

# **F-Secure Policy Manager**

## **Administrator's Guide**



# Contents

<b>Chapter 1: Introduction.....</b>	<b>7</b>
System requirements.....	8
Policy Manager Server.....	8
Policy Manager Console.....	8
Main components.....	9
Features.....	10
Product registration.....	11
Policy-based management.....	11
Management Information Base.....	12
<b>Chapter 2: Installing the product.....</b>	<b>15</b>
Security issues.....	16
Installing Policy Manager in high-security environments.....	16
Installation order.....	16
Installing Policy Manager Server.....	17
Download and run the installation package.....	17
Select components to install.....	17
Complete the migration wizard.....	18
Complete installation of the product.....	18
Check that the installation was successful.....	19
Changing the web browser path.....	19
Uninstalling the product.....	19
<b>Chapter 3: Using Policy Manager Console.....</b>	<b>21</b>
Overview.....	22
Basic information and tasks.....	22
Logging in.....	22
Client Security management.....	23
Advanced mode user interface.....	23
Policy domain tree.....	24
Contents of the Advanced mode user interface.....	24
Messages pane.....	26
The toolbar.....	26
Menu commands.....	27
Managing domains and hosts.....	28
Adding policy domains.....	28
Adding hosts.....	29
Software distribution.....	32

Push installations.....	33
Policy-based installation.....	35
Local installation and updates with pre-configured packages.....	36
Information delivery.....	38
Managing policies.....	38
Settings.....	38
Discarding undistributed changes to settings.....	38
Restrictions.....	39
Configuring settings.....	39
Policy inheritance.....	39
Managing operations and tasks.....	40
Alerts.....	40
Viewing alerts and reports.....	40
Configuring alert forwarding.....	41
Reporting tool.....	41
Policy domain / host selector pane.....	42
Report type selector pane.....	42
Report pane.....	43
Bottom pane.....	43
Viewing and exporting a report.....	43
Preferences.....	44
Connection-specific preferences.....	44
Shared preferences.....	44
<b>Chapter 4: Maintaining Policy Manager Server.....</b>	<b>47</b>
Backing up & restoring Policy Manager data.....	48
Creating the backup.....	48
Restoring the backup.....	48
Exporting and importing signing keys.....	48
Replicating software using image files.....	49
<b>Chapter 5: Updating virus definition databases.....</b>	<b>51</b>
Automatic updates with Automatic Update Agent.....	52
How Automatic Update Agent works.....	52
The benefits of using Automatic Update Agent.....	52
Using Automatic Update Agent.....	53
Configuring Automatic Update Agent.....	53
How to read the log file.....	54
Forcing Automatic Update Agent to check for new updates immediately.....	55
Updating the databases manually.....	55
Troubleshooting.....	55
<b>Chapter 6: Using the product on Linux.....</b>	<b>57</b>

Overview.....	58
Installation.....	58
Install Automatic Update Agent and Policy Manager Server.....	59
Install Policy Manager Console.....	60
Uninstalling the product.....	61
Frequently asked questions.....	62
<b>Chapter 7: Web Reporting.....</b>	<b>67</b>
Generating and viewing reports.....	68
Generating a report.....	68
Creating a printable report.....	68
Automated report generation.....	69
Maintaining Web Reporting.....	69
Web Reporting error messages and troubleshooting.....	69
Error messages.....	69
Troubleshooting.....	69
Changing the Web Reporting port.....	70
<b>Chapter 8: Policy Manager Proxy.....</b>	<b>71</b>
Overview.....	72
<b>Chapter 9: Troubleshooting.....</b>	<b>73</b>
Policy Manager Server and Policy Manager Console.....	74
Policy Manager Web Reporting.....	77
Policy distribution.....	77
<b>Chapter 10: llaunchr error codes.....</b>	<b>79</b>
Error codes.....	80
<b>Chapter 11: FSII remote installation error codes.....</b>	<b>83</b>
Error codes.....	84
<b>Chapter 12: NSC notation for netmasks.....</b>	<b>87</b>
NSC notation details.....	88



## Introduction

---

### Topics:

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

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

Policy Manager can be used for:

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

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

## 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:	<p>Microsoft Windows:</p> <ul style="list-style-type: none"> <li>• Microsoft Windows Server 2003 SP1 or higher (32-bit); Standard, Enterprise, Web Edition or Small Business Server editions</li> <li>• Windows Server 2003 SP1 or higher (64-bit); Standard or Enterprise editions</li> <li>• Windows Server 2008 SP1 (32-bit); Standard, Enterprise or Web Server editions</li> <li>• Windows Server 2008 SP1 (64-bit); Standard, Enterprise, Web Server, Small Business Server or Essential Business Server editions</li> <li>• Windows Server 2008 R2 with or without SP1; Standard, Enterprise or Web Server editions</li> </ul> <p>Linux:</p> <ul style="list-style-type: none"> <li>• Red Hat Enterprise Linux 4, 5 and 6</li> <li>• CentOS 5</li> <li>• openSUSE Linux 11</li> <li>• SUSE Linux Enterprise Server 10 and 11</li> <li>• SUSE Linux Enterprise Desktop 11</li> <li>• Debian GNU Linux 5</li> <li>• Ubuntu 8.04, 10.04</li> </ul>
Processor:	P4 2Ghz or multi-core 3GHz CPU, depending on the operating system and the size of the managed environment.
Memory:	1 - 2 GB RAM, depending on the operating system and the size of the managed environment.
Disk space:	6 - 10 GB of free disk space, depending on the size of the managed environment.
Network:	100 Mbit network.

---

### Policy Manager Console

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

---

Operating system:	<p>Microsoft Windows:</p> <ul style="list-style-type: none"> <li>• Windows XP Professional (SP2 or higher)</li> </ul>
-------------------	---

- Windows Vista (32-bit or 64-bit) with or without SP1; Business, Enterprise or Ultimate editions
- Windows 7 (32-bit or 64-bit) with or without SP1; 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 with or without SP1; Standard, Enterprise or Web Server editions

Linux:

- Red Hat Enterprise Linux 4, 5 and 6
- CentOS 5
- openSUSE Linux 11
- SUSE Linux Enterprise Server 10 and 11
- SUSE Linux Enterprise Desktop 11
- Debian GNU Linux 5
- Ubuntu 8.04, 10.04

Processor:	P4 2 GHz processor.
Memory:	512 MB - 1 GB of RAM, depending on the operating system and the size of the managed environment.
Disk space:	200 MB of free disk space.
Display:	Minimum 16-bit display with resolution of 1024x768 (32-bit color display with 1280x1024 or higher resolution recommended).
Network:	100 Mbit network.

---

## 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.

<b>Policy Manager Server</b>	Policy Manager Server is the repository for policies and software packages distributed by the administrator, as well as status information and alerts sent by the managed hosts. Communication between Policy Manager Server and the managed hosts is accomplished through the standard <i>HTTP protocol</i> , which ensures trouble-free performance on both <i>LAN</i> and <i>WAN</i> .
<b>Management Agent</b>	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.
<b>Web Reporting</b>	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.
<b>Update Server &amp; Agent</b>	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/](http://www.f-secure.com/en_EMEA/estore/license-terms/)) and privacy policy ([http://www.f-secure.com/en\\_EMEA/privacy.html](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.

## Policy-based management

---

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

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

- Remotely controlling and monitoring the behavior of the products.

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

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

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

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

<b>Default policy files</b>	The default policy file contains the default values (the factory settings) for a single product that are installed by the setup. Default policies are used only on the host. If neither the base policy file nor the incremental policy file contains an entry for a variable, then the value is taken from the default policy file. New product versions get new versions of the default policy file.
<b>Base policy files</b>	Base policy files contain the administrative settings and restrictions for all the variables for all F-Secure products on a specific host (with domain level policies, a group of hosts may share the same file). A base policy file is signed by Policy Manager Console, protecting the file against changes while it is passing through the network and while it is stored in the host's file system. These files are sent from Policy Manager Console to Policy Manager Server. The host periodically polls for new policies created by Policy Manager Console.
<b>Incremental policy files</b>	Incremental policy files are used to store local changes to the base policy. Only changes that fall within the limits specified in the base policy are allowed. The incremental policy files are then periodically sent to Policy Manager Console so that current settings and statistics can be viewed by the administrator.

