Deletes the file automatically when a virus is detected. Note that this option also deletes the object the virus is attached to, so this option is not recommended.
Report only	Indicates that a virus is found, and does not let you open the infected object. This option only reports, it does not take any action against the virus.

Rootkit Scanning

In this section you can:

- Turn rootkit scanning on or off.
- Include or exclude rootkit scanning from full computer check.
- Specify whether detected suspicious items are shown in the disinfection wizard and in the scanning report after a full computer check.

Scheduled Scanning

The **Configure scheduled scanning in advanced mode...** link takes you to the **Advanced mode** user interface, where scheduled scanning can be configured.

Manual Boot Sector Scanning

In this section you can:

- Turn manual scanning for floppy disk boot sectors on or off.
- Select the action to take when an infection is found.

Spyware control

The settings displayed on this page are spyware-specific, and provide additional spyware-specific settings for real-time and manual scanning.

Applications Excluded from Spyware Scanning

This table displays a list of spyware and riskware that the administrators have allowed to run on the hosts.

Spyware and Riskware Reported by Hosts

This table displays spyware and riskware that the hosts have reported, and spyware and riskware that are quarantined at the host(s). The table displays the type and the severity for each detected spyware and riskware application. All spyware and riskware with the **Potentially active** status were allowed to run on the host by the administrator.

If you want users to be able to decide the spyware and riskware items that are allowed, you can do so with the **Allow users to define the allowed spyware items** drop-down list.

Quarantine management

This page is used to manage malware that has been quarantined on managed hosts.

Quarantine content

This table displays a list of quarantined items on the hosts. Each table row displays the object type, name, file path and the number of hosts on which the object has been quarantined.

Actions to perform on quarantined objects

This table displays a list of the quarantined objects that have been processed. The quarantined objects are either released (allowed) or deleted. The action indicated here is distributed to the managed hosts, so whenever the malware in question is detected on a host, the selected action is applied. When the action is set to **Release**, an appropriate exclusion rule needs to be in place on the **Spyware control** or **Real-time scanning** page, depending on the object type, to prevent the object from being quarantined in future.

The applied actions are automatically cleaned from this table once there are no pending actions left for the corresponding hosts (no hosts report this object as quarantined).

E-mail scanning

This page includes separate settings for incoming and outgoing e-mail scanning. The settings in the **General** section are common for both.

Incoming E-mail Scanning

In this section you can:

- Turn incoming e-mail scanning on or off.

- Select the action to take when an incoming infected attachment is detected.
- Select the action to take when scanning fails.
- Select the action to take when malformed message parts are detected.

Outgoing E-mail Scanning

In this section you can:

- Turn outgoing e-mail scanning on or off.
- Select the action to take when an outgoing infected attachment is detected.
- Select the action to take when scanning fails.
- Select the action to take when malformed message parts are detected.
- Select if the blocked messages are saved in the end user's outbox.

General

In this section you can:

- Select whether e-mail scanning also scans compressed attachments.
- Select whether scanning progress is shown and define the time after which it is shown.
- Select whether a scanning report is shown if infected e-mails are found or if scanning fails.

Web traffic scanning

The settings displayed on this page are related to the scanning of web traffic, for example downloaded files.

General

In this section you can turn HTTP scanning on or off.

HTTP Scanning

- Select the action to take on infection.
- Select the action to take on scanning failure.
- Select whether compressed files are included in scanning.

Trusted HTTP Sites

This table displays a list of HTTP sites that are defined as trusted. Downloads from these sited are not scanned for viruses.

Firewall security levels

The settings on this page are used for determining the overall firewall security level on the selected host or domain.

General

In this section you can:

- Select the predefined security level for the host.
- Configure security level autoselection by clicking **Configure security level autoselection in advanced mode...**. This takes you to the **Advanced mode** user interface.
- Enable the firewall rules of the current security level to be applied to inbound and outbound packets by selecting **Enable firewall engine**.
- Enable the use of the trusted interface.
- Turn application control on or off.

Firewall Security Levels Table (Global)

This table displays the security levels that are available globally in the system. The security levels table is the same for all policy domains, but enabling and disabling individual security levels can be done per policy domain.

Network Quarantine

In this section you can:

- Turn network quarantine on or off.
- Specify the virus definitions age, after which **Network Quarantine** is activated.
- Specify whether turning real-time scanning off on the host activates **Network Quarantine**.

Intrusion Prevention

In this section you can:

- Turn intrusion prevention on or off.
- Select the action to take when a malicious packet is detected. The options available are:
  - Log and drop.
  - Log without dropping.
- Define the centralized alert severity.
- Define the alert and performance level.

Firewall rules

This page is used to define the rules applied to the different firewall security levels.

Firewall Rules Table

This table lists the rules defined for different security levels. You can select the level from the **Internet Shield security level being edited** drop-down menu. When the selected security level is changed, the rules associated with the new security level are displayed in the table.

When the firewall is in use, the firewall rules are checked in the order in which they are displayed in the table, from top to bottom. For security levels with the **Normal** filtering mode, it is possible to define domain or host-specific rules. When **Allow users to define new rules** is selected, the end users are also allowed to define new rules for that security level. The table also displays the location for these rules.

The **Firewall Rules** table displays the following information for each rule:

- Whether the rule is turned on or off
- The name and comment for the rule
- The type of rule (allow/deny)
- The related service and direction: **<=** for an inbound service, **=>** for an outbound service and **<=>** for a bidirectional service.
- The affected remote hosts
- Whether alert sending is turned on or off
- Whether the rule is applied only when a dialup link is used.

To move the location where user-defined new rules are placed in the table, click **User defined rules go here**. You can then use the **Move Up** and **Move Down** buttons to move where the slot in the table.

In addition, **Application control** will automatically create rules on the host for applications that have been allowed. The rules are placed just before the first **Deny rest** rule in the rules table, which is the first deny rule with the **All traffic** service and **Any** remote host. The rules allow incoming packets to server applications,

and the firewall then allows outgoing reply packets from the server applications. Outgoing packets from ordinary applications need to be allowed by the rules in the firewall rules table.

Firewall 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. It is most often described by what protocol and port it uses.

Firewall Services Table (Global)

This table displays a list of services that have been defined for the firewall. It is also possible to create or allow the end users to create new services for the firewall.

You can also restrict users from adding new services by clicking **Restricted** and then selecting **Fixed size** in the dialog that opens. When this is selected, end users cannot add or delete rows from the tables.

Application control

The settings on this page are used to control applications that use inbound and outbound network connections.

Application Rules for Known Applications

This section displays a list of known applications and the rules defined for them for inbound and outbound connection attempts.

Unknown Applications Reported by Hosts

This list displays applications that the hosts have reported and for which no rules exist yet.

In this section you can also:

- Select the default action for client applications.
- Select the default action for server applications.
- Select whether new applications are reported to you by selecting the Report new unknown applications check box.

Automatic decisions

This section allows you to select whether the user is prompted for a decision when the application has been identified by DeepGuard or the real-time protection network.

Message for User

This section contains the following options:

- Select whether users see default messages on connection attempts from an unknown application
- **Define default messages...** opens the **Define Messages** window where you can define messages for known and unknown applications on allow, deny and user decision.

Browsing protection

The settings on this page define the browsing protection settings for hosts that have Client Security 9 or higher installed.

Exploit Shield

In this section, you can select whether browsing protection uses exploit shields to block access to web sites that contain exploits.

Exploit shields identify and prevent malicious web sites from using such vulnerabilities to, for example, force an unauthorized download that contains malware. Exploit shields do not protect you against files that you

download intentionally and may contain malware; that type of security threat is covered by virus and spyware scanning.

Reputation based protection

The settings in this section define how ratings for web sites are shown and whether web sites rated as harmful are blocked for users. These safety ratings are based on information from several sources, such as F-Secure malware analysts and F-Secure partners, as well as ratings given by other users of browsing protection.

Trusted sites

If browsing protection blocks access to a page that you trust and want users to access, you can define it as a trusted site. All trusted sites will be listed here.

Advanced settings

You can click **Configure advanced settings** to go to the browsing protection settings in the **Advanced mode** view.

Alert sending

The settings on this page define how alerts are shown and forwarded to administrators.

General

In this section you can select the alerting language.

E-mail Alert Sending

- Define the e-mail server address (SMTP).
- Define the e-mail sender address and e-mail subject to be used when forwarding alerts by e-mail.

Alert Forwarding

This table can be used to configure where the alerts that are of certain severity are to be forwarded.

Centralized management

This page includes settings that control how Client Security settings are applied within the network.

General

This section contains the following options:

- **Allow users to change all settings...**

  This option makes all the settings throughout the **Anti-virus** and **Advanced mode** user interface non-final, which means that users are allowed to change any setting.

- **Do not allow users to change any settings...**

  This option makes all the settings throughout the **Anti-virus** and **Advanced mode** user interface final, which means that users are not allowed to change any setting.

- **Clear all settings...**

  This option restores the default settings for all Client Security components.

- **Allow users to suspend all downloads and updates**

  This option defines whether the user is allowed to temporarily suspend network communications, for example automatic polling of policies, sending statistics and automatic updates.

  This option is useful for hosts that sometimes use a slow dial-up connection.

- **Allow users to uninstall F-Secure products**

  Deselecting this option prevents end-users from uninstalling F-Secure software from their computer. Uninstallation always requires administrative rights. This applies to all Windows operating systems, even to Windows NT/2000/XP where the end-user has administrative rights.

  In order to uninstall software locally, you need to either select this option or shut down the Management Agent service first, and then proceed with the uninstallation.

- **Allow users to unload products;**

  The possible values are: **Allowed always**; **Allowed only in stand-alone installations**; **Not allowed**.

  This option specifies whether the user is allowed to unload all F-Secure products temporarily, for example in order to free memory for games or similar applications. Note that the main functions of the products are disabled during the time the product is unloaded and thus the computer becomes vulnerable to viruses and attacks.

- **Slow connection definition**

  This variable defines which network connections are regarded as slow. The unit used is kilobits per second. Note that the nominal speed of the connection is not relevant, but the actual speed of the connection is measured. The default value, `0` (zero), means that all connections are regarded as fast.

Policy Manager Server settings

- **Policy Manager Server**

  URL address of Policy Manager Server.

- **Incoming packages polling interval**

  Defines how often the host tries to fetch incoming packages from Policy Manager Server, for example base policy files. The default value is 10 minutes.

- **Outgoing packages update interval**

  Defines how often the host tries to send new versions of periodically sent information, for example statistics, to Policy Manager Server. The default value is 10 minutes.

Status tab

The different pages on the **Status** tab display detailed information on the status of certain components of centrally managed Client Security applications.

If you select a domain in the **Policy domains** tab, the **Status** tab displays the status of all hosts in that domain. If a single host is selected, the **Status** tab displays the status of that host.

Note: By right-clicking the column headers on the **Status** pages you can configure which columns are displayed on that page.

Context menu on Status tab

By right-clicking any row on a **Status** tab page you can access a context menu that contains the following options:

- **Copy as text** copies the currently selected row(s) and column headings from the table as text.
- **Select all** selects all rows in the table.
- **Select hosts in domain tree** can be used to select the hosts and display their location in the domain tree.

Overall protection

The **Overall protection** page displays a summary of the protection features enabled on each host:

- Whether real-time scanning is enabled or disabled.
- Internet Shield security level currently in use.
- Whether incoming e-mail scanning and outgoing e-mail scanning are enabled or disabled.
- Whether reputation-based protection is in use.
- Whether exploit shields are in use.

Automatic updates

The Automatic updates page displays a summary of the virus definition databases for products installed on hosts:

- The date and time when virus definitions were last updated.
- Virus definitions version.
- The date and time when virus definitions on F-Secure Gateway products were last updated.
- Update delta, which is the time between the last virus definitions update on the host and the last time the host has sent statistics to Policy Manager.
- Virus definitions version on Gateway products.
- The date and time when spyware definitions were last updated.
- Spyware definitions version.
- The date and time when spam definitions on Gateway products were last updated.
- Spam definitions version on Gateway products.

