F-Secure Policy Manager

Administrator's Guide

Contents

Chapter 1: Introduction.....7

1.1 Main components.....8
1.2 Features.....8
1.3 What's new.....9
1.4 Product registration.....9
1.4.1 Upstream reporting.....10
1.5 Basic terminology.....10
1.6 Policy-based management.....10
1.6.1 Management Information Base.....11

Chapter 2: Installing the product.....12

2.1 System requirements.....13
2.1.1 Policy Manager Server.....13
2.1.2 Policy Manager Console.....14
2.2 Installing the product on Windows.....15
2.2.1 Installation steps.....15
2.2.2 Changing the web browser path.....17
2.2.3 Uninstalling the product.....17
2.3 Installing the product on Linux.....17
2.3.1 Installation steps.....17
2.3.2 Upgrading the product.....19
2.3.3 Uninstalling the product.....19

Chapter 3: Using Policy Manager Console.....21

3.1 Overview.....22
3.2 Basic information and tasks.....22
3.2.1 Logging in.....22
3.2.2 Dashboard.....23
3.2.3 Adding new users.....23
3.2.4 Switching between standard and advanced views.....24
3.2.5 Policy domain tree.....25
3.2.6 Messages pane.....25
3.2.7 Product upgrade notifications.....25
3.3 Managing domains and hosts.....26
3.3.1 Adding policy domains.....26
3.3.2 Adding hosts.....26
3.4 Managing policies.....31
3.4.1 Configuring settings.....31
3.4.2 Checking modified settings.....32
3.4.3 Adding notes to settings.....32

3.4.4 Discarding undistributed changes to settings....33
3.4.5 Restrictions....33
3.4.6 Using password-protected uninstallation....33
3.4.7 Copying policy settings between Policy Manager instances....33
3.4.8 Policy inheritance....34
3.5 Managing operations and tasks....36
3.5.1 Remote collection of diagnostics reports....36
3.6 Alerts....37
3.6.1 Viewing alerts and reports....37
3.6.2 Sending alerts by email....37
3.6.3 Forwarding alerts to syslog server....38
3.6.4 Configuring alert forwarding for a specific domain....38
3.7 Reporting tool....39
3.7.1 Viewing and exporting a report....39
3.8 Using data mining to get information about managed hosts....39
3.8.1 Running queries on managed endpoint data....40
3.8.2 Publishing saved queries for reports and external use....40
3.8.3 Example of using data mining....41
3.9 How to check that the network environment is protected....41
3.9.1 Checking that all the hosts have the latest policy....41
3.9.2 Checking that the hosts have the latest virus definitions....41
3.9.3 Checking that there are no disconnected hosts....42
3.9.4 Viewing scanning reports....42
3.9.5 Viewing alerts....42
3.9.6 Creating a weekly infection report....43
3.9.7 Monitoring a possible network attack....43

Chapter 4: Maintaining Policy Manager Server....44

4.1 Malware definition updates....45
4.1.1 Checking the malware definitions on Policy Manager Server....46
4.1.2 Updating malware definitions in isolated networks....46
4.2 Backing up and restoring Policy Manager data....49
4.3 Creating the backup....49
4.4 Restoring the backup....49
4.5 Restoring an automatically saved backup on Linux....50
4.6 Exporting and importing signing keys....50
4.7 Replicating software using image files....50
4.8 Re-indexing search data....51
4.9 Running the database maintenance tool....51
4.9.1 Database maintenance troubleshooting....52

Chapter 5: Web Reporting....54

5.1 Viewing reports....55
5.2 Scheduling reports....55
5.3 Changing the Web Reporting port....56

Chapter 6: Policy Manager Proxy.....57

6.1 Overview.....58

6.1.1 When should you use Policy Manager Proxy?.....58

6.2 Setting up Policy Manager Proxy.....59

6.3 Centralized management of Policy Manager Proxy.....60

Chapter 7: Software distribution.....61

7.1 Push installations.....62

7.1.1 Autodiscover Windows hosts.....62

7.1.2 Autodiscover hosts from an Active Directory server.....63

7.1.3 Push install to Windows hosts.....63

7.1.4 Push install after target host selection.....64

7.2 Policy-based installation.....64

7.2.1 Using policy-based installation.....65

7.3 Local installation and updates with pre-configured packages.....66

7.3.1 Using the customized remote installation package.....66

7.3.2 How to prepare MSI installation packages with Policy Manager for Linux.....67

7.4 Local installation and Policy Manager.....67

7.4.1 System requirements.....67

7.4.2 Installation steps.....68

7.5 Upgrading managed software.....68

Chapter 8: Managing endpoint security.....69

8.1 Migration of Email and Server Security settings.....70

8.2 Configuring virus and spyware protection.....70

8.2.1 Configuring automatic updates.....70

8.2.2 Configuring real-time scanning.....72

8.2.3 Using Security Cloud for malware scanning.....74

8.2.4 Configuring scheduled scanning.....74

8.2.5 Configuring DeepGuard.....75

8.2.6 Configuring web traffic (HTTP) scanning.....76

8.2.7 Managing quarantined objects.....78

8.2.8 Hiding notifications on managed hosts.....79

8.2.9 Hiding the local user interface on managed hosts.....79

8.2.10 Preventing users from changing settings.....79

8.2.11 Monitoring viruses on the network.....80

8.2.12 Testing your antivirus protection.....80

8.3 Configuring firewall settings.....80

8.3.1 Turning on the firewall.....81

8.3.2 Configuring network quarantine.....81

8.3.3 Firewall settings for version 14 clients and newer.....82

8.4 Configuring application control.....84

8.4.1 Configuring application control.....84

8.4.2 Creating a new application control profile.....84

8.4.3 Adding exclusion rules.....85

8.4.4 Example: Preventing a vulnerable version from running....86
8.4.5 Example: Preventing applications from automatically opening downloaded files....87
8.5 How to protect your users' sensitive data....87
8.5.1 Protecting secure connections on managed hosts....88
8.6 Blocking unsuitable web content....88
8.6.1 Web content categories....88
8.6.2 Selecting the content categories to block....90
8.7 Using Device Control....90
8.7.1 Configuring Device control....90
8.7.2 Limiting access permissions for removable drives....90
8.7.3 Blocking hardware devices....91
8.7.4 Granting access to specific devices....91
8.8 Managing software updates....92
8.8.1 Installing software updates automatically....92
8.8.2 Handling manually downloaded software updates....92
8.8.3 Excluding software updates from automatic installation....93
8.8.4 Checking the status of software updates in your network....93
8.8.5 Allowing end users to manage software updates....94
8.8.6 Configuring a third-party HTTP proxy for Software Updater....94
8.9 Rapid Detection & Response....95
8.9.1 Activating endpoint sensors....95
8.9.2 Checking the status of endpoint sensors....95
8.9.3 Isolating hosts from the network....96

Chapter 9: Virus information....97

9.1 Malware information and tools on the F-Secure web pages....98
9.2 How to send a virus sample to F-Secure....98
9.2.1 How to package and send a virus sample....98
9.2.2 Finding new malware....98
9.2.3 What should be sent....99

Chapter 10: Windows Management Instrumentation....100

10.1 WMI integration....101
10.2 WMI classes for integration....101
10.2.1 WMI classes....101

Chapter 11: Troubleshooting....106

11.1 Policy Manager Server and Policy Manager Console....107
11.2 Policy Manager Web Reporting....109
11.3 Policy distribution....109
11.4 Frequently asked questions for Linux versions....110

Appendix A: Configuring older versions of Client Security....112

A.1 Configuring spyware scanning....113
A.1.1 Setting up spyware control for the whole domain....113

A.1.2 Launching spyware scanning in the whole domain....114
A.1.3 Allowing the use of a spyware or riskware component....114
A.2 Configuring alert sending....114
A.2.1 Sending virus alerts to an email address....114
A.2.2 Disabling alert pop-ups....115
A.3 Excluding a web site from HTTP scanning....115
A.4 Firewall settings for Client Security 13 and older....116
A.4.1 Configuring security levels and rules....116
A.4.2 Configuring rule alerts....118
A.4.3 Using alerts to check that the firewall works....120
A.5 Configuring Network access control....121
A.5.1 Setting up Network access control for the first time....122
A.5.2 Creating a rule for an unknown application on root level....122
A.5.3 Editing an existing Network access control rule....123
A.5.4 Turning off Network access control pop-ups....123
A.6 Advanced features: firewall....124
A.6.1 Managing firewall properties remotely....124
A.6.2 Configuring security level autoselection....125
A.6.3 Troubleshooting connection problems....126
A.6.4 Adding new services....126

Appendix B: Using Policy Manager with a MySQL database....129

B.1 Migrating H2 data to MySQL using the command line....130

Chapter

1

Introduction

Topics:

- Main components
- Features
- What's new
- Product registration
- Basic terminology
- Policy-based management

Policy Manager provides a central location for managing security applications across different operating systems.

Policy Manager can be used for:

- setting and distributing security policies,
- installing application software to local and remote systems,
- monitoring the activities of all systems in the enterprise for 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. This helps you to make sure that the entire domain is protected, and to modify the protection settings when necessary. You can also restrict the users from making changes to the security settings, and be sure that the protection is always up-to-date.

1.1 Main components

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

Policy Manager Server is the repository for policies and software packages distributed by the administrator, as well as status information and alerts sent by the managed hosts. Communication between Policy Manager Server and the managed hosts is secured with the HTTPS protocol, although non-sensitive data, such as updates to the virus definitions database, are handled through the standard HTTP protocol.

Web Reporting

Web Reporting is an enterprise-wide, web-based graphical reporting system included in Policy Manager Server. With Web Reporting you can quickly create graphical reports based on historical trend data, and identify computers that are unprotected or vulnerable to virus outbreaks.

1.2 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 installed automatically ('pushed') by Automatic Update Agent, or manually ('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 ConfigMgr (System Center Configuration Manager) 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), email, and report files and creation of event statistics. You can also set Policy Manager to forward alerts to a third-party syslog server.

Performance management

- Statistics and performance data handling and reporting.

Task management

- Management of virus scanning tasks and other operations.

Differences between Windows and Linux

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

- Push installation features
- Microsoft Windows Installer (MSI) package support (for 14.x client versions, you can prepare MSI packages for distribution, see How to prepare MSI installation packages with Policy Manager for Linux on page 67 for details)
- Autodiscovery of workstations on the network

1.3 What's new

This section highlights the major improvements for this release of Policy Manager.

Data mining	The new data mining view allows administrators to search and browse the data collected in Policy Manager to resolve issues, verify concerns, and create queries for custom reports or exporting data. For more information, see Using data mining to get information about managed hosts on page 39 .
New and improved Web Reporting	This redesigned version of Web Reporting includes a wider range of reports and features. For more information, see Web Reporting on page 54 .
Support for Atlant for Virtual Environments	Policy Manager 15.00 introduces a new **Virtual security** settings tree for configuring Offload Scanning Agent and F-Secure Atlant for Virtual Environments, which replaces F-Secure Scanning and Reputation Server. For more information, see the user guide for F-Secure Atlant.

See the release notes for the full list of changes and further information.

1.4 Product registration

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

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

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

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

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

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

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

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

What if I have several Policy Manager installations?

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

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

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

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

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

Who should I contact for help?

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

1.4.1 Upstream reporting

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

Why does F-Secure collect data?

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

What information is sent?

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

Where is the information stored and who can access it?

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

1.5 Basic terminology

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

HOST	Host refers to a computer that is centrally managed with Policy Manager.
POLICY	A security policy is a set of well-defined rules that regulate how sensitive information and other resources are managed, protected, and distributed. The management architecture of F-Secure software uses policies that are centrally configured by the administrator for optimum control of security in a corporate environment. The information flow between Policy Manager Server and the hosts is accomplished by transferring policy files.
POLICY DOMAIN	Policy domains are groups of hosts or subdomains that have a similar security policy.
POLICY INHERITANCE	Policy inheritance simplifies the defining of a common policy. In Policy Manager Server, each policy domain automatically inherits the settings of its parent domain, allowing for easy and efficient management of large networks. The inherited settings may be overridden for individual hosts or domains. When a domain's inherited settings are changed, the changes are inherited by all of the domain’s hosts and subdomains. The policy can be further refined for subdomains or even individual hosts. The granularity of policy definitions can vary considerably among installations. Some administrators might want to define only a few different policies for large domains. Other administrators might attach policies directly to each host, achieving the finest granularity.

1.6 Policy-based management

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

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

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

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

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

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

Default policy files	The default policy file contains the default values (the factory settings) for a single product that are installed by the setup. Default policies are used only on the host. If neither the base policy file nor the incremental policy file contains an entry for a variable, then the value is taken from the default policy file. New product versions get new versions of the default policy file.
Base policy files	Base policy files contain the administrative settings and restrictions for all the variables for all F-Secure products on a specific host (with domain level policies, a group of hosts may share the same file). Base policy files are created on Policy Manager Server, and all related communication with Policy Manager Console is handled via HTTPS.
Incremental policy files	Incremental policy files are used to store local changes to the base policy. Only changes that fall within the limits specified in the base policy are allowed. The incremental policy files are then periodically sent to Policy Manager Server so that current settings and statistics can be viewed by the administrator.

1.6.1 Management Information Base

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

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

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

Settings	Used to manage the workstation in the manner of an SNMP. The managed products must operate within the limits specified here.
Statistics	Delivers product statistics to Policy Manager.
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 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.

Chapter

2

Installing the product

Topics:

- System requirements
- Installing the product on Windows
- Installing the product on Linux

This section explains the steps required to install Policy Manager.

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

2.1 System requirements

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

2.1.1 Policy Manager Server

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

Operating system:	• Microsoft Windows:
	  • Windows Server 2008 R2 with latest SP; Standard, Enterprise or Web Server editions
	  • Windows Server 2012; Essentials, Standard or Datacenter editions
	  • Windows Server 2012 R2; Essentials, Standard or Datacenter editions
	  • Windows Server 2016; Essentials, Standard or Datacenter editions
	  • Windows Server 2019; Essentials, Standard or Datacenter editions (Server Core is supported)
	• Linux (only 64-bit versions of all distributions listed are supported):
	  • Red Hat Enterprise Linux 6, 7, 8
	  • CentOS 7, 8
	  • openSUSE Leap 43, 15
	  • SUSE Linux Enterprise Server 11, 12, 15
	  • SUSE Linux Enterprise Desktop 11, 12, 15
	  • Debian GNU Linux 9, 10
	  • Ubuntu 16.04, 18.04, 20.04
	  • Oracle Linux 8

Processor:	Dual-core 2GHz CPU or higher.
Memory:	4 GB RAM.
Disk space:	10 GB of free disk space. For managing Premium clients, an additional 10 GB of space is required for serving software updates.
Network:	100 Mbit network.
Browser:	• Firefox • Internet Explorer • Google Chrome

2.1.2 Policy Manager Console

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

Operating system:	• Microsoft Windows:
	  • Windows 7 (64-bit) with or without SP1; Professional, Enterprise or Ultimate editions
	  • Windows 8 (64-bit), any edition
	  • Windows 8.1 (64-bit), any edition
	  • Windows 10 (64-bit)
	  • Windows Server 2008 R2 with latest SP; Standard, Enterprise or Web Server editions
	  • Windows Server 2012; Essentials, Standard or Datacenter editions
	  • Windows Server 2012 R2; Essentials, Standard or Datacenter editions
	  • Windows Server 2016; Essentials, Standard or Datacenter editions
	  • Windows Server 2019; Essentials, Standard or Datacenter editions
	  Note: Server Core installation option is not supported.
	• Linux (only 64-bit versions of all distributions listed are supported):
	  • Red Hat Enterprise Linux 6, 7, 8
	  • CentOS 7, 8
	  • openSUSE Leap 43, 15
	  • SUSE Linux Enterprise Server 11, 12, 15
	  • SUSE Linux Enterprise Desktop 11, 12, 15
	  • Debian GNU Linux 9, 10
	  • Ubuntu 16.04, 18.04, 20.04
	  • Oracle Linux 8

Processor:	2 GHz or higher CPU.
Memory:	2 GB of RAM.
Disk space:	300 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.

2.2 Installing the product on Windows

This section describes how to install the product on Windows computers.

2.2.1 Installation steps

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

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 https://www.f-secure.com/en/web/business_global/downloads.
   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.
   - Select Policy Manager Console if you have already installed Policy Manager Server on a separate machine.

   Note: If you are only installing Policy Manager Console, you do not need to set the administrator account password or the Policy Manager Server modules.

2. Choose the destination folder and then click **Next**.
   It is recommended to use the default installation directory. If you want to install the product in a different directory, you can click **Browse** and select a new directory.

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

3. Enter and confirm a password for your admin user account, then click **Next**.
   Use this password to log in to Policy Manager Console with the user name `admin`.
4. Select the Policy Manager Server modules to enable:
   - The **Host** module is used for communication with the hosts. Non-sensitive data, such as updates to the virus definitions database, is transferred over HTTP, whereas any sensitive data is transferred using the secured HTTPS protocol. The default HTTP port is 80, and the default HTTPS port is 443.
   - The **Administration** module is used for communication with Policy Manager Console. The default HTTPS port is 8080.

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

     By default, access to the **Administration** module is restricted to the local machine. If you want to use Policy Manager Console on a different computer, clear the **Restrict access to the local machine** checkbox.

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

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

5. Click **Next** to continue.

If you have already installed Policy Manager Server and want to use Policy Manager Console on a different computer:

1. Set the `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data Fellows\F-Secure\Management Server 5\RestrictLocalhost` registry key value to `0`.
2. Restart the Policy Manager Server service.

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. Specify the HTTP proxy configuration if the Policy Manager host does not have a direct internet connection.
   a) Edit the HTTP proxy configuration file.
      - Windows: `<F-Secure installation folder>\Management Server 5\data\fspms.proxy.config`
      - Linux: `/var/opt/f-secure/fspms/data/fspms.proxy.config`

   b) Add the proxy as a new line, using the following format:
      `http_proxy=[http://][user[:password]@]<address>[:port].`
      Use percent encoding for any reserved URI characters in the user name or password. For example, if the password is `ab%cd`, you need to enter it as follows:
      `http_proxy=http://user:ab%25cd@proxy.example.com:8080/.`
   c) Restart the Policy Manager Server service.

   Note: Policy Manager supports a single HTTP proxy configuration and there is no fallback to a direct internet connection when an HTTP proxy is defined.

4. Restart your computer if you are prompted to do so.

Run Policy Manager Console

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

To continue:

1. Run Policy Manager Console.

   Depending on your operating system, you can run Policy Manager Console either from the **Start** menu or by double-clicking the desktop icon.

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

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

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

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

2.2.2 Changing the web browser path

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

If you want to change the web browser path:

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

2.2.3 Uninstalling the product

Follow these steps to uninstall Policy Manager components.

To uninstall any Policy Manager components:

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

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

2.3 Installing the product on Linux

This section describes how to install the product on Linux computers.

2.3.1 Installation steps

You can install Policy Manager Server and Policy Manager Console either on the same computer or on separate ones.

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, CentOS, and Suse distributions:

- Policy Manager Server requires both 32-bit and 64-bit versions of the `libstdc++` library. Make sure that the `libstdc++` and `libstdc++.i686` packages are installed before you install Policy Manager Server.

Debian and Ubuntu distributions:

- Both 32-bit and 64-bit versions of the `libstdc++` library must be installed prior to installing Policy Manager Server. Use Multiarch capabilities (https://wiki.debian.org/Multiarch/HOWTO) to install the 32-bit library onto 64-bit platforms.
- Install the `libstdc++6` and `libstc++6:i386` packages 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.

Install Policy Manager Server

The first step is to install F-Secure Policy Manager Server.

1. Log in as `root`.

2. Open a terminal.
3. To install, enter the following command:

Distribution type	Command
Ubuntu and Debian-based distributions	`dpkg -i fspms_<version_number>.<build number>_amd64.deb`
RPM-based distributions	`rpm -i fspms-<version_number>.<build number>-1.x86_64.rpm`

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

   Press Enter to choose the default setting (shown in square brackets).
5. Log in as a normal user and enter the following command to check the status of the components:
   - `/etc/init.d/fspms status`

   Alternatively, you can open your browser and go to the following URLs:
   - `http://localhost` - Policy Manager Server status
   - `https://localhost:8081` - Web Reporting status
6. Specify the HTTP proxy configuration if the Policy Manager host does not have a direct internet connection.
   a) Edit the HTTP proxy configuration file.
      - Windows: `<F-Secure installation folder>\Management Server 5\data\fspms.proxy.config`
      - Linux: `/var/opt/f-secure/fspms/data/fspms.proxy.config`

   b) Add the proxy as a new line, using the following format:
      `http_proxy=[http://][user[:password]@]<address>[:port].`

      Use percent encoding for any reserved URI characters in the user name or password. For example, if the password is `ab%cd`, you need to enter it as follows:
      `http_proxy=http://user:ab%25cd@proxy.example.com:8080/.`

   c) Restart the Policy Manager Server service.