## Management Information Base

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

In Policy Manager, the MIB structure is used for defining the contents of the policy files. Each variable has an *Object Identifier (OID)* and a value that can be accessed using the *Policy API*. In addition to basic SNMP MIB definitions, the F-Secure MIB concept includes many extensions that are needed for complete policy-based management.

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

Settings	Used to manage the workstation in the manner of an SNMP. The managed products must operate within the limits specified here.
Statistics	Delivers product statistics to Policy Manager Console.
Operations	Operations are handled with two policy variables: (1) a variable for transferring the operation identifier to the host, and (2) a variable for informing Policy Manager Console about the operations that were performed. The second variable is transferred using normal statistics; it acknowledges all previous operations at one time. A custom editor for editing operations is associated with the subtree; the editor hides the two variables.
Private	The management concept MIBs may also contain variables which the product stores for its internal use between sessions. This way, the product does not need to rely on external services such as Windows registry files.

## Traps

Traps are the messages (including alerts and events) that are sent to the local console, log file, remote administration process, etc. The following types of traps are sent by most F-Secure products:



Info. Normal operating information from a host.



Warning. A warning from the host.



Error. A recoverable error on the host.



Fatal error. An unrecoverable error on the host.



Security alert. A security hazard on the host.

---



## Installing the product

---

### Topics:

- [Security issues](#)
- [Installing Policy Manager in high-security environments](#)
- [Installation order](#)
- [Installing Policy Manager Server](#)
- [Changing the web browser path](#)
- [Uninstalling the product](#)

This section explains the steps required to install Policy Manager.

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

## Security issues

---

Policy Manager Server utilizes *Jetty Web Server* technology, and even though we do the utmost to deliver secure and up-to-date technology we advise you to regularly consult the following site for information on Jetty technology and security.

You will find a list of Jetty security reports at <http://docs.codehaus.org/display/JETTY/Jetty+Security>.

 **Note:** You will find important information about installation and security in the release notes. Read these notes carefully.

## Installing Policy Manager in high-security environments

---

Policy Manager is designed to be used in internal corporate networks mainly for managing F-Secure anti-virus products, and should not be used over public networks such as the Internet.

 **Note:** When installing Policy Manager in high-security environments, you should make sure that the *administration port* (by default port 8080) and the *host port* (by default port 80) are not visible on the Internet.

### Built-in security features

Access to Policy Manager is restricted to users who have an account. An unauthorized user can therefore not deploy any changes to managed hosts.

As an alternative to installing the components separately, Policy Manager Console and Policy Manager Server can be installed on the same machine, and access limited to the localhost. Remote administrator access to Policy Manager Console can be arranged by using a secure remote desktop product.

Communication between Policy Manager Server and Policy Manager Console is secured using the HTTPS protocol.

### Web Reporting in high-security environments

Web Reporting is designed to be used in internal corporate networks for generating graphical reports of, for example, Client Security virus protection status and alerts. F-Secure does not recommend using Web Reporting over public networks such as Internet.

An alternative for high-security environments is to limit access to Web Reporting to localhost only during the installation. After this, only the person who has physical access to the localhost can use Web Reporting.

## Installation order

---

You should install Policy Manager components in a specific order when installing them on separate machines.

To install Policy Manager, please follow this installation order (unless you are installing Policy Manager Server and Policy Manager Console on the same machine, in which case setup installs both of these components during the same installation process):

1. Policy Manager Server,
2. Policy Manager Console,
3. managed point applications.

## Installing Policy Manager Server

---

This section contains instructions for installing Policy Manager Server.

To install Policy Manager Server, you need physical access to the server machine.

Communication between Policy Manager Server and other components is secured through the HTTPS protocol.

The information stored by Policy Manager Server includes the following files:

- Policy domain structure.
- Policy data, which is the actual policy information attached to each policy domain or host.
- User account information.
- Base policy files generated from the policy data.
- Status information, including incremental policy files, alerts, and reports.
- Autoregistration requests sent by the hosts.
- Product installation and virus definition database update packages.
- Statistics and historical trend data about the hosts.

## 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](http://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. Enter and confirm a password for your admin user account, then click **Next**.

Use this password to log in to Policy Manager Console with the user name `admin`.

5. 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 include the new port number in the **Connections** URL when logging in to Policy Manager Console.

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

6. Click **Next** to continue.

## Complete the migration wizard

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

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

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

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

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

 **Note:** The `commdir` data and signing keys from a previous version of Policy Manager will not be removed after upgrading, and can be used if you need to roll back to the previous version.

 **Note:** Policy-based installation operations and the time period for considering hosts disconnected are not migrated when upgrading. You can set the time period in the **Tools > Server configuration** dialog box.

## 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.

## Check that the installation was successful

The next stage is to check that the product was installed correctly.

To determine if your installation was successful:

1. Open a web browser on the machine where Policy Manager Server was installed.
2. Enter `https://localhost:8080` as the address (if you used the default admin port number during the installation) and press Enter.  
If the server installation was successful, a welcome page will be displayed.

## 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.



## Using Policy Manager Console

---

### Topics:

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

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

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

## Overview

---

This section provides some general information about Policy Manager Console.

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

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

With Policy Manager Console, an administrator user can:

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

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

Read-only users can:

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

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

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

## Basic information and tasks

---

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

### Logging in

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

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

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

It is also possible to have multiple connections to a single server. After selecting the connection, enter your Policy Manager Console user name and password. The user name and password are specific for your Policy Manager user account, and are not linked to your network or network administrator password. The password for the `admin` user is defined when installing the program, and other users (either with admin or read-only access) are created through Policy Manager Console.

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

### Connection properties

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

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

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

### Adding new users

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

1. Select **Tools > Users** from the menu.  
The **Users** dialog box appears, with all current users listed.
2. Click **Add** to add a new user.
3. Enter a user name and password for the new user.
4. Select **Read-only access** if you want to limit the user's access, then click **OK**.  
The new user will appear on the users list, and will now be able to access Policy Manager.

 **Note:** Any user with full admin access will be able to delete any other user, but there must be at least one user with full admin access. If a user account is deleted while that user is logged in, they will be logged out and prompted to log in the next time a connection to Policy Manager is required.

### Changing your password

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

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

## Client Security management

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

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

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

### Advanced mode user interface

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

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

## Policy domain tree

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

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

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

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.

## Contents of the Advanced mode user interface

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

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

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

### Using help

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

### Editing policy settings

You can edit common policy settings in the main application area.

Select a product (e.g. Management Agent) on the **Policy** tab and expand the tree to view the available settings and operations for the product. When you click on a tree node, Policy Manager Console will display the field where you can change the selected setting.

You can edit the policy settings normally, and either allow or disallow user changes.

### Defining policy settings

Most policy setting pages use either a text field or drop-down field to define the setting.

In addition to the field for entering or selecting the value for the policy variable, most settings have three buttons available: **Clear**, **Force value** and **Show domain values**.

## Clear

The **Clear** button clears the current value, after which the field will either display the inherited value (grey text), or no value at all. **Clear** is available only if there is a value defined for the currently selected domain or host.

## Force value

**Force value** is available only when a policy domain is selected. You can enforce the current domain setting to also be active 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 cautiously: all values defined in the subdomain or hosts under the selected domain are discarded, and cannot be restored.

## Show domain values

**Show domain values** is available only when a policy domain is selected. You can 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. It is possible to open more than one **Domain value** dialog simultaneously.

## Viewing the status

You can view the settings and statistics of a policy domain in the main application area.

To view the status:

1. Open the **Status** tab.
2. Select the product.  
Policy Manager Console will render a product view for the selected product, where you can view the more important local settings and statistics.

 **Note:** Values cannot be edited, but the **MIB** help texts can be displayed by clicking a field or its label.

For the policy domains, the **Status** tab will show the domain level status overview: number of hosts in the domain, and list of disconnected hosts.