The virus definitions date and version information is also displayed for hosts that have Anti-virus for Citrix Servers, Anti-virus for Windows Servers,Internet Gatekeeper or Anti-virus for Microsoft Exchange installed.

Virus protection

The **Virus protection** page displays the following information:

- Last infection date.
- Last infection name.
- Last infected object.
- Last infection action taken.
- The total number of infections.

Internet Shield

The **Internet Shield** page displays the following information:

- Latest attack date and time in the **Latest attack timestamp** column.
- Latest attack service.
- Latest attack source.
- Recent attacks (this column can be sorted by clicking on the column header).
- Recent attacks reset time.

Installed software

The **Installed software** page displays a summary of the software installed on the host(s):

- Client Security software version (including the build number and possible hotfixes).
- List of anti-spyware hotfixes.
- Whether Internet Shield is installed.
- Whether e-mail scanning is installed.
- Whether web traffic scanning is installed.
- Whether browsing protection is installed.
- Whether DeepGuard is installed.

- Policy Manager Proxy version.

Centralized management

The **Centralized management** page displays a summary of information relating to central management:

- Policy file timestamp.
- Policy file counter; this is the number of the policy file currently in use on the host.
- The date when the last statistics update has been sent to Policy Manager.
- Whether the host is disconnected (this column can be sorted by clicking on the column header).
- The number of new security alerts.
- The number of new fatal errors.

Host properties

The **Host properties** page displays the following information for each host:

- The WINS name of the host.
- The IP address of the host.
- The DNS name of the host.
- The operating system of the host.

Alerts tab

The **Alerts** tab displays alerts from the selected host(s) and domain(s), and it can also be used to manage the alert reports.

The **Alerts** tab displays the following information for each alert:

- severity,
- date and time,
- description,
- host and user, and
- the product the alert relates to.

When an alert is selected in the alert list, the lower half of the page displays more specific information about the alert: product, severity, originating host, and so on. Client Security scanning alerts may also have an attached report. This report will be displayed in the lower half of the page.

By clicking **Configure alert forwarding** you can access the **Settings** tab and **Alerts** page, where you can configure alert forwarding.

Reports tab

The **Reports** tab displays virus scanning reports from the selected host(s) and domain(s), and it can also be used to manage the scanning reports.

The **Reports** tab displays the following information about each report:

- severity,
- date and time,
- description,
- host and user, and
- the product the report relates to.

When a row is selected in the reports list, the corresponding scanning report is displayed in the lower half of the page.

Installation tab

The **Installation** tab is the first one that opens when Policy Manager Console is installed.

The **Installation** tab contains shortcuts to all installation-related features. It also displays a list of available software installation packages.

Autodiscover Windows hosts...	Autodiscover will automatically discover Windows domains and hosts, push install software and import new hosts into the policy domain tree.
Push install to Windows hosts...	Push installation allows direct installation to specific Windows hosts based on IP addresses or host names. With this feature it is possible to push install software to hosts even if they do not appear in the NT domain browse list of the **Autodiscover** view.
Import autoregistered hosts...	Hosts will send autoregistration messages to Policy Manager whenever the first product is installed to the hosts. These new hosts are taken under policy management by importing them to the policy domain tree.
Installation packages...	The **Installation packages** view shows the available installation packages and detailed information on their content.

Note: Due to the changes in automatic updates, virus definitions on the server can no longer be updated manually by invoking the operation from Policy Manager Console. It is only possible to update them manually on Policy Manager Server by using a special tool.

Operations tab

We recommend that you use the operations available on this tab if there has been a virus outbreak in the LAN.

The **Operations** tab contains two operations:

Update virus definitions operation	With this operation you can order the selected hosts or all hosts in the selected domain to get new virus definitions at once.
Scan for viruses and spyware operation	With this operation you can order the selected hosts or all hosts in the selected domain to scan for viruses and spyware at once.

Both of these operations are recommended to be used if there has been a virus outbreak in the LAN.

The toolbar

The toolbar contains buttons for the most common Policy Manager Console tasks

	Saves the policy data.
	Distributes the policy.
	Go to the previous domain or host in the domain tree selection history.
	Go to the next domain or host in the domain tree selection history.
	Go to the parent domain.
	Cuts a host or domain.
	Pastes a host or domain.
	Adds a domain to the currently selected domain.
	Adds a host to the currently selected domain.
	Displays the **Properties** box of a host or domain.
	Launches the **Autodiscover Windows Hosts** tool. New hosts will be added to the currently selected policy domain.
	Starts push installation to Windows hosts.
	Imports autoregistered hosts to the currently selected domain. Green signifies that the host has sent an autoregistration request.
	Displays available installation packages.
or	Displays all alerts. The icon is highlighted if there are new alerts. When you start Policy Manager Console, the icon is always highlighted.

Menu commands

This section provides a reference of the available menu commands in Policy Manager Console.

Menu	Command	Action
File	New policy	Creates a new policy data instance with the Management Information Base (MIB) defaults. This command is rarely needed because existing policy data will usually be modified and saved using the **Save as** command.
	Open policy	Opens previously saved policy data.
	Save policy changes	Saves current policy data.
	Save policy as	Saves policy data with a specified name.
	Distribute policies	Distributes the policy files.
	Export host policy file	Exports the policy files.
	Exit	Exits Policy Manager Console.
Edit	Cut	Cuts selected items.
	Paste	Pastes items to selected location.
	Delete	Deletes selected items.
	New policy domain	Adds a new domain.
	New host	Adds a new host.
	Import autoregistered hosts	Imports hosts that have sent an autoregistration request.
	Autodiscover Windows hosts	Imports hosts from the Windows domain structure.
	Push install to Windows hosts	Installs software remotely, and imports the hosts specified by IP address or WINS name.
	Find	Search for a string in the host properties. All hosts in the selected domain are searched.
	Domain/host properties	Displays the **Properties** page of the selected host or policy domain.
View	Embedded restriction editors	Toggles between the embedded restriction editor and the restrictions dialog box.
	Messages pane	Shows/hides the **Message** pane at bottom of screen.
	Open on new message	If selected, the **Message** pane opens automatically when a new message is received.
	Back	Takes you to the previous domain or host in the domain tree selection history.
	Forward	Takes you to the next domain or host in the domain tree selection history.
	Parent domain	Takes you to the parent domain.
	All alerts	Opens the **Alerts** page with all alerts showing.
	Advanced mode	Changes to the **Advanced mode** user interface.

Menu	Command	Action
	Anti-virus mode	Changes to the **Anti-virus mode** user interface, which is optimized for centrally managing Client Security.
	Refresh <Item>	Manually refreshes the status, alert, or report view. The menu item changes according to the selected page or tab.
	Refresh All	Manually refreshes all data affecting the interface: policy, status, alerts, reports, installation packages, and autoregistration requests.
Tools	Installation packages	Displays installation packages info in a dialog box.
	Change passphrase	Changes login passphrase (the passphrase protecting the Policy Manager Console private key).
	Reporting	Lets you select the reporting methods and the domains/hosts and products included in the reports.
	Preferences	Sets the local properties for Policy Manager Console. These properties only affect the local installation of Policy Manager Console.
Help	Contents	Displays the **Help** index.
	Register	Opens a dialog to allow you to register the product.
	Contact Information	Displays contact information for F-Secure.
	About F-Secure Policy Manager Console	Displays version information.

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, settings can be defined as final, which means that the users are not allowed to change them. Final always forces the policy: the policy variable overrides any local host value, and the end user cannot change the value as long as the **Final** restriction is set. If the settings have not been defined as final, the users are allowed to change them.

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 the user cannot change the setting, because it has been defined as final. 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 the user is 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.

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.

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.

Chapter

4

Setting up the managed network

Topics:

- *Logging in*
- *Managing domains and hosts*
- *Adding hosts*
- *Local installation and Policy Manager*
- *Installing on an infected host*
- *Checking that the management connections work*

Policy Manager offers you several ways to deploy Client Security in your company:

- In a Windows domain you can use the **Autodiscover** and **Autoregistration** features to automate the creation of the managed domain.
- If there are many computers running Unix or Linux, or if there are also servers to manage, all of them can still be connected to Policy Manager, and their security applications can be administered from one single location.

There are also some issues that you should take into consideration, so that you can profit the most from the centralized management of the security applications later on. This includes, for example, planning the structure of the managed domain carefully beforehand.

When planning the structure of the managed domain, you should consider grouping end users with similar security needs into the same subdomain, and grouping laptops and desktops in their own subdomains. In this way you can define the optimal security settings for computers that can be connected to different LANs or use dialup connections, as well as computers that are always connected to the company network.

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 define multiple connections to a single server. After selecting the connection, enter your Policy Manager Console passphrase. This is the passphrase that you defined when you installed the program. This is not your network administrator password.

You can start the program in read-only mode, in which case you do not need to enter a passphrase. In this case, however, you will not be allowed to make changes.

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).

Note that it is possible to make copies of existing connections. This makes it easy to define multiple connections to the same server, with slightly different connection preferences for different usages. For example, an existing connection can be taken as a template, and different connection preferences can be tested with the new copy without affecting the original settings.

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 HTTP URL of Policy Manager Server.

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

The **Public key file** and **Private key file** paths specify what management key-pair to use for this connection. If the specified key files do not exist, Policy Manager Console will generate a new key-pair.

Changing communication preferences

In the communication preferences, you can set how often the server is polled for status information and a time limit, after which hosts are considered disconnected.

The **Connection properties** dialog box is open (for example by clicking **Options** on the **Login** dialog box).

To change the communication preferences:

1. Select the **Communication** tab.
2. Change the **Host connection status** if necessary.

   Host connection status controls when hosts are considered disconnected from Policy Manager. All hosts that have not contacted Policy Manager Server within the defined interval are considered disconnected. The disconnected hosts will have a notification icon in the domain tree and they will appear in the **Disconnected hosts** list in the **Domain** status view.

   Note: It is possible to define an interval that is shorter than one day by simply typing in a floating point number in the setting field. For example, with a value of `0.5` all hosts that have not contacted the server within 12 hours are considered disconnected. Values less than one day are normally useful only for trouble shooting purposes, because in a typical environment some hosts are naturally disconnected from the server every now and then. For example, laptop computers may not be able to access the server daily, but in most cases this is perfectly acceptable behavior.

3. Click **Polling period options** to change the polling intervals.
   The **Polling period** dialog box opens.
4. Modify the polling intervals to suit your environment.

   The communication protocol selection affects the default polling intervals. If you are not interested in certain management information, you should switch unnecessary polling off by clearing the polling item you want to disable. However, automatic polling should be disabled only if some performance problems occur. **Disable All Polling** disables all of the polling items. Whether or not automatic polling is disabled, manual refresh operations can be used to refresh the selected view.

After Policy Manager Console startup these settings can be edited normally from the **Preferences** view.

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.

Adding policy domains

This topic describes how to add new policy domains.

To add a new policy domain:

1. Select **Edit** ➤ **New policy domain** from the menu.
   Alternatively:
   - Click in the toolbar.
   - Press Ctrl+ Insert.

   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.

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.

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 autoregistered hosts

Another possibility for importing hosts into Policy Manager Console is by using the *autoregistration* feature.

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 autoregistered hosts:

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

   When the operation is completed, the host is added to the domain tree. The autoregistered hosts can be imported to different domains based on different criteria, such as the hosts's IP or DNS address. The **Autoregistration** view offers a tabular view to the data which the host sends in the autoregistration message. This includes the possible custom autoregistration properties that were included in the remote installation package during installation.
2. You can perform the following actions on the **Autoregistration** view:
   - You can sort autoregistration 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 autoregistration properties are visible in the table.

Using autoregistration import rules

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

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

- WINS name, DNS name, Dynamic 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, dynamic IP address
  - These support 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 autoregistration import rules in which it is used as import criteria.

3. Create a new Autoregistration 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, click the cell where you want to add a value and click **Edit**.
   d) Enter the value in the cell.
   The import criteria is defined.