   Note: Policy Manager supports a single HTTP proxy configuration and there is no fallback to a direct internet connection when an HTTP proxy is defined.

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

Install Policy Manager Console

Next, you need to install Policy Manager Console.

1. Log in as `root`.

   If you are installing the product on an Ubuntu distribution, you should log in as a normal user that has been added to `/etc/sudoers`.
2. Open a terminal.
3. To install type:

Distribution type	Command
Ubuntu and Debian-based distributions	`dpkg -i fspmc_<version_number>.<build number>_amd64.deb`
RPM-based distributions	`rpm -i fspmc-<version_number>.<build number>-1.x86_64.rpm`

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

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

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

   a) Check which groups the user belongs to:

      ```
      groups <user id>
      ```

      For example, if the user is Tom:

      ```
      groups Tom
      ```

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

      ```
      /usr/sbin/usermod -aG fspmc <user id>
      ```

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

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

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

2.3.2 Upgrading the product

Follow these steps to upgrade your installation from a previous version.

Before you start upgrading the product, create a full backup of the Policy Manager data (for example H2 database, preferences). For more information, see Backing up and restoring Policy Manager data on page 49 .

Note: You should uninstall Automatic Update Agent if you do not need it for any other F-Secure products on the same machine.

Note: Policy Manager Server requires Linux capabilities. Make sure this package is installed before installing Policy Manager Server. For SUSE Linux Enterprise Server 11 and SUSE Linux Enterprise Desktop 11, you might need to explicitly enable Linux File System Capabilities by adding `file_caps=1` as a kernel boot option (see SUSE Linux Enterprise Server 11 release notes for more details: https://www.suse.com/releasenotes/x86_64/SUSE-SLES/11-SP4).

1. Upgrade Policy Manager Server:

Distribution type	Command
Ubuntu and Debian-based distributions	`# dpkg -i fspms_<version_number>.<build_number>_amd64.deb`
RPM-based distributions	`# rpm -U fspms-<version_number>.<build_number>-1.x86_64.rpm`

2. Upgrade Policy Manager Console:

Distribution type	Command
Ubuntu and Debian-based distributions	`# dpkg -i fspmc_<version_number>.<build_number>_amd64.deb`
PM-based distributions	`# rpm -U fspmc-<version_number>.<build_number>-1.x86_64.rpm`

3. Run the database maintenance tool before starting Policy Manager Server:

   ```
   /opt/f-secure/fspms/bin/fspms-db-maintenance-tool
   ```

2.3.3 Uninstalling the product

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

You must uninstall the three components in this order:

1. Policy Manager Server

2. 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
Ubuntu and Debian-based distributions	**a.** `dpkg -r f-secure-policy-manager-server` **b.** `dpkg -r f-secure-policy-manager-console`
RPM-based distributions	**a.** `rpm -e f-secure-policy-manager-server` **b.** `rpm -e 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:

a. `rm -rf /var/opt/f-secure/fspms`
b. `rm -rf /var/opt/f-secure/fsaus`
c. `rm -rf /etc/opt/f-secure/fspms`
d. `rm -rf /etc/opt/f-secure/fsaus`
e. `rm -rf /opt/f-secure/fspmc`

Chapter

3

Using Policy Manager Console

Topics:

- Overview
- Basic information and tasks
- Managing domains and hosts
- Managing policies
- Managing operations and tasks
- Alerts
- Reporting tool
- Using data mining to get information about managed hosts
- How to check that the network environment is protected

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

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

3.1 Overview

This section provides some general information about Policy Manager Console.

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

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

With Policy Manager Console, an administrator user can:

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

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

Read-only users can:

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

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

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

3.2 Basic information and tasks

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

3.2.1 Logging in

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

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

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

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

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

Policy Manager Server generates an instance-specific, self-signed certificate when it is installed. When connecting to the server, Policy Manager Console tries to validate the server certificate and shows a warning if the validation is unsuccessful. Once the certificate's fingerprint is confirmed by an administrator, it is saved to the `Administrator.properties` configuration.

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.

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

Changing your password

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

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

3.2.2 Dashboard

The dashboard in Policy Manager Console gives you an overview of the current status of the managed network.

In addition to showing you relevant, real-time information on the status of Policy Manager, the managed network, and network activity, the dashboard also provides direct links to more details and quick paths to resolve potential issues.

The dashboard shows you the following information:

- Server CPU status.
- Number of pending and unmanaged hosts. Click either of these to see details.
- Status of administrator features: email notifications, scheduled reporting, alert forwarding, Active Directory, and Policy Manager Proxy. Click any of these to go to the relevant pages or to see more details.
- Status of updates and disk space, amount of downloaded and distributed data.
- Server events. These include virus definition updates, user activity, and warnings. Click the download icon to export the log as a CSV file.
- Host issues. This list shows you the current status of the main issues that affect the managed hosts. Click any of the issues to see a detailed list of the affected hosts and the proposed solution for each case.

You can click **Summary** to switch to a different view of the network status.

3.2.3 Adding new users

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

As of Policy Manager version 13.00, you can import individual users or user groups from Active Directory in addition to creating users locally.

Note: As of version 13.00, Policy Manager uses LDAPS (secure LDAP) by default to connect to the Domain Controller (DC) for Active Directory. On Windows, Policy Manager uses the Windows trust store to handle authentication to the DC seamlessly. On Linux, you must import the company certificate in Policy Manager Server's Java runtime trust store to authenticate the DC. For more information, see Importing the company certificate for Active Directory authentication on Linux on page 27 . Alternatively, you can use plain LDAP to connect to the DC.

The **Users** view shows you name of the user as well as their access level and when they were last logged in to Policy Manager. The icons represent the type of user (local, imported from Active Directory, user group).

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

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

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

2. To create a single user locally:
   a) Click **Create local user**.
   b) Enter the user name and password for the new user and select the domain access.
   c) Select **Read-only access** if you want to limit the user's access.
   d) Click **OK**.
3. To import users from Active Directory:
   a) Click **Import from Active Directory**.
   b) Enter the credentials for your Active Directory server, then click **Next**.
   c) Select the user or group to import.

      You can use the search field to find specific accounts.
   d) Click **Next**.
   e) Select the domain access for the imported user or group.
   f) Select **Read-only access** if you want to limit the user's access.
   g) Click **Done**.

The new user or group is shown on the **Users** list, and can now access Policy Manager.

For imported groups, you can click **See members** to view details of the individual users who belong to the group.

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

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

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

3.2.4 Switching between standard and advanced views

As of version 12.20, Policy Manager Console provides two different views for the **Settings** and **Status** tabs.

Standard view is optimized for managing Client Security and provides quick access to the majority of the relevant settings and information. **Advanced view** provides access to all available settings for all managed F-Secure products.

To switch between views:

1. Go to the **Settings** or **Status** tab.
2. Click **Standard view** or **Advanced view**.

Note: By default, **Advanced view** opens on the root node. When you switch views, Policy Manager Console remembers the last selected node and page for the current session.

Contents of the Advanced view

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

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

- **Installation** tab: you can view and edit installation information.

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

Using help

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

3.2.5 Policy domain tree

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

On the **Domain tree**, you can do the following:

- Add a new policy domain by clicking the following icon on the toolbar:

Note: A new policy domain can be created only when a parent domain is selected.

- Add a new host by clicking the following icon:

- Find a host.
- View the properties of a domain or host. All hosts and domains should be given unambiguous names.
- Import new hosts.
- Autodiscover hosts from a Windows domain.
- Delete domains.
- Move hosts or domains, using cut and paste operations.
- Export a policy file.

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

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

3.2.6 Messages pane

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

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

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

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

3.2.7 Product upgrade notifications

When you start Policy Manager Console, it notifies you of new available versions for either Policy Manager itself or any of your managed applications.

Note: You can also manually check if there are any upgrades available by selecting **Help** > **Check for product upgrades** from the menu.

Available upgrades are shown on the **Product upgrades** tab of the **Messages** pane, listing the available new versions of your software along with the corresponding links for you to download the new versions. The upgrade messages apply only to applications that are relevant for your managed environment.

Policy Manager also sends a server alert email to the defined recipients for each new available upgrade.

When you install a Policy Manager upgrade or import the installation package for a managed application, the corresponding message automatically disappears from the **Product upgrades** list.

If you do not need to install an upgrade, you can mark it as ignored to skip it.

3.3 Managing domains and hosts

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

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

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

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

3.3.1 Adding policy domains

This topic describes how to add new policy domains.

To add a new policy domain:

1. Click the following icon on the toolbar:

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

3.3.2 Adding hosts

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

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

- Import hosts from an Active Directory.
- Import hosts directly from your Windows domain.
- Use host import rules to automatically import newly connected hosts that already have F-Secure security software installed.
- Create hosts manually by using the **New host** command.

Importing hosts from an Active Directory

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

There are three ways that you can connect your Active Directory to Policy Manager:

- Create a synchronization rule: Use this approach if you want to fully replicate your Active Directory tree in Policy Manager. Any changes in Active Directory are automatically replicated in your domain tree, for example if you add, remove, or move an organization unit.
- Create a notification rule: Use this option if you do not want synchronize your Active Directory and Policy Manager domain trees automatically, but still want to monitor the network for unprotected hosts. Any unprotected hosts are added to the list of unmanaged hosts, where you can then add them to the domain tree.
- Import structure manually: If you only want to import the Active Directory tree, but do not want to synchronize or monitor the tree for any future changes, you can use this option.

In addition to these options, you can use the Active Directory distinguished name as the import criteria when creating host import rules.

Importing the company certificate for Active Directory authentication on Linux

To use the default LDAPS (secure LDAP) connection to the Domain Controller (DC) for Active Directory, you must import the company certificate in Policy Manager Server's Java runtime trust store to authenticate the DC.

Note: Whenever you install a new version of Policy Manager, the certificate file is overwritten. This means that you need to repeat the steps given here after each upgrade.

To import and apply the certificate:

1. Fetch your Active Directory certificate.

   You can use one of the following methods:

   - Go to the root of the C drive and look for an automatically generated AD certificate file, which has a `.crt` extension.
   - Run `certutil -ca.cert server.crt`. This saves the CA certificate as server.crt.
   - Follow the steps given online in Exporting the LDAPS Certificate, but do not export the private key in step 10, and select **DER encoded binary X.509 (.CER)** as the export file format in step 11.

2. Copy the certificate file to the Policy Manager host, for example to `/home/user/Downloads/server.crt`.
3. Run the following command to go to Policy Manager's JRE directory:

   ```
   cd /opt/f-secure/fspms/jre/
   ```

4. Run `keytool` to apply the certificate:

   ```
   ./bin/keytool -importcert -keystore ./lib/security/cacerts -file
   /home/user/Downloads/server.crt
   ```

   `keytool` prompts you to enter a password. Use the default keystore password, `changeit`.

5. Enter `yes` when asked if you trust this certificate, and press Enter.
6. Restart the Policy Manager service:

   ```
   /etc/init.d/fspms restart
   ```

Creating an Active Directory synchronization rule

Synchronization rules define a link between an Active Directory subtree and your policy domain tree, after which any changes in Active Directory are automatically synchronized and any new hosts are detected in Policy Manager.

Note: Subtrees that are marked for synchronization in the Policy Manager domain tree are read-only and you cannot make any changes to them from the console.

1. On the **Active Directory** tab, click **Create synchronization rule**.
2. Enter the server address for your Active Directory server and a user name and password that provide at least read access, then click **Next**.
3. Select the Active Directory container that you want to import, then click **Next**.
4. Select the target policy domain for importing the structure, then click **Next**.

   Important: If you select **root** as the target policy domain, the entire policy tree becomes read-only. We recommend that you create or use a separate subtree for the Active Directory structure.

5. Click **Done** to run the synchronization rule.
   The Active Directory structure is added to your policy domain tree and synchronized. Any new detected hosts that already have F-Secure software installed are automatically imported to the appropriate location in the domain tree, and any other new hosts are added to the list of unmanaged hosts.

Creating an Active Directory notification rule

You can use a notification rule to handle importing hosts from Active Directory to Policy Manager, for example if you want to maintain separate structures, but still want to monitor your network environment for any unprotected hosts.

1. On the **Active Directory** tab, click **Create notification rule**.
2. Enter the server address for your Active Directory server and a user name and password that provide at least read access, then click **Next**.
3. Select the Active Directory container that you want to import, then click **Next**.

4. Click **Done** to run the notification rule.
   The Active Directory is checked, and any new detected hosts are added to the list of unmanaged hosts.

Manually importing from Active Directory

When you import from Active Directory manually, the structure is imported to the selected domain, but Policy Manager does not poll the Active Directory for new hosts.

1. On the **Active Directory** tab, click **Import structure manually**.
2. Enter the server address for your Active Directory server and a user name and password that provide at least read access, then click **Next**.
3. Select the Active Directory container that you want to import, then click **Next**.
4. Select the target policy domain for importing the structure, then click **Next**.

   Important: If you select **root** as the target policy domain, the entire policy tree becomes read-only. We recommend that you create or use a separate subtree for the Active Directory structure.

5. Once the structure is imported, click **Close**.

Note: You can create host import rules to import hosts connecting later, using the Active Directory distinguished name as the import criteria.

Handling unmanaged hosts

When you have created an Active Directory synchronization or notification rule, any new hosts added to the linked Active Directory appear in Policy Manager as unmanaged hosts.

The current number of unmanaged hosts detected is shown above the domain tree in Policy Manager. If you have set up email notifications for server alerts, you also receive alerts indicating the total number of unmanaged hosts.

To process unmanaged hosts:

1. On the **Hosts outside the domain tree** pane, click **Unmanaged**.
   The **Unmanaged hosts** dialog shows you a list of all the currently detected, unmanaged hosts from the linked Active Directory structure.
2. Select any hosts that you want to ignore, then click **Ignore hosts**.

   For example, if any hosts have a valid reason for not having antivirus software installed, you can ignore them so that they do not show up in later alerts.

   Tip: Use **Hide ignored hosts** to toggle the visibility of the ignored hosts.

3. Select the hosts that you want to add to the Policy Manager domain tree, then click **Start installation**.
   The selected hosts are added to the policy domain tree and you can start installing the necessary security software.

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.

Related Concepts

Software distribution on page 61

Importing new hosts

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

You can do this only after the client software has been installed on the hosts and after the hosts have sent a connection request to Policy Manager.

To import new hosts:

1. Click the following icon on the toolbar:

   Alternatively:

   - Select **Edit** > **Import new hosts** from the menu.
   - Select **Import new hosts** from the **Installation** view.

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

2. You can perform the following actions on the **New hosts** view:

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

Related Tasks

Using the customized remote installation package on page 66
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.

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`. You can also use multiple wildcards, for example `ab*4*`.
  - 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.

   - 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 the following icon on the toolbar:

   - Press Insert.

3. Enter an identifier for the new host and click **OK**.

   This operation is useful in the following cases:

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

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

Handling disconnected hosts automatically

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

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

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

3.4 Managing policies

This section describes how to configure and distribute policies.

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

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

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

3.4.1 Configuring settings

You can change the policy settings in both the **Standard view** and **Advanced view**.

Most settings for managed hosts are available in **Standard view**. Some settings, for example for older product versions, are only available in **Advanced view**.

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.

To configure the policy settings:

1. Go to the **Settings** page.

   In **Standard view**:

   a) Select the branch for the platform that you want to configure.
   b) Edit the settings as necessary.

   To change the settings in **Advanced view**:

   a) Click **Advanced view** in the upper-right corner of the **Settings** page.
   b) Browse the policy tree.
   c) Change the values of the policy variables.

2. Click the following icon to distribute the policy:

3. Review the listed changes to the policy settings, then click **Distribute**.

   You can click the listed items to view the corresponding page in the settings.

   If you want to revert the changes, click **Clear all settings**.

Tip: You can also distribute the policies by selecting **File** > **Distribute** from the menu or by pressing CTRL + D.

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

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

3.4.2 Checking modified settings

Domains and hosts that include modified settings are highlighted on the **Domain tree**.

The **Domain tree** shows a yellow line next to domains and hosts that include changes. This allows you to check what settings have changed for the specific domain or host and cancel the changes if necessary.

The modified domains are highlighted by default. You can change the settings from the menu, under **Tools** > **Preferences**.

To see the changes for a domain or host:

1. Right-click a highlighted domain or host in the **Domain tree**.
2. Select **Show modified settings** in the context menu.
   The **Modified settings** view shows you all the changes for the selected domain or host, sorted by the **Settings** pages.
3. Click any of the listed changes to change focus to the corresponding page and field.
4. If you want to cancel all the listed changes, click **Clear all settings**.
5. Click **Close**.

3.4.3 Adding notes to settings

As of version 12.20, you can add notes to the policy settings in Policy Manager Console, for example to record the reasons for changing a setting.

Any notes added to settings are visible in both **Standard view** and **Advanced view**.

Notes are inherited within the policy domain; any inherited notes are shown with a gray icon. You can add further comments for a specific host or subdomain to inherited notes.

Icon	Description
	No notes available for this setting. Click to add a note.
	A note has been added for this setting. Click to view or edit the note.
	A note for this setting has been inherited. Click to view or edit the note.
	Click this icon in the note editor to delete the note.

Notes are also shown in the **Domain policy values** dialog and in inheritance reports.

To add a note:

1. Click the note icon next to the setting to which you want to add a note.
   The note editor appears.
2. Enter the text that you want to add.
3. Click anywhere outside the note editor to save your comment and close the editor.
   The time and user name for the last change to the note are recorded, and the icon changes to indicate that there is a note for the setting.

   Note: Even though the note is automatically saved, it is not visible to other administrators until you distribute the policy.

4. Click the following icon to distribute the policy:

Note: The time of the last change to a note is updated when the policy is distributed.

To delete any note, click the note icon, then click the trash icon in the note editor and confirm that you want to delete the note.

Note: You cannot delete inherited notes (shown with a gray icon). You can only delete notes on the domain level where they have been added.

3.4.4 Discarding undistributed changes to settings

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

Select **File** > **Discard policy changes** from the menu.
The settings will revert to what they were when the policy was last distributed. If the changes have already been distributed, you need to manually revert the changes and redistribute the policy.

3.4.5 Restrictions

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

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

3.4.6 Using password-protected uninstallation

As of version 12.20, you can set an uninstallation password for managed hosts to prevent the unauthorized or accidental uninstallation of client software on the hosts.

Note: Check the release notes for your client software to see if the version supports password-protected uninstallation.

When password-protected uninstallation is in use, uninstalling client software managed by Policy Manager on a host requires the user to enter the uninstallation password. Without the correct password, uninstallation is canceled.

Note: Password-protected uninstallation also applies to distributed Policy Manager components that are installed on managed hosts.

To set up password-protected uninstallation in **Standard view**:

1. Select the target domain or host.
2. Go to the **Settings** tab and select the **Centralized management** page.
3. Under **Uninstallation password**, click **Set password**.
4. In the **Set uninstallation password** dialog, enter and confirm the password that you want to use, then click **OK**.
5. Click the following icon to distribute the policy:

The password that you set must now be entered when uninstalling managed client software locally. If you want to stop using password-protected uninstallation, click **Remove password**.

3.4.7 Copying policy settings between Policy Manager instances

If your environment includes multiple instances of Policy Manager, you can copy the policy settings from one instance to another.

Copying the policy settings involves exporting all non-default settings from one Policy Manager instance to a JSON file, which you can then import to another instance. Only the settings that you have modified are included in the exported file.

To copy the policy settings:

1. In the Policy Manager Console domain tree, select the domain that you want to copy the settings from.
2. Select **Tools** > **Export policy settings** from the menu.

3. Check the listed settings and click the **Browse** button.

   Select **Include Firewall and Application control profiles** and **Include settings from parent domains** if you also want to include those settings in the exported file.