3. Click any disconnected host to quickly change the policy domain selection into that host.  
This way it is possible to investigate if the disconnected host managed to send some alerts or useful statistics before the disconnection. This information may help to investigate why the host was disconnected. If the reason is clear, for example, if the host's F-Secure software has been uninstalled, the host can be deleted normally.
4. After investigating one disconnected host, you can go back to the previously selected domain level by clicking the  button in the toolbar.

The **Domain status** view also offers two shortcut operations for handling a greater number of disconnected hosts: selecting all disconnected hosts and deleting all disconnected hosts. Both operations can be accessed through the **Disconnected host** tree root node context menu.

 **Caution:** Deleting all disconnected hosts is potentially a dangerous operation, as it is possible that some existing hosts are for some natural reason temporarily disconnected longer than the allotted threshold days. Always check the disconnection threshold value from **Tools > Server configuration > Hosts** before deleting hosts. If a still existing host is deleted accidentally, all host specific alerts, report, status and policy settings will be lost. However, the host will send an autoregistration message once it discovers that it has been removed from Policy Manager. The host can be re-imported to the domain tree, but from the Policy Manager point of view it's like any other newly added host.

## Messages pane

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

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

There are three categories of messages: **Information**, **Warnings**, and **Errors**. Each **Messages** view tab can contain messages of all three severities. You can delete a category in the displayed context menu by right-clicking on a tab. By right-clicking on an individual message, a context menu is displayed with **Cut**, **Copy**, and **Delete** operations.

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

## The toolbar

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

---

	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 <b>Properties</b> box of a host or domain.
	Launches the <b>Autodiscover Windows Hosts</b> tool. New hosts will be added to the currently selected policy domain.
	Starts push installation to Windows hosts.
	Imports new 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	Distribute policies	Distributes the policies.	
	Discard policy changes	Discards any undistributed changes to the policy that were made since the last time the policy was distributed.	
	Export host policy file	Exports the policy files.	
	Exit	Exits Policy Manager Console.	
	Cut	Cuts selected items.	
Edit	Paste	Pastes items to selected location.	
	Delete	Deletes selected items.	
	New policy domain	Adds a new domain.	
	New host	Adds a new host.	
	Import Active Directory structure	Starts the Active Directory import wizard.	
	Import new hosts	Imports new hosts that have sent a request to be added to the policy domain.	
	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 <b>Properties</b> page of the selected host or policy domain.	
	View	Messages pane	Shows/hides the <b>Message</b> pane at bottom of screen.
		Open on new message	If selected, the <b>Message</b> 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 <b>Alerts</b> page with all alerts showing.	
Advanced mode		Changes to the <b>Advanced mode</b> user interface.	
Anti-virus mode		Changes to the <b>Anti-virus mode</b> 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 information on installation packages in a dialog box.	

Menu	Command	Action
	Reporting	Lets you select the reporting methods and the domains/hosts and products included in the reports.
	Users	Opens the <b>Users</b> dialog box, where you can add or delete Policy Manager users.
	Change password	Opens the <b>Change password</b> dialog box, where you can change the password for your user account.
	Server configuration	Opens the <b>Server configuration</b> dialog box, where you can export/import signing keys and set the time limits for disconnecting hosts and removing disconnected hosts.
	Preferences	Sets the local properties for Policy Manager Console. These properties only affect the local installation of Policy Manager Console.
Help	Contents	Displays the <b>Help</b> 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.

## 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.

### Importing hosts from an Active Directory structure

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

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

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

### Adding hosts in Windows domains

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

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

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

### Importing new hosts

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

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

To import new hosts:

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

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

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

## Using import rules

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

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

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

- WINS name, DNS name, custom properties
  - These support \* (asterisk) as a wildcard. The \* character can replace any number of characters. For example: `host_test*` or `*.example.com`.
  - Matching is not case-sensitive, so upper-case and lower-case characters are treated as the same character.
- IP address
  - This supports exact IP address matching (for example: `192.1.2.3`) and IP sub-domain matching (for example: `10.15.0.0/16`).

1. You can hide and display columns in the table by using the right-click menu that opens when you right-click any column heading in the **Import rules** window.

Only the values in the currently visible columns are used as matching criteria when importing hosts to the policy domain. The values in the currently hidden columns are ignored.

2. You can add new custom properties to be used as criteria when importing hosts.

One example of how to use the custom properties is to create separate installation packages for different organizational units, which should be grouped under unit-specific policy domains. In this case you could use the unit name as the custom property, and then create import rules that use the unit names as the import criteria. Note that custom property names that are hidden are remembered only until Policy Manager Console is closed. To add a new custom property:

- a) Right-click a column heading and select **Add new custom property**.  
The **New custom property** dialog opens.
- b) Enter a name for the custom property, for example the unit name, then click **OK**.  
The new custom property now appears in the table, and you can create new import rules in which it is used as import criteria.

3. Create a new import rule:

- a) Click **Add** on the **Import rules** tab.  
The **Select target policy domain for rule** dialog opens displaying the existing domains and sub-domains.
- b) Select the domain for which you want to create the rule and click **OK**.

- c) Select the new row that was created and click the cell where you want to add a value.
- d) Enter the value in the cell.  
The import criteria is defined.
- e) Select **Apply rules automatically when new hosts connect to the server** if you want the rules to be applied automatically for any new connected hosts.  
This option is turned on for new installations of Policy Manager, and turned off for upgraded installations by default to emulate the behavior of the previous version.

- When new hosts are imported, the rules are verified in top-down order, and the first matching rule is applied. You can change the order of the rules by clicking **Move down** or **Move up**.
- If you want to create several rules for a domain, you can use the **Clone** option. Start by creating one rule for the domain. Then select the row and click **Clone**. Now you can edit the criteria on the new duplicated row.

4. When you want to start the import operation, select the **New hosts** tab and click **Import**.

The import rules you have defined will be validated before importing starts.

After the hosts have been imported, you will see a summary dialog displaying the number of successfully imported hosts and the number of unsuccessful import operations. Note that an empty set of conditions is always treated as matching.

## Creating hosts manually

This topic describes how to create hosts manually.

To create a host manually:

1. Select the target domain.
2. Select **Edit > New host** from the menu.

Alternatively:

- Click  in the toolbar.
- Press Insert.

This operation is useful in the following cases:

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

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

## Handling disconnected hosts automatically

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

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

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

## Host properties

This section provides an overview of the host properties that can be viewed and edited in Policy Manager Console.

To view host properties, right-click on the appropriate host and from the menu that opens, select **Properties** (alternatively press alt + enter).

Every host has a UID as its identity. This is a unique identifier that is retrieved directly from the host status and cannot be edited in Policy Manager Console.

The **Display as** field allows you to enter a name of your choice to identify the host. This will replace the real identity of the host when displayed in the domain tree.

## Software distribution

---

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

<b>Push installations</b>	Policy Manager can install software to new hosts that are not yet under centralized management. Hosts can be browsed from Windows domains using the <b>Autodiscover Windows hosts</b> feature, or the target host can be specified directly by WINS name or IP address using the <b>Push install to Windows host</b> feature. In addition to first time installations, push installation features can be used to update or repair installations whenever the policy-based installations are not suitable.
<b>Policy-based installations</b>	Policy Manager can initiate installation and update operations with policy based triggering. This requires that the hosts are already under centralized management, i.e. included in a policy domain in Policy Manager Console.
<b>Local installations and updates from CD-ROM</b>	Installation can be performed independently on the host by running the setup directly from the CD-ROM. After installation, Management Agent sends a registration message to Policy Manager. The administrator can then view and accept the new host by choosing the <b>Import new hosts</b> command from the <b>Edit</b> menu in Policy Manager Console.
<b>Local installation and updates with pre-configured packages</b>	Instead of using the standard CD-ROM setup, you can use Policy Manager to prepare a customized installation package (JAR or MSI) that includes information about the settings used for the installation. The end user's computer can be set up silently, since the pre-configured package contains all of the settings that are normally requested from the user.
<b>F-Secure virus definition database updates</b>	Policy Manager can update the latest anti-virus databases by downloading them automatically from the F-Secure Automatic Update site. Managed hosts will fetch the updates from Policy Manager according to the host policy, either automatically or with remotely triggered operations.