   - When autoregistered 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 **Autoregistered hosts** tab and click **Import**.

   The importing 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 treated as always 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.

   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.

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.

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.
2. Select the products to install and click **Next** to continue.

   You can choose to force reinstallation if applications with the same version number already exist.
3. 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.
4. 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.

5. Review the installation summary.
6. 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.
7. 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.
8. 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.
9. To see this list, select the **Installation** tab (alternatively select the top domain on the **Policy domain** tree).

Policy-based installation

Base policy files are used to start installations on hosts that have Management Agent installed.

Policy Manager Console creates an operation-specific installation package, which it stores on Policy Manager Server, 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. Policy Manager Console discovers the new status information and shows the results.

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

Using the installation editor

The installation editor must be used on those hosts that already have Management Agent installed.

To use the installation editor:

1. Open the **Policy** tab and select the root node (the **F-Secure** sub-tree).
   Alternatively, open the **Install** tab.
   The **Installation editor** opens.
2. In the **Installation editor**, select the products to be installed on the currently selected host or policy domain.
   The **Installation editor** contains the following information about the products that are installed on your target policy domain or host:

Product name	Name of the product, which is either installed on a host or domain, or which can be installed with an available installation package.
Installed version	Version number of the product. If there are multiple versions of the product installed, all version numbers will be displayed. For hosts, this is always a single version number.
Version to install	Version numbers of the available installation packages for the product.
Version being installed	The current version being installed on a host or domain.
Progress	Progress of the installation task. The **Progress** field displays information that is different for hosts and for domains.

- If a host is selected, the **Progress** field displays one of the following messages:

In progress	The installation operation has been started (added to policy data), but the host has not yet reported the operation's success or failure.
Failed	The installation or uninstallation operation failed. Click the button in the **Progress** field for detailed status information.
Completed	The installation or uninstallation operation succeeded. This message will disappear when the **Installation editor** is closed.
(Empty field)	No operations are active. The **Installed version** field displays the currently installed product version.

- If a domain is selected, the **Progress** field displays one of the following:

<number> hosts left - **<number> installations failed**	Number of hosts left and number of failed installations. Click the button in the **Progress** field for detailed status information.
Completed	The installation or uninstallation operation succeeded on all hosts.
(Empty field)	No operations are active. The **Installed version** field displays all currently installed product versions.

3. When all required version numbers are selected, click **Start**.

The **Installation editor** launches the **Installation wizard**, which queries the user for the installation parameters. The **Installation editor** then prepares a distribution installation package that is customized for the specific installation operation. The new package is saved on Policy Manager Server.

Note: The **Start** button is used to start the installation operations selected in the **Version to install** field. If the **Installation editor** is closed without first clicking the **Start** button, then all changes will be discarded.

4. Because the installation operation uses policy-based triggering, you must distribute new policy files.

   The policy file will contain an entry that tells the host to fetch the installation package and perform the installation.

   Note that 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. In any case, it is possible to remove the installation operation from the policy by clicking **Stop all**. This will cancel the installation operations defined for the selected policy domain or host. It is possible to stop all installation tasks in the selected domain and all subdomains by selecting the **Recursively cancel installation for subdomains and hosts** option in the confirmation dialog.

   The **Stop all** button is enabled only if the current host or domain has an installation operation defined. Any subdomain operations do not affect the button state. **Stop all** only removes the operation from the policy. If a host has already polled the previous policy file, it may try to carry out the installation operation even though it is no longer visible in the **Installation editor**.

Remote uninstallation:

Uninstallation can be performed as easily as an update. A distribution package is created that contains only the software needed to uninstall the product. If the product does not support remote uninstallation, the **Installation editor** does not display an option for uninstallation.

Choosing **Reinstall** will reinstall the current version. This option should only be used for troubleshooting. Most of the time, there is no reason to reinstall a product.

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`….

Local installation and updates with pre-configured packages

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

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

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

Using the customized remote installation package

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

To use the customized remote installation JAR 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, JAR or MSI, 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 JAR 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. Select the installation type.

   The default, **Centrally managed installation**, is recommended. You can also prepare a package for a stand-alone host.