4. Select a location and name for the exported JSON file, then click **Export**.
5. If necessary, copy the exported file to a location that you can access on other Policy Manager instances.
6. In Policy Manager Console for the instance that you want to copy the settings to, select the domain that you want to copy the settings to.
7. Select **Tools** > **Import policy settings**.
8. Click the **Browse** button to select the previously exported JSON file and click **Import**.
9. Check the listed settings and click **Import**.
   The new settings are applied to the selected domain.
10. Click the following icon to distribute the policy:

3.4.8 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.

Related Concepts

Reporting tool on page 39

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

How settings inheritance is displayed on the user interface

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

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

Locking and unlocking all settings on a page at once

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

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

Allow user changes	Unlocks all the settings that have a lock symbol displayed beside them on the current page. After this the users can change these settings.

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

Settings inheritance in tables

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

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

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

Index inheritance in tables

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

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

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

3.5 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 **Advanced view**, under the selected product's **Operations** branch on the **Policy** tab.

2. Click **Start** to start the selected operation.
3. The operation begins on the host as soon as you have distributed the new policy and the host has fetched the policy file.

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

3.5.1 Remote collection of diagnostics reports

To assist in troubleshooting issues on managed hosts, you can collect diagnostics reports from the managed software remotely in Policy Manager.

To collect the diagnostics from a selected host, you can run the F-Secure Support Tool task on the **Operations** tab in Policy Manager Console. You can only run the operation for one host at a time. Once the log files are collected on the host, they are uploaded to Policy Manager Server and you can download them in Policy Manager Console.

Note: Remote collection of diagnostics only supports F-Secure Client Security versions 12.10 and newer and Email and Server Security versions 12.00 and newer.

3.6 Alerts

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

3.6.1 Viewing alerts and reports

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

When an alert is received, the following button will light up:

To view the alerts:

1. Click the following button:

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

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

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

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

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

3.6.2 Sending alerts by email

You can set Policy Manager to send alerts for the managed environment to one or more recipients by email.

You can send alerts both for Policy Manager Server notifications and for managed hosts. Policy Manager Server alerts are each sent as individual emails, but multiple host alerts can be included in the same email. Policy Manager checks for new alerts that are received from managed hosts every ten minutes.

To set email forwarding for alerts:

1. Select **Tools** > **Server configuration** from the menu.
2. Click **Email alerts**.

3. Enter the email addresses for the recipients.

   All recipients will receive all of the alerts generated by the system.

4. Select either **Host and server alerts** or **Server alerts only** as the alert type to send by email.
5. If you include host alerts, set the minimum alert severity and how many alerts you want to see in individual emails.

   Note: If the number of alerts for the polling period exceeds the selected amount, the email shows you the most recent alerts and prompts you to check the remaining alerts in Policy Manager Console.

6. Click **OK**.

The following server alerts are sent:

- `Anti-virus databases are <n> days old`: security alert, generated when the antivirus definition databases are more than 5 days old.
- `Anti-virus database version is unknown`: warning, generated if the database version cannot be detected, for example if Policy Manager cannot connect to the Automatic Update Agent.
- `Software Updater databases are <n> days old`: security alert, generated if the Software Updater databases are more than one week old.
- `Software Updater databases are missing`: security alert, generated if there is no Software Updater database available on Policy Manager.
- `<n> new host(s) waiting to be imported`: warning, generated if there are new hosts that do not match any import rule and are waiting to be imported manually.
- `<n> unmanaged host(s) discovered`: warning, generated when new, unmanaged hosts are detected.
- `Upgrade available: <product name> <product version>. To see more information and get the upgrade, go to <link to the download page>.` This message is sent whenever a new upgrade is available for Policy Manager or any of your managed F-Secure applications.

The host alerts vary according to the managed software that triggers them.

Logging information on the forwarded alerts is stored to the following file: `<F-Secure installation folder>\Management Server 5\logs\fspms-alert-forwarding.log`.

3.6.3 Forwarding alerts to syslog server

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

Currently, both TCP and UDP transport protocols are supported.

To configure alert forwarding:

1. Select **Tools** > **Server configuration** from the menu.
2. Click **Syslog**.
3. Select **Forward alerts to syslog** and enter the server address.

   By default, alerts are forwarded to syslog using UDP port number 514. If you want to use a different port, enter the port number after the server address, for example, `example.com:8080`.

4. Select the message format.

   Syslog (RFC 3164), **Common Event Format**, and **Log Event Extended Format (LEEF)** messages are supported.

5. Click **OK**.

3.6.4 Configuring alert forwarding for a specific domain

In addition to the alert forwarding that applies to your whole managed network, you can also use domain-specific settings.

Note: To see all configured alert forwarding, select **Tools** > **Alert forwarding** from the menu.

1. Right-click the domain that you want to configure on the **Domain tree**.
2. Select **Alert forwarding for domain** in the context menu.
3. To send email alerts for the domain:

   a) Select **Forward alerts via email** on the **Email alerts** tab.

b) Enter the recipient email addresses.
c) Select the type and severity of alerts to send, as well as the language for the sent emails.

4. To send alerts for the domain to a syslog server:
   a) Select **Forward alerts to syslog server** on the **Syslog** tab.
   b) Enter the server address to use and select the message format and protocol.
5. If you want to use a different mail server than the default one, select **Use custom mail server** on the **Mail server** tab and enter the required details.
6. Click **OK**.

3.7 Reporting tool

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

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

3.7.1 Viewing and exporting a report

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

To use the **Reporting tool**:

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

   Alternatively:

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

   The **Reporting tool** opens.
2. Select the domains and/or hosts you want to include in the report.
   - Select **Recursive** if you want all hosts under the selected domains to be included in the report.
3. Select the report type.
4. Select the products to include in the report, if necessary.
5. Select report type-dependent configurations for the currently selected report, if necessary.
6. View or export the report:
   - Click **View** in the bottom pane to generate the report and view it in HTML format with your default web browser. If no default web browser has been defined, a dialog box appears prompting you to define your web browser.
   - Click **Export** in the bottom pane to generate the report and save it as a file. The file path and report format are defined in the **File save** dialog box that appears after clicking **Export**.

3.8 Using data mining to get information about managed hosts

The Data mining feature in Policy Manager provides an advanced tool to find and browse information to help resolve issues and create queries for use in custom reports and external monitoring systems.

The data that Policy Manager collects from managed endpoints includes information about blocked malware, malicious sites, and other incidents. In addition, each host reports statistics on the endpoint protection state, platform information, missing software updates, and so on.

Data mining allows you to run queries that drill down through the large amount and variety of data to find what you need to resolve issues quickly. It also gives you the flexibility to dynamically group and analyze your managed hosts independent of the domain structure.

Data mining applies two levels of filtering to the data collected from hosts: data sets and properties. The four types of data set currently available are hosts, alerts, software updates, and deleted hosts. The available properties vary according to the selected data set, and only the relevant property filters are shown. You can also use the search functionality to find matches from any relevant item properties, including those that have unique values such as GUID, WINS, and IP addresses.

Items from one data set typically have related items in another data set, for example hosts can be linked to alerts or software updates. For example, after filtering a subset of Windows 7 hosts, you can link them to missing software updates

for analysis. Alternatively, you can filter only servers and check the subset of real-time protection alerts, then go to missing software updates to verify if any similar patches are missing.

The results of your queries are available for exporting in CSV format, and you can save any queries for later use and publish them to create custom reports for Web Reporting. You can also use published queries for use in external monitoring systems via REST API.

Related Tasks

Re-indexing search data on page 51
The search index in Policy Manager uses the Apache Solr framework and provides data for Web Reporting, Data mining, and other functionality within the product.

3.8.1 Running queries on managed endpoint data

You can use the data set and property filters in Data mining to create queries that find matching hosts and other information in your managed network.

1. Select **Root** on the **Domain tree**.
2. Select the **Data mining** tab.
3. Click **Data set** and select the type of data set that you want to examine.

   Note: You can also click **Search** to match details from any data set or properties to the text that you enter.

   The item counter shows how many total results are found, and the property filters are updated according to the selected data set value.
4. Click the properties to select the filters for your query.

   For properties that contain multiple values, you can click the pin icon to show that property as a widget on the page. This can be useful to see the correlation between the properties and if you want to see the filter values as part of the query results.

   Note: The property filters show the 100 most frequent values. If a value is not listed, enter it manually.
5. Click the **Found** link to see the query results.

   By default, the first 10 results are shown. Click **Set limit** if you want to change how many results are shown.

   The results include the data for all applicable properties. If you want to change what information is shown, click **Select fields** and choose the fields for each type of data set.
6. If you want to see other data sets relating to your current query, click **Show related alerts**, **Show related hosts**, or **Show related software updates**, depending on the current data set.
   The selected data set is added below your initial query results.
7. To export the results of any selected data set as a CSV file, click **Export data** and enter a file name.
8. Click **Save query** and enter a name for the new query if you want to use it again later or publish it for use in reports.

   To replace an existing query, select the query from the list and click **OK**.

   All selected properties and related data sets included in your query are saved and available under **My queries**.

3.8.2 Publishing saved queries for reports and external use

You can publish saved Data mining queries to view the results in Web Reporting and to generate API calls for use in external monitoring systems.

1. Select **Root** on the **Domain tree**.
2. Select the **Data mining** tab.
3. Click **My queries**.
   This lists your currently saved queries and their status. Only published queries are available for reports and use via API.
4. Select the query that you want to use.
5. To view the query results in Web Reporting, click **Open as report**.
   This opens Web Reporting in your default browser and shows you the selected custom report.
6. To get the URL for an API call that you can use in external systems, click **Copy API URL**.

Select the type of API call that you want:

- **Query output as JSON**: Use this if you want an API call that returns the full query results in JSON format.
- **Items as CSV**: Use this if you want an API call that returns the query results for a single data set.
- **values as CSV**: Use this if you want an API call that returns the set of values for a single property. This is only available for properties that you have pinned in the query.

The selected API URL is copied to your clipboard.

3.8.3 Example of using data mining

This example shows you how to find managed hosts that match specific parameters and what alerts those hosts have generated.

The example query given here shows the Windows 10 hosts that have F-Secure Client Security Premium 14.20 installed and are missing critical software updates, as well as the infection alerts that these hosts have generated.

1. Select **Root** on the **Domain tree**.
2. Select the **Data mining** tab.
3. Click **Data set** and select **Hosts**.
4. Click **Operating system** and select **Windows 10**.
5. Click **Software Updater status** and select **Critical updates missing**.
6. Click **Product** and select **Client Security Premium 14.20**.
7. Click the **Found** link to see the list of matching hosts and their details.
8. Click **Show related alerts**.
9. Click **Alert type** and select **Infection**.
10. Click the **Found** link to see details of the infection alerts for the matching hosts.

3.9 How to check that the network environment is protected

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

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

3.9.1 Checking that all the hosts have the latest policy

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

1. Select **Root** on the **Domain tree**.
2. Go to the **Dashboard** > **Summary** tab and check how many hosts of the entire domain have the latest policy.
3. If all hosts do not have the latest policy, click **View hosts' latest policy update**.
   This takes you to the **Status** tab and **Centralized management** page.
4. On the **Centralized management** page, check which of the hosts do not have the latest policy.

   You can also see the possible reasons for this; for example, the host is disconnected or there has been a fatal error on the host.

3.9.2 Checking that the hosts have the latest virus definitions

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

1. Select **Root** on the **Domain tree**.
2. Go to the **Dashboard** > **Summary** tab and check what is displayed in the **Virus protection for endpoints** section beside **Virus definitions**.
3. If the virus definitions on some hosts are outdated, there are two alternatives:

   - You can select the **Status** tab and the **Overall protection** page to see which hosts do not have the latest virus definitions. Then select these hosts in the **Policy domains** tab, go to the **Operations** tab and click **Update virus definitions**. This orders the selected hosts to fetch new virus definitions at once.

- Alternatively, click the **Update virus definitions** link. This takes you to the **Operations** tab. Once on the **Operations** tab, click **Update virus definitions**. This orders all hosts to fetch new virus definitions at once.

3.9.3 Checking that there are no disconnected hosts

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

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

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

3.9.4 Viewing scanning reports

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

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

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

3.9.5 Viewing alerts

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

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

When an alert is received, the following button will light up:

To view the alerts:

1. Click the following button:

   Alternatively, you can click **View alerts by severity** on the **Dashboard** > **Summary** tab.

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

Ack	Click the **Ack** button to acknowledge an alert. If all of the alerts are acknowledged, the **Ack** button will be dimmed.
Severity	The problem's severity. Each severity level has its own icon:

		Info	Normal operating information from a host.
		Warning	A warning from the host.
		Error	Recoverable error on the host.
		Fatal error	Unrecoverable error on the host.
		Security alert	Security hazard on the host.
Date/Time	Date and time of the alert.		
Description	Description of the problem.		
Host/User	Name of the host/user.		
Product	The F-Secure product that sent the alert.		

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

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

3.9.6 Creating a weekly infection report

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

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

3.9.7 Monitoring a possible network attack

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

1. Select **Root** on the **Domain tree**.
2. Go to the **Dashboard** > **Summary** tab.
3. Check what is displayed beside **Most common latest attack**.
4. If there has been an attack, you can access more detailed information by clicking **View Internet Shield status**. This takes you to the **Status** tab and **Internet Shield** page, where you can see detailed information on the latest attacks on different hosts.

Chapter

4

Maintaining Policy Manager Server

Topics:

- Malware definition updates
- Backing up and restoring Policy Manager data
- Creating the backup
- Restoring the backup
- Restoring an automatically saved backup on Linux
- Exporting and importing signing keys
- Replicating software using image files
- Re-indexing search data
- Running the database maintenance tool

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

4.1 Malware definition updates

Version 13.00 of Policy Manager introduces a new protocol for distributing updates to all F-Secure products.

Compared to the previous approach to distributing updates (with Automatic Update Agent), the new protocol provides considerable benefits in bandwidth consumption and ease of maintenance. Policy Manager now only downloads updates that are required for the client software installed on managed hosts. For example, if you do not have any managed server software, any updates for such products are not downloaded.

Updates for older clients are not downloaded if the managed environment has no clients with an AUA component of version 9.x or older.

The server maintains a cache of downloaded updates, which typically takes up to 2-3 GB of disk space.

Each update is downloaded only when requested by the managed client software. The process for the on-demand downloading of updates is typically as follows:

1. The server regularly refreshes the metadata for the latest F-Secure updates. By default, this happens every 10 minutes.
2. Clients regularly poll the server to check if new updates are available.
3. When a client notices a new update, it requests the data.
4. The server accepts the request and starts downloading the update from the Internet asynchronously. The server also instructs the client to check the update status again in roughly 10 minutes.
5. The client receives the requested update the next time it polls the server.

If a client was shut down for a very long time and the F-Secure cloud cannot determine the incremental updates for the old definitions, it instructs the server to send the full update archive to the client.

Migration and file locations

Automatic Update Agent (AUA) is no longer installed as part of Policy Manager. The AUA configuration file, which was previously used as the HTTP proxy source for Internet connections, is now replaced with the `fspms.proxy.config` file. The proxy settings are migrated during upgrade.

On Windows, AUA is automatically uninstalled during upgrade if it is no longer needed for other products, such as Server Security, that are installed on the same machine. On Linux, you need to uninstall AUA manually if it is no longer needed, for example for Linux Security.

Note: Only the first proxy is migrated, multiple HTTP proxies are no longer supported. This also means that there is no fallback to a direct Internet connection when a HTTP proxy is defined.

The locations of configuration and log files are as follows:

HTTP proxy configuration file	This is located under the server's data folder: • Windows: `<F-Secure installation folder>\Management Server 5\data\fspms.proxy.config` • Linux: `/var/opt/f-secure/fspms/data/fspms.proxy.config`
Log files	Downloading and distribution events are logged to `fspms-download-updates.log` and `fspms-serve-updates.log` files, which can be found under the server's logs folder: • Windows: `<F-Secure installation folder>\Management Server 5\logs` • Linux: `/var/opt/f-secure/fspms/logs`
Downloaded updates	The downloaded updates are stored in the following folder: • Windows: `<F-Secure installation folder>\Management Server 5\data\guts2\updates` • Linux: `/var/opt/f-secure/fspms/data/guts2/updates`

Migrated data

The list of updates needed for version 12 and older clients, which was previously stored in the AUA configuration file, is migrated to `channels.json`:

- Windows: `<F-Secure installation folder>\Management Server 5\config\channels.json`
- Linux: `/opt/f-secure/fspms/config/channels.json`

4.1.1 Checking the malware definitions on Policy Manager Server

You can check the status and distribution of malware definitions on the Dashboard tab.

1. Go to the **Dashboard** tab.
2. Click **Show details** in the upper-right section of the page.
   This opens the update status view. The downloaded updates for version 13 clients and version 12 or older are shown on separate tabs. If there are no clients of one of these versions within your managed network, the corresponding tab is empty.

4.1.2 Updating malware definitions in isolated networks

Policy Manager offers two options for updating virus definitions in isolated networks that have no direct connection to the Internet.

If your network configuration allows Policy Manager to access internal resources, which in turn can access the Internet, we recommend that you use Policy Manager Proxy as the source for updates.

If using Policy Manager Proxy is not permitted, you can use a tool provided with Policy Manager to fetch the updates as an archive and copy that to the server where Policy Manager is installed.

Using Policy Manager Proxy to update malware definitions

If your network setup does not allow Policy Manager to connect to the Internet, but allows connections to internal resources that can access the Internet, you can use Policy Manager Proxy to keep the malware definitions up to date.

This is the most convenient option for isolated networks, as it does not require any subsequent actions after you have set up Policy Manager Proxy and completed the configuration in Policy Manager.

To minimize network communication between Policy Manager Proxy and Policy Manager Server, you can now install the proxy in standalone mode. This mode makes Policy Manager Proxy fully autonomous:

- It does not need access to Policy Manager Server
- It does not serve any client requests except for downloading malware definitions

To set up Policy Manager Proxy for an isolated network:

1. Start the installation of Policy Manage Proxy (version 13.10 or higher) on a host that has Internet access to the F-Secure update service (http://guts2.sp.f-secure.com).
2. To activate standalone mode, use a `0.0.0.0` loopback interface IP as the Policy Manager Server address when installing the proxy.
3. Configure Policy Manager Server to use the proxy as the source for virus definitions.
   a) Open the additional Java arguments configuration:
      - On Windows, open the registry and go to `HKLM\SOFTWARE\Wow6432Node\Data Fellows\F-Secure\Management Server 5\additional_java_args`.
      - On Linux, open the `fspms.conf` configuration file and look for the additional_java_args parameter.

   b) Edit the string value for **additional_java_args**.
      Add the following value:

```
-Dguts2ServerUrl=http://<proxy_address>/guts2
```

4. Restart the Policy Manager Server service (`fspms`).

Using archives to update malware definitions

When you cannot use a connection to an intermediate proxy due to security policies, you can update the malware definitions using the tool provided with Policy Manager.

The tool for downloading updates is bundled with Policy Manager and can be extracted with the provided scripts. When you run it on any machine with internet access, the tool downloads the latest updates and required diffs to generate an all-in-one archive.

You can import the generated archive to a Policy Manager Server that is configured to not connect to the Internet for requested definitions updates, but to instead distribute only updates that are imported from the archive.

By default, the tool uses the `data\updates` folder to store the downloaded update binaries. It also stores the update history to use as a reference for downloading the relevant diffs to the latest version.

The version history is important for the tool, as it defines the number of diffs to provide to Policy Manager and then serve to managed clients. The default history depth is 10 and is modified using the update_diffs_count property. The longer the history, the more time it takes to download diffs from F-Secure Cloud, because it takes time to generate the diffs from older versions. You can configure the number of download attempts and the time between them in `configuration.properties`.

The process can be automated by scheduling the download and subsequent import operations. You can customize the path to the updates archive to make it easier to transfer, for example using a shared network drive.

Note: Make sure that Policy Manager Server has permission to delete the updates archive, as it removes it after completing the import.

To update the malware definitions:

1. Prepare the tool.

   Note: You have to prepare the tool the first time before you use it. To update the malware definitions later, you only have to run the tool (step 3).

   a) Run the following command to prepare the tool.

      Running the tool only works on the same platform that you use to prepare the tool. For example, if you prepare the tool on a Linux computer, the tool only works on Linux versions of Policy Manager.