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

If access to the public key is required when distributing software to hosts, it can be downloaded from the Policy Manager Server welcome page.

## 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.  
You can import new installation packages on this page if necessary. The `Forced reinstallation` option is always turned on in all installation packages, so the application will be reinstalled if the host already has the same version number of the application installed.
2. Choose to accept the default policy, or specify which host or domain policy should be used as an anonymous policy, and click **Next** to continue.
3. Choose the user account and password for the push installation by selecting either **This account** (the current account) or **Another user**.

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

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

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

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

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

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

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

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

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

6. When the **Status** line displays finished, the process has finished and you can select in which domain the new hosts should be placed using the import settings.
7. Click **Finish**.  
Policy Manager Console will place the new hosts in the domain that you selected, unless you specified another domain in this dialog. You can also choose not to place the hosts to any domain automatically. The new hosts will send autoregs and the hosts can be imported that way.  
After a few minutes, the products that were installed will be listed.
8. To see this list, select the **Installation** tab (alternatively select the top domain on the **Policy domain** tree).

## Policy-based installation

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

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

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

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

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

### Using policy-based installation

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

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

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

To use policy-based installation:

1. Open the **Installation** tab.  
On the **Installation** tab, **Policy-based installations** table shows the status of any current installation operations, and the **Installed products summary** table lists the products that are currently installed on managed hosts.
2. Click **Install** under the **Policy-based installations** table to start the remote installation wizard.
3. Complete the remote installation wizard with the necessary details.  
The information entered in the remote installation wizard is used to prepare the customized package specific for this installation operation. The installation package will be then distributed to the selected domain or hosts once the policy is distributed.  
Once the remote installation wizard is complete, the installation operation and status will appear on the **Policy-based installations** table as a new row.
4. Distribute the policy.  
Once the installation operation is complete, the product name, version and number of hosts running the product are shown on the **Installed products summary** table.

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

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

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

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

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

## Local installation and updates with pre-configured packages

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

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

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

### Using the customized remote installation package

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

To use a customized installation package:

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

## 8. 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 properties in the installation package. A host will add these custom properties to the message it sends to the Policy Manager after local installation. These customer-specific properties will appear together with the standard host identification properties in the **New hosts** view. The custom property name will be the column name, and the value will be presented as a cell value.

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

## 10. When you reach the last wizard page, click **Finish** to continue.

## 11. You can also install an exported JAR to the hosts by running the `ilaunchr.exe` tool.

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

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

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

**ILAUNCHR** has the following command line parameters:

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

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

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

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

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

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

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

## Information delivery

All of the installation information is delivered as files through Policy Manager Server.

The installation packages are JAR archives that can be viewed (in WinZip, for example), but other files types (such as the policy files and INI files) are used for triggering the actual installation process.

Before Policy Manager Console can start any installation, the initial installation package must be transferred to Policy Manager Server. The installation packages are available from two sources:

- The installation CD-ROM, or
- The F-Secure website.

Normally new remote installation packages are installed from the CD-ROM, and Policy Manager setup moves the packages automatically to the server. If a remote installation package is obtained some other way, you can import the package by clicking **Import** in the **Installation packages** dialog box.

Policy Manager Console will verify that the new installation package is signed with the F-Secure private key before allowing the package to be used.

## Managing policies

---

This section describes how to configure and distribute policies.

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

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

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

## Settings

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

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

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

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

## Discarding undistributed changes to settings

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

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

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

## Restrictions

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

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

## Configuring settings

Settings are changed by modifying the policy variables.

To configure settings:

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

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

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

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

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

## Policy inheritance

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

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

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

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

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

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

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

## Index inheritance in tables

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

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

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

## Managing operations and tasks

---

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

To launch an operation from Policy Manager Console:

1. Select one of the actions from the **Operations** tab.  
You can also see available operations in the **Advanced mode** view, under the selected product's **Operations** branch on the **Policy** tab.
2. Click **Start** to start the selected operation.
3. The operation begins on the host as soon as you have distributed the new policy and the host has fetched the policy file.

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

## Alerts

---

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

### Viewing alerts and reports

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

To view the alerts:

1. Open the **Alerts** tab.  
All alerts received will be displayed in the following format:

<b>Ack</b>	Click the <b>Ack</b> button to acknowledge an alert. If all the alerts are acknowledged, the <b>Ack</b> button will be dimmed.		
<b>Severity</b>	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.
<b>Date/Time</b>	Date and time of the alert.		
<b>Description</b>	Description of the problem.		
<b>Host/User</b>	Name of the host/user.		
<b>Product</b>	The F-Secure product that sent the alert.		

---

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

- To view reports, click on the **Scanning reports** tab, or select **Product view > Messages** from the menu. The **Scanning reports** tab has the same structure as the **Alerts** tab. **Alerts** tables and **Scanning reports** tables can be sorted by clicking on the column heading.

## Configuring alert forwarding

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

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

To configure alert forwarding:

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

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

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

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

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

## Reporting tool

---

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

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

## Policy domain / host selector pane

In the **Policy domain / host selector** pane you can select the domains and/or hosts you are interested in from the reporting point of view.

The domain selected on policy domain tree of the main application area is selected by default in the **Reporting tool**.

By selecting the **Recursive** check box, all hosts that are recursively under the selected domains in the domain hierarchy are also included in the report.

## Report type selector pane

You can select the type of report you want to run in this pane.

In the **Report type selector** pane you can do the following:

- Select the type of report to be made.
- Select the filtering by product (only information on selected products is included in the report).

The following report types are currently available:

Report type	Description
<b>Policy</b>	Export/view reports containing values of all policy variables of the selected products from the selected domains. You can also select the <b>Inheritance</b> check box if you want inheritance information to be included in the report.
<b>Inheritance</b>	Export/view reports containing values of all policy variables of the selected products from the selected domains, that are not inherited from any upper level domain i.e. values of all policy variables that are overridden in the selected domains.
<b>Status</b>	Export/view reports containing the values of all local settings and status variables of the selected products from the selected domains.
<b>Properties</b>	Export/view reports containing values of all domain-component property fields. You can also use the <b>Property selector</b> check boxes to select which property fields are to be included in the report.
<b>Alert</b>	Export/view reports containing information of all alerts at the selected domains. You can also use the <b>Sort order selector</b> to define the sort order among alert description fields. You can use the <b>Severity selector</b> to select the alert severities to be included in the report.
<b>Configuration</b>	Export/view reports containing information of installed products of the selected products from the selected domains.
<b>Anti-Virus</b>	Export/view reports containing values of domain status of product versions and virus definition database updates.

## Report pane

After selecting a report type, you can select type-dependent configurations in this pane.

In the **Report** pane, you can:

- Select report type-dependent configurations for the currently selected report type. With the report type dependent configurations, the user can adjust more filtering to the report to be made.
- Find a description for the currently selected **Report type**.

Configurations to currently known report types are:

- **Policy report type dependent configurations** allows you to select the inheritance information of policy values to be included in the report.
- **Properties report type dependent configurations** allows you to select the information to be included in the report based on identities, platform, miscellaneous and polling properties.
- **Alert report type dependent configurations** allows you to sort alerts by the alert description fields and select the severities of alerts to be included in the report.

## Bottom pane

After a report is configured, you can select an action to take in the bottom pane of the **Reporting tool**.

In the bottom pane, you can:

- Reset the defaults to all user interface components.
- Launch the report exporting process.
- Launch the report viewing process.
- Stop the report generating process.
- Close the **Reporting tool** user interface. This does not stop generation of the report to be exported; it is run in the background. The report being generated for viewing can be stopped from the dialog that appears.

## Viewing and exporting a report

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

To use the **Reporting tool**:

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

Alternatively:

- Launch the **Reporting tool** from the context menu in the main application area.

The **Reporting tool** opens.