   A summary page shows your choices for the installation.
9. 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 autoregistration properties to the installation package. A host will add these custom properties to the autoregistration 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 **Autoregistration** 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 autoregistration 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 **Autoregistration** view, and after that the hosts from another unit can be imported to their target domain.
10. When you reach the last wizard page, click **Finish** to continue.
11. You can install the 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
```

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.

Note: When installing Client Security to be managed by Policy Manager, select **Central management with F-Secure Policy Manager** when the management selection step is displayed during setup. You will also be asked to provide the location of the Policy Manager public key (`admin.pub`, created when installing Policy Manager Console) and the network address of the Policy Manager Server in use. These details are required to ensure secure communication with Policy Manager.

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:	• 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:	• Windows 7 32-bit and 64-bit • Windows Vista 32-bit and 64-bit • Windows XP SP2 or newer
Memory:	• 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:	• 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

You need the product CD, a valid subscription key and an Internet connection. If multiple users share and use the computer, log on with administrator privileges to install this product.

To install the software:

1. Insert the Installation CD.

   The installation should start automatically. If it does not, go to Windows Explorer, double-click on the CD-ROM icon and double-click the `setup.exe` file to start the installation.

   The first installation dialog box appears.
2. Select the installation language and click **Next** to continue.
3. Read the license agreement. To accept the agreement and to continue, click **Accept**.
4. Enter your subscription key and click **Next** to continue.

   Note: If you want to evaluate the product, leave the **My subscription key is** field empty and click **Next**. In the **Evaluation Options** dialog box, select the service to evaluate.

   - If you purchased the product on a CD from a shop, you can find the subscription key on the cover of the Quick Installation Guide.
   - If you downloaded the product from the F-Secure eStore, the subscription key is included in the confirmation e-mail of the purchase order.

   Note: Use only the subscription key delivered with the product. You can use the subscription key for the number of installations your license is for (see the 'F-Secure License' note in this guide). If you have problems in registering, please contact F-Secure Technical Support.
5. Select the installation type:

   - Automatic installation: The product is installed automatically. Existing security products may be automatically replaced. The product is installed to the default directory.
   - Step by step installation: You can make selections during the installation. You can for example, change the installation directory. However, we recommend using the default directory.
6. Click **Next**.
7. After the installation is complete, remove the Installation CD.
8. The computer restarts automatically. To restart immediately, select **Restart now**.
9. 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.

   Tip: To learn more about the product, you can access the online help by clicking the **Help** button in the product. You can find the online help also on the Installation CD.

Installing on an infected host

If the host on which you are going to install Client Security is infected with some variant of the Klez virus, you should run the Klez removal tool on the host before starting the installation.

The `Ilaunchr.exe` installation tool cannot be run on a computer that is infected with Klez.

You can download the Kleztool from ftp://ftp.europe.f-secure.com/anti-virus/tools/kleztool.zip.

The `kleztool.zip` package contains a `kleztool.txt` file, in which you can find the instructions for running Kleztool on the infected computer. Read these instructions carefully before proceeding.

Checking that the management connections work

You can check that the management connections are working by following the steps given here.

1. Check the **Policy distribution status** on the **Summary** tab.
2. Save and distribute the polices if necessary.
3. Go to the **Status** tab and select the **Centralized management** page.
4. Check the timestamp and counter of the policy file currently in use.

Chapter

5

Configuring virus and spyware protection

Topics:

- *Configuring automatic updates*
- *Configuring real-time scanning*
- *Configuring DeepGuard*
- *Configuring rootkit scanning (Blacklight)*
- *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 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.

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.

How do automatic updates work?

The Automatic Update Agent installed with Client Security downloads the automatic updates from the configured update sources.

The Automatic Update Agent tries to download updates in the following order:

1. If Policy Manager Proxy is 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 Policy Manager Proxy is 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 F-Secure update server.
6. After that the client tries to download the updates directly from F-Secure update server.

Note: If Client Security is set to download neighborcast updates it may also download updates from other Client Security installations that have neighborcast enabled.

Automatic update settings

On the **Automatic updates** page on the **Settings** tab, you can specify whether you want Client Security to automatically receive virus and spyware definition updates.

To allow automatic updates, select **Enable automatic updates**. You should always enable automatic updates.

Specify the update polling interval in the **Interval for polling updates from F-Secure Policy Manager Server** field.

Policy Manager Proxies is a list of Policy Manager Proxy servers available to you. The Automatic Update Agent installed with Client Security connects to them in the priority order specified in this table.

If you want to use HTTP proxy, select **From browser settings** or **User-defined** from the **Use HTTP proxy** drop-down menu. Then specify the **HTTP proxy address**.

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 save and distribute the policy.

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 save and 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.

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**.

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.

Real-time scanning settings

The settings available on the **Settings** ➤ **Real-time scanning** page are described here.

To enable real-time scanning, select **Real-time scanning enabled**. To disable real-time scanning, clear **Real-time scanning enabled**.

The following options are available for selecting what to scan:

- **All Files**

  All files will be scanned, regardless of their file extension. This option is not recommended for general use because it might slow down the system performance considerably.

- **Files with These Extensions**

  Files with specified extensions will be scanned. To specify files that have no extension, type . . You can use the wildcard ? to represent any letter. Enter each file extension separated by a space. This option is recommended for real-time protection. New file extensions are also added to the list automatically when the virus definition databases are updated.

- **Enable excluded extensions**

  You can specify whether some files will not be scanned, and enter the extensions that will be excluded from scanning in the **Excluded extensions** field. This is most useful when scanning is set to **All Files**.

- **Enable excluded objects**

  Excluded objects are individual files or folders, which are normally set locally. They can also be set from Policy Manager Console by right-clicking the **Enable excluded objects** check box and selecting **Locate in Advanced Mode**.

- **Scan network drives**

  Select this check box to scan files that you access on network drives.

  Important: In Client Security the **Scan network drives** setting is turned off by default.

- **Scan when created or modified**

  Normally files are scanned when they are opened for reading or executing. When a file is opened for writing, or a new file is created, and this setting is selected, the file is also scanned when it is closed. With this setting enabled, changes in new or modified files are detected immediately when they are closed. This setting is turned on by default and it is recommended to leave it turned on.

- **Decide action on infection automatically**

  For Client Security 9 or higher and Anti-virus for Windows Servers 9 or higher, you can select this option to let the program automatically decide what action to take whenever an infection is detected during scanning.

- **Custom action on infection**

  If automatic decisions are turned off, you can select the default action that the program will take when an infected file is detected from this drop-down menu. Choose one of the following actions:

Action	Definition
Ask after scan	Starts the Disinfection Wizard when an infected file is detected.
Disinfect automatically	Disinfects the file automatically when a virus is detected.
Rename automatically	Renames the file automatically when a virus is detected.
Delete automatically	Deletes the file automatically when a virus is detected. Note that this option also deletes the file the virus is attached to, so this option is not recommended.
Report only	Indicates that a virus is found, and does not let you open the infected object. This option only reports the virus, but does not take any action against it.
Quarantine automatically	Moves the infected file automatically into the Quarantine repository.

- **Protect the "Hosts" file**

  When turned on, the "Hosts" file will be protected against modifications by spyware. Some malware may try to use this file to substitute the IP address of a well-known DNS name with the IP address of a malicious web site.

- **Scan for tracking cookies**

  When this setting is turned on, tracking cookies will be detected. Real-time scanning will only detect tracking cookies that are stored on disk, not cookies that are only stored in the web browser's cache. Manual scanning will detect cookies stored both on disk and in the web browser's cache.

File extension handling

Client Security has a list of included extensions defined in the policy (this can be ‘all files’). **Included extensions** can also be part of a virus definitions update. These included extensions are first combined by Client Security, and then any excluded extensions are removed from that list to determine the actual list of files to scan. This applies to real-time scanning, manual scanning and e-mail scanning.

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 save and distribute the policy.

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 save and distribute the policy.

Excluding Microsoft Outlooks'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 save and distribute the policy.

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.

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).
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.

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.

Configuring rootkit scanning (Blacklight)

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.

Rootkit scanning settings

The settings for rootkit scanning are displayed on the **Manual scanning** page of the **Settings** tab.

Rootkit scanning can be run as a manual operation or as part of a full computer check.

Select **Enable rootkit scanning** to enable scanning for files and drives hidden by rootkits. This option also enables users to run local quick scans for rootkits and other hidden items.

Select **Include rootkit scanning in full computer check** to scan for items hidden by rootkits when a full computer check is started from the local host, or when a manual scanning operation is launched from Policy Manager Console.

Select **Report suspicious items after full computer check** to specify that detected suspicious items are shown in the disinfection wizard and in the scanning report after a full computer check. When this option is selected, you can see from the scanning reports whether any items hidden by rootkits have been detected on the managed hosts.

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 save and 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 **Reports** tab.

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.

E-mail scanning settings

The e-mail scanning settings are displayed on the **E-mail scanning** page of the **Settings** tab.

To enable the scanning of incoming e-mail messages and attachments (POP3 traffic), select **Enable incoming e-mail scanning**.

To enable the scanning of outgoing e-mail messages and attachments (SMTP traffic), select **Enable outgoing e-mail scanning**.

You can select what to do when an infected e-mail message is detected. The following actions are available:

- Incoming e-mail scanning:
  1. **Action on incoming infected attachment**:
     - **Disinfect Attachment** starts the disinfection wizard whenever an infected attachment is detected.
     - **Remove Attachment** deletes the attachment.
     - **Report Only** ignores the attachment but reports it to the administrator.
  2. **Action if scanning fails**:
     - **Remove Attachment** deletes the attachment.
     - **Report Only** ignores the failed scan but reports it to the administrator.
  3. **Action on malformed message parts**:
     - **Drop Message Part** deletes the message.
     - **Report Only** ignores the malformed message part but reports it to the administrator.
- Outgoing e-mail scanning:
  1. **Action on outgoing infected attachment**:
     - **Block E-Mail Message** prevents you from sending the e-mail.
     - **Report Only** ignores the attachment but reports it to the administrator.
  2. **Action if scanning fails**:
     - **Block E-Mail Message** prevents you from sending the e-mail.
     - **Report Only** ignores the failed scan but reports it to the administrator.
  3. **Action on malformed message parts**:
     - **Drop Message Part** deletes the message.
     - **Report Only** ignores the malformed message part but reports it to the administrator.

Caution: The **Report Only** option can be dangerous and should not be used in normal operation.

To save the blocked e-mail messages in the end-users' **Outbox** folder, select **Save blocked e-mails in outbox**. The user must move, delete or modify the blocked message in their **Outbox** to be able to send more messages.

The file types that are included and excluded from e-mail scanning are based on the settings given on the **Real-time scanning** page.

If you want the end user to see a dialog box when large files are being scanned, select **Show progress when scanning large files**, and define the time limit in the **Show progress after this time** field.

If you want that a scanning report is displayed to the end user after the scanning has completed, select **Show report when infections are found**.

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 save and distribute the policy.

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.

Web traffic scanning settings

The settings for HTTP scanning, which are displayed on the **Settings** ➤ **Web traffic scanning** page, are described here.

To turn HTTP scanning on, select **Enable HTTP scanning**.

From the **Action on infection** drop-down list you can select what to do when an infection is found in HTTP traffic. The actions available are:

- **Block** blocks access to the infected file.
- **Report Only** ignores the infection but reports it to the administrator.

From the **Action on scanning failure** drop-down list you can select what to do if a file in HTTP traffic cannot be scanned. This setting is used, for example, when handling password-protected archives. The actions available are:

- **Block** blocks the file that could not be scanned.
- **Report Only** ignores the file but reports it to the administrator.

Select **Scan inside compressed files** to scan inside compressed `ZIP`, `ARJ`, `LZH`, `RAR`, `CAB`, `TAR`, `BZ2`, `GZ`, `JAR` and `TGZ` files.

You can specify a list of trusted sites in the **Trusted sites** table. The content of the trusted sites will not be scanned for viruses.

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 save and distribute the policy.

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 save and distribute the policy.

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.

Spyware control settings

The settings for spyware scanning are described here.

Spyware scanning is included as part of real-time scanning and manual scanning. When **Real-time scanning enabled** is selected on the **Real-time scanning** page, spyware scanning is also turned on. Similarly, whenever a manual scan is run, spyware is automatically included in the scan. The action taken when spyware is detected is determined by the action selected on the **Real-time scanning** and **Manual scanning** pages.