      - Windows: `<F-Secure installation folder>\Management Server 5\bin\prepare-fspm-definitions-update-tool.bat <destination folder>`
      - Linux: `/opt/f-secure/fspms/bin/prepare-fspm-definitions-update-tool <destination folder>`

   b) Modify the tool configuration, if necessary.

      - `conf\channels.json`: this contains a list of the channels to be updated. By default, it includes updates for all the supported clients managed by Policy Manager, so we recommend that you leave only those that are necessary for your environment.
      - `conf\configuration.properties`: among other settings, you can specify a HTTP proxy here, if needed.

   c) Transfer the prepared binaries to a machine that has Internet access.

2. Prepare the environment.

   a) Open the additional Java arguments configuration to configure Policy Manager Server to run in isolated mode.

      - On Windows, open the registry and go to `HKLM\SOFTWARE\Wow6432Node\Data Fellows\F-Secure\Management Server 5\additional_java_args`.
      - On Linux, open the `fspms.conf` configuration file and look for the additional_java_args parameter.

   b) Edit or add the string value **additional_java_args** with the following value: `-DisolatedMode=true` to the Java arguments configuration.

   c) Restart Policy Manager Server to switch it to isolated mode

3. Transfer updates.

   a) Run the tool.

- Windows: `fspm-definitions-update-tool.bat`
- Linux: `fspm-definitions-update-tool`

The resulting archive contains the full set of the latest definitions and diffs to this version. If all data is up to date, no archive is generated.

b) Transfer the prepared archive (`data\f-secure-updates.zip` by default) to the Policy Manager Server machine.

Note: Do not change the archive file name or destination path, as they are hardcoded.

- Windows: `<F-Secure installation folder>\Management Server 5\data\f-secure-updates.zip`
- Linux: `/var/opt/f-secure/fspms/data/f-secure-updates.zip`

c) Run the following command to import the prepared updates.

- Windows: `<F-Secure installation folder>\Management Server 5\bin\import-f-secure-updates.bat`
- Linux: `/opt/f-secure/fspms/bin/import-f-secure-updates`

Updating malware definitions on isolated Client Security hosts

If you have installed Client Security on hosts that do not have a network connection, you can update the malware definitions using the tool provided with Policy Manager.

Note: This procedure applies to Client Security versions 13 and newer and to Client Security for Mac versions 15.00 and newer.

The tool for downloading updates is bundled with Policy Manager and can be extracted with the provided scripts. When you run it on any machine with internet access, the tool downloads the latest updates and required diffs to generate an all-in-one archive.

By default, the tool uses the `data\updates` folder to store the downloaded update binaries. It also stores the update history to use as a reference for downloading the relevant diffs to the latest version.

In addition to the update binaries, you also need the `fsaua-update` tool to import the prepared updates. This tool is included in the Client Security installation package: `C:\Program Files (x86)\F-Secure\Client Security\fsaua-update.exe`.

To update the malware definitions:

1. Run the following command on the Policy Manager machine to prepare the tool:
   - Windows: `<F-Secure installation folder>\Management Server 5\bin\prepare-fspm-definitions-update-tool.bat <destination folder>`
   - Linux: `/opt/f-secure/fspms/bin/prepare-fspm-definitions-update-tool <destination folder>`
2. Transfer the prepared binaries to a machine that has internet access, if necessary.
3. Modify the tool configuration, if necessary:
   - `conf\channels.json`: this contains a list of the channels to be updated. By default, it includes updates for all the supported clients managed by Policy Manager, so we recommend that you leave only the Client Security versions necessary for your environment.
4. Run the tool:
   - Windows: `fspm-definitions-update-tool.bat`
   - Linux: `fspm-definitions-update-tool`

   The resulting archive contains the full set of the latest definitions and diffs to this version. If all data is up to date, no archive is generated.
5. Transfer the prepared archive (`data\f-secure-updates.zip` by default) to the isolated host: directory on the isolated Client Security host.

- Client Security: Transfer the archive to the `C:\Program Files (x86)\F-Secure\Client Security` directory on the host.
- Client Security for Mac: Transfer the archive to any convenient directory on the host.

6. Launch the update on the isolated host:
   - Client Security: Run `C:\Program Files (x86)\F-Secure\Client Security\fsaua-update.exe` with administrator privileges.
   - Client Security for Mac: Run `sudo /usr/local/f-secure/bin/guts2-standalone-update --updateFile <path to f-secure-updates.zip>`.

4.2 Backing up and 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.

You can set Policy Manager to automatically backup the server data on a regular schedule. You can choose when the backups should be taken and how many backups you want to store - as more backups are created, the oldest ones are deleted.

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

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

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

4.3 Creating the backup

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

Any backups you take are stored in the `<F-Secure installation folder>\Management Server 5\data\backup` folder.

1. Select **Tools** > **Server configuration** from the menu.
2. Select **Backup**.
3. To set up a schedule for automatic backups:
   a) Select **Enable automatic backup**.
   b) Select either a **Daily** or **Weekly** backup schedule and select when you want the automatic backups to be taken.
4. Select how many backups you want to keep.
5. If you want to take a backup immediately, click **Backup now**.
6. Click **OK**.

4.4 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 contents of the backup that you want restore from the `<F-Secure installation folder>\Management Server 5\data\backup` folder to the `<F-Secure installation folder>\Management Server 5\data\h2db` folder.
3. Restart the Policy Manager Server service.
4. Reopen the Policy Manager Console management sessions.

4.5 Restoring an automatically saved backup on Linux

If necessary, you can restore a backup of Policy Manager's H2 database, which contains your domain and policy data.

When you set Policy Manager to automatically take regular backups of the H2 database, the backup files are stored in the `var/opt/f-secure/fspms/data/backup` folder, with the individual backup files named by date and time (`<yyyy_mm_dd_nn_nn_nn>.backup.zip`).

To restore the backup data:

1. Stop the Policy Manager service:

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

2. Check that the Policy Manager Java process is stopped:

   ```
   # ps -efl | grep java
   ```

   If the process is still running, wait until it shuts down completely or check the process again after a while.

3. Overwrite the `fspms.h2.db` file under `/var/opt/f-secure/fspms/data/h2db` with the corresponding file from the zipped backup.
4. Restart the Policy Manager service.

4.6 Exporting and importing signing keys

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

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

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

   To export your current signing keys:

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

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

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

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

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

4.7 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.

Client Security 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.

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 Client Security.
2. Configure Client Security 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. Use the `C:\Program Files (x86)\F-Secure\Client Security\BusinessSuite\resetuid.exe` utility to reset the unique ID for the distributable image.

   Note: For Client Security version 13.x clients, you need to run the command as `C:\Program Files\F-Secure\Common\fsmautil resetuid` from the command prompt. The directory may be different if you are using a localized version of Windows or if you have specified a non-default installation path.

   For Client Security and Server Security version 14.x clients, the distributable image must use a different ID generation method than the original installation package:

   a) Run the following command to check the current ID method: `C:\Program Files (x86)\F-Secure\Client Security\BusinessSuite\resetuid.exe showuid`
   b) Reset the unique ID to use a different ID generation method.
      For example, if the current ID uses `SMBIOS`, run the following command to reset to `RANDOMGUID`: `C:\Program Files (x86)\F-Secure\Client Security\BusinessSuite\resetuid.exe resetuid randomguid`

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 Client Security 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.

4.8 Re-indexing search data

The search index in Policy Manager uses the Apache Solr framework and provides data for Web Reporting, Data mining, and other functionality within the product.

The search index data in itself is not included in the product backups, although the data that it uses to compile the index is. In some cases, you may need to re-index the data to ensure that the Data mining feature and Web Reporting are working properly.

1. Select **Tools** > **Server configuration** from the menu.
2. Click the **Search index** tab.
3. Click **Re-index data**.
   This recompiles the data for the search index from the H2 database and event files.

4.9 Running the database maintenance tool

Policy Manager includes a database maintenance tool that optimizes and checks the integrity of your database.

Note: Before running the maintenance tool, check that there is enough free disk space available on the computer where Policy Manager is installed. The disk space requirements for the maintenance tool depend on the size of your database, but as a guideline you should have at least twice as much free space as the size of your database.

Database maintenance is automatically started as part of any Policy Manager upgrade or re-installation to ensure that the database structure is compatible with the latest version.

The maintenance tool creates a backup of your database, after which it verifies the database integrity and then applies the updated schema to the contents of the database. It also cleans up any invalid data to optimize the size and performance of the database.

To run the database maintenance tool manually:

1. Stop the Policy Manager service.
2. Start the maintenance tool.
   - On Windows, run `<F-Secure installation folder>\Management Server 5\bin\fspms-db-maintenance-tool.exe`. When the maintenance tool opens, click **Start maintenance**.

- On Linux, run the `/opt/f-secure/fspms/bin/fspms-db-maintenance-tool` script.

The progress and details of the maintenance steps are shown.

Note: The maintenance tool may skip some of the maintenance steps, for example if the database schema is already up to date. However, the overall maintenance can still be successful even with skipped steps.

3. On Windows, after the maintenance steps have run, click **Close**.
4. Restart the Policy Manager service.

If the maintenance is not successful, no changes are applied to the database and Policy Manager Server is not started.

4.9.1 Database maintenance troubleshooting

This section describes some of the warnings that may appear when running the database maintenance tool and how you can resolve them.

Note: In addition to the critical issues and warnings listed here, the integrity verification step is skipped if the database revision is unknown. This does not stop the maintenance process; the tool proceeds to run the remaining steps.

Critical issues

If a critical error occurs during the maintenance process, the remaining steps are skipped and no changes are applied. In addition, when you close the maintenance tool, Policy Manager Server does not start up automatically; this is to prevent upgrading the database schema so that the original database remains intact.

Backup

If the maintenance tool cannot create a backup of the database, it is most likely due to insufficient free disk space. If this happens:

1. Finish the setup.
2. Free up some additional disk space.
3. Run the maintenance tool manually.
4. Start the Policy Manager Server service.

Integrity verification

This step fails with a critical error only when the management keys or domain tree tables cannot be processed. In the latter case, the tool exports the management keys to the Policy Manager Server data folder (the path is shown in the details dialog), so that you can import this key pair into a fresh database to avoid re-deploying the clients or using a key replacer tool.

If the integrity check of the critical tables fails, then the previous installation was most likely already broken. If this occurs, we recommend that you delete the corrupt database, start Policy Manager Server and import the rescued or previously exported management key pair to a newly created database. You can also contact technical support and provide a copy of the database backup to see if it can be rescued.

You can also try running the maintenance tool on an earlier backup:

1. Finish the setup.
2. Check that the Policy Manager Server service has stopped.
3. Copy the earlier backup to the Policy Manager Server data folder, replacing the broken database.
4. Run the database maintenance tool.

Database schema upgrade

A critical error during this step may be due to insufficient disk space. If this is the case, free up some additional disk space and run the maintenance tool on the backup that it created during the upgrade.

If a critical error occurs during this step, and your previous installation of Policy Manager was working, you can revert to the previous version as follows:

1. Finish the setup.
2. Uninstall Policy Manager.
3. Restore the original database from the backup copy.
4. Install the previous version of Policy Manager.

You can also try running the maintenance tool on an earlier backup, as described for issues in the integrity verification step.

If a critical error occurs during this step, we recommend that you create a support ticket that includes the broken database.

Warnings

If there are any issues during the maintenance process that prompt a warning, the process will still continue, but a warning icon is shown for the step and details are given in a separate dialog.

Integrity verification	• A warning is displayed if non-critical data is lost during this step. • This may be due to insufficient disk space. If this is the case, you can free up some additional disk space and run the maintenance tool on the backup that it created during the upgrade. • If the lost data originated from managed hosts (for example, status, alert, or report data), you do not need to do anything and some of the data will be recovered at some stage. • If the details for the warning indicate a loss of user data (for example, policies, host import rules, or Active Directory rules), you can try running the maintenance tool on an earlier backup. If this does not recover the lost data, the administrator needs to re-enter the data manually in Policy Manager Console.
Database schema upgrade	• There are very few known issues that prompt a warning for this step. • One possible cause is an issue when moving the SMTP server credentials from the database to secure storage. • If any data is lost, you can try running the maintenance tool on an earlier backup once the setup is complete. If this does not recover the lost data, the administrator needs to re-enter the data manually in Policy Manager Console.

Chapter

5

Web Reporting

Topics:

- Viewing reports
- Scheduling reports
- Changing the Web Reporting port

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

Web Reporting provides several standard reports that give detailed information on the status of the managed environment, infections, and software updates. In addition, queries that you create and publish with the Data mining feature are available as custom reports. You can create printable versions of the reports and create schedules for regular delivery of the reports.

The reports use donut, treemap, and bar charts as well as tables to present the data, depending on the report type. For the data presented in tables, you can select the column that is used to sort the data and choose which columns are shown.

Note: The new version of Web Reporting introduced in Policy Manager 15.00 does not include reports configured in previous versions. If you have upgraded from a previous version of Policy Manager and need to access earlier reports, you can click the link on the Web Reporting login page.

Related Tasks

Re-indexing search data on page 51
The search index in Policy Manager uses the Apache Solr framework and provides data for Web Reporting, Data mining, and other functionality within the product.

5.1 Viewing reports

Web Reporting includes several standard reports and also shows any custom reports based on Data mining queries that you have published in Policy Manager Console.

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

1. 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 open it from the **Start** menu: **Start** > **F-Secure Policy Manager Server** > **Web Reporting**.
2. Enter your Policy Manager Console user name and password to log in if prompted.
   The Web Reporting page opens, showing a list of the available reports. Each report has a category tag: **Environment**, **Malware protection**, **Software updates**, or **Custom report**. Reports under the **Custom report** category are based on published Data mining queries. The other report categories are for the standard set of reports.
3. Select one of the listed reports.
   The selected report opens. The data presented depends on the report. Custom reports show the data in tables, while standard reports may include both table data and charts.
4. Modify the report settings and presentation if necessary:
   - To change the domain scope of the report, click the scope selector at the top of the page and select a domain. By default, the scope is set to **Root** when you open Web Reporting.
   - If you want to see the reported data for a different time period, select **Last 24 hours**, **Last 30 days**, **Last 7 days**, or **Last 90 days** from the **Time period** drop-down menu.
   - To change what columns are shown in a report table, click the column icon and select or clear the columns as needed.
   - Click the sort icons on any table columns to change how the data is sorted.
   - Some reports contain clickable links, for example to show host details or descriptions for software updates.
5. To view a printable version of a report, click **Print**.
   This opens the report in a new tab for printing.

5.2 Scheduling reports

You can configure Web Reporting to send regular reports by email to one or more recipients.

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

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

To configure the report scheduling:

1. On the Web Reporting main page, click the **Schedules** icon.
2. Click **Create schedule**.
3. Select the domain, reports, frequency, and language for the scheduled report delivery.

   Note: You cannot schedule reports for individual hosts, only for domains. You can use the root domain if you want the reports to cover all configured domains.
4. In the **Recipients** field, enter the email addresses that should receive the reports.

   Use semi-colons to separate multiple addresses.
5. Click **Save**.

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

If you want to check that the report emails are delivered correctly, click the action button for the report and select **Send reports now**.

5.3 Changing the Web Reporting port

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

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

1. Stop Policy Manager Server.
2. Open the `HKEY_LOCAL_MACHINE\SOFTWARE\Data Fellows\F-Secure\Management Server 5` registry key.

   On 64-bit operating systems, the registry key path is `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data Fellows\F-Secure\Management Server 5`.
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.

Chapter

6

Policy Manager Proxy

Topics:

- Overview
- Setting up Policy Manager Proxy
- Centralized management of Policy Manager Proxy

This section provides a brief introduction to installing and using Policy Manager Proxy in your managed network.

6.1 Overview

Policy Manager Proxy reduces the load on networks to solve bandwidth problems in distributed installations of Client Security.

Policy Manager Proxy offloads heavy traffic from the master server to optimize costly, high-latency traffic. For example, the proxy node gets the necessary installation packages for software updates from the master server, and the managed hosts then retrieve the packages from the proxy node. This means that the master server no longer needs to handle the distribution load.

Secure connections are used both between hosts and proxy, and proxy and master server. This means that the proxy node certificates must be pre-configured. Managed hosts connect to the configured proxy nodes using the Policy Manager Proxies table.

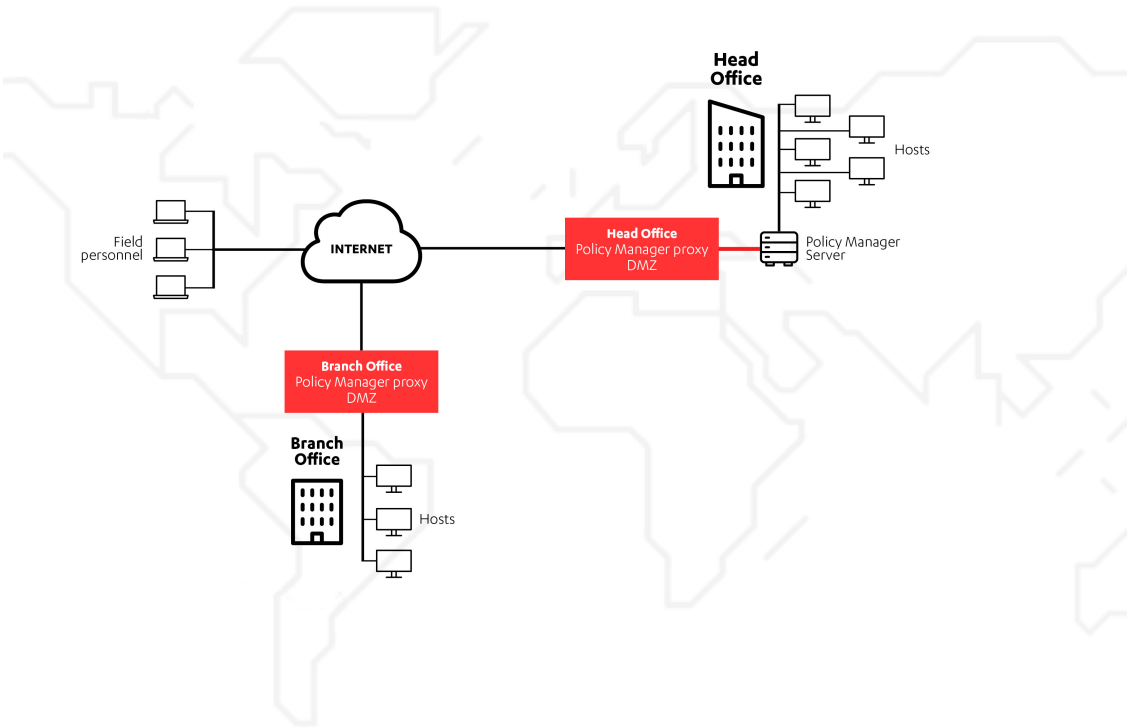
Note: Although the installation packages are distributed to hosts by the proxy node, Software Updater XML databases are always downloaded from the master Policy Manager Server. This traffic always bypasses proxy nodes.

Policy Manager Proxy can be configured to function as a reverse proxy. The proxy type defines if data requested by hosts, such as anti-virus definitions and software updates, is retrieved directly from the internet or from the configured upstream Policy Manager or other proxy. Forward proxy is used to decrease traffic between networks, for example a branch office and headquarters. Reverse proxy is used in environments where the proxy has no direct connection to the internet, for example. Reverse proxy is also used to decrease the load on the master server (or other forward proxy). By default the proxy is installed in forward mode.

6.1.1 When should you use Policy Manager Proxy?

You do not have to use Policy Manager Proxy in your managed network, but it can provide certain advantages.

The effects of Policy Manager Proxy are most obvious in large, vastly spread networks; for example, a large corporation with remote offices in different parts of the globe. The following figure is an example of a situation where Policy Manager Proxy is useful:



The benefits of using Policy Manager Proxy include:

- Less network bandwidth consumption. In particular, you should use Policy Manager Proxy when you have a group of workstations that are located far away from your Policy Manager Server.

- Quicker delivery of malware definition updates. This is especially true when you have a group of workstations separated from your Policy Manager Server by a slow connection.
- Less load on Policy Manager Server. In large-scale networks, Policy Manager Proxy can take care of the majority of requests from managed hosts.

In addition to the scenario outlined above, if you are using Policy Manager in a network environment where it has no Internet connection, you can use Policy Manager Proxy to handle malware definition updates.

6.2 Setting up Policy Manager Proxy

Follow these steps to install Policy Manager Proxy for either Windows or Linux.