2. Select the domains and/or hosts you want to include in the report.

- Select **Recursive** if you want all hosts under the selected domains to be included in the report.

3. Select the report type.

4. Select the products to include in the report, if necessary.

5. Select report type-dependent configurations for the currently selected report, if necessary.

6. View or export the report:

- Click **View** in the bottom pane to generate the report and view it in HTML format with your default web browser. If no default web browser has been defined, a dialog box appears prompting you to define your web browser.
- Click **Export** in the bottom pane to generate the report and save it as a file. The file path and report format are defined in the **File save** dialog box that appears after clicking **Export**.

## Preferences

Preference settings are either shared or applied to the specific connection.

### Connection-specific preferences

To edit these, select **Preferences** from the **Tools** menu; only the current connection object is affected.

Tab	Setting	Meaning
<b>Alerts and reports</b>		These options control: <ul style="list-style-type: none"> <li>the time period from which to show alerts,</li> <li>the time period from which to show reports.</li> </ul>
<b>Push installation</b>	<b>Installation timeout</b>	The maximum time Policy Manager Console waits for the results of an installation operation.
	<b>Browsing timeout</b>	Important only if the <b>Hide already managed hosts</b> option is in use. This is the maximum time allowed to access the host registry.
	<b>Maximum concurrent network operations</b>	You can adjust the number of network operations. The default is recommended, but if you have a slow network connection that is causing problems when you are push installing, decrease the number of concurrent network connections accordingly.
	<b>Progress indicator</b>	You can choose to display the progress indicator to end users during remote installation.

### Shared preferences

These apply to all connections defined in a particular installation of Policy Manager Console.

Tab	Setting	Meaning
<b>Appearance &gt; General options</b>	<b>Language</b>	Language selection. You can select the local language of your operating system or the default English setting. All objects that do not support the system's local language will be displayed in English. You must restart Policy Manager Console for the change to take effect.
	<b>Font</b>	Font used throughout Policy Manager Console. The font change will take place after restarting the program.
	<b>Look &amp; feel</b>	Defines the appearance and behavior of the user interface components. The change will take place after restarting the program.
<b>Push installation</b>	<b>Clear cache</b>	You may clear all cached information concerning browsed hosts and installed software to free up disk space.
<b>Location</b>	<b>HTML browser path</b>	The full path to the HTML browser's executable file. The browser is utilized for displaying online help pages and anti-virus reports.

Tab	Setting	Meaning
	<a href="#">Message logs path</a>	You can select this to enter the path to a directory where log files for each tab on the <a href="#">Message</a> view are created. Each log file contains the title of the corresponding tab and a message per line including severity and creation time.
<a href="#">Anti-Virus</a>	<a href="#">Virus definitions</a>	With this value you can define the time after which virus definitions are shown as outdated in <a href="#">Anti-virus</a> mode.



## Maintaining Policy Manager Server

---

### Topics:

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

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

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

## Backing up & restoring Policy Manager data

---

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

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

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

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

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

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

## Creating the backup

---

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

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

## Restoring the backup

---

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

To restore backed up Policy Manager data:

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

## Exporting and importing signing keys

---

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

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

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

To export your current signing keys:

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

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

  - a) Click **Replace**.
  - b) Browse to the location of the keys you want to import, then click **OK**.
  - c) Enter the passphrase for the imported signing keys, then click **OK**.

A notification will appear to confirm that the signing keys were successfully exported or replaced.
3. Click **OK** to close the **Server configuration** dialog box.

## Replicating software using image files

---

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

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

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

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

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

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

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

4. Shut down the computer.

 **Note:** Do not restart the computer at this stage.

5. Create the disk image file.

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



## Updating virus definition databases

---

### Topics:

- *Automatic updates with Automatic Update Agent*
- *Using Automatic Update Agent*
- *Forcing Automatic Update Agent to check for new updates immediately*
- *Updating the databases manually*
- *Troubleshooting*

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

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

## Automatic updates with Automatic Update Agent

---

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

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

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

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

### How Automatic Update Agent works

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

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

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

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

### The benefits of using Automatic Update Agent

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

#### Optimized downloads of virus definition updates

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

### Resumable data transfers

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

### Automated updates

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

## Using Automatic Update Agent

---

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

### Configuring Automatic Update Agent

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

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

To configure Automatic Update Agent:

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

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

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

Examples:

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

3. Specify the polling interval:

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

```
poll_interval=1800
```

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

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

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

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

## How to read the log file

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

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

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

Every message in the log contains the following information:

- The date and time the message was generated.

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

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

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

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

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

### Messages in `fsaua.log`

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

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

### How to check from the log that everything works?

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

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

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

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

## Forcing Automatic Update Agent to check for new updates immediately

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

To do this:

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

## Updating the databases manually

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

1. Connect to `http://support.f-secure.com/` from another computer.
2. Download the `fsdbupdate.exe` tool.
3. Transfer the `fsdbupdate.exe` tool to your computer, for example, by using a memory stick or other removable media and run it.

## Troubleshooting

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

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

<b>Problem</b>	<b>Reason</b>	<b>Solution</b>
There was a server error or an unspecified error.	Unknown	-

## Using the product on Linux

---

### Topics:

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

Policy Manager can also be installed on Linux.

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

## Overview

---

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

### Differences between Windows and Linux

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

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

### Supported distributions

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

Supported distribution	Packaging system
Red Hat Enterprise Linux 4, 5 and 6	RPM
CentOS 5	RPM
SUSE Linux Enterprise Server 10 and 11	RPM
SUSE Linux Enterprise Desktop 11	RPM
openSUSE 11	RPM
Debian GNU Linux 5	DEB
Ubuntu 8.04, 10.04	DEB

## Installation

---

Policy Manager is installed in three parts.

The product components must be installed in the following order:

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

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

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

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

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

### Installation notes

Red Hat and Suse distributions:

- Some platforms require the `libstdc++` compatibility library. Install the following packages before installing Policy Manager Server:
  - For Red Hat Enterprise Linux 4, 5 and 6, install the `compat-libstdc++-33` package.
  - For 32-bit openSuse 11, install the `libstdc++33` package.
  - For 64-bit openSuse 11, install the `libstdc++33` and `libstdc++33-32bit` packages.
- When installing Policy Manager Server and Policy Manager Console on a 64-bit platform, you need to use the 64-bit version of the installation packages.

Debian and Ubuntu distributions:

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

## Install Automatic Update Agent and Policy Manager Server

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

1. Log in as `root`.

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

2. Open a terminal.

3. To install, enter the following commands:

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

Distribution type	Command
	<pre>sudo dpkg -i f-secure-policy-manager-server_&lt;version_number&gt;.&lt;build number&gt;_i386.deb</pre>

- To configure, type `/opt/f-secure/fspms/bin/fspms-config` and answer the questions. For Ubuntu distributions, type `sudo /opt/f-secure/fspms/bin/fspms-config`. Press Enter to choose the default setting (shown in square brackets).
- Log in as a normal user and enter the following commands to check the status of the components:
  - `/etc/init.d/fsaua status`
  - `/etc/init.d/fspms status`

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

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

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

## Install Policy Manager Console

Next, you need to install Policy Manager Console.

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

- Open a terminal.

- To install type:

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

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

- Add users to the `fspmc` user group.  
This needs to be done before they can run Policy Manager Console:
  - Check which groups the user belongs to:

```
groups <user id>
```

For example, if the user is Tom:

```
groups Tom
```

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

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

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

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

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

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

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

 **Note:** On Red Hat Enterprise Linux 4, you need to log out and then log in again before using the **Programs** menu item. Also, since the `sg` command does not accept the `<command>` argument, you can use `newgrp` on the command line:

- `newgrp fspmc`
- `/opt/f-secure/fspmc/fspmc`

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

## Uninstalling the product

---

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

You must uninstall the three components in this order:

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

1. Log in as `root`.

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

2. Open a terminal.

3. Enter the following commands in the given order:

Distribution type	Command
<b>Debian-based distributions</b>	
	1. <code>dpkg -r f-secure-policy-manager-server</code>
	2. <code>dpkg -r f-secure-automatic-update-agent</code>
	3. <code>dpkg -r f-secure-policy-manager-console</code>
<b>RPM-based distributions</b>	
	1. <code>rpm -e f-secure-policy-manager-server</code>
	2. <code>rpm -e f-secure-automatic-update-agent</code>
	3. <code>rpm -e f-secure-policy-manager-console</code>
<b>Ubuntu distributions</b>	
	1. <code>sudo dpkg -r f-secure-policy-manager-server</code>
	2. <code>sudo dpkg -r f-secure-automatic-update-agent</code>

**Distribution type****Command**

3. `sudo dpkg -r f-secure-policy-manager-console`

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

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

## Frequently asked questions

---

You can find answers to common problems here.