The **Applications excluded from spyware scanning** table displays the spyware and riskware items that have been allowed by the administrator.

The **Spyware and riskware reported by hosts** table contains the following information:

Spyware and riskware reported by hosts	
Spyware or Riskware Name	Displays the name of the spyware object or riskware.
Type	Displays the spyware type. The type can be adware, data miner, dialer, malware, monitoring tool, porn dialer, riskware, vulnerability, worm, cookie (tracking cookie) or misc (miscellaneous).
Severity	Displays the severity of the spyware item. This is a value from 3 to 10.
Host	Displays the name of the host on which the spyware item was found.
Spyware Status	Displays the current status of the spyware item. The statuses are: **Potentially active** - The spyware item is still potentially active on the host. No action has been taken on the host against the spyware item.

Spyware and riskware reported by hosts	
	Removed - The spyware item has been removed from the host. **Quarantined** - The spyware item was quarantined on the host. **Currently In quarantine** - The spyware item is currently in quarantine on the host.
Timestamp	Displays the date and time when the spyware item was found on the host.

The spyware reported by hosts will be cleaned if you run a manual spyware scan on the hosts, as well as when quarantined spyware is removed periodically on the hosts.

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 save and distribute the policy.

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 save and distribute the policy.

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 save and distribute the policy.

Managing quarantined objects

Quarantine management gives you the possiblity 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.

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 save and distribute the policy.

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 save and distribute the policy.

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.

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 save and distribute the policy.

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 porential outbreaks as quickly as possible.

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 save and distribute the policy.

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 save and distribute the policy.

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 **Reports** tabs to see the scanning reports from different hosts.

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.europe.f-secure.com/virus-info/eicar_test_file.shtml*.

You can test your antivirus protection as follows:

1. You can download the `EICAR` test file from *http://www.europe.f-secure.com/virus-info/eicar_test_file.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.

Chapter

6

Configuring Internet Shield

Topics:

- *Global firewall security levels*
- *Design principles for security levels*
- *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*

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.

Global firewall security levels

If you do not need to customize the firewall settings for your network, there are several pre-configured security levels to choose from.

The global firewall security levels that exist in Internet Shield are:

Network quarantine	If network quarantine is turned on, this security level will be automatically selected when the network quarantine criteria on the host are met. This security level allows the downloading of automatic updates and connections to Policy Manager Server.
Block all	This security level blocks all network traffic.
Mobile	This security level allows normal web browsing and file retrievals (HTTP, HTTPS, FTP), as well as e-mail and Usenet news traffic. Encryption programs, such as VPN and SSH are also allowed. Everything else is denied and the denied inbound TCP traffic generates alerts. Local rules can be added after the malware probes detection.
Home	This security level allows all outbound TCP traffic and FTP file retrievals. Everything else is denied and denied inbound TCP traffic generates alerts. Local rules can be added to enable new network functionality.
Office	This security level allows all outbound TCP traffic and FTP file retrievals. Everything else is denied by default and only malicious connection attempts generate alerts. Local rules can be added to enable new network functionality.
Strict	This security level allows outbound web browsing, e-mail and News traffic, encrypted communication, FTP file transfers and remote updates. Everything else is denied, and inbound malware probes and TCP connection attempts generate alerts.
Normal	This security level allows all outbound traffic, and denies some specific inbound services. It is still possible to add rules with Application control, so that most networking applications work properly when allowed.
Disabled	In this security level all network traffic, inbound and outbound, is allowed and no alerts are generated. Local rules cannot be created.

Design principles for security levels

The basic principles of design behind security levels are described here.

Each security level has a set of pre-configured firewall rules. In addition, you can create new rules for all security levels for which the **Filtering mode ➤ Normal** is displayed in the **Firewall security levels** table. The rules in the **Firewall security levels table** are read from top to bottom.

When you create new security levels, you should consider the following main principle for defining the firewall rules associated with them:

- Allow only the needed services, and deny all the rest. This minimizes the security risk. The drawback is that when new services are needed, the firewall must be reconfigured, This, however, is a small price to pay for increased security.

The opposite concept - to deny dangerous services and allow the rest - is not acceptable, because no one can tell with certainty which services are dangerous or might become dangerous in the future when a new security problem is discovered.

A good security level would look something like this:

1. Deny rules for the most dangerous services or hosts, optionally with alerting.
2. Allow rules for much-used common services and hosts.
3. Deny rules for specific services you want alerts about (e.g. trojan probes) with alerting.
4. More general allow rules.
5. Deny everything else.

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.

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 save and 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.

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 save and distribute the policy.

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 save and 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. Tun 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 save and distribute the policy.

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.

Network quarantine settings

The network quarantine settings are located on the **Firewall security levels** page.

In the **Network quarantine** section you can:

- Turn network quarantine on or off.
- Specify the virus definitions age that activates network quarantine.
- Specify whether turning off real-time scanning on a host activates network quarantine.

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 save and distribute the policy.

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.

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.

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 form 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.

Direction	Explanation
<=	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 save and 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.

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.

Application control settings

The settings available on the **Settings** ➤ **Application control** page are described here.

The application control page displays the following information:

Application rules for known applications	
Application	Displays the executable file name.
Act as Client (out)	The following actions are available: **Deny**, **Allow**, **User Decision**.
Act as Server (in)	The following actions are available: **Deny**, **Allow**, **User Decision**.

Application rules for known applications	
Description	Displays the internal description of the executable, usually the name of the application. You can also modify the description.
Message	Displays the associated message (if any) which was created together with the rule.
Publisher	Displays the publisher of the application.
Version	Displays the internal version description of the executable.

Unknown applications reported by hosts

For unknown applications, the information displayed is the same as for known applications, except that the unknown applications do not have any defined rules or associated messages yet.

You can decide what happens when the application tries to connect to the network with the **Default action for client applications** and **Default action for server applications** selections. The possible actions are:

Action	Description
Deny	Denies all of the application's connections to the network.
Allow	Allows all of the applications's connections to the network.
User Decision	Prompts the user to decide what to do every time the application connects to the network.

If you want to let the end users to decide what to do with outbound connection attempts, you can reduce the number of pop-ups they see by selecting **Do not prompt for applications that DeepGuard has identified**.

Application control does not limit plug-ins in browsers like Netscape or Microsoft Internet Explorer. All plug-ins have the same capabilities as the browser itself. However, you should advise the end-users to install only trusted plug-ins.

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.

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 save and distribute the policy.

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 save and distribute the policy.

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 save and distribute the policy.

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 save and 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.

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.

Intrusion prevention settings

The intrusion prevention settings can be found in the **Intrusion prevention** section on the **Firewall security levels** page.

- **Enable intrusion prevention**

  If turned on, intrusion prevention is used to monitor inbound traffic in order to find intrusion attempts. If turned off, intrusion prevention does not monitor traffic.

- **Action on malicious packet**

  The options available are:

  - **Log and drop the packet** means that the packet is logged into the alertlog with the packet header information (IPs, ports and protocol) and it is not allowed to pass through the intrusion prevention component.
  - **Log without dropping the packet** means that the packet is logged into the alertlog with the packet header information (IPs, ports and protocol) but it is also allowed to pass through the intrusion prevention component.

- **Alert severity**

  The options available are: **No alerting**, **Informational**, **Warning**, **Security alert**. Intrusion attempts can be set to use different severities depending on how administrator or local user wants to see the messages.

- Detection sensitivity

  This parameter is used for two purposes; it reduces the number of alerts and it also affects the performance of the local machine. If you use a smaller value, the number of false positives is reduced.

  - 10 = maximum network performance, minimum alerts
  - 50 = only 50% (the most important and malicious ones) of the IPS patterns are verified and reported in case of match.
  - 100 = all preprogrammed patterns are verified and reported in case of match.
  - The smaller the number is, less patterns are verified.
  - A recommended value for home users is 100%
  - A recommended value for desktops is 25%

What is a false positive?

A false positive is an alert that wrongly indicates that the related event has happened. In Internet Shield, the alert text usually indicates this by using words like "probable" or "possible". These kind of alerts should be eliminated or minimized.

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 save and distribute the policy.

Chapter

7

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*

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.

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.

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.

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.

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** ➤ **Preferences** from the menu, then select the **Communications** tab in the **Preferences** window. You will see the currently defined time in the **Host connection** section.

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 **Reports** tab.
   The scanning information from the selected hosts is displayed in the **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.

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.

Creating a weekly infection report

If you want to create a weekly infection report (or some other report to be generated at regular intervals), you have two options.

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

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.

Chapter

8

Upgrading software

Topics:

- *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.

Using the installation editor

The installation editor must be used on those hosts that already have Management Agent installed.

To use the installation editor:

1. Open the **Policy** tab and select the root node (the **F-Secure** sub-tree).
   Alternatively, open the **Install** tab.
   The **Installation editor** opens.
2. In the **Installation editor**, select the products to be installed on the currently selected host or policy domain.
   The **Installation editor** contains the following information about the products that are installed on your target policy domain or host:

Product name	Name of the product, which is either installed on a host or domain, or which can be installed with an available installation package.
Installed version	Version number of the product. If there are multiple versions of the product installed, all version numbers will be displayed. For hosts, this is always a single version number.
Version to install	Version numbers of the available installation packages for the product.
Version being installed	The current version being installed on a host or domain.
Progress	Progress of the installation task. The **Progress** field displays information that is different for hosts and for domains.

- If a host is selected, the **Progress** field displays one of the following messages:

In progress	The installation operation has been started (added to policy data), but the host has not yet reported the operation's success or failure.
Failed	The installation or uninstallation operation failed. Click the button in the **Progress** field for detailed status information.
Completed	The installation or uninstallation operation succeeded. This message will disappear when the **Installation editor** is closed.
(Empty field)	No operations are active. The **Installed version** field displays the currently installed product version.

- If a domain is selected, the **Progress** field displays one of the following:

<number> hosts left - **<number> installations failed**	Number of hosts left and number of failed installations. Click the button in the **Progress** field for detailed status information.
Completed	The installation or uninstallation operation succeeded on all hosts.
(Empty field)	No operations are active. The **Installed version** field displays all currently installed product versions.

3. When all required version numbers are selected, click **Start**.
   The **Installation editor** launches the **Installation wizard**, which queries the user for the installation parameters. The **Installation editor** then prepares a distribution installation package that is customized for the specific installation operation. The new package is saved on Policy Manager Server.

   Note: The **Start** button is used to start the installation operations selected in the **Version to install** field. If the **Installation editor** is closed without first clicking the **Start** button, then all changes will be discarded.

4. Because the installation operation uses policy-based triggering, you must distribute new policy files.

   The policy file will contain an entry that tells the host to fetch the installation package and perform the installation.

   Note that 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. In any case, it is possible to remove the installation operation from the policy by clicking **Stop all**. This will cancel the installation operations defined for the selected policy domain or host. It is possible to stop all installation tasks in the selected domain and all subdomains by selecting the **Recursively cancel installation for subdomains and hosts** option in the confirmation dialog.