1. Fetch `admin.pub` from the master Policy Manager:
   - Download it from the master Policy Manager using your browser (`https://<policy manager server IP/host name>:<https port number>`);
   - Export it from Policy Manager Console; or
   - Retrieve it from the host if the Policy Manager Proxy host is already running Server Security or Linux Security and is connected to the master Policy Manager.
2. Run the Policy Manager Proxy installer.
3. When prompted, enter the path to the retrieved `admin.pub` file.
4. Enter the credentials for your administrator account on the master Policy Manager Server.

   This is required for authorizing the enrollment of the TLS certificate.
5. Complete the installation wizard.

   Note: By default the proxy is installed in forward proxy mode. To switch to reverse mode:
   - On Windows, open the registry, go to `HKLM\SOFTWARE\Wow6432Node\Data Fellows\F-Secure\Management Server 5\additional_java_args` and specify the following parameter: `-DreverseProxy=true`.
   - On Linux, set the following additional Java argument in the `fspms.conf` configuration file, after the additional_java_args parameter: `-DreverseProxy=true`.

   In forward mode, the proxy downloads database and Software Updater updates from the internet. In reverse mode, the proxy downloads the updates from the Policy Manager Server.

   You can check that the installation was successful by going to the Proxy welcome page (`https://proxy_name:<HTTPS_port>`, where `<HTTPS_port>` is the HTTPS port that you entered during installation) in your browser.
6. Specify the HTTP proxy configuration if the Policy Manager Proxy host does not have a direct internet connection.

   Note: The HTTP proxy that you configure is only used when Policy Manager Proxy is installed in forward proxy mode, and only for internet connections. Connections to Policy Manager (to communicate certificates, policies, and status, for example) are made directly to the Policy Manager Server. In reverse proxy mode, all connections are made directly to the Policy Manager Server.

   a) Edit the HTTP proxy configuration file.
      - Windows: `<F-Secure installation folder>\Management Server 5\data\fspms.proxy.config`
      - Linux: `/var/opt/f-secure/fspms/data/fspms.proxy.config`

   b) Add the proxy as a new line, using the following format:
      `http_proxy=[http://][user[:password]@]<address>[:port].`

      Use percent encoding for any reserved URI characters in the user name or password. For example, if the password is `ab%cd`, you need to enter it as follows:
      `http_proxy=http://user:ab%25cd@proxy.example.com:8080/.`

   c) Restart the Policy Manager Server service.

   Note: Policy Manager Proxy supports a single HTTP proxy configuration and there is no fallback to a direct internet connection when an HTTP proxy is defined.

You can now configure endpoints to use the proxy by specifying the priority order of proxy nodes in the Policy Manager Proxy table.

6.3 Centralized management of Policy Manager Proxy

Policy Manager Proxy instances are shown in the Policy Manager domain tree as ordinary hosts with a dedicated icon to distinguish them.

The installed proxies are included alongside other products in the Policy Manager tabs and reports. Installed proxies report their status to the server, and in addition to the basic host properties, the following information is delivered:

- Malware and Software Updater definitions distributed to connected hosts
- Amount of free disk space
- Used disk space by data type
- Statistics of proxied traffic

Policy Manager Proxy receives the following policy settings from Policy Manager Server:

- Communication polling interval
- Maximum disk space allocated to caching Software Updater updates

Installed proxies generate host alerts if the malware or Software Updater definitions are out of date.

Note: If Server Security is installed on the same machine as Policy Manager Proxy, the two products are shown as separate hosts in the domain tree so that they can be organized differently.

Chapter

7

Software distribution

Topics:

- Push installations
- Policy-based installation
- Local installation and updates with pre-configured packages
- Local installation and Policy Manager
- Upgrading managed software

Policy Manager offers many ways to install and update managed software.

The **Installation** tab has shortcuts to all the installation features.

7.1 Push installations

This section describes how to push installation packages to hosts.

Note: Push installation is not supported for Mac clients. The Client Security for Mac installation package is distributed using JAR archives, which administrators can configure with the console's **Remote installation wizard** and export to the hosts for installation.

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 Windows domains or fetches information from an Active Directory server to allow the user to select the target hosts from a list, 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 check that any firewalls do not block access to the target computer. Policy Manager Console uses TCP port 135 for remote procedure call (RPC) access and port 445 for network and file sharing access. The target computer and Policy Manager Console both use Policy Manager Server's host port to report the installation result.

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

Push installation works as follows:

1. Policy Manager Console uploads the installation package to the remote host's admin (`ADMIN$`) share. This requires that file sharing is enabled on the remote host.
2. Policy Manager Console uses the remote procedure call (RPC) service to install and start the push installation service on the target computer with the appropriate parameters. The purpose of this service is to start the installer and to communicate the installation results to Policy Manager.
3. If the installation cannot start, this is communicated directly to Policy Manager Console.
4. When the installation is finished, the results are sent to Policy Manager Server via HTTP. Policy Manager Console polls the server for the results and reports them.

7.1.1 Autodiscover Windows hosts

Target hosts within Windows domains 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 following icon on the toolbar:

3. Select **NT Domains**.
4. From the domain 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.

5. 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.

6. Click **Install** to continue.

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

7.1.2 Autodiscover hosts from an Active Directory server

You can also use the Autodiscover feature to select hosts from an Active Directory server.

To select target hosts:

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

   Alternatively, click the following icon on the toolbar:

3. Select **Active Directory**.
4. Enter the address for the domain server and your user name and password.
5. Click **List hosts**.

   When the list of hosts has been fetched, select **Hide already managed hosts** if you only want to see hosts that do not have any managed software installed yet.

6. Select the hosts to which you want to install managed software.

   If you want to select all the listed hosts, click **Check all**.

7. Click **Install** to continue.

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

7.1.3 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 following icon on the toolbar:

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.

7.1.4 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).

7.2 Policy-based installation

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

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

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

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

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

7.2.1 Using policy-based installation

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

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

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

To use policy-based installation:

1. Open the **Installation** tab.
   On the **Installation** tab, **Policy-based installations** table shows the status of any current installation operations, and the **Installed products summary** table lists the products that are currently installed on managed hosts.
2. Click **Install** under the **Policy-based installations** table to start the remote installation wizard.
3. Complete the remote installation wizard with the necessary details.

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

   Once the remote installation wizard is complete, the installation operation and status will appear on the **Policy-based installations** table as a new row.
4. Distribute the policy.
   Once the installation operation is complete, the product name, version and number of hosts running the product are shown on the **Installed products summary** table.

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

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

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

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

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

7.3 Local installation and updates with pre-configured packages

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

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

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

Note: When configuring and exporting an installation package for Mac hosts, do not rename the exported file, as the file name contains various metadata related to Policy Manager.

7.3.1 Using the customized remote installation package

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

To use a customized installation package:

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

   Policy Manager Console displays the **Remote installation wizards** that collect all necessary setup information for the selected products.

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

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

    a) Copy `ilaunchr.exe` and the exported JAR to a location where the login script can access them.

    b) Enter the command:`ilaunchr <package name>.jar` where `<package name>` is replaced by the actual name of the JAR package being installed.

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

    ILAUNCHR has the following command line parameters:

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

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

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

    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
```

Related Tasks

Importing new hosts on page 28
Another option for adding hosts in Policy Manager Console is to import new hosts.

7.3.2 How to prepare MSI installation packages with Policy Manager for Linux

For version 14.x clients, you can prepare MSI packages for distributed installation within your managed network even if you have both Policy Manager Server and Policy Manager Console running on Linux.

With the Linux version of Policy Manager, you cannot use the base MSI file extracted from the JAR installation package to roll out F-Secure products to Windows hosts. However, you can use a command line tool to prepare the MSI file for distributed installation.

Note: These instructions apply only to Client Security and Server Security versions 14.x.

1. Export the client installation JAR package from Policy Manager Console.
2. Extract the content of the JAR archive on a Windows host.
3. Run the following command:
   - For Client Security: `program\inst\one-launcher.exe --install --prepare_msi_only --msi OneClientCS.msi`
   - For Server Security: `program\inst\one-launcher.exe --install --prepare_msi_only --msi OneClientSS.msi`

   The correct command is also given as the `preparemsicommand` property in the `package.hdr` file, which you can find in the root folder of the extracted content.

   This command updates the `.msi` file given as the parameter for the `--msi` option. You can use this prepared MSI file to distribute the F-Secure product to Windows hosts in your network.

If the target MSI package is not updated, the log file may be useful for troubleshooting purposes. The location of the log file depends on your access rights when running the preparation command:

- With administrator rights and user access elevation:
  `C:\ProgramData\F-Secure\Log\BusinessSuite\one-launcher.u.log`
- Without user access elevation:
  `C:\Users\user\AppData\Local\F-Secure\Log\BusinessSuite\one-launcher.u.log`

7.4 Local installation and Policy Manager

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

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

7.4.1 System requirements

Read the following before starting to use the product.

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

Processor:	• Intel Pentium 4 2 GHz or higher

Operating system:	• Windows 7, 32-bit and 64-bit • Windows 8.1, 32-bit and 64-bit • Windows 10, 32-bit and 64-bit **Note:** You need to have the latest Service Pack installed for your operating system. **Note:** You need Windows Universal C Runtime installed before you install the product.
Memory:	• 1 GB of RAM or more for 32-bit operating systems, 2 GB or more for 64-bit operating systems
Disk space:	2 GB free hard disk space
Internet connection:	Required to receive updates and use cloud-based features

7.4.2 Installation steps

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

To install the product:

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

   Policy Manager Console displays the **Remote installation wizards** that collect all necessary setup information for the selected products.

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

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

7.5 Upgrading managed software

You can remotely upgrade F-Secure anti-virus software already installed on hosts by using the **Installation editor**.

The editor creates policy-based installation tasks that each host in the target domain will carry out after the next policy update.

Note: It is also possible to upgrade Client Security by using any other installation scheme.

Chapter

8

Managing endpoint security

Topics:

- Migration of Email and Server Security settings
- Configuring virus and spyware protection
- Configuring firewall settings
- Configuring application control
- How to protect your users' sensitive data
- Blocking unsuitable web content
- Using Device Control
- Managing software updates
- Rapid Detection & Response

This section contains information on how to configure F-Secure endpoint security products for managed hosts in your network.

The topics in this section focus on the settings for F-Secure Client Security and F-Secure Server Security.

The settings for F-Secure Linux Security 64 are available in Policy Manager Console on the **Settings** > **Linux** pages. You can find more information on managing the settings in the Linux Security 64 documentation.

The settings for F-Secure Client Security for Mac are similar to those for the Windows product, but more limited in scope. These settings are available in Policy Manager Console under the **Settings** > **Mac** pages.

The settings for F-Secure Email and Server Security are combined under the **Windows**, **Microsoft Exchange**, and **Microsoft SharePoint** pages on the **Settings** tab. The server-related **Windows** settings apply to the local protection for hosts where Email and Server Security is installed. For more information on the settings, see the Email and Server Security Administrator's Guide.

Related concepts

Configuring older versions of Client Security on page 112

8.1 Migration of Email and Server Security settings

Existing settings for the Microsoft Exchange and Microsoft SharePoint protection features of F-Secure Email and Server Security are migrated to the **Standard view** for using 14.x versions of the product.

The existing settings are also preserved in **Advanced view** for managing older versions of Email and Server Security.

If you have Email and Server Security installed on managed hosts, it is important to check all the migrated settings. As all previously defined match lists and message templates are moved to the **Root** domain, it is especially important to check those. You also need to check all references to the match lists and message templates in the **Microsoft Exchange** and **Microsoft SharePoint** settings, including those used in scheduled scanning tasks.

8.2 Configuring virus and spyware protection

Virus and spyware protection consists of automatic updates, manual scanning, scheduled scanning, real-time scanning, spyware scanning, DeepGuard, email scanning and browsing protection.

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

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

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

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

8.2.1 Configuring automatic updates

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

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

Configuring automatic updates from Policy Manager Server

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

In **Standard view**, this is configured as follows:

1. Select **Root** on the **Domain tree**.
2. Go to the **Settings** tab and select **Windows** > **Centralized management**.
3. Make sure that the polling interval defined in **Interval for polling updates from F-Secure Policy Manager Server** is suitable for your environment.
4. If your network includes hosts with Client Security version 13.x installed, make sure that **Enable automatic updates** is selected.
5. If you want to restrict users from changing these settings, click the lock symbol beside the settings.
6. Click the following icon to distribute the policy:

Configuring Policy Manager Proxy

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

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

In **Standard view**:

1. Select the subdomain where you want to use the Policy Manager Proxy on the **Policy domains** tab.
2. Go to the **Settings** tab and select **Windows** > **Centralized management**.
3. Click **Add** next to the **Policy Manager Proxies** table to add new servers to the list of available proxy servers. This opens the **Policy Manager Proxy server properties** window.
4. Enter a priority number for the Policy Manager Proxy in the **Priority** text box.

   The priority numbers are used to define the order in which the hosts try to connect to the Policy Manager Proxy. Use, for example, 10 for the Policy Manager Proxy in the office where the host is normally located, and 20, 30 and so on for the other proxies.
5. Enter the URL of the Policy Manager Proxy server in the **Address** text box, then click **OK**.
6. Repeat the above steps to add the other servers to the list.
7. When you have added all proxies to the list, check that they are in the correct order.

   If necessary, you can modify their order by altering the priority numbers.
8. If the policy domain includes hosts with Client Security 13.x installed, make sure that **Enable automatic updates** is selected.
9. If you want to restrict users from changing these settings, click the lock symbols beside the settings.
10. Click the following icon to distribute the policy:

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

Configuring hosts to download updates from each other

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

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

- A Policy Manager Server
- A Policy Manager Proxy
- Another managed host (for example Client Security) with neighborcast enabled.

To enable neighborcast:

1. Select the target domain.
2. Go to the **Settings** tab and select the **Centralized management** page.
   a) To set hosts in the selected domain to download updates from other hosts, select **Enable neighborcast client**.
   b) To set hosts in the selected domain to serve updates to other hosts, select **Enable neighborcast server**.
3. To change the port used for neighborcast, enter the new port number in **Neighborcast port**.
4. If you want to use neighborcast only within a specific network, enter that network mask in the **Neighborcast discovery address** field.

   For example, you can set neighborcast to work only within your office network, so that the feature is turned off whenever a managed computer is outside the office. In practice, whenever the computer is outside the specified network, the HTTP and UDP ports are not in listening mode and the client does not make any broadcast requests.

Note: We recommend using this network restriction, as it increases the security of managed hosts.

5. Click the following icon to distribute the policy:

8.2.2 Configuring real-time scanning

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

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

Enabling real-time scanning for the whole domain

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

In **Standard view**:

1. Select **Root** on the **Domain tree**.
2. Go to the **Settings** tab and select **Windows** > **Real-time scanning**.
3. Select **Enable real-time scanning**.
4. Select **Files with these extensions** from the **Files to scan:** drop-down list.
5. Select how to handle infected files from the settings under the **Actions on malware detection** sections.
   The settings are divided into two groups so that you can choose different settings for workstations and servers.
6. Check that the other settings on this page are suitable for your system, and modify them if necessary.
7. Click the following icon to distribute the policy:

Using AMSI integration to identify script-based attacks

Antimalware Scan Interface (AMSI) is a Microsoft Windows component that allows the deeper inspection of built-in scripting services.

Note: AMSI integration is only available on Windows 10 hosts that are running version 15 or newer products.

Advanced malware uses scripts that are disguised or encrypted to avoid traditional methods of scanning. Such malware is often loaded directly into memory, so it does not use any files on the device.

AMSI is an interface that applications and services that are running on Windows can use to send scanning requests to the antimalware product installed on the computer. This provides additional protection against harmful software that uses scripts or macros on core Windows components, such as PowerShell and Office365, or other applications to evade detection.

1. Select the target domain.
2. Go to the **Settings** tab and select **Windows** > **Real-time scanning**.
3. Select **Enable Antimalware Scan Interface (AMSI)**.
4. Click the following icon to distribute the policy:

Excluding files from real-time scanning

You may want real-time scanning to skip certain files, either based on the file extension or the file path.

For example, you might not want to scan Microsoft Outlook's `.PST` file to avoid slowing down the system unnecessarily, as PST files are typically very large and take a long time to scan.

In **Standard view**:

1. Select **Root** on the **Domain tree**.
2. Go to the **Settings** tab and select **Windows** > **Real-time scanning**.

   To select files based on their file extension:

   a) Select **Do not scan files with the following extensions**.
   b) Enter the extension in **Excluded extensions**.

   Note: The extensions should be added without the preceding `.` (dot). Separate multiple extensions with spaces.

   To select files based on their location or checksum (hash):

   a) Select **Do not scan the following files and applications**.
   b) Click **Add**.
   c) Select the scope.

      Select **All** if you want the exclusion to apply to both real-time and manual scanning.

   d) Select the identification method.

      Select **File path** if the file always uses the same path.

      Select **Folder path** if you want scanning to skip all files in a specific folder.

      Select **Application SHA-1** if the path for the file may vary across different hosts. Note that this option is only available for the real-time scanning scope.

   e) Enter the path or hash that you want to exclude from scanning.
      For example:

      - File name: `text.txt` (all files named `text.txt` are not scanned).
      - Full file path: `C:\test\text.txt` (the `text.txt` file in the `C:\test` folder is not scanned).
      - Folder path: `C:\test` (all contents in the `C:\test` folder are not scanned).

      For more information on using wildcards, see
      https://community.f-secure.com/t5/Business/Using-wildcards-in-exclusions/ta-p/20428.

      Note: DeepGuard does not support exclusions that are configured using wildcards or device names.

      You can also add a comment if you want to keep a record of why the file or application was excluded.

   f) Click **OK**.
3. If you do not want to allow users to exclude files or applications from scanning, select **Prevent users from adding scanning exclusions**.
4. Click the following icon to distribute the policy:

Excluding processes from real-time scanning

To optimize disk performance on managed hosts, you may want to exclude some processes from scanning.

In **Standard view**:

1. Select **Root** on the **Domain tree**.
2. Go to the **Settings** tab and select **Windows** > **Real-time scanning**.
3. Select **Do not scan the following processes**.
4. Enter each process to exclude on its own line in **Excluded processes**.

   Enter the full path for each process, for example `C:\Program Files\Application\app1.exe`. You can also use system environment variables in the path, for example `%ProgramFiles%\Application\app1.exe`.

   Note: Any files that the excluded processes access are also excluded from scanning.

5. Click the following icon to distribute the policy:

8.2.3 Using Security Cloud for malware scanning

F-Secure's Security Cloud is a cloud network that houses the various databases and automated analysis systems, which support and enhance the performance of F-Secure security products.

Services connect to Security Cloud to retrieve the most up-to-date details of threats seen in the wild by other protected machines, which makes the response more efficient and effective. The service queries the reputation details of all objects, such as files and URLs. These queries contain anonymous metadata about the object, such as file size and anonymized path, and are sent to the Security Cloud for combined data analysis. Security Cloud does not collect IP addresses or other private information, queries are completely anonymous to maintain privacy.

By evaluating the combined metadata with information drawn from the in-house databases and various other sources, the automated analysis systems provide a fully-informed, up-to-date risk assessment for the object, immediately blocking threats that have been seen previously by any other service or device that is connected to Security Cloud. This also removes the need to perform any further analysis of the object, which reduces the impact on the system resources that the service uses.

In **Standard view**:

1. Select the target domain.
2. Go to the **Settings** tab and select **Windows** > **Real-time scanning**.
3. Select **Use Security Cloud**.

   Note: The Security Cloud setting applies to all scanning types, not just real-time scanning.

4. Click the following icon to distribute the policy:

8.2.4 Configuring scheduled scanning

You can add a scheduled scanning task in **Advanced view**.

In this example, a scheduled scanning task is added in a policy for the whole policy domain. The scan is to be run weekly, every Monday at 8 p.m, starting from August 25, 2009.

In **Advanced view**:

1. Select **Root** on the **Domain tree**.
2. On the **Policy** tab, select **F-Secure** > **F-Secure Anti-Virus** > **Settings** > **Scheduler** > **Scheduled tasks**.
   The currently set scheduled tasks are displayed on the **Scheduled tasks** table. Now you can add scheduled scanning as a new task.
3. Click **Add**.
   This adds a new row to the **Scheduled tasks** table.
4. Click the **Name** cell on the row you just created and then click **Edit**.
5. The **Name** cell is now activated and you can enter a name for the new task.

   For example, `Scheduled scanning for all hosts.`
6. Next click the **Scheduling parameters** cell, and then click **Edit**.
7. Now you can enter the parameters for the scheduled scan.

   A scheduled scan that is to be run weekly, every Monday starting at 8 p.m, from August 25, 2009 onwards, is configured as follows: `/t20:00 /b2009-08-25 /rweekly`

   Note: When the **Scheduling parameters** cell is selected, the parameters that you can use and their formats are displayed as a help text in the **Messages** pane (below the **Scheduled tasks** table).

8. Select the task type by clicking the **Task type** cell and then clicking **Edit**.

9. From the drop-down list that opens select **Scan local drives**.
   The scanning task is now ready for distribution.
10. Click the following icon to distribute the policy:

Running scheduled scans on specific weekdays and days of the month:

When you are configuring a weekly scheduled scan, you can also define specific weekdays when the scan is to be run. Similarly, when you are configuring a monthly scheduled scan, you can define specific days of the month when the scan is to be run. For both of these, you can use the `/Snn` parameter:

- For weekly scheduled scans you can use `/rweekly` together with parameters `/s1` - `/s7`. `/s1` means Monday and `/s7` means Sunday.

  For example, `/t18:00 /rweekly /s2 /s5` means that the scan is run every Tuesday and Friday at 6 p.m.

- For monthly scheduled scans you can use `/rmonthly` together with parameters `/s1` - `/s31`.

  For example, `/t18:00 /rmonthly /s5 /s20` means that the scan is run on the 5th and 20th of each month at 6 p.m.

Note: If you do not define a weekday, weekly scheduled scans are run on each Monday by default. Monthly scheduled scans are run on the first day of each month by default, if you have not defined a specific day.

8.2.5 Configuring DeepGuard

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

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

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

To turn on DeepGuard:

1. Go to the **Settings** tab and select **Windows** > **Real-time scanning**.
2. Select **Enable DeepGuard**.
3. Select **Block rare and suspicious files** if you want to use DeepGuard's prevalence-based rules to block files that may not be commonly recognized.

   Note: This feature is only available for version 15 and newer clients.

4. Click the following icon to distribute the policy:

DataGuard

DataGuard is a feature that strengthens DeepGuard by monitoring specific folders to prevent untrusted applications from modifying files on managed hosts.

DataGuard is especially useful against any new ransomware that is able to get past other security layers.

In Policy Manager, you can set the folders that DataGuard monitors and protects. There are predefined options for the default folders for user content, such as Documents, Music, Pictures, etc. You can also set the trusted applications that are allowed to access the protected folders and modify the files there. Applications that are not considered trusted are stopped if they try to modify any protected files.

Setting up DataGuard

You can define the folders that DataGuard protects on managed computers, and add trusted applications that you do not want DataGuard to block

When DataGuard is turned on, untrusted applications and malware (including ransomware) cannot modify files in folders that you define as protected.

Note: Be careful in selecting the protected folders and trusted applications for DataGuard. Adding a wide range of data (either lots of folders or, for example, `C:\`) can cause a lot of unnecessary interruptions. Also, adding a very wide scope of locations to the trusted applications list may allow malware to modify protected files.

To use DataGuard:

1. Go to the **Settings** tab and select **Windows** > **DataGuard**.
2. Select **Turn on DataGuard protection**.
3. In the **Protected data folders** table, select the folders that you want to protect.

   To add more protected folders:

   a) Enter the folder path in the **Folder** field.

   You can use environment variables in the path. User environment variables apply to the corresponding paths for each Windows user account on the computer. The supported variables are: `%UserProfile%`, `%HomeDrive%`, `%HomePath%`, `%ProgramData%`, `%WinDir%`, `%SystemRoot%`, `%SystemDrive%`, `%ProgramFiles%`, and `%ProgramFiles(x86)%`.

   b) Add a description for the new folder in the **Comments** field.

   Note: Universal Naming Convention (UNC) paths are also supported for the protected folders.

4. Select the applications that are allowed to modify files that are in protected folders.
5. Select **Discover trusted applications automatically** if you want to allow known, trusted system applications to modify the protected folders.
6. Add more trusted applications to the table if necessary.

   - To add a single application, enter the full path to the executable including file name and extension.
   - To add a folder that may contain several applications, enter the path to the folder.

   Note: Some applications and standard Windows features may require adding more than one application file to the list of trusted applications. For example, the print-to-PDF functionality in Windows uses the following executable files: `<Windows folder>\System32\spoolsv.exe` and `<Windows folder>\System32\printfilterpipelinesvc.exe`.

7. Click the following icon to distribute the policy:

We recommend that you apply the common practices and tools for your organization when considering the protected folders and trusted applications for DataGuard. It is also a good idea to apply specific rules for separate policy domains where possible. For example, if your domain tree is structured according to teams or departments, you can apply separate rules for developers and salespeople.

8.2.6 Configuring web traffic (HTTP) scanning

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

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

Web traffic scanning uses the following criteria for rating web sites:

Unknown/unrated	• URLs that have not yet been analyzed • URLs that are inaccessible at the time of testing

Safe	• URLs that have been analyzed as safe • URLs where users can knowingly download spyware, riskware, or adware
Suspicious	• URLs that are linked to spamming activities • URLs that are linked to scam-like activities
Malicious	• URLs where the content contains script codes that download or install a malicious file • URLs that belong to drive-by download sites • URLs where the content exploits browser or system vulnerabilities • URLs or content that contain XSS or SQL injections • URLs where the content contains malicious iframes • URLs that belong to phishing sites • URLs that are linked to hacking and other malicious activities • URLs that have been taken down due to malicious behavior

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

Enabling web traffic scanning for the whole domain

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

In **Standard view**:

1. Select **Root** on the **Domain tree**.
2. Go to the **Settings** tab and select **Windows** > **Web traffic scanning**.
3. Set **HTTP scanning enabled** to **All Content Types**.
4. Check that the other settings on this page are suitable for your system, and modify them if necessary.
5. Click the following icon to distribute the policy:

Blocking specific content types

You use the **Advanced protection** setting for web traffic scanning to block access to content types that may be vulnerable to use for malicious purposes, for example Adobe Flash or Microsoft Silverlight.

By default, the **Advanced protection** setting is turned off.

Web traffic scanning can block the following content types on unknown web sites:

- JAR
- Executables
- Adobe Flash
- Adobe Acrobat
- Microsoft Silverlight
- Microsoft Office files

In **Standard view**:

1. On the **Settings** > **Windows** > **Web traffic scanning** page, go to **Advanced protection**:
   - Select **Included content types** to block only those file types that are on the **Included** list.
   - Select **All except excluded content types** to block all file types except those that are on the **Excluded** list.
2. On the **Included** list, add the file types that you want to block.

   Note: Web traffic scanning only blocks content for web sites that have an unknown safety rating.

3. On the **Excluded** list, add any file types that you want to allow even on unknown web sites.

Blocking botnet communication

Botnet Blocker is a security feature that aims to prevent botnet agents from communicating with their command and control servers.

The feature uses DNS reputation data to verify the security of queries when translating DNS requests to IP addresses.

To configure Botnet Blocker in **Standard view**:

1. Go to the **Settings** tab and select **Windows** > **Web traffic scanning**.
2. Under **Botnet blocker**, set the filtering to use for DNS queries.

   By default, this set to **Block unsafe queries**.
3. Set the alert level to use for notifications of blocked DNS queries.
4. Click the following icon to distribute the policy:

8.2.7 Managing quarantined objects

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

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

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

Deleting quarantined objects

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

In **Standard view**:

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

Releasing quarantined objects

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

In **Standard view**:

1. Select the target domain.
2. Create an exclusion rule for the object.

   Exclusion rules are required to make sure that the object will not be quarantined again in future. If the object is listed as a virus or infected file:

   a) Go to the **Settings** > **Windows** > **Quarantine management** page and copy the object's file path.
   b) Go to the **Settings** tab and select **Windows** > **Real-time scanning**.
   c) Check that **Do not scan the following files and applications** is selected.

d) Click **Add** next to the exclusion table.
e) Select **All scans** as the scope, select **File path**, and paste the object's file path to the path field.
f) Click **OK**.

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

8.2.8 Hiding notifications on managed hosts

You can hide the security notifications and computer restart prompts from end users.

Policy Manager includes separate settings for the visibility of notifications on workstations and servers.

In **Standard view**:

1. Select the target domain.
   To hide security notifications and computer restart prompts from end users:
   a) Go to the **Settings** tab and select **Windows** > **Centralized management**.
   b) Under **User notifications**, select **Administrators only** from drop-down lists for workstations and servers.
2. Click the following icon to distribute the policy:

8.2.9 Hiding the local user interface on managed hosts

You can hide the user interface for products so that end users do not see the product and cannot modify its settings.

In **Standard view**:

1. Select the target domain.
2. Go to the **Settings** tab and select **Windows** > **Centralized management**.
3. Under **Local user interface**, clear the **Enable local user interface** checkbox.
4. Click the following icon to distribute the policy:

8.2.10 Preventing users from changing settings

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

There are different possibilities for doing this:

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

Setting all virus protection settings as final

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

In **Standard view**:

1. Select **Root** on the **Domain tree**.

2. Go to the **Settings** tab and select **Windows** > **Centralized management**.
3. Select **Do not allow users to change any settings**.
4. Click **Yes**.
5. Click the following icon to distribute the policy:

8.2.11 Monitoring viruses on the network

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

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

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

8.2.12 Testing your antivirus protection

To test that the managed security products operate correctly, you can use a special test file that is detected as though it were a virus.

This file, known as the EICAR Standard Anti-Virus Test File, is also detected by several other antivirus programs. You can also use the EICAR test file to test your email scanning. EICAR is the European Institute of Computer Anti-virus Research. The Eicar info page can be found at http://www.f-secure.com/v-descs/eicar.shtml.

You can test your antivirus protection as follows:

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

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

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

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

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

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

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

8.3 Configuring firewall settings

This section provides an overview of the firewall settings and how you can configure them to suit your network.

The firewall protects computers against unauthorized access from the internet as well as against attacks originating from inside the LAN.

F-Secure product versions 14.00 and newer use the Windows Firewall component. F-Secure's firewall profiles provide an additional security layer on top of the Windows Firewall user rules and other domain rules. The F-Secure firewall profiles or rules are not applied if Windows Firewall is off. Therefore, we recommend that you always keep the firewall on.

Older product versions use F-Secure's own firewall component. This contains predefined security levels, each of which has a set of pre-configured firewall rules associated with them. Different security levels can be assigned to different users based on, for example, company security policy, user mobility, location, and user experience.