Question	Answer
Where are the log files and configuration files located in the Linux version?	<p>You can list all files and their places by entering the following commands as a normal user:</p> <ul style="list-style-type: none"> <li>• RPM-based distributions: <code>rpm -ql f-secure-&lt;component_name&gt;</code>.</li> <li>• Debian-based distributions: <code>dpkg -L f-secure-&lt;component_name&gt;</code>.</li> </ul> <p>You will find the log files in the following locations:</p> <ul style="list-style-type: none"> <li>• Policy Manager Console: <code>/opt/f-secure/fspmc/lib/Administrator.error.log</code>.</li> <li>• Automatic Update Agent logs runtime errors, warnings and other information via <code>syslog</code>, which is typically in <code>/var/log/messages</code></li> <li>• Policy Manager Server: <code>/var/opt/f-secure/fspms/logs</code> and <code>/var/opt/f-secure/fsaus/log</code>.</li> </ul> <p>You will find the configuration files in the following locations:</p> <ul style="list-style-type: none"> <li>• Policy Manager Console: <code>/opt/f-secure/fspmc/lib/Administrator.properties</code>.</li> <li>• Automatic Update Agent: <code>/etc/opt/f-secure/fsaua/fsaua_config</code></li> <li>• Policy Manager Server: <code>/etc/opt/f-secure/fspms/fspms.conf</code>.</li> </ul>

Question	Answer
Why are the files located so unusually?	All files for Policy Manager have their own location according to the File Hierarchy Standard. For more information on FHS, go to <a href="http://www.pathname.com/fhs/">http://www.pathname.com/fhs/</a> .
Why doesn't Policy Manager Server start?	Make sure you have run the configuration script: <code>/opt/f-secure/fspms/bin/fspms-config</code> .  You can also check that the ports configured for Policy Manager Server are active by logging in as <code>root</code> and running the <code>netstat -lnpt</code> command.
How can I start, stop, restart or check the status of Policy Manager components?	Automatic Update Agent: <code>/etc/init.d/fsaua {start stop restart status}</code>  Policy Manager Server: <code>/etc/init.d/fspms {start stop restart status}</code>
How can I specify an HTTP proxy?	You can run the configuration script <code>/opt/f-secure/fsaua/bin/fsaua-config</code> or edit the configuration file manually. The directive is <code>http_proxies=http://address:port/</code> .  Remember to restart Automatic Update Agent in order to take the new settings into use.
How can I change the default ports (80 and 8080) in which Policy Manager Server listens for requests?	These ports are configured with the configuration script: <code>/opt/f-secure/fspms/bin/fspms-config</code> .
How can I change the default port (8081) in which Web Reporting listens for requests?	The Web Reporting port is configured with the Policy Manager Server configuration script: <code>/opt/f-secure/fspms/bin/fspms-config</code> .
Can I set up my own schedule for updating F-Secure virus definitions?	Yes. Automatic updates are achieved by using the operating system's own scheduling daemon, <code>cron</code> . Just edit or add your own scheduling entry to the <code>/etc/crontab</code> file.  For example, to schedule virus definitions updates for every 10 minutes, add this line to <code>/etc/crontab</code> :  <code>*/10 * * * * fspms /opt/f-secure/fspms/bin/fsavupd</code>  For more on configuring automatic updates using <code>cron</code> , see <code>man cron</code> and <code>man 5 crontab</code> . In most of the cases you can configure the scheduled updating of F-Secure virus definitions with the <code>/opt/f-secure/fspms/bin/fspms-config</code> command.
How can I update F-Secure virus definitions manually?	Log in as an <code>fspms</code> user and run the updating tool by typing:

Question	Answer
	<pre>sudo -u fspms /opt/f-secure/fspms/bin/fsavupd --debug</pre> <p>The optional <code>--debug</code> flag forces more verbose diagnostic messages.</p>
<p>How can I publish F-Secure virus definitions manually from the latest <code>fsdbupdate</code> package?</p>	<p>Download the latest <code>fsdbupdate.run</code> tool from <a href="http://download.f-secure.com/latest/fsdbupdate.run">http://download.f-secure.com/latest/fsdbupdate.run</a>. Log in as <code>root</code> and run this tool:</p> <pre>./fsdbupdate.run</pre> <p>This will update all databases in Automatic Update Agent. After this, you need to publish these updates to the Update Server and Policy Manager Server by either having <code>fsavupd</code> scheduled in <code>crontab</code> or by manually running the <code>fsavupd</code> command:</p> <pre>sudo -u fspms /opt/f-secure/fspms/bin/fsavupd</pre>
<p>Is there any diagnostic tool I can use?</p>	<p>Yes. Please use <code>fsdiag</code> to collect information about your system and related packages. When logged in as <code>root</code>, run:</p> <pre>/opt/f-secure/fspms/bin/fsdiag</pre> <p>All relevant information will be stored into the <code>fsdiag.tar.gz</code> archive located in the current directory. You can then send that file to F-Secure Customer Support by request.</p>
<p>I get the warning <code>...Another Automatic Update Server was found... during startup</code>. What should I do?</p>	<ol style="list-style-type: none"> <li>1. Check if another Automatic Update Server is running and still using the TCP sockets: <pre>netstat -anp   grep bwserver ps axuw   grep bwserver</pre> </li> <li>2. Stop the other Automatic Update Server by running: <pre>kill `pidof bwserver` kill -9 `pidof bwserver`</pre> </li> <li>3. Restart Policy Manager Server: <pre>/etc/init.d/fspms stop rm -f /var/lock/subsys/fsaus /var/run/fsaus.pid /etc/init.d/fspms start</pre> </li> </ol>
<p>How can I install software to remote hosts from Policy Manager Console on Linux?</p>	<p>You can export installation packages to JAR files and use the <code>ilaunchr.exe</code> tool to install software on hosts, for example by using logon scripts. Please follow the process defined in the manual. You will find the <code>ilaunchr.exe</code> tool in the <code>/opt/f-secure/fspmc/bin</code> directory.</p>

Question	Answer
How can I configure Policy Manager for use in large environments?	<ul style="list-style-type: none"><li data-bbox="852 220 1453 346">• Increase the Incoming packages polling interval and Outgoing packages update interval values to 30 - 60 minutes in Policy Manager Console.</li><li data-bbox="852 357 1453 451">• Use Policy Manager Proxy installation(s) to minimize the load on Policy Manager Server caused by serving database updates to clients.</li></ul>

---



## Web Reporting

---

### Topics:

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

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

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

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

## Generating and viewing reports

---

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

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

### Generating a report

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

You can generate a web report as follows:

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

### Creating a printable report

You can also print a generated report.

To get a printable version of the page:

1. Click the **Printable version** link in the upper right corner of the page.  
This opens a new browser window with the contents of the main frame in printable format.
2. Print the page with your browser's normal print functionality.

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

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

## Automated report generation

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

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

You have two possibilities:

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

## Maintaining Web Reporting

---

This section covers the most common Web Reporting maintenance tasks.