   The **Stop all** button is enabled only if the current host or domain has an installation operation defined. Any subdomain operations do not affect the button state. **Stop all** only removes the operation from the policy. If a host has already polled the previous policy file, it may try to carry out the installation operation even though it is no longer visible in the **Installation editor**.

Remote uninstallation:

Uninstallation can be performed as easily as an update. A distribution package is created that contains only the software needed to uninstall the product. If the product does not support remote uninstallation, the **Installation editor** does not display an option for uninstallation.

Choosing **Reinstall** will reinstall the current version. This option should only be used for troubleshooting. Most of the time, there is no reason to reinstall a product.

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`….

Chapter

9

Local host operations

Topics:

- *Scan manually*
- *Scan at set times*
- *Where to find firewall alerts and log files*
- *Connecting to Policy Manager and importing a policy file manually*
- *Suspending downloads and updates*
- *Allowing users to unload F-Secure products*

You might need to perform the operations listed in this section when you suspect that there is a virus on a local host or if you need to perform some other administrative tasks locally.

Scan manually

You can scan your computer manually, if you suspect that you have *malware* on your computer.

How to select the type of manual scan

You can scan your whole computer or scan for a specific type of *malware* or a specific location.

If you are suspicious of a certain type of *malware*, you can scan only for this type. If you are suspicious of a certain location on your computer, you can scan only that section. These scans will finish a lot quicker than a scan of your whole computer.

To start manually scanning your computer:

1. On the main page, click the arrow under **Scan**.
   The scanning options are shown.
2. Select the type of scan.
   If you want to change the scanning settings, select **Change scanning settings...**.
3. If you selected **Choose what to scan**, a window opens in which you can select which location to scan.

The **Scan Wizard** opens.

Types of scan

You can scan your whole computer or scan for a specific type of malware or a specific location.

The following lists the different types of scan:

Scan type	What is scanned	When to use this type
Full computer scan	Your entire computer (internal and external hard drives) for viruses, spyware and riskware	When you want to be completely sure that there is no malware or riskware on your computer. This type of scan takes the longest time to complete. It combines the quick malware scan and the hard drive scan. It also checks for items that are possible hidden by a rootkit.
Choose what to scan	A specific file, folder or drive for viruses, spyware and riskware	When you suspect that a specific location on your computer may have malware, for example, the location contains downloads from potentially dangerous sources, such as peer-to-peer file sharing networks. Time the scan will take depends of the size of the target that you scan. The scan completes quickly if, for example, you scan a folder that contains only a few small files.
Scan hard drives	All the internal hard drives on your computer for viruses, spyware and riskware	This type of scan goes through all the hard disks of the computer. Unlike the quick malware scan, this scan type does not specifically go through the parts of your system that contain installed program files, but scans also all data files, such as documents, music, images, and videos. This type of scan is slow and recommended only if the quick malware scan has not found any malware and if you want to be sure that the other parts of your computer do not contain malicious files.
Virus and spayware scan	Parts of your computer for viruses, spyware and riskware	This type of scan is much quicker than a full scan. It searches only the parts of your system that contain installed program files.This scan type is recommended if you want to quickly

Scan type	What is scanned	When to use this type
		check whether your computer is clean, because it is able to efficiently find and remove any active malware on your computer.
Rootkit scan	Important system locations where a suspicious item may mean a security problem. Scans for hidden files, folders, drives or processes	When you suspect that a rootkit may be installed on your computer. For example, if malware was recently detected in your computer and you want to make sure that it did not install a rootkit.

Clean malware automatically

If *malware* is found during the scan, you can either let the program automatically decide how to clean your computer or you can decide yourself for each item.

1. Select either of:

Option	What will happen
Handle automatically (recommended)	The program decides what to do to each *malware* item to automatically clean your computer.
I want to decide item by item	The program asks what you want to do to each *malware* item.

2. Click **Next**.

View the results of manual scan

You can view a report of the scanning results after the scan is complete.

Note: You might want to view this report because the action you selected may not always be the action that was performed. For example, if you chose to clean an infected file, but the *virus* could not be removed from the file, the product may have performed some other action to the file.

To view the report:

1. Click **Show Report**.

   The report includes:

   - The number of *malware* found.
   - The type of *malware* found and links to descriptions of the *malware* on the Internet.
   - The actions applied to each *malware* item.
   - Any items that were excluded from the scan.
   - The scanning engines that were used to scan for *malware* .

   Note: The number of scanned files can differ depending on whether files are scanned inside archives during the scan. If archived files have been scanned earlier, the scan results may be saved in the cache memory.

2. Click **Finish** to close the **Scan Wizard**.

Tip: You can view the results of the last scan also by clicking **Settings** ➤ **Computer** ➤ **Manual scanning**. Click **View last scanning report**.

Scan at set times

You can scan your computer for *malware* at regular intervals, for example daily, weekly or monthly.

Scanning for *malware* is an intensive process. It requires the full power of your computer and takes some time to complete. For this reason, you might want to set the program to scan your computer when you are not using it.

Schedule a scan

You can set the program to scan your computer at regular times, for example, weekly, daily, or monthly.

To schedule a scan:

1. On the main page, click **Settings**.
2. Select **Computer** ➤ **Scheduled scanning** .
3. Select **Turn on scheduled scanning**.
4. Select which days you would like to regularly scan for *viruses* and *spyware* .

Option	Description
Daily	To scan every day.
Weekly	To scan on selected days during the week. Select on which days to scan from the list to the right.
Monthly	To scan on up to three days a month. To select which days: **1.** Select one of the **Day** options. **2.** Select the day of the month from the list next to the selected day. **3.** Repeat if you want to scan on another day.

5. Select when you want to start the scan on the selected days.

Option	Description
Start time	The time when the scan will start. You should select a time when you expect to not be using the computer.
After computer is not used for	Select a period of idle time after which the scanning starts if the computer is not used.

Cancel a scheduled scan

If you want to continue to use your computer when a scheduled scan starts, you may want to cancel the scheduled scan.

Scheduled scanning may have a noticeable effect of your computers performance. To cancel the scheduled scan:

Note: In centrally managed mode you may not be able to cancel a scheduled scan.

1. Click **Scheduled scan has started** link on the **Virus and spyware scanning** flyer.

   The flyer stays for about 15 seconds, after which it disappears. If you do not click the link on the flyer, you cannot cancel the scheduled scanning any more.
2. Click **Cancel** on the **Virus and spyware scanning** window.

3. Click **Close**.

The scheduled scan is canceled. The next scheduled scan will start as usual.

View the results of scheduled scan

When a scheduled scan finishes you can check if *malware* were found.

To check the results of a scheduled scan:

1. Click the **Scheduled scan has finished** on the **Virus and spyware scanning** flyer.
2. Click **Show Report** to see what happened during the scan.

   Note: If you opened the dialog from the **Flyer History** dialog, the **Show report** button is disabled. You cannot see the results of previous scheduled scans.

3. Click **Close** to close the dialog.

Tip: You can view the results of the last scan also by clicking **Settings** ➤ **Computer** ➤ **Scheduled scanning**. Click **View last scanning report**.

Where to find firewall alerts and log files

By viewing the firewall alerts and log files, you can find out how network connections are protected on your computer.

View firewall alerts

You can view a list of all generated firewall alerts.

The list contains alerts that the firewall and intrusion prevention have caused.

To view the list:

1. On the main page, click **Settings**.
2. Select **Network connections** ➤ **Firewall** .
3. Click the **Rules** tab.
4. Click **Show alert log**.
   The **Firewall alerts** dialog box opens and shows the following information:

Field	Description
Time	Time of the alert.
Remote address	*IP address* of the computer from which you have received traffic, or sent traffic to.
Hits	Shows how many times a similar alert has been generated.
Description	An alert text that has been added for the *firewall rule* . If an intrusion attempt has caused the alert, the field shows information on the intrusion attempt *pattern* .

5. To view alert details, select the alert and click **Details** .
6. To move to the next or previous alert, click the **Prev** or **Next** button.
7. After viewing the details, click **Close** to close the **Firewall alerts** details dialog box.
8. Click **Close** to close the **Firewall alerts** list dialog box.

Firewall alert information

A firewall alert contains information on the traffic that caused the alert.

A firewall alert contains the following information:

Field	Description
Description	An alert text that has been added for the *firewall rule* . If the alert is caused by an intrusion attempt, the alert shows information on the intrusion attempt *pattern* .
Action	Shows what happened, for example that the *firewall* blocked or allowed the traffic.
Time	The date and time when the alert was generated.
Direction	Shows whether the traffic is inbound or outbound (from a remote computer to your own computer or vice versa).
Protocol	The used *IP protocol* .

Field	Description
Services	Shows the *firewall services* to which this traffic matched.
Remote address	The *IP address* of the remote computer.
Remote port	The *port* on the remote computer.
Local address	The *IP address* of your own computer.
Local port	The *port* on your own computer.

View the *action log*

If a program, such as a network game, does not work, you can check in the action log if application control has denied the program from connecting to the Internet.

The *action log* is a text file (`action.log`) that automatically collects information about the network connections. The maximum size of the file is 10 MB. After the file becomes full, the old log entries are deleted.

To view the *action log* :

1. On the main page, click **Settings**.
2. Select **Network connections** ➤ **Logging** .
3. Click **Show action log**.

The *action log* opens in a default text editor or viewer, for example, Notepad.

Monitor network traffic with packet logging

You can start packet logging if you want to gather information about the *IP* network traffic.

How does packet logging work

The *packet log* collects information about the *IP* network traffic.

By default, the packet logging is turned off. Packet logging is mainly aimed at experienced users who are familiar with computer networks.

You can turn the packet logging on if you have created your own set of *firewall rules* , and want to check how they block traffic. You can also do this if you suspect malicious network activity.

Information is gathered into 10 files (`packetlog.0-packetlog.9`). Each time you turn on the logging, the *packet log* is collected into a new file. After the tenth file becomes full, the next log is collected again to the first file. In this way, you can view the previous logs while a new log is generated.

In addition to the *IP* traffic, the *packet log* also collects information about other types of network traffic, for example, about the *protocols* needed by your *Local Area Network* (LAN). This information includes, for example, *routing* information.

The *packet log* is in *hexadecimal* format and supports *tcpdump* format. This allows you to open the log files also in a packet logging program other than the default *packet log* viewer. You can also use a network *protocol* analyzer program to analyze the contents further.

Start packet logging

You can start packet logging if you suspect malicious network activity, or for example, a network game stops working.

To start logging:

1. On the main page, click **Settings**.
2. Select **Network connections** ➤ **Logging** .

3. Use the recommended logging time and file size that are shown in the **Logging time** and **Max log file size** fields. You can also change them if you want to.
4. Click **Start logging** . A new file is added to the log files list. The size of the file increases as information is gathered in the file. If the list already contains 10 log files, the next log is gathered into an existing file.
5. To stop the logging manually, click **Stop logging** . The logging stops automatically after the defined logging time period has elapsed, or the defined maximum log file size has been reached.

A new log file is generated and added to the log files list.

View the *packet log*

After you have generated a *packet log* , you can open it for viewing.

To view the *packet log* :

1. On the main page, click **Settings**.
2. Select **Network connections** ➤ **Logging** .
3. Select the *packet log* you want to view and click **Details** .
   The default *packet log* viewer opens. The upper pane of the window shows all the logged connections.

You can view the following information:

Field	Description
Time	Time in seconds from the moment when logging was started. If the defined logging time is 60 seconds, the starting time for the first *packet* is close to 0 seconds, and the starting time for the last *packet* is close to 60 seconds.
Drop (dir)	Shows whether the *firewall* let through or dropped the *packet* , and shows the direction of the *packet* : • **No** : Allowed the *packet* . • **Yes** : Dropped the *packet* . • **In** : Inbound *packet* . • **Out** : Outbound *packet* . This information is not available if you view the file in a packet logging program other than the default *packet log* viewer.
Protocol	The used *IP protocol* .
Source	Source *IP address* of the *packet* .
Destination	Destination *IP address* of the *packet* .
ID	*IP packet* header information: Identifier of the packet.
TTL	*IP packet* header information: *Time To Live* value of the *packet* defines the number of network devices through which the *packet* can travel before it is discarded.
Len	*IP packet* header information: Total length of the *packet* .
Description	Description of the *packet* .

The pane on the right shows you the traffic types and their information.

The lower pane of the window shows the information in *hexadecimal* and *ASCII* format.

If you want to view all types of network traffic (and not only *IP* traffic), clear the **Filter non IP** checkbox.

Connecting to Policy Manager and importing a policy file manually

If you need to initialize a connection from the local host to Policy Manager Server, you can do it by following these steps.

1. On the local host, go to the **Central management** page, where you can see the date and time of the last connection to Policy Manager Server.
2. Click **Check now** to initiate a new connection.
   If you need to import a new policy file manually to a host, you first have to export a host-specific policy from Policy Manager Console and then import it to the host, which is done as follows:
3. In Policy Manager Console:
   a) Select the host on the **Policy domains** tab.
   b) Right-click on the selected host and select **Export host policy file** from the context menu that opens.
   c) Save the host's policy file on some transfer media, for example on a diskette.
4. In the Client Security local user interface:
   a) Click **Import policy manually...**.
   b) In the window that opens, browse to find the `Policy.bpf` file you want to import to the host.

   Policy file importing is meant primarily for troubleshooting purposes. In normal operation policy files are always transferred automatically. Policy export and import operations can be used to restore the connection to Policy Manager if the managed host has become disconnected because of a misconfigured policy.

Suspending downloads and updates

You can allow users to suspend network communications, for example if they are sometimes using a dial-up connection.