Note: If you use a GPO or third-party firewall, in most cases you need to turn off F-Secure firewall profiles to avoid conflicts. If this is the case, make sure that the **Enable firewall configuration through Policy Manager** setting on the **Settings** > **Windows** > **Firewall** page is not selected.

Related concepts

Firewall settings for Client Security 13 and older on page 116

This section describes the settings that you can configure for F-Secure's firewall.

8.3.1 Turning on the firewall

Keep the firewall turned on to block intruders from accessing computers in your managed network.

1. Select **Root** on the **Domain tree**.
2. Go to the **Settings** tab and select **Windows** > **Firewall**.
3. Click **14.x clients**.
4. Select **Enable firewall configuration through Policy Manager**.

   Note: If you use a GPO or third-party firewall, in most cases you need to make sure that this setting is not selected to avoid conflicts.

5. Select **Enable firewall**.
6. Click the following icon to distribute the policy:

8.3.2 Configuring network quarantine

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

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

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

Turning network quarantine on in the whole domain

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

In **Standard view**:

1. Select **Root** on the **Domain tree**.
2. Go to the **Settings** tab and select **Windows** > **Firewall**.
3. Select **Enable network quarantine**.
4. Specify the **Virus definitions age to activate network quarantine**.
5. If you want to restrict the host from accessing the network when real-time scanning is turned off, select **Activate network quarantine on host if real-time scanning is disabled**.
6. Click **Configure network isolation rules** to modify the firewall rules for quarantined hosts.
7. Click the following icon to distribute the policy:

Fine-tuning network quarantine

Network quarantine is implemented by forcing hosts to use a restricted set of firewall rules.

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

Note: For product versions 13 and older, quarantined hosts are forced to the **Network quarantine** firewall security level. This security level has a restricted set of firewall rules. Similarly to the network isolation rules for newer product versions, you can add new **Allow** rules to the security level, but should not restrict access further.

8.3.3 Firewall settings for version 14 clients and newer

This section describes the settings that you can configure for F-Secure's firewall profiles, which provide an additional layer of security for Windows Firewall.

Note: You must have Windows Firewall turned on for your network via Group Policy Object (GPO) to manage the firewall settings through Policy Manager. If Windows Firewall is turned off via GPO, Policy Manager cannot override those settings and the firewall policies will not be applied.

Selecting the active firewall profile for a domain

You can set a specific firewall profile for any domain within your managed network.

1. Select the target domain.
2. Go to the **Settings** tab and select **Windows** > **Firewall**.
3. Click **14.x clients**.
4. Select the firewall profile for the domain from the **Workstation host profile** and **Server host profile** drop-down lists.

   Note: The default profile for F-Secure Server Security clients is set to **Server**.

5. Click the following icon to distribute the policy:

Creating a new firewall profile for a domain

You can create a new firewall profile by cloning an existing one.

In **Standard view**:

1. Select the target domain.
2. Go to the **Settings** tab and select **Windows** > **Firewall**.
3. Click **14.x clients**.
4. In the **Profile being edited** drop-down, select the profile that you want to clone.
5. Click **Clone**.
6. Enter a name for the new profile, then click **OK**.
7. Configure the settings and rules for the new profile.
8. Click the following icon to distribute the policy:

Adding firewall rules

You can add new rules to firewall profiles that have been added within the scope of your domain access.

1. Select the target domain.
2. Go to the **Settings** tab and select **Windows** > **Firewall**.
3. Click **14.x clients**.
4. In the **Profile being edited** drop-down, select the profile that you want to edit.
5. Click **Add rule**.
6. Enter a name for the rule and select the type (either **Allow** or **Block**), then click **Next**.

   Note: For **Block** rules, select **Send an alert when the rule blocks a connection** if you want to receive alerts when the rule is triggered.

7. For each network service that you want the rule to include:
   a) Click **Add**.
   b) Select the service from the **Service** drop-down list.
   c) Select the traffic direction from the **Direction** drop-down list.

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

8. Click **Next**.
9. Specify the remote addresses that apply for the rule, then click **Next**.
10. Specify the scope for the rule, then click **Finish**.
    The new rule is added to the **Firewall rules** table for the selected profile.
11. Click the following icon to distribute the policy:

Related tasks

Creating a new network service for firewall rules on page 83
If you need a network service that is missing from the set of default services, you can add it separately for use in custom firewall rules.

Creating a new network service for firewall rules

If you need a network service that is missing from the set of default services, you can add it separately for use in custom firewall rules.

1. Go to the **Settings** tab and select **Windows** > **Firewall**.
2. Click **14.x clients**.
3. Click **Configure network services** below the **Firewall rules** list.
4. Click **Add**.
5. Enter a name for the service.
6. Select the IP protocol number, then click **Next**.
7. Enter the initiator ports, then click **Next**.
8. Enter the responder ports, then click **Finish**.

You can now select the new network service when you add or edit your custom firewall rules.

Hiding certain firewall profiles from end users

If you do not want end users to have the full set of firewall profiles available for selection, you can hide specific profiles so that they do not appear in the client settings on managed hosts.

To hide a firewall profile from end users:

1. Select the target domain.
2. Go to the **Settings** tab and select **Windows** > **Firewall**.
3. Click **14.x clients**.
4. Under **Changing profiles**, click **Hide profiles from users**.
5. In the **Hidden firewall profiles** view, click **Add**.
6. Select the profile that you want to hide, then click **OK**.
7. Click **Close**.
8. Click the following icon to distribute the policy:

8.4 Configuring application control

Application control prevents execution and installation of applications, and prevents them from running scripts.

Note: Application control is only available for F-Secure product versions 14 and newer.

Application control reduces the risks that malicious, illegal, and unauthorized software pose in the corporate environment. It provides the following features:

- Security: Pre-configured security rules designed by F-Secure penetration testers cover attack vectors that are used to breach into corporate environments.
- Policy enforcement: Based on a simple rule editor, policy enforcement helps the administrator define which applications are blocked, allowed, or monitored.

8.4.1 Configuring application control

Application control prevents execution and installation of applications, and prevents them from running scripts.

Note: Application control is only available for F-Secure product versions 14 and newer.

Application control reduces the risks that malicious, illegal, and unauthorized software pose in the corporate environment. It provides the following features:

- Security: Pre-configured security rules designed by F-Secure penetration testers cover attack vectors that are used to breach into corporate environments.
- Policy enforcement: Based on a simple rule editor, policy enforcement helps the administrator define which applications are blocked, allowed, or monitored.

Turn on application control to prevent the execution and installation of applications, and to prevent them from running scripts:

1. Select **Root** on the **Domain tree**.
2. Go to the **Settings** tab and select **Windows** > **Application control**.
3. Select **Enable Application control**.
4. Select the profile to use in the **Host profile** drop-down list.
5. Click the following icon to distribute the policy:

8.4.2 Creating a new application control profile

You can create a new application control profile by cloning an existing one.

In **Standard view**:

1. Select the target domain.
2. Go to the **Settings** tab and select **Windows** > **Application control**.
3. Select the profile that you want to clone from the **Profile being edited** drop-down list.
4. Click **Clone**.
5. Enter a name for the new profile, then click **OK**.
6. Select how you want to handle applications in the **Default rule applied to all applications** drop-down list.

   The selected action is applied to any applications that are not covered by the exclusion rules for the profile.
7. Configure the exclusion rules for the new profile.
8. Click the following icon to distribute the policy:

8.4.3 Adding exclusion rules

Application control's exclusion rules give you a way to define the applications that you want to explicitly allow or block.

Any applications that match the conditions that you set within the rules are excluded from the default rule for the profile. For example, if the default rule is **Allow**, you can create rules to specify the applications or locations that you want to block. Another example could be that you want to receive a report of any applications that match the triggering conditions, even though they are still allowed or blocked based on the default rule for the profile.

In **Standard view**:

1. Select the target domain.
2. Go to the **Settings** tab and select **Windows** > **Application control**.
3. Select the profile that you want to edit from the **Profile being edited** drop-down list.

   Note: You cannot edit the exclusion rules for any profiles that are marked as **Predefined**.

4. Click **Add rule**.
   This opens the exclusion rule wizard.
5. Enter a name and description for the rule.
6. Select the **Event** and **Action** for the rule.

   The following table lists the available event types and when they are triggered.

Event	Description
Run application	A combination of Start process and Load dynamic library. Triggers when an executable file or script is launched and when a DLL is about to get loaded into a process.
Run installation	Triggers when `msiexec.exe` is launched with some MSI package as a command line parameter.
Start process	Triggers when an executable file or script is launched.
Load dynamic library	Triggers when a DLL is about to get loaded into a process.
File access	Triggers when a file matching the target conditions is opened or accessed by an application.

   For example, if you select **Run application** as the event and **Block** as the action, the rule prevents applications from running if they match the conditions for the rule.

7. Click **Add condition**.

   You can add multiple conditions to the same rule to get the scope that you want.

   Note the following when adding conditions to an exclusion rule:

   - If you use attribute `Target SHA1` or `Parent SHA1` in the exclusion rule condition, you have to use **Start process** as the event type.
   - If a dynamic link library (.dll) is blocked and you want it to be allowed by Application Control, you have to use the **Load dynamic library** event type in the exclusion rule. In a case like this, you cannot therefore use attribute `Target SHA1` nor `Parent SHA1` in the exclusion rule.
   - Attributes `Target file names mismatch` and `Parent file names mismatch` kick in when the binary filename is different from the "Original filename" found under file Properties > Details.

8. Select the attribute, operator, and value for each condition.

   The following table explains the attributes that you can select to match the condition values.

Selected attribute	Description
Target	Values of the actual application. For example, **Target file name** is the actual file that you want to block.
Parent	Values of the process that launches the application. For example, **Parent file name** is the file that launches the application that you want to block.

For example, if you want to block Internet Explorer, `iexplore.exe` is the target and `explorer.exe` (Windows Explorer) is the parent.

The following table explains how different operators work with the values that you enter.

Selected condition	Description
Equals	The value must be exactly the same as the target, for example, `iexplore.exe`.
Not equals	The value may be anything except the target.
Less, Greater, Less or equals, Greater or equals	These apply to numeric values, for example if you select **Target product version** as the attribute.
Contains	The selected attribute must contain the value, for example, `explore`.
Starts with	The selected attribute must start with the value, for example, `ie`.
Ends with	The selected attribute must end with the value, for example, `explore.exe`.

9. Click **OK**.
10. Change the order of the rules if necessary.

    The rules listed for the profile are applied in priority order from the top down.
11. Click the following icon to distribute the policy:

Note: If there are any issues with the rule, for example if some information is missing or invalid, the host sends an alert to Policy Manager.

8.4.4 Example: Preventing a vulnerable version from running

To use Application control to prevent vulnerable applications from running, for example, to block an unpatched version, use a Target file version attribute.

For example, a program had a vulnerability that was patched in version 1.2.4. To block any version older than 1.2.4 from running, do the following.

1. Create the following exclusion rule:
   a) Give the rule a name: `Block an unpatched program`.
   b) From the **Event** drop-down menu, select **Run application**.
   c) From the **Action** drop-down menu, select **Block**.
2. Then, add the first condition to the exclusion rule:
   a) From the attribute drop-down menu, select **Target file description**.

Note: To find the file description, right-click the file in the File Explorer and select Properties.

b) From the operator drop-down menu, select **Contains**.
c) In the value field, enter the name of the unpatched program as it appears in the file description. For example, "Internet Explorer".

Note: As "Internet Explorer" is in the target file description, the program is blocked regardless of the file name or its location.

3. Then, add the second condition to the exclusion rule:
   a) From the attribute drop-down menu, select **Target file version**.
   b) From the operator drop-down menu, select **Less or equals**.
   c) In the value field, enter `1.2.3.*.*`.

   Note: The condition for the target file version is "less or equal to 1.2.3.*.*" The asterisk indicates that only major and minor fields are used in the comparison.

8.4.5 Example: Preventing applications from automatically opening downloaded files

To use Application control to block applications from launching downloaded files automatically, define the application and download folder paths.

For example, to prevent Microsoft Excel from automatically opening files that are downloaded through your browser or other applications, do the following:

1. Create the following exclusion rule:
   a) Give the rule a name: `Block downloaded Excel files`.
   b) From the **Event** drop-down menu, select **Start process**.
   c) From the **Action** drop-down menu, select **Block**.
2. Then, add the first condition to the exclusion rule:
   a) From the attribute drop-down menu, select **Target path**.
   b) From the operator drop-down menu, select **Contains**.
   c) In the value field, enter the name of the name of the `exe` file, for example `excel.exe`.
3. Then, add the second condition to the exclusion rule:
   a) From the attribute drop-down menu, select **Target command line**.
   b) From the operator drop-down menu, select **Contains**.
   c) In the value field, enter the path to your default download folder, for example `C:\Users\default\Downloads\`.

8.5 How to protect your users' sensitive data

Connection control provides additional protection for managed hosts against harmful activity when accessing online banks or making transactions online.

Connection control automatically detects secure connections to online banking web sites, and blocks any connections that do not go to the intended site. When you open a recognized banking site, only connections to sites that are considered safe are allowed.

If an end-user needs to access a blocked web site to complete an ongoing transaction, they can temporarily allow access to the blocked page or end the Connection control session.

Connection control currently supports the following browsers on managed Windows hosts:

- Google Chrome (latest two major versions)
- Mozilla Firefox (latest two major versions)
- Internet Explorer 11 (Windows 8.1, Windows 7, both 32-bit and 64-bit versions)
- Internet Explorer 10 (Windows 8, Windows 7, both 32-bit and 64-bit versions)
- Internet Explorer 8 and 9 (Windows Vista, 32-bit and 64-bit versions)

8.5.1 Protecting secure connections on managed hosts

You can turn Connection control on for the policy under the Browsing protection settings.

Note: Browsing protection must be turned on to use Connection control.

When Connection control is turned on and a user opens a recognized banking site in their browser, a notification appears at the top of their screen to indicate that the Connection control session has started. When they have completed their ongoing transaction, the user can end the session to resume normal browsing.

Note: Connection control installs extensions (plug-in applications that provide extra features) on browsers on the managed hosts. If the extensions are not in use, Connection control may not work properly.

To turn on Connection control in **Standard view**:

1. Select the target domain.
2. Go to the **Settings** tab and select **Windows** > **Browsing protection**.
3. Select **Connection control enabled**.
4. Enter any additional web sites that you want to trigger Connection control on managed hosts in the **Privacy-protected sites** list.

   For example, if you want extra protection for any secure sites that are commonly used within your organization, you can add them to the list.

   Note: Connection control only supports web sites that use HTTPS.

5. Click the following icon to distribute the policy:

If the browser extensions need to be turned on manually:

- On Firefox, select **Tools** > **Add-ons** from the menu and click **Enable** next to the extension.
- On Chrome, select **Settings** from the menu, then click **Extensions** and select **Enable** next to the extension.
- On Internet Explorer, select **Tools** > **Manage Add-ons**, select the browser extension and click **Enable**.

8.6 Blocking unsuitable web content

You can block managed hosts' access to web sites and pages that contain unsuitable content with Web content control.

Web content control uses F-Secure's reputation analysis data to categorize web sites and block access to any sites that contain content selected for the policy.

8.6.1 Web content categories

Use the categories listed here to block access to web sites based on the results of F-Secure's Network Reputation Service (NRS) content analysis.

Abortion	Web sites that contain information or images on abortion, abortion clinics and centers, and abortion topics in general. For example, discussion forums that may be pro-life or pro-choice.
Adserving	Web links that point to various flash, text, video or image files or other similar files that contain advertisements.
Adult	Web sites that are aimed at an adult audience with content that is clearly sexual, or containing sexual innuendo. For example, sex shop sites or sexually-oriented nudity.
Alcohol and tobacco	Web sites that display or promote alcoholic beverages or smoking and tobacco products, including manufacturers such as distilleries, vineyards, and breweries. For example, sites that promote beer festivals and web sites of bars and night clubs.
Anonymizers	Web sites that allow or instruct people how to bypass network filters, including web-based translation sites that allow people to do so. For example, sites that provide lists of public proxies that can be used to bypass possible network filters.

Auctions	Web sites of online marketplaces where people can buy and sell their products or services. This includes sites that provide lists of products or services even though the actual transaction may happen somewhere else.
Banking	Web sites of banks and other financial institutions, including savings and investment banks, securities trading and foreign exchange trading sites.
Blogs	Weblogs where people or institutions publish information and can share news, stories, videos, and photos. Due to their individual nature, the themes addressed in blogs can vary widely and they can include any topics.
Chat	Online portals and messengers where people can chat with each other via text, audio, or video. For example, web-based chat and instant messaging applications, and chat sites.
Dating	Web sites that provide a portal for finding romantic or sexual partners. For example, matchmaking sites or mail-order bride sites.
Drugs	Web sites that promote drug use. For example, sites that provide information on purchasing, growing, or selling any form of these substances.
Entertainment	Web sites related to the entertainment industry, such as television shows, books, comics, movies and theaters, and art galleries. For example, television and radio program guides and music, tv, and movie review sites.
Gambling	Web sites where people can bet online using real money or some form of credit. For example, online gambling and lottery web sites, and blogs and forums that contain information about gambling online or in real life.
Games	Online gaming web sites and web sites where people can play, download, or buy games.
Hacking	Web sites that promote seeking and exploiting weaknesses in computer systems or computer networks for profit, challenge, or enjoyment. For example, sites that contain hacking guides and hacking tools.
Hate	Web sites that indicate prejudice against a certain religion, race, nationality, gender, age, disability, or sexual orientation. For example, sites that promote damaging humans, animals or institutions, or contain descriptions or images of physical assaults against any of them.
Job search	Web sites of employment agencies and contractors, and where people can search and find new jobs. For example, career search engines, career-networking groups and employment web sites.
Payment service	Web sites that process payments between shopping sites and banks or other financial services, such as credit cards. These include sites that can be used for payments in general.
Scam	Web sites that bait people by promising prizes after they fill in a survey, take a quiz, or perform similar actions. For example, sites that are pretending to be affiliated with a reputable company that is giving away prizes.
Shopping	Web sites where people can purchase any products or services, including sites that contain catalogs of items that facilitate online ordering and purchasing and sites that provide information on ordering and buying items online.
Social networking	Networking portals that connect people in general or with a certain group of people for socialization, business interactions, and so on. For example, sites where you can create a member profile to share your personal and professional interests. This includes social media sites such as Twitter.
Software download	Online portals for downloading various software.
Spam	Web sites that have been collected from spam mails.
Streaming media	Web sites that deliver streaming video or audio content either for free or through a subscription model.

Violence	Web sites that may incite violence or contain gruesome and violent images or videos. For example, sites that contain information on rape, harassment, snuff, bomb, assault, murder, and suicide.
Illegal downloads	Unauthorized file sharing or software piracy web sites. For example, sites that provide illegal or questionable access to software, and sites that develop and distribute programs that may compromise networks and systems.
Weapons	Web sites that contain information, images, or videos of weapons or anything that can be used as a weapon to inflict harm to a human or animal, including organizations that promote these weapons, such as hunting and shooting clubs. This category includes toy weapons such as paintball guns, airguns, and bb guns.
Webmail	Web sites that allow people to create and access their email accounts through a web browser. For example, this includes Yahoo! Mail and Gmail, and local, ISP-linked web mail services.

8.6.2 Selecting the content categories to block

You can select the web content categories that you want to block under the Web content control settings.

In **Standard view**:

1. Select the target domain or host.
2. Go to the **Settings** tab and select **Windows** > **Web content control**.
3. Under **Disallowed site categories**, select the categories that you want to block for managed hosts.
4. Enter the addresses of any additional web sites that you want to block or allow, regardless of their content category, in the **Disallowed sites** list and **Trusted sites** list respectively.
5. Click the following icon to distribute the policy:

8.7 Using Device Control

Device Control blocks certain hardware devices to protect the network.

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

8.7.1 Configuring Device control

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

Follow these instructions to configure Device control.

1. Go to the **Settings** tab and select **Windows** > **Device control**.
2. To turn on Device control, select **Device control enabled**.
3. Set the type of alert that is sent to the administrator when a device is blocked.
4. The **Device access rules** table contains rules for blocking devices.

   A device that has **Access Level** set to **Blocked** cannot be accessed, when the rule is set as active.

8.7.2 Limiting access permissions for removable drives

Device Control allows you to specify the access permissions for removable drives, such as USB sticks and portable hard drives.

1. Go to the **Settings** tab and select **Windows** > **Device control**.
2. Select the access permissions under **Removable storage devices**:
   - Select **Allow write access** if you want to allow users to copy files to removable drives. If this is not selected, users will have read-only access to any allowed removable drives.

- Select **Allow executables to run** if you want to allow users to run executable files, such as `.exe` or `.msi` files, that are located on a removable drive.

8.7.3 Blocking hardware devices

You can block the access to devices with predefined rules.

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

1. Go to the **Settings** tab and select **Windows** > **Device control**.
2. On the **Device access rules** table, select the row for the device that you want to block, and click **Edit**.
3. Set **Access Level** to **Blocked** to block the selected device.

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

8.7.4 Granting access to specific devices

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

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

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

1. Get the hardware ID for the device that you want to allow.
   The hardware ID has to be more specific than the ID which is used to block the device.
2. Go to the **Settings** tab and select **Windows** > **Device control**.
3. On the **Device access rules** table, click **Add**.
4. Enter the hardware ID for the device as the **Hardware ID** in the new rule.
5. Set **Access Level** to **Full access** to allow the use of the device.
6. Set **Active** to **Yes** for the new rule.

Finding hardware ID for a device

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

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

1. Select the target host.
2. Select the **Status** tab and select **Advanced view**.
3. Go to **F-Secure Device Control** > **Statistics** > **Devices** > **Devices**.
   Use **Hardware IDs**, **Compatible IDs** and **Device Class** columns to find the ID of the device that has been blocked.
   If you are not sure which ID is sufficiently unique to define a specific device:
   a) Go to **F-Secure Device Control** > **Settings** > **Report installed devices**.
   b) Set **Report installed devices** to **Yes**.
   c) Go to the **F-Secure Device Control** > **Statistics** > **Devices** > **Devices** table.
   d) Find the device that you want and compare the reported IDs.

   Note: You can right-click the table and select **Export table as text** to make it easier to compare them.
4. If you cannot find the ID using the statistics or the device has not been blocked yet, open Windows **Device Manager** in the client computer.
5. Find the device which ID you want to know in the list of devices.
6. Right-click the device and select **Properties**.
7. Go to **Details** tab.
8. Select one of the following IDs from the drop-down menu and write down its value:
   - Hardware IDs

- Compatible IDs
- Device class guid
- Parent ID

Note: For external storage devices, this is the only ID that includes the unique serial number of the device.

8.8 Managing software updates

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

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

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

Note: This feature does not support all managed products or versions. Check the release notes for your product to see if your current version is supported.

Note: Policy Manager only downloads and updates the Software Updater databases if you have hosts that have Software Updater installed.

8.8.1 Installing software updates automatically

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

In **Standard view**:

1. Select the target domain.
2. Go to the **Settings** tab and select **Windows** > **Software Updater**.
3. Select **Enable Software Updater**.
4. Select how you want managed hosts to fetch the software updates next to **Download software updates from Policy Manager**.
   - **Always**: The managed hosts fetch the updates from Policy Manager Server or Proxy when they are available.
   - **If possible**: The managed hosts fetch the updates from Policy Manager Server or Proxy if they are available, otherwise they download the updates from the internet.
   - **Never**: The managed hosts always fetch the updates from the internet.
5. Under **Automatic installation**, select the security update categories and schedule that you want to use.
6. Select **Run the task even if a scheduled start is missed** if you want the updates to be installed as soon as possible on hosts that are not available when the scheduled installation is run.
7. Select **Allow further installation of software updates before restarting** if you want to minimize the amount of restarts needed on managed hosts.
8. Click the following icon to distribute the policy:

8.8.2 Handling manually downloaded software updates

For software updates that cannot be downloaded automatically, you can import the update packages to Policy Manager for distribution.

Some software vendors require a user account or other authentication to access the update packages. This means that they cannot be downloaded automatically. Policy Manager receives notifications of any such software updates from the managed hosts.

With Policy Manager, you can download the packages manually, import them, and manage their distribution to hosts.

In **Standard view**:

1. Select **Root** on the **Domain tree**.
2. Select the **Software updates** tab.
3. Click **Manual downloads**.
   Manual downloads shows you the available updates that need to be downloaded manually.
4. Click the link shown under **Download package** or click **Copy link** and paste it to your browser.
5. Follow the instructions shown on the vendor's website to download the update package.

   Note: You can also replace the stored package for an update if necessary, for example if the file did not download fully.

6. When the update package is downloaded, click **Browse** and select the downloaded file.
   The status for the update changes to **Imported** and it is ready for distribution.
7. Click **Close**.

Policy Manager distributes the software update according to the settings for your network.

8.8.3 Excluding software updates from automatic installation

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

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

In **Standard view**:

1. Select the target domain.
2. To manually enter the details for the software updates that you want to exclude:
   a) Go to the **Settings** tab and select **Windows** > **Software Updater**.
   b) Under **Exclude software from automatic installation**, click **Add**.
   c) Enter the details for the update that you want to exclude.

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

      You can also select a software vendor to exclude. If you select a vendor and do not enter any other details, all updates for that vendor's software are excluded.

3. To exclude a software update from the current list of available updates:
   a) On the **Software updates** page, right-click the update that you want to exclude.
   b) Select **Exclude by Software** to use the update name given in the **Software** column or **Exclude by Bulletin ID** to use the bulletin ID.

      Note: If you exclude an update by its software name, any other updates that use the same name are also excluded.

4. Click the following icon to distribute the policy:

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

8.8.4 Checking the status of software updates in your network

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

The **Software updates** page provides a list of updates for the software in use within your network. Each entry on the list includes the software in question, category, ID and description for the update, corresponding knowledge base (KB)

number, as well as the update status if a single host is selected. If you select a domain or multiple hosts, you can click **View hosts** to see the update status. From this page, you can check which computers are missing selected updates, and also install the missing updates to those computers.

The **Status** column in the **Missing software update** view also shows you if you need to download the update package manually, or if the package has already been downloaded manually. These status links open the **Manual downloads** view.

Tip: You can also use the **Search missing updates** field on the **Software updates** page to find hosts that are missing an update. You can use any of the visible criteria for the update as a keyword for your search.

Tip: In **Advanced view**, you can turn off checking for missing service packs and updates that are not security-related.

Installing missing software updates

You can install missing software updates manually.

To install the missing software updates:

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

8.8.5 Allowing end users to manage software updates

You can allow users to see the Software Updater options in the local user interface so that they can install available updates.

Note: This feature is only available for version 15 and newer clients.

In **Standard view**:

1. Select the target domain.
2. Go to the **Settings** tab and select **Windows** > **Software Updater**.
3. Select **Show Software Updater options to users**.
4. Click the following icon to distribute the policy:

8.8.6 Configuring a third-party HTTP proxy for Software Updater

You can set up Software Updater to receive its updates through an external HTTP proxy.

As of version 12.20, Policy Manager works as a proxy for the software update packages by default, and the default cache size is set to 10 GB (you can configure this setting in Policy Manager Console). However, some organizations or network setups may require the use of a dedicated third-party proxy.

To configure the proxy and caching for Software Updater updates:

1. Install and configure the proxy of your choice.
   For example, with Squid, make the following configurations in `squid.conf`:
   a) Set the disk cache to 100 GB:
   ```
   cache_dir ufs /var/spool/squid 100000 16 256
   ```
   b) Set the maximum caching file size:
   ```
   maximum_object_size 2048 MB
   ```
   c) Configure the proxy to be used for software updates only (Software Updater is identified by its User-Agent name):
   ```
   acl FSecSwUp browser F-SecureSoftwareUpdater
   http_access allow FSecSwUp
   http_access deny all
   ```

Once the caching proxy is up and running, it needs to be added to the Software Updater policy.

2. Configure the Software Updater policy in **Advanced view**:
   a) Set **F-Secure Software Updater** > **Settings** > **Communications** > **Use HTTP Proxy** to **User-defined**
   b) In **F-Secure Software Updater** > **Settings** > **Communications** > **User-defined proxy**, enter the address and port for the proxy (`http://<proxy_address>:<port_number>`).

8.9 Rapid Detection & Response

You can manage the distribution and basic operations of F-Secure Rapid Detection and Response sensors with Policy Manager.

Note: More advanced incident-related information and operations are available in the F-Secure Rapid Detection and Response portal. Click here to see the documentation for the portal.

F-Secure Rapid Detection and Response is a leading context-level endpoint detection and response (EDR) solution for companies.

Organizations can be breached in many ways. Increasingly, the attacks are fileless and do not require attackers to install malware on desktops or laptops. Advanced Persistent Threats (APT) and cyber threats are an extremely costly problem for companies. They are difficult to recognize just using traditional protection methods. Also, these attacks can be difficult to analyze and respond to. Defending against these attacks requires both the latest technological solutions and the expertise to analyze and understand the available data.

With its deep bi-directional intelligence and high level of automation, F-Secure Rapid Detection and Response protects against advanced threats even before breaches happen. It detects incidents with lightweight sensors, which are installed on monitored hosts in the organization. Sensors collect data on behavioral events, such as files being accessed, processes or network connections being created, or something being written into the registry or system log. These events are then further analyzed in the backend. The solution does not just to do real-time detections, but also makes detections based on applying new rules to old data.

Often targeted attacks could go unnoticed for months or even years. With F-Secure Rapid Detection and Response, you can prevent the attack from breaching critical servers through the targeted hosts.

8.9.1 Activating endpoint sensors

Endpoint sensors are lightweight, discreet sensors, which are included in Client Security 14.10 and Server Security 14.00 and newer. These sensors collect behavioral data from endpoint devices and are specifically designed to withstand a wide range of attacks.

You need an activation keycode for registering the Rapid Detection and Response (RDR) sensors. Contact your F-Secure partner to get your RDR for Business Suite keycode.

In **Standard view**:

1. Select the target domain.
2. Go to the **Settings** tab and select **Windows** > **Rapid Detection & Response**.
3. Enter your sensor activation keycode for the corresponding host type (workstations or servers).
4. Select **Enable Rapid Detection & Response**.
5. Click the following icon to distribute the policy:

8.9.2 Checking the status of endpoint sensors

You can see the status of deployed Rapid Detection and Response endpoint sensors on the **Status** tab.

Policy Manager shows you the connection status of the sensors as well as any errors related to activation, for example if the subscription is not valid or has expired.

To check the status of endpoint senors:

Select the **Status** tab and go to the **Rapid Detection & Response** page.
This page shows you basic information on the endpoint sensors in your managed network.

More details and operations are available in the Rapid Detection & Response portal. The **Status** > **Rapid Detection & Response** page in Policy Manager has a link that opens the portal in your web browser. You will receive access credentials for the portal in connection with your sensor activation keycodes.

8.9.3 Isolating hosts from the network

You can isolate one or more hosts from the network.

Note: Use network isolation with caution and only in case of a network attack.

To isolate a host from the network:

1. Select the target host in the policy domain tree.
2. Go to the **Operations** tab.
3. Click **Isolate** under **Network isolation**.
   This isolates the selected host from the network.
4. To reconnect an isolated host to the network, click **Release** on the **Operations** tab.

Isolated hosts are shown on the **Host issues** section of the dashboard.

Chapter

9

Virus information

Topics:

- Malware information and tools on the F-Secure web pages
- How to send a virus sample to F-Secure

This section contains useful general information about viruses and virus handling.

9.1 Malware information and tools on the F-Secure web pages

You can find a list of sources of information about malware and useful tools on the F-Secure web site.

For information of the latest security threats you can check these sources:

- The F-Secure blog: https://labsblog.f-secure.com/
- A list of vulnerabilities in common software is here: https://www.f-secure.com/en/web/labs_global/vulnerability-protection
- You can also read our guidelines for dealing with threats here: https://www.f-secure.com/en/web/labs_global/removal-instructions

Before sending us a sample you may consider trying our **Rescue CD**. This is a tool that starts it's own operating system and so can find some malware that cannot be found from within Windows. You can find it here: https://www.f-secure.com/en/web/labs_global/rescue-cd.

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

9.2 How to send a virus sample to F-Secure

This section covers information on sending a virus sample to the F-Secure Labs.

9.2.1 How to package and send a virus sample

All files should be sent in ZIP archive only.

To package the virus samples you can download a trial version of WinZip at http://www.winzip.com/. A free InfoZIP utility is also available at http://www.info-zip.org/pub/infozip/.

All ZIP packages should be named using only English letters and numbers. You can use long file names.

To be sure that we receive the ZIP archive, protect the ZIP file with the password `infected`. Otherwise any malware sample you attempt to send to us may be removed by an intermediary server as a safety measure. Using the "infected" password is an industry standard, and content scanning gateways that scan HTTPS traffic usually let it through. If the file is corrupted along the way, please contact the vendor of your content scanning gateway, or allow the `analysis.f-secure.com` server in your gateway configuration.

Submit the packaged sample through the F-Secure sample submission portal at https://www.f-secure.com/sas.

9.2.2 Finding new malware

If you suspect that your computer has an unknown infection that is not detected by your antivirus software, you can use this checklist to get more information.

1. Check the root of %PROGRAMFILES%, %APPDATA%, %PROGRAMDATA% for any `exe` files or directory names that look randomly generated.
2. Download Autoruns, Process Explorer, and Sigcheck from Microsoft Sysinternals (http://sysinternals.com).

   Note: You should do this on a separate system and rename the tools, as malware quite often self-terminates when it detects Sysinternals tools and knows that it is being investigated.

3. Check all automatically starting programs with Autoruns.

   To get more readable results, use filtering options to hide signed and Microsoft files. However, some malware uses stolen certificates or install a fake root certificate, so use this approach with caution.

   Entries with "(verified)" in the publisher column are unlikely to be malware.
4. If Autoruns did not find anything, check your system with Process Explorer.
5. Use Sigcheck to check the integrity of file signatures.
   Anything with a broken signature is either infected with a virus or indicates a disk problem.
6. Check your system with GMER rootkit detector (http://www.gmer.net/).

9.2.3 What should be sent

Here you will find what files and details to send, as viruses are not all of the same type, so they cannot all be sent in one specific way.

Note: As a rule of thumb, if a file is already detected and is not a false alarm, there is no need to send us a sample.

The following lists what to send according to the virus types:

1. Malware (malicious programs):

   If you are sending a sample of a suspected standalone malware (worm, backdoor, trojan, dropper), specify the location of the file on the infected system and the way it was started (registry, `.ini` files, `Autoexec.bat`, etc.). A description of the source of the file is also useful.

2. A false alarm from one of our antivirus products:

   If you receive a missed or incorrect detection, or a false alarm with Client Security, check that you have the latest virus definition databases in use. If you still get a false alarm even with the latest databases in use, try to send us the following:

   - the file in question,
   - the Client Security version number,
   - the last virus definition updates date,
   - a description of the system configuration,
   - a description of how to reproduce the problem, and
   - the Client Security scanning report file.

3. An infection or a false alarm on a CD:

   If an infection or false alarm is on a CD, you can send the CD to our office in Finland.

   Please include a description of the problem, and a printed Client Security report, if possible. We will return your CD if it has no infection. Send the CD and accompanying information to:

   Virus information

   Security Labs

   F-Secure Corporation

   Tammasaarenkatu 7

   PL 24

   00181 Helsinki

   Finland

Chapter

10

Windows Management Instrumentation

Topics:

- WMI integration
- WMI classes for integration

Policy Manager provides Windows Management Instrumentation (WMI) integration, which you can use, for example, to integrate Remote Monitoring and Management (RMM) tools with Client Security.

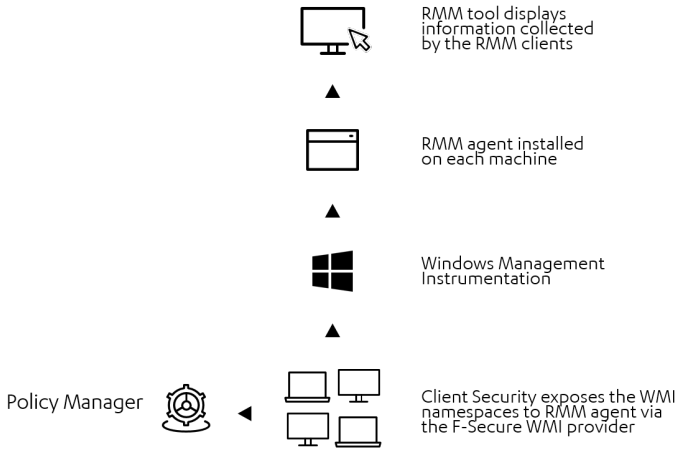
On a service provider level, WMI integration is often used to provide better management of several functions, such as asset discovery and management, configuration, process and service automation, security services, and backups.

10.1 WMI integration

F-Secure Policy Manager uses a Windows Management Instrumentation (WMI) interface to collect read-only status information on F-Secure client applications.

The WMI interface uses a vendor-specific agent installed on the host to forward the collected information to the management console server. No configuration options or general security management functionality are exposed through the WMI interface.

Administrators can also use the WMI interface to remotely start a full scan of the host computers.



The following classes can be retrieved from Client Security clients through the WMI interface:

- Product version
- Real-time scanning status
- Virus definition database information
- Firewall status
- Firewall security level (profile)
- Firewall versions
- Application Control status
- Time of last connection to Policy Manager
- Time of last policy update from Policy Manager
- Name of Policy Manager profile in use
- DeepGuard status
- Browsing protection status
- Email filtering status
- Software Updater status (status of automatic installation of security updates, counts for missing updates split by type; critical, important, and other)

10.2 WMI classes for integration

This appendix provides details on the classes used for Windows Management Instrumentation (WMI) integration in F-Secure Policy Manager.

10.2.1 WMI classes

This section provides details on the classes used for WMI integration in the product.

AvDefinition

Provides information on the Anti-Virus engine.

Property Name	Description	Type
EngineId	Unique identifier of the corresponding engine.	uint32
EngineName	User-friendly name of the corresponding engine.	string
EngineVersion	Version of the corresponding engine.	string
UpdateSerialNumber	Unique identifier of the installed update.	string
UpdateTime	Time when the update was installed.	datetime

AvScanResult

Result of the scan for viruses.

Property Name	Description	Type
StartTime	Time when scan was started.	datetime
EndTime	Time when scan finished.	datetime
InfectedFilesCount	Number of infected files found in the scan.	uint32
InfectedSectorsCount	Number of infected sectors found in the scan.	uint32
ScanningReportFilePath	File path to the scan report.	string

Profile

Provides information on the currently installed profile.

Property Name	Description	Type
ProfileName	User-friendly name of the profile.	string
SeriesName	Name of the profile package.	string
InstallationTime	Time when the profile was installed.	datetime

Component

Provides a summary for the product component.

Property Name	Description	Type
Enabled	State of the component.	boolean

SimpleComponent : Component

Default implementation of the base class.

Property Name	Description	Type
Enabled		boolean

API

Provides basic information on the F-Secure WMI namespace API.

Property Name	Description	Type
Version	Actual version of this API.	string

Product

Provides information on the currently installed security product.

Property Name	Description	Type
Name	Name of the product.	string
Version	Version of the product.	string
Build	Build of the product.	string

AntiVirus

Provides information on anti-virus modules and allows running a full computer scan.

Property Name	Description	Type
RealTimeScanning	Status information for real-time scanning.	Component
DeepGuard	Status information for DeepGuard.	Component
AvDefinitionsUpdateTime	Time of latest update to Anti-Virus definitions.	datetime
AvDefinitions	List of installed Anti-Virus engines.	AvDefinition

Method Name	Description	Return Type
ScanComputer	Starts a full computer scan and waits for completion.	AvScanResult

Firewall : Component

Provides information on F-Secure Firewall.

Property Name	Description	Type
Enabled	Current state of F-Secure Firewall.	boolean
SecurityLevel	Current security level of F-Secure Firewall.	string
ApplicationControl	Current state of Application Control.	Component
Version	Version of F-Secure Firewall.	string
Build	Build of F-Secure Firewall.	string

CentralManagement

Provides information on interaction with the protection service.

Property Name	Description	Type
LastConnectionTime	Time of the last connection to the protection service.	datetime
PolicyUpdateTime	Time of latest policy update.	datetime
Profile	Currently installed profile.	Profile

SoftwareUpdater : Component

Provides information on F-Secure Software Updater.

Property Name	Description	Type
Enabled	State of F-Secure Software Updater.	boolean
InstallSecurityUpdatesAutomatically	Type of updates installed automatically by Software Updater. • 0: None • 1: Critical • 2: Critical and important • 3: All	uint32

Property Name	Description	Type
MissingCriticalUpdatesCount	Number of missing critical updates.	uint32
MissingImportantUpdatesCount	Number of missing important updates.	uint32
MissingOtherUpdatesCount	Number of missing updates other than critical and important.	uint32

Internet

Provides information on Internet security components.

Property Name	Description	Type
BrowsingProtection	State of browsing protection.	Component
EmailFiltering	State of email filtering.	Component

Host identifier

Provides information on the managed host.

Property Name	Description	Type
HostIdentity	Unique identifier for the host.	string
HostIdentityType	Type of the host's unique identifier (for example `SMBIOSGUID`, `RANDOMGUID`, `WINS`, or `MAC`).	string

Chapter

11

Troubleshooting

Topics:

- Policy Manager Server and Policy Manager Console
- Policy Manager Web Reporting
- Policy distribution
- Frequently asked questions for Linux versions

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

11.1 Policy Manager Server and Policy Manager Console

Issues regarding Policy Manager Server and Policy Manager Console.

Why doesn't Policy Manager Server start?

Runtime errors, warnings and other information can be found in the files:

`<F-Secure>\Management Server 5\logs\fspms-webapp-errors.log` and `<F-Secure>\Management Server 5\logs\fspms-service.log`

Check that the access rights (`properties/security/permissions`) includes the Local Service user account. If Local Service is not listed as an authorized user, add the user manually, and set the access rights to **Full Control**. Propagate the access rights to the `Management Server 5` directory (by default `C:\Program Files\F-Secure\Management Server 5`, or `C:\Program Files (x86)\F-Secure\Management Server 5` on 64-bit operating systems) and all its subdirectories. After these changes, restart the Policy Manager Server service or reboot the computer.

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.

Where are the log files and configuration files located for Policy Manager Server?

The log files are located in:

`<F-Secure>\Management Server 5\logs`

The configuration files are in:

`<F-Secure>\Management Server 5\config`

Where are the Policy Manager Console log files located?

The log file is:

`<F-Secure>\Administrator\lib\administrator.error.log`

Policy changes applied with the **Distribute policy** operation are logged to:

`fspms-policy-audit.log`

I have lost the admin password. Can I retrieve or reset the password?

If you have lost the password for the `admin` user, or if the account was accidentally deleted, you can reset the user account for Policy Manager on Windows with the following tool:

`<F-Secure>\bin\reset-admin-account.bat`

For Policy Manager on Linux, use the following script to reset the user account:

`/opt/f-secure/fspms/bin/fspms-reset-admin-account`

Note: You need to stop Policy Manager Server manually before running the reset tool.

How can the server role change stop Policy Manager Server from working?

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.

The easiest way to restore Policy Manager Server after a server role change is to re-install Policy Manager Server with the **Keep existing settings** option selected. This will recreate the Policy Manager Server account and reset all file access rights to the correct ones.

How can Windows security hardening stop Policy Manager Server from working?

Access rights restrictions, especially restrictions under the `%SystemRoot%` directory (`c:\windows` or `c:\winnt`) 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.

You must allow the Local Service account to 'read' the following directories:

`%SystemRoot%`

`%SystemRoot%\system32`

`%SystemRoot%\system32\drivers`

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.

Why does Policy Manager Console lose the connection to Policy Manager Server?

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.

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.

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.

Useful Windows networking settings are:

`HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\MaxUserPort` (maximum number of network ports, default = 5000)

`HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpTimedWaitDelay` (time to wait before closing inactive network connection, default = 240 seconds).

The `netstat -an` command can be used to check whether there are too many connection open to the server.

How can I change the ports where the server listens for requests?

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.

If you need to change the port numbers after installation:

1. Stop Policy Manager Server.
2. Open the `HKEY_LOCAL_MACHINE\SOFTWARE\Data Fellows\F-Secure\Management Server 5` registry key. On 64-bit operating systems, the registry key path is `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data Fellows\F-Secure\Management Server 5`.
3. Edit the `AdminPortNum` (admin module), `HttpPortNum`, and `HttpsPortNum` (host module) values and enter the new port numbers.

   Make sure **Decimal** is selected as the **Base** option when entering the new port number.
4. Start Policy Manager Server.

Caution: If you have workstations already configured to access Policy Manager Server (through the Policy Manager Server host module) you should not change the Policy Manager Server host port where agents communicate, since you might reach a state where the workstations will not be able to contact the server.

11.2 Policy Manager Web Reporting

The locations of log and configuration files.

The log files are located in:

`<F-Secure>\Management Server 5\Web Reporting\logs`

The configuration files are in:

The `HKEY_LOCAL_MACHINE\SOFTWARE\Data Fellows\F-Secure\Management Server 5` registry key

See also the Policy Manager Server configuration files:

`<F-Secure>\Management Server 5\config`

11.3 Policy distribution

Information on error messages you may see during policy distribution, and for the reasons and solutions.

"<setting name>" has value out of restriction **"<setting name>" has invalid restriction** **"<setting name>" has invalid value: "<value>"**	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. When a domain includes hosts that have different product versions installed, the MIB settings from the newest product version are used for editing the policy values. As result, policy distribution may fail on hosts that have older versions of the software installed, because the older versions do not support the new policy settings or values. Reason 2: You entered an integer value that is outside of the range restrictions. Solution: 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: **1.** Group the hosts into subdomains based on the installed product version. For example, group hosts that have Client Security 6.x installed into one sub-domain, and hosts that have Client Security 7.x installed into another domain. **2.** Set most of the settings on the root domain and create a sub-domains for exceptions. This is a good solution if you have only a few hosts with the older software versions installed.
"<setting name>" is required but undefined	Reason: The setting is required but it is currently empty. Solution: Enter a value or apply the **Clear** operation to re-inherit the value from parent domain or MIB. If the value is empty on several domain levels, you may need to apply the **Clear** operation several times.

11.4 Frequently asked questions for Linux versions

You can find answers to common problems on Linux platforms here.

Question	Answer
Where are the log files and configuration files located in the Linux version?	You can list all files and their places by entering the following commands as a normal user: • RPM-based distributions: `rpm -ql f-secure-<component_name>`. • Debian-based distributions: `dpkg -L f-secure-<component_name>`. You will find the log files in the following locations: • Policy Manager Console: `/opt/f-secure/fspmc/lib/Administrator.error.log`. • Policy Manager Server: `/var/opt/f-secure/fspms/logs`. You will find the configuration files in the following locations: • Policy Manager Console: `/opt/f-secure/fspmc/lib/Administrator.properties`. • Policy Manager Server: `/etc/opt/f-secure/fspms/fspms.conf`.
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 http://www.pathname.com/fhs/.
Why doesn't Policy Manager Server start?	Make sure you have run the configuration script: `/opt/f-secure/fspms/bin/fspms-config`. You can also check that the ports configured for Policy Manager Server are active by logging in as `root` and running the `netstat -lnpt` command.
How can I start, stop, restart or check the status of Policy Manager components?	Policy Manager Server: `/etc/init.d/fspms {start|stop|restart|status}`
How can I specify an HTTP proxy?	The HTTP proxy configuration file is located in the server's data folder `/var/opt/f-secure/fspms/data/fspms.proxy.config`. Remember to restart Policy Manager Server 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: `/opt/f-secure/fspms/bin/fspms-config`.
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: `/opt/f-secure/fspms/bin/fspms-config`.
Can I set up my own schedule for updating F-Secure virus definitions?	The server refreshes metadata for the latest F-Secure updates every 10 minutes by default. To modify the default interval for refreshing the updates metadata, use the following additional Java argument: `-DupdatePollingInterval=n`, where `n` is minutes, any integer value >= 1.

Question	Answer
How can I update F-Secure virus definitions manually?	As of version 13.00, Policy Manager Server does not support manual polling as used for Automatic Update Agent in previous versions. Restart Policy Manager Server to force a virus definitions check or customize the polling interval as described in the previous question.
How can I publish F-Secure virus definitions manually from the latest `fsdbupdate` package?	As of version 13.00, Policy Manager Server does not support `fsdbupdate.run` as used for Automatic Update Agent in previous versions. For details on the new solution, see Updating malware definitions in isolated networks on page 46 .
How can I stop downloading some or all 12.x updates?	The server automatically stops downloading all 12.x updates when all clients are upgraded to newer versions. You can modify the subscription list manually in the `/opt/f-secure/fspms/config/channels.json` configuration file.
Is there any diagnostic tool I can use?	Yes. Please use `fsdiag` to collect information about your system and related packages. When logged in as root, run: `/opt/f-secure/fspms/bin/fsdiag` All relevant information will be stored into the `fsdiag.tar.gz` archive located in the current directory. You can then send that file to F-Secure Customer Support by request.
How can I install software to remote hosts from Policy Manager Console on Linux?	You can export installation packages to JAR files and use the `ilaunchr.exe` tool to install software on hosts, for example by using logon scripts. Please follow the process defined in the manual. You will find the `ilaunchr.exe` tool in the `/opt/f-secure/fspmc/bin` directory.
How can I configure Policy Manager for use in large environments?	• Increase the `Host polling interval` values to 30 - 60 minutes in Policy Manager Console. • Use Policy Manager Proxy installation(s) to minimize the load on Policy Manager Server caused by serving policies, database updates, software updates, and installation packages to clients.

Appendix A

Configuring older versions of Client Security

Topics:

- Configuring spyware scanning
- Configuring alert sending
- Excluding a web site from HTTP scanning
- Firewall settings for Client Security 13 and older
- Configuring Network access control
- Advanced features: firewall

This section contains information on settings that only apply to F-Secure Client Security versions 13 and older.

Related concepts

Managing endpoint security on page 69

A.1 Configuring spyware scanning

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

Note: F-Secure Client Security versions 14 and newer do not support the spyware scanning settings included in distributed policies.

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

A note about cleaning