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

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

## Web Reporting error messages and troubleshooting

---

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

### Error messages

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

- Browser error message: **The connection was refused when attempting to contact <location>**  
Your browser could not contact Policy Manager Server at all. The link you have might point to the wrong machine or to the wrong port, Policy Manager Server is not installed on that machine, or the Policy Manager Server service is not running. Check all of these in this order. A firewall may also prevent the connection.
- Error message: **Web Reporting lost its database connection, this may require restarting the Policy Manager Server service.**

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

### Troubleshooting

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

Try these steps in the following order:

1. Reload the page.

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

## Changing the Web Reporting port

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

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

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

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

## Policy Manager Proxy

---

### Topics:

- [Overview](#)

This section provides a brief introduction to Policy Manager Proxy.

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

## Overview

---

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

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

## Troubleshooting

---

### Topics:

- [Policy Manager Server and Policy Manager Console](#)
- [Policy Manager Web Reporting](#)
- [Policy distribution](#)

This section contains troubleshooting information and frequently asked questions about Policy Manager.

If you encounter problems when using the product, you can find possible solutions in this section.

## Policy Manager Server and Policy Manager Console

Issues regarding Policy Manager Server and Policy Manager Console are described here.

Question	Answer
Why doesn't Policy Manager Server start?	<p>Runtime errors, warnings and other information can be found in the files:</p> <pre>&lt;F-Secure&gt;\Management Server 5\logs\fspms-webapp-errors.log and &lt;F-Secure&gt;\Management Server 5\logs\fspms-sersvice.log</pre> <p>Check that the access rights (properties/security/permissions) includes the Local Service user account. If Local Service is not listed as an authorized user, add the user manually, and set the access rights to <b>Full Control</b>. Propagate the access rights to the Management Server 5 directory (by default C:\Program Files\F-Secure\Management Server 5) and all its subdirectories. After these changes, restart the Policy Manager Server service or reboot the computer.</p> <p>The Local Service account is the Windows system account, and the Policy Manager Server service is started under this user account. With normal installation, the directory access rights for the Management Server 5 directory are automatically set correctly. If the directory is copied by hand or, for example, restored from backup, the access rights might be deleted. In this case execute the steps described in the previous paragraph.</p>
Where are the log files and configuration files located for Policy Manager Server?	<p>The log files are located in:</p> <pre>&lt;F-Secure&gt;\Management Server 5\logs</pre> <p>The configuration files are in:</p> <pre>&lt;F-Secure&gt;\Management Server 5\conf</pre>
Where are the Policy Manager Console log files located?	<p>The log file is:</p> <pre>&lt;F-Secure&gt;\Administrator\lib\administrator.error.log</pre> <p>Policy changes applied with the <b>Distribute policy</b> operation are logged to:</p> <pre>fspms-policy-audit.log</pre>
The migration wizard didn't start up during installation. Can I run it separately outside installation?	<p>You can start the migration wizard by running this executable:</p> <pre>&lt;F-Secure&gt;\Management Server 5\bin\fspms-migration-wizard.exe</pre>

Question	Answer
I have lost the admin password. Can I retrieve or reset the password?	<p>If you have lost the password for the <code>admin</code> user, or if the account was accidentally deleted, you can reset the user account with the following tool:</p> <pre data-bbox="852 331 1458 359">&lt;F-Secure&gt;\bin\reset-admin-account.bat</pre> <p> <b>Note:</b> You need to stop Policy Manager Server manually before running the reset tool.</p>
How can the server role change stop Policy Manager Server from working?	<p>The Domain Controller server and Member/Standalone server use different types of accounts: domain accounts on Domain Controller and local accounts on Member server. Because Policy Manager Server uses its own account to run, this account becomes invalid with the role change.</p> <p>The easiest way to restore Policy Manager Server after a server role change is to re-install Policy Manager Server with the <b>Keep existing settings</b> option selected. This will recreate the Policy Manager Server account and reset all file access rights to the correct ones.</p>
How can Windows security hardening stop Policy Manager Server from working?	<p>Access rights restrictions, especially restrictions under the <code>%SystemRoot%</code> directory (<code>c:\windows</code> or <code>c:\winnt</code>) can stop Policy Manager Server from starting, as its own account (Local Service) needs to be able to read the network related DLL and SYS files.</p> <p>You must allow the Local Service account to 'read' the following directories:</p> <pre data-bbox="852 1184 1315 1308">%SystemRoot% %SystemRoot%\system32 %SystemRoot%\system32\drivers</pre> <p>Some service restrictions can also prevent the Policy Manager Server service from starting. For more information on these please consult the Microsoft Windows Server documentation.</p>
Why does Policy Manager Console lose the connection to Policy Manager Server?	<p>If Policy Manager Console is run on a separate computer from Policy Manager Server, then the connection may be affected by network problems. There have been numerous reports where, for example, a network switch change caused loss-of-connection problems between Policy Manager Console and Policy Manager Server. Usually these problems are fixed by updating the network drivers to the latest version in the affected machines or by reconfiguring the new switch and the network cards on the Policy Manager Console and Policy Manager Server machines.</p>

Question	Answer
	<p>If Policy Manager Console is installed on the same computer as Policy Manager Server, then there is a risk that Policy Manager Server could be under such a heavy network load that it does not have any free network connections available. Policy Manager Console and all hosts are competing for the same network resources.</p> <p>Possible solutions are to increase the polling intervals of hosts, to change the Windows networking timeouts shorter, or to increase the number of Windows networking ports.</p> <p>Useful Windows networking settings are:</p> <p>HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\MaxUserPort (maximum number of network ports, default = 5000)</p> <p>HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpTimedWaitDelay (time to wait before closing inactive network connection, default = 240 seconds).</p> <p>The <code>netstat -an</code> command can be used to check whether there are too many connection open to the server.</p>
<p>How can I change the ports where the server listens for requests?</p>	<p>By default, the Policy Manager Server admin module (the component that handles requests coming from Policy Manager Console) listens in port 8080, and the Policy Manager Server host module (the component that handles requests from workstations) listens in port 80. These can be changed during installation.</p> <p>If you need to change the port numbers after installation:</p> <ol style="list-style-type: none"> <li>1. Stop Policy Manager Server.</li> <li>2. Open the <code>HKEY_LOCAL_MACHINE\SOFTWARE\Data Fellows\F-Secure\Management Server 5</code> registry key.</li> <li>3. Edit the <code>AdminPortNum</code> (admin module) and <code>HttpPortNum</code> (host module) values and enter the new port numbers. <p>Make sure <b>Decimal</b> is selected as the <b>Base</b> option when entering the new port number.</p> </li> <li>4. Start Policy Manager Server.</li> </ol> <p> <b>Caution:</b> If you have workstations already configured to access Policy Manager Server (through the Policy Manager Server host module) you should not change the Policy Manager Server host port where agents communicate, since you might reach a state where the</p>

Question	Answer
	workstations will not be able to contact the server.

## Policy Manager Web Reporting

The locations of log and configuration files are given here.

Question	Answer
Where are the log files and configuration files located for Web Reporting?	<p>The log files are located in:</p> <pre>&lt;F-Secure&gt;\Management Server 5\Web Reporting\logs</pre> <p>The configuration files are in:</p> <p>The HKEY_LOCAL_MACHINE\SOFTWARE\Data Fellows\F-Secure\Management Server 5 registry key</p> <p>See also the Policy Manager Server configuration files:</p> <pre>&lt;F-Secure&gt;\Management Server 5\conf</pre>

## Policy distribution

You will find information on common error messages relating to policy distribution here.

Question	Answer
When distributing a policy, Policy Manager Console shows an error message about an invalid policy value. What should I do?	See below for information on error messages you may see during policy distribution, and for the reasons and solutions.