This option is configured from Policy Manager Console. It is useful for hosts that sometimes use a slow dial-up connection. When this option is enabled, the user is allowed to temporarily suspend network communications, for example automatic polling of policies, sending statistics and automatic updates.

1. Select the host in the **Policy domains** tab.
2. Go to the **Settings** tab and select **Centralized management**.
3. Select **Allow users to suspend all downloads and updates**.
4. Click to save and distribute the policy.

Allowing users to unload F-Secure products

You can allow users to unload products, for example to free up memory.

This option is configured from the Policy Manager Console. It specifies whether the user is allowed to unload all F-Secure products temporarily, for example in order to free memory for games or similar applications.

Note: Note that the main functions of the products are disabled during the time the product is unloaded and thus the computer becomes vulnerable to viruses and attacks.

1. Select the host in the **Policy domains** tab.
2. Go to the **Settings** tab and select **Centralized management**.
3. Select one of the options from the **Allow users to unload products** drop-down menu.
4. Click to save and distribute the policy.

Chapter
10

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 provides information on where to find out about viruses and how to handle viruses you encounter.

Malware information and tools on the F-Secure web pages

You can find a list of sources of information about malware and useful tools at http://www.f-secure.com/security_center/.

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 it's own operating system and so can find some malware that cannot be found from within Windows. You can find it from the Security Center: *http://www.f-secure.com/security_center/*.

Instructions on how to use the **RescueCD** are included in the downloaded file.

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.

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*.

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\APPPEND.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*.

   If the infection is on a floppy disk, create a DCF image of the infected diskette and send the `.DCF` image file to us. You can download the DCF utility from our ftp site at: *ftp://ftp.f-secure.com/anti-virus/tools/dcf53.zip*.

   You can also send the infected diskette by mail to our Helsinki office (see address below). Please include a description of the problem. Note that we do not send diskettes back.

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.

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

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.

Chapter

11

Setting up the Cisco NAC plugin

Topics:

- *Installing the Cisco NAC plugin*
- *Importing posture validation attribute definitions*
- *Using attributes for the application posture token*

F-Secure participates in the Network Admission Control (NAC) collaboration led by Cisco Systems®. NAC can be used to restrict the network access of hosts that have too old virus definition databases, or anti-virus or firewall modules disabled.

The F-Secure NAC plug-in communicates with Cisco® Trust Agent (CTA), a client software on the hosts that collects the security-related information from the host and communicates the data to Cisco Secure Access Control Server (ACS). Based on this data, an appropriate access policy is applied to the host.

For more information about NAC, see *http://www.cisco.com/go/nac/*.

The installation package for Client Security contains an option to install the Cisco NAC Plugin. When you select this option, the CTA must already be installed on the host. In addition to this, the ACS server must be configured to monitor F-Secure product-related security attributes.

Installing the Cisco NAC plugin

The Cisco NAC plugin can be installed on hosts both locally and remotely.

1. Local installations: when installing Client Security locally, select **Cisco NAC Plugin** in the **Components to install** dialog.
2. Remote installations: when installing Client Security remotely, select **Cisco NAC Plugin** in the **Components to install** dialog.

   Note: For more information, see the Cisco NAC documentation.

Importing posture validation attribute definitions

You need to add posture validation attribute definitions related to F-Secure products to the Cisco Secure ACS Posture Validation Attributes definition file.

1. Use the **CSUtil** tool on the Cisco Secure ACS server.
2. Use the following command:

   `CSUtil.exe -addAVP fsnacpva.def`

   The `fsnacpva.def` file is included in the product installation package.

   Note: For more information about **CSUtil**, see the Cisco ACS documentation.

Using attributes for the application posture token

Here you will find details on how to configure the Cisco ACS server to monitor product-related security attributes.

To configure the Cisco ACS server to monitor F-Secure product-related security attributes, do the following:

1. Click the **External user databases** button on the Cisco ACS server user interface.
   This opens the **External user databases** page.
2. Click **Database configuration**.
   This opens the **External user databases configuration** page.
3. Click **Network admission control**.
4. Click **Configure**.
5. Select **Create new local policy**.
6. You can use the following Client Security related attributes in the rules for *Application Posture Tokens*:
   - Posture validation attributes for Anti-Virus:

Attribute-name	Type	Example
Software-Name	string	`F-Secure Anti-Virus`
Software-Version	version	`8.0.0.0`
Dat-Date	date	`[the date of database]`
Protection-Enabled	unsigned integer	`1`=enabled, `0`=disabled

   - Posture validation attributes for Firewall:

Attribute-name	Type	Example
Software-Name	string	`F-Secure Internet Shield`
Software-Version	version	`8.0.0.0`
Protection-Enabled	unsigned integer	`1`=enabled, `0`=disabled

Chapter

12

Advanced features: virus and spyware protection

Topics:

- *Configuring scheduled scanning*
- *Advanced DeepGuard settings*
- *Configuring Policy Manager Proxy*
- *Configuring automatic updates on hosts from Policy Manager Proxy*
- *Excluding an application from the web traffic scanner*

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.

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 is opened.
2. Select **Root** on the **Policy domains** tab.
3. On the **Policy** tab, select **F-Secure** ➤ **F-Secure Anti-Virus**.
4. Select the **Scheduling table** page.
   The currently set scheduled tasks are displayed on the **Scheduling** table. Now you can add scheduled scanning as a new task.
5. Click the **Add** button.
   This adds a new row in the **Scheduling** table.
6. Click the **Name** cell on the row you just created and then click **Edit**.
7. The **Name** cell is now activated and you can enter a name for the new task.

   For example, `Scheduled scanning for all hosts`.
8. Next click the **Scheduling parameters** cell, and then click **Edit**.
9. 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).
10. Select the task type by clicking the **Task type** cell and then clicking **Edit**.
11. From the drop-down list that opens select **Scan local drives**.
    The scanning task is now ready for distribution.
12. Click to save and 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.

Advanced DeepGuard settings

This section covers the advanced settings relating to DeepGuard.

Notifying user on a deny event

You can configure the product to notify users when DeepGuard denies an event they have initiated.

To notify the user when DeepGuard automatically denies an event:

1. Select **View** ➤ **Advanced mode** from the menu.
   The **Advanced mode** user interface is opened.
2. Select **Root** on the **Policy domains** tab.
3. On the **Policy** tab, select **F-Secure** ➤ **F-Secure DeepGuard** ➤ **Settings** ➤ **Show notification flyer on deny events** .
4. Select **Yes** in the main application area.
5. Click to save and distribute the policy.

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 save and distribute the policy.

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 save and distribute the policy.

The application rule cannot be over-ridden locally by the user.

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.

Configuring automatic updates on hosts from Policy Manager Proxy

A list of proxies through which the hosts fetch updates can be configured on the **Settings** tab.

If you need to configure this from a managed host's local user interface, you can do it as follows:

1. Go to the **Automatic updates** page and click **Advanced...**.
2. Select **Automatic updates** ➤ **Policy Manager Proxy**.

   On the **Policy Manager Proxy** page, you can view and edit the addresses from which the local Client Security gets automatic updates.

   The addresses are used from top to bottom, i.e. the first address on the list is the one used by default.
3. Click **Add** to add the proxy on the list.
4. Enter the name of the first proxy in the field and then click **OK**.
5. Repeat this for the other proxies you want to add.

   To change the order of the servers, select the one you wish to move and click the up or down arrows on the right to move it.
6. When you have added all the proxies, click **OK**.

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** ➤ **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 save and distribute the policy.

Chapter

13

Advanced features: Internet Shield

Topics:

- *Managing Internet Shield properties remotely*
- *Configuring security level autoselection*
- *Troubleshooting connection problems*
- *Adding new services*
- *Setting up dialup control*

This section covers some advanced Internet Shield features and also contains some troubleshooting information.

Managing Internet Shield properties remotely

This section describes how you can manage Internet Shield properties remotely.

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. On the **Policy** tab, select **F-Secure Internet Shield**.
4. Select the **Logging** tab.
   This variable normally shows the status of the packet logging; **Disabled** means that it is not running, and **Enabled** that it is currently running on the host.
5. To turn off logging completely, make sure that it is set to **Disabled**, and select the **Final** check box.
6. Distribute the policy to enforce the change.

To later undo this change, clear the **Final** check box 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.

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. Save and distribute the policy to enforce the change.

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**.
4. To make sure packet filtering is always turned on, set this variable to **Yes** and select the **Final** check box.
5. Distribute the policy to enforce the change.

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**.
4. Select the **Security level autoselection** page.
5. 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.
6. Click **Add** to add the first security level, in this example **Office**.
7. 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.
8. Click **Add** to add the second security level, in this example **Mobile**.
9. 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.
10. Click to save and distribute the policy.

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.

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.

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

Protocol name	Protocol number	Full name
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.

Setting up dialup control

Dialup control lets you create lists of phone numbers allowed and blocked from the users dialup modem.

To turn on dialup control:

1. Select **View** ➤ **Advanced mode** from the menu to switch to the **Advanced mode** user interface.
2. From the **Policy** tab select **F-Secure** ➤ **F-Secure Internet Shield** ➤ **Settings** ➤ **Dialup control** ➤ **Dialup control**.
3. Select **Enabled** to turn dialup control on.
4. Click to save and distribute the policy.

Allowing and blocking phone numbers

You can allow or block specific phone numbers from being used for dialup connections.

To add a new allowed or blocked number:

1. Select **View** ➤ **Advanced mode** from the menu to switch to the **Advanced mode** user interface.
2. From the **Policy** tab select **F-Secure** ➤ **F-Secure Internet Shield** ➤ **Settings** ➤ **Dialup control** ➤ **Phone Numbers**.
3. Click **Add**.
4. Double-click the **Priorities** cell for the new row to set the priority for the rule.

   If two rules match a phone number, the rule with the smallest numbered priority will apply i.e. a rule with priority `1` will override a rule with priority `3`.
5. Double-click the **Phone number** cell for the new row to add the phone numbers the rule applies to.

   You can use the following characters to apply a rule to multiple phone numbers:

Character	Applies to	Example
?	Matches any single digit	`1?3` matches the following numbers: 103, 113, 123,133,143, 153,163,173,183,193.
*	Matches any number of digits	`0800*` matches all phone numbers that begin with 0800

6. Select **Allow** or **Deny** to allow or block the modem from calling the matching phone numbers.
7. Double-click the **Comment** cell for the new row and add a description to explain the purpose of the rule to other users.
8. Select **Yes** to enable the new rule.
9. Click to save and distribute the policy.

Using call logging

You can use call logging to keep a log of all dialed numbers used.

To turn on the logging of dialed numbers:

1. Select **View** ➤ **Advanced mode** from the menu to switch to the **Advanced mode** user interface.
2. From the **Policy** tab select **F-Secure** ➤ **F-Secure Internet Shield** ➤ **Settings** ➤ **Dialup control** ➤ **Number logging**.
3. Select **Enabled** to log numbers that the modem calls.

4. Click to save and distribute the policy.

Chapter
14

Modifying prodsett.ini

Topics:

- *Configurable prodsett.ini settings*

This section contains a list of the settings that can be edited in `prodsett.ini`.

Caution: Do not edit any `prodsett.ini` settings in that are not included in this section.

Note: Dependency between `RequestInstallMode` and `InstallMode` settings:

The `RequestInstallMode` setting can override the selection for components, which have `InstallMode=0`.

Configurable prodsett.ini settings

You can edit edit the settings described here in the `prodsett.ini` file.

[F-Secure common]	Common settings
CD-Key=XXXX-XXXX-XXXX-XXXX-XXXX	Enter the subscription key of the installation package here.
SetupLanguage=ENG	Enforced Installation language. If the setting is empty or defined as `AUTO`, the installation language is automatically chosen at the host based on the default system locale. The chioce is limited by the set of supported languages (see SupportedLanguages).
SetupMode=1	`1` = Network client (default). If `SetupMode=1`, the corresponding centralized management settings should be defined in the [PMSUINST.DLL] section. `2` = Stand-alone setup mode.
SupportedLanguages=ENG FRA DEU FIN SVE ITA	List of languages supported by the installation package. You can make the set of languages smaller by leaving out some unnecessary languages and repacking the package. When you add support for a new language to the package you should add that language here to make it effective.
InstallLanguages=ENG FRA DEU FIN SVE ITA	List of languages being installed at the host. This setting typically equals `SupportedLanguages`. You can make the set of languages smaller if you want some unnecessary languages not to be installed. When you add new language support to the package you should add that language here to make it effective for the installed software. The language files of the language defined by the SetupLanguage setting are always installed independently of the InstallLanguages setting.
SecurityPolicy=0 | 1 | 2	The files and folders installed to NTFS and the product's registry keys are protected with the NT security permissions according to the defined `SecurityPolicy`: `0` = no special policy applied; files and folders inherit the security permissions from the parent. `1` = less strict policy; files and folders are protected with permissions granting full access to authorized

[F-Secure common]	Common settings
	users and administrators, and read-only access to everyone. `2` = strict policy; files and folders are protected with permissions granting full access to administrators, read-write access to power users, read-only access to users, and no access to everyone. Note: When `SecurityPolicy = 1` or `2`, setup overwrites the access control lists (ACLs) of existing files, folders ,and registry keys. If you have specifically configured ACLs, for example, by adding users to them, you need to reconfigure them after the installation.

[Silent Setup]	Settings for unattended automatic installation
DestinationDirUnderProgramFiles=F-Secure	Default destination path. Do not change this setting unless your company follows a specific installation policy.
Reboot=2	`1` = Reboot automatically after installation. **Attention:** This option executes a forced reboot at the host without prompting the user to save his/her work. Do not use this option until you are absolutely sure about the safety of this type of reboot for the target computer. `2` = Reboot after prompting the user for a confirmation (default). **Note:** This choice executes a normal reboot at the host, and therefore in some cases the user could delay the restart or completely prevent it. `3` = Do not reboot after installation.

[FSMAINST.DLL]	Settings for Management Agent
RequestInstallMode=1	This component is always installed when you are installing a networked client. You do not need to edit the `RequestInstallMode` or `InstallMode` settings for this component.
ManagementKey=\\server\path\admin.pub	Location of the management public key.
ManagedStandAlone=	Meaningful only in stand-alone installations. `0` = Normal stand-alone installation, no policy files can be imported (default). `1` = Installed components can be managed with manually imported policies.

[FSMAINST.DLL]	Settings for Management Agent
win2000renamefiles=fsrec.2k|fsrec.sys;fsfilter.2k|fsfilter.sys;fsgk.2k|fsgk.sys	Do not modify these settings!
InstallFSPKIH=0	
InstallNetworkProvider=0	
InstallGINA=0	
RedefineSettings=0	
ServiceProviderMode=0	
MibVersion=	
GatekeeperVersion=	
StatisticsFilterPattern1=	
UseOnlyUID=	`0` = Management Agent only uses all available identities (DNS name, IP address, WINS name, Unique Identity) to identify itself for the first time to the Policy Manager Server. `1` = Management Agent only uses its unique identity to identify itself to the Policy Manager Server.
Debug=1	`0` = Do not generate debug information (default). `1` = Write debug information into the debug log during installation and uninstallation.
InstallMode=0 | 1	This component is always installed when you are installing a networked client. You do not need to edit the `RequestInstallMode` or `InstallMode` settings for this component.

[PMSUINST.DLL]	Settings for Policy Manager support
RequestInstallMode=0	This component is always installed when you are installing a networked client. You do not need to edit the `RequestInstallMode` or `InstallMode` settings for this component.
FsmsServerUrl=http://fsmsserver	URL to Policy Manager Server.
FsmsExtensionUri=/fsms/fsmsh.dll	Do not change this setting.
FsmsCommdirUri=/commdir	Do not change this setting.
Debug=1	`0` = Do not generate debug information (default). `1` = Write debug information into the debug log during installation and uninstallation.
InstallMode=0 | 1	This component is always installed when you are installing a networked client. You do not need to edit

[PMSUINST.DLL]	Settings for Policy Manager support
	the `RequestInstallMode` or `InstallMode` settings for this component.

[FSAVINST.DLL]	Settings for Client Security - virus protection
RequestInstallMode=1	`0` = Install this component as defined in the `InstallMode` setting. `1` = Install this component if newer, or not installed (default). `2` = Install this component if there is no existing version of it installed, or if the same or an older version exists.
EnableRealTimeScanning=1	`0` = Disable real-time scanning `1` = Enable real-time scanning (default).
Debug=1	`0` = Do not generate debug information (default). `1` = Write debug information into the debug log during installation and uninstallation.
InstallMode=0 | 1	`0` = Do not install this component (default). `1` = Install this component, except if a newer version already exists.

[FSSGSUP.DLL]	Settings for conflict detection and removal module
RequestInstallMode=1	This component is always run during the installation. You do not need to edit the `RequestInstallMode` or `InstallMode` settings for this component
Debug=0 | 1	`0` = Do not generate debug information (default). `1` = Write debug information into the debug log during installation and uninstallation.
InstallMode=0 | 1	This component is always run during the installation. You do not need to edit the `RequestInstallMode` or `InstallMode` settings for this component
SidegradeAction=0	`0` = Remove all found conflicts automatically (default). `1` = Cancel installation if any conflicting software is found installed.

[ES_Setup.DLL]	Settings for the installation of e-mail scanning
RequestInstallMode=1	`0` = Install this component as defined in the `InstallMode` setting. `1` = Install this component if newer, or not installed (default).

[ES_Setup.DLL]	Settings for the installation of e-mail scanning
	`2` = Install this component if there is no existing version of it installed, or if the same or an older version exists.
Debug=0 | 1	`0` = Do not generate debug information (default). `1` = Write debug information into the debug log during installation and uninstallation.
InstallMode=0 | 1	`0` = Do not install this component (default). `1` = Install this component, except if a newer version already exists.

[FWESINST.DLL]	Settings for internal common component FWES.
RequestInstallMode=1	`0` = Install this component as defined in the `InstallMode` setting. `1` = Install this component if newer, or not installed (default). `2` = Install this component if there is no existing version of it installed, or if the same or an older version exists.
Debug=0 | 1	`0` = Do not generate debug information (default). `1` = Write debug information into the debug log during installation and uninstallation.
InstallMode=0 | 1	`0` = Do not install this component (default). `1` = Install this component, except if a newer version already exists.

[FWINST.DLL]	Settings for Client Security - Internet Shield
RequestInstallMode=1	`0` = Install this component as defined in the `InstallMode` setting. `1` = Install this component if newer, or not installed (default). `2` = Install this component if there is no existing version of it installed, or if the same or an older version exists.
Debug=0 | 1	`0` = Do not generate debug information (default). `1` = Write debug information into the debug log during installation and uninstallation.
InstallMode=0 | 1	`0` = Do not install this component (default). `1` = Install this component, except if a newer version already exists.
InstallDC=0 | 1	`0` = Do not install Dial-up Control (default).

[FWINST.DLL]	Settings for Client Security - Internet Shield
	`1` = Install Dial-up Control
InstallNetworkQuarantine=0 | 1	`0` = Do not install Network Quarantine (default). `1` = Install Network Quarantine.
DisableWindowsFirewall=0 | 1	`0` = Do not disable Windows Firewall (on XP SP2 or later) (default). `1` = Disable Windows Firewall after Internet Shield installation.

[FSBWINST.DLL]	Settings for Automatic Update Agent
RequestInstallMode=1	`0` = Install this component as defined in the `InstallMode` setting. `1` = Install this component if newer, or not installed (default). `2` = Install this component if there is no existing version of it installed, or if the same or an older version exists.
InstallMode=0 | 1	`0` = Do not install this component (default). `1` = Install this component, except if a newer version already exists.

[FSPSINST.DLL]	Settings for Client Security - Network Scanner
RequestInstallMode=1	`0` = Install this component as defined in the `InstallMode` setting. `1` = Install this component if newer, or not installed (default). `2` = Install this component if there is no existing version of it installed, or if the same or an older version exists.
Debug=0 | 1	`0` = Do not generate debug information (default). `1` = Write debug information into the debug log during installation and uninstallation.
InstallMode=0 | 1	`0` = Do not install this component (default). `1` = Install this component, except if a newer version already exists.
DisableScanningForApps= Wget.exe,mplayer.exe	Disables Network Scanning for certain executables. This is a comma-separated list of executable names without paths. **Note:** No spaces are allowed between the items.
EnableHTTPScanning=1	`0` = HTTP Scanning disabled

[FSPSINST.DLL]	Settings for Client Security - Network Scanner
	`1` = HTTP Scanning enabled
StartImmediatelyForApps= iexplore.exe,firefox.exe, netscape.exe,opera.exe, msimn.exe,outlook.exe, mozilla.exe	This setting defines which executables should start HTTP scanning immediately. Other processes will go in scanning mode only after the first access to an external server port 80. This is a comma-separated list of executable names without paths. **Note:** No spaces are allowed between the items.

[FSNACINS.DLL]	Settings for Cisco NAC Plugin
RequestInstallMode=1	`0` = Install this component as defined in the `InstallMode` setting. `1` = Install this component if newer, or not installed (default). `2` = Install this component if there is no existing version of it installed, or if the same or an older version exists.
CTAversion=1.0.55	`CTAversion` defines the version of the Cisco Trust Agent included in the package. Cisco Trust Agent installation package can be updated by replacing the `ctasetup.msi` file in the directory where `prodsett.ini` resides.
Debug=0 | 1	`0` = Do not generate debug information (default). `1` = Write debug information into the debug log during installation and uninstallation.
InstallMode=0 | 1	`0` = Do not install this component (default). `1` = Install this component, except if a newer version already exists.

Chapter
15

E-mail scanning alert and error messages

Topics:

- *Alert and error messages*

This section provides a list of the alert and error messages that e-mail scanning can generate.

Alert and error messages

A list of the messages generated by e-mail scanning is given below.

Message title	Message ID	Definition	Message content
E-Mail Scanning Session Failed: System Error	602		Connection to the `<server name>` server was terminated by E-mail scanning due to a system error. E-mail scanning continues to be functional.
E-Mail Scanning Malfunctioning: System Error	603		E-mail scanning is not functioning due to a severe error. If the problem persists, please contact the system administrator.
E-Mail Scanning Message Parser Failed: System Error	604		Could not scan an e-mail due to message parser error. The session was not aborted, the specific message was not scanned.
E-Mail Scanning Initialization Failed	610		E-mail scanning initialization failed, reason: `<for reason description, see above>`

E-Mail Attachment Virus Alert	620-623	When a virus is found the virus is treated based on the configuration set on F-Secure Client Security **Advanced** configuration.
		Action taken options:
		• Infection was only reported
		• Attachment was disinfected
		• Attachment was dropped
			`E-Mail Virus Alert!`
			
			`Infection: <Name of the virus>`
			`Attachment: <Email message part, attached file that was infected>`
			`Action: <Action taken>`
			`Message <Message ID>`
			
			`from: <Email header: sender filed email address>`
			`to: < Email`

Message title	Message ID	Definition	Message content
		• Infected e-mail was blocked	`header: recipient filed email addresses>` `  subject: < Email header: The title subject filed of the message >`

Malformed E-Mail Alert	630-633	When a malformed message is found it is treated based on the configuration set on F-Secure Client Security **Advanced** configuration.
		Action taken options:
		• Malformed message part was only reported
		• Malformed message part was dropped
		• Malformed e-mail was blocked
			`Malformed E-Mail Alert!`
			`Description: <description of the malformation>`
			`Message part: <malformed message part>`
			`Action: <Action taken>`
			`Message < Message ID>`
			`  from: <Email header: sender filed email address>`
			`  to: < Email header: recipient filed email addresses>`
			`  subject: < Email header: The title subject filed of the message >`

E-Mail Attachment Scanning Failure	640-643	When a scan fails, the message is treated based on the configuration set in **Advanced** configuration.
		Reasons for scanning failure:
		• Per file scanning time-out triggered
		• Per e-mail scanning time-out triggered
		• Attachment was a password protected zip file
		• Error while scanning the attachment (not enough disk space, memory etc.)
		Action taken options
		• Scanning failure was only reported
		• Attachment was dropped
			`E-Mail Attachment Scanning Failure`
			`Reason: <Description of the scanning failure>`
			`Attachment: <The attachment causing the scanning failure>`
			`Action: <Action Taken>`
			`Message < Message ID>`
			`  from: <Email header: sender filed email address>`
			`  to: < Email header: recipient filed email addresses>`
			`  subject: < Email header: The title subject filed of the message >`

Message title	Message ID	Definition	Message content
		• E-mail was blocked	

Chapter
16

Products detected or removed during client installation

Topics:

- *Product list*

The products listed in this section are either detected so that the user can manually uninstall them or automatically uninstalled during the F-Secure Client Security installation process.

Product list

A list of the products that are detected and removed during installation is given below.

- Agnitum Outpost Firewall Pro 1.0
- AOL Safety and Security Center
- avast! Antivirus
- AVG Anti-Virus 7.0
- AVG Free Edition
- AVG Anti-Virus 7.1
- AVG 7.5
- Avira AntiVir PersonalEdition Classic
- Avira AntiVir PersonalEdition Premium
- Avira AntiVir Windows Workstation
- Avira Premium Security Suite
- BitDefender Antivirus v10
- BitDefender Antivirus Plus v10
- BitDefender 8 Free Edition
- BitDefender 9 Internet Security
- BitDefender Internet Security v10
- BitDefender 9 Professional Plus
- BitDefender 9 Standard
- BitDefender Total Security 2008
- Bsecure Internet Protection Services v.4.5
- BullGuard 7.0
- CA Anti-Virus
- CA eTrust Antivirus
- eTrust EZ Antivirus
- EZ Firewall
- CA Internet Security Suite
- Cisco VPN Client Firewall
- Dr Solomon's VirusScan
- EarthLink Protection Control Center
- EarthLink Software
- EarthLink Toolbar
- EMBARQ Toolbar (Powered by EarthLink)
- PC Antivirus
- F-PROT Antivirus for Windows
- FortiClient
- F-Secure Anti-spyware
- F-Secure Anti-Virus Client Security
- Incompatible F-Secure product
- Broken or incompletely uninstalled product
- F-Secure VPN+ Client
- G DATA AntiVirenKit (German version only)
- G DATA InternetSecurity (German version only)
- G DATA TotalCare (German version only)
- AntiVirenKit 2005
- H+BEDV AntiVir Personal Edition

- iProtectYou 7.09
- Jiangmin Antivirus Software (English version only)
- K7 TotalSecurity 2006
- Kaspersky Anti-Spam Personal
- Kaspersky Anti-Virus 6.0 (English version only)
- Kaspersky Internet Security 6.0 (English version only)
- Kaspersky Internet Security 7.0 (English version only)
- Kaspersky(TM) Anti-Virus Personal 4.0
- Kaspersky(TM) Anti-Virus Personal Pro 4.0
- Kaspersky(TM) Anti-Virus Personal 4.5
- Kaspersky Anti-Virus Personal Pro
- Kaspersky Anti-Virus Personal
- Kerio Personal Firewall
- Kingsoft Internet Security (English version only)
- McAfee SecurityCenter
- McAfee VirusScan
- McAfee VirusScan Enterprise
- McAfee VirusScan Home Edition
- McAfee Internet Security
- McAfee Uninstall Wizard
- McAfee Personal Firewall
- McAfee Personal Firewall Plus
- McAfee Privacy Service
- McAfee SecurityCenter
- McAfee SpamKiller
- McAfee VirusScan Professional Edition
- McAfee Total Protection
- McAfee Browser Protection Service
- McAfee Virus and Spyware Protection Service
- McAfee Personal Firewall Express
- McAfee Firewall Protection Service
- McAfee Firewall
- Windows Live OneCare
- NAI ePolicy Orchestrator Agent
- NIC v5.50
- Norman Personal Firewall 1.42
- Norman Virus Control
- NOD32 antivirus system (English, French, German, Hungarian, Romanian and Spanish, simplified Chinese, traditional Chinese, Czech, Croatian, Italian, Japanese, Dutch, Polish, Portuguese Russian and Slovenian versions only)
- PureSight Parental Control
- Radialpoint Security Services
- Radialpoint Servicepoint Agent 1.5.11
- Sophos Anti-Virus
- Sophos AutoUpdate
- Sophos Remote Management System
- Sunbelt Personal Firewall
- Norton AntiVirus 2003
- Norton AntiVirus 2005
- Norton 360

- Norton AntiVirus 2004 (Symantec Corporation)
- Norton AntiVirus
- Norton AntiVirus Corporate Edition
- Norton Internet Security
- Norton Internet Security 2005
- Norton Internet Security 2006 (Symantec Corporation)
- Norton Internet Security 2007
- Norton Internet Security 2008
- Norton Security Online
- Norton SystemWorks 2004 Professional (Symantec Corporation)
- Norton SystemWorks 2005 (Symantec Corporation)
- Norton Personal Firewall (Symantec Corporation)
- Norton Personal Firewall 2005
- Symantec AntiVirus
- Symantec AntiVirus Client
- Symantec Client Security
- Symantec Endpoint Protection
- LiveUpdate 1.7 (Symantec Corporation)
- LiveUpdate 1.80 (Symantec Corporation)
- LiveUpdate 2.6 (Symantec Corporation)
- LiveUpdate 1.6 (Symantec Corporation)
- LiveUpdate
- LiveUpdate 2.0 (Symantec Corporation)
- LiveUpdate 3.3 (Symantec Corporation)
- Panda Antivirus 2007
- Panda Antivirus + Firewall 2007
- Panda ClientShield
- Panda Internet Security 2008
- Panda Antivirus Platinum
- Panda Platinum Internet Security
- Panda Platinum 2005 Internet Security (English version only)
- Panda Platinum 2006 Internet Security
- Panda Internet Security 2007
- Panda Titanium Antivirus 2004
- Panda Titanium Antivirus 2005 (English, French and Spanish versions only)
- Panda Titanium 2006 Antivirus + Antispyware
- Trend Micro Officescan (Windows 2000 only)
- Trend Micro OfficeScan Client
- PC-cillin 2003
- Trend Micro PC-cillin Internet Security 12
- Trend Micro PC-cillin Internet Security 2005
- Trend Micro PC-cillin Internet Security 2006
- Trend Micro Internet Security
- Trend Micro AntiVirus 2007
- Trend Micro PC-cillin Internet Security 2007
- Trend Micro Internet Security Pro
- ZoneAlarm
- ZoneAlarm Security Suite
- ZoomTownInternetSecurity v.4.5