Error message	Reason	Solution
"<setting name>" has value out of restriction	Reason 1: The value selected from a choice list is not among the choices on a sub-domain or host, too high or low values are specified as range restriction boundaries, or an empty choice list is specified.	Divide the hosts into subdomains so that it is possible to set the new value for hosts with the new software installed, and to use some older policy values for other hosts. To do this:
"<setting name>" has invalid restriction		
"<setting name>" has invalid value: "<value>"	When a domain includes hosts that have different product versions installed, the MIB settings from the newest product version are used for editing the policy values. As result, policy distribution may fail on hosts that have older versions of the	<ol style="list-style-type: none"> <li>Group the hosts into subdomains based on the installed product version. For example, group hosts that have Client Security 6.x installed into one sub-domain, and hosts that have Client Security 7.x installed into another domain.</li> </ol>

Error message	Reason	Solution
	software installed, because the older versions do not support the new policy settings or values.	<b>2.</b> Set most of the settings on the root domain and create a sub-domains for exceptions. This is a good solution if you have only a few hosts with the older software versions installed.
	Reason 2: You entered an integer value that is outside of the range restrictions.	
"<setting name>" is required but undefined	The setting is required but it is currently empty.	Enter a value or apply the <b>Clear</b> operation to re-inherit the value from parent domain or MIB. If the value is empty on several domain levels, you may need to apply the <b>Clear</b> operation several times.

---

## llaunchr error codes

---

### Topics:

- [Error codes](#)

If you encounter errors in the **llaunchr** component, you can find the cause of the error by checking the error codes listed in this section.

This section provides information on error codes related to the **llaunchr** component.

## Error codes

When `Ilaunchr.exe` is completed silently, it reports installation results with the standard exit codes.

With the login script, you can test for the cause of the problem. Here is one example, which you can insert into your login script:

```
Start /Wait ILaunchr.exe \\server\share\mysuite.jar /U
if errorlevel 100 Go to Some_Setup_Error_occurred
if errorlevel 5 Go to Some_Ilaunchr_Error_occurred
if errorlevel 3 Go to Problem_with_JAR_package
if errorlevel 2 Go to User_does_not_have_admin_rights
if errorlevel 1 Go to FSMA_was_already_installed
if errorlevel 0 Echo Installation was OK!
```

Error codes:

Error code	Description
0	Installation OK.
1	FSMA already installed.
2	User has no administrative rights.
3	JAR not found.
4	JAR corrupted.
6	Error occurred when unpacking an installation package.
7	Target disk has insufficient free space for installation.
8	File <code>package.ini</code> was not found in JAR file.
9	File <code>package.ini</code> did not contain any work instructions.
10	Wrong parameters in command line or <code>.ini</code> file.
11	Error in initializing a new working process.
12	Error in creating the install process for setup.
13	Could not create a <code>temp</code> directory.
14	Undefined error.
100	Data needed for silent installation is missing. Invalid JAR file.
101	Update is disabled. (Setup attempted to update the installation.)
102	Setup was unable to read the <code>product.ini</code> file.
103	Invalid data is encountered in <code>prodsett.ini</code> .
104	Management Agent canceled the installation or conflicting software was found. Installation aborted.
105	The subscription key was entered incorrectly or is missing. Installation aborted.
110	Out of disk space.
111	The destination drive is not local.
120	The user has no administrative rights to the machine.

Error code	Description
130	Setup was unable to copy non-packed files to the target directory.
131	Setup was unable to copy uninstallation plug-in to the product target directory.
132	Setup was unable to copy <code>product.ini</code> file to the <code>temp</code> directory.
133	Error occurred while copying product file to the destination directory.
134	Unable to copy <code>prodsett.ini</code> .
140	Newer version of suite was detected.
150	Setup was unable to load product plug-in dll.
151	Setup was unable to load installation support dll.
152	Setup was unable to load wrapper dll.
160	Setup was unable to initialize a cabinet file.
170	Management Agent Setup plug-in returned error.
171	Plug-in returned an unexpected code.
172	Plug-in returned a wrapper code.
173	One of the previous install/uninstall operations was not completed. Reboot is required to complete it.
174	The target machine was rebooted to complete one of the previous install/uninstall operations. Please push installation again.
200	Partial Success. Installation of some products failed.

---



## FSII remote installation error codes

---

### Topics:

- [Error codes](#)

If you encounter problems in remote installation operations, you can find the cause by checking the information given here.

This section describes the most common error codes and messages that can occur during the [Autodiscover Windows Hosts](#) operation.

## Error codes

Here you will find descriptions for the most common error codes and messages appearing in remote installation operations.

### Windows error codes

Error code	Description
1057	The user account name is invalid or does not exist.
5	Access denied. If using <b>This Account</b> , it is important that the administrator is logged on to the Policy Manager Console machine with domain administrator privileges. With <b>Domain Trusts</b> , make sure you have logged on to Policy Manager Console using the account from the trusted domain.
1069	Logon failure. In most cases, the entered password is wrong.
1722	RPC server is unavailable. This error message might appear if the host was restarted immediately after installation and Policy Manager Console did not have time to verify that the installation was successfully completed.
1219	Policy Manager Console has open network connections to the target workstation. Close the connections before trying to open connections with another user account.

### Error messages

Error message	Description
<b>The required privilege is not granted for the current account and should be added manually.</b>	By default even the administrator does not have a required <b>Act as part of operating system</b> privilege on the Policy Manager Console machine. Without this privilege, Windows NT does not allow FSII to authenticate the entered user accounts. To add this privilege to administrator's account on Policy Manager Console, use <b>Windows NT User Manager &gt; Policies &gt; User Rights</b> .
<b>Management Agent canceled the installation or some conflicting software was found. Installation aborted.</b>	The Management Agent portion of setup cancels the whole installation in the following situations: <ul style="list-style-type: none"> <li>• When it detects conflicting third party software.</li> <li>• There are various other possibly reasons including: the wrong URL to Policy Manager Server.</li> </ul>
<b>The CD-KEY was entered incorrectly or is missing. Installation aborted.</b>	The installation on the remote host cannot start because the subscription key was entered improperly. Check the syntax.
<b>Out of disk space in target host</b>	The destination host does not have enough disk space. Usually at least 20 MB is required.

Error message	Description
<b>Management Agent installation failed to fatal FSMAINST error, see host log files for details.</b>	Fatal installation error occurred during Management Agent installation. It is recommended that Management Agent be installed manually to the host. It is also possible to try to find out the <code>ERROR</code> keyword from the <code>fswssdbg.log</code> file located in the target Windows directory.
<b>Newer F-Secure product detected, installation aborted</b>	If the target host has a newer product version already installed, the installation cannot be completed without first uninstalling it.
<b>Invalid data is encountered in prodsett.ini.</b>	The <code>prodsett.ini</code> configuration file has invalid information. If you have edited it manually, make sure the syntax is correct. It is recommended to export JAR files and use <b>ILAUNCHR</b> to install instead of directly editing <code>prodsett.ini</code> .

---



## NSC notation for netmasks

---

### Topics:

- [NSC notation details](#)

This section provides details on the NSC notation standard.

You will find information on combining a network address with its associated netmask in this section.

## NSC notation details

NSC notation is a standard shorthand notation, which combines a network address with its associated netmask.

NSC notation defines the number of contiguous one-bits in the netmask with a slash and a number following the network address. Here is a simple example:

Network address	Netmask	NSC notation
192.168.0.0	255.255.0.0	192.168.0.0/16
192.168.1.0	255.255.255.0	192.168.1.0/24
192.168.1.255	255.255.255.255	192.168.1.255/32

NSC notation is not compatible with networks that use "comb" style netmasks, where all one-bits are not contiguous. The following table gives the number of bits for each permitted netmask.

The .0.0.0/0 is a special network definition reserved for the default route.

Netmask	Bits
128.0.0.0	1
192.0.0.0	2
224.0.0.0	3
240.0.0.0	4
248.0.0.0	5
252.0.0.0	6
254.0.0.0	7
255.0.0.0	8
255.128.0.0	9
255.192.0.0	10
255.224.0.0	11
255.240.0.0	12
255.248.0.0	13
255.252.0.0	14
255.254.0.0	15
255.255.0.0	16
255.255.128.0	17
255.255.192.0	18
255.255.224.0	19
255.255.240.0	20
255.255.248.0	21
255.255.252.0	22
255.255.254.0	23
255.255.255.0	24
255.255.255.128	25
255.255.255.192	26
255.255.255.224	27

<b>Netmask</b>	<b>Bits</b>
255.255.255.240	28
255.255.255.248	29
255.255.255.252	30
255.255.255.254	31
255.255.255.255	32

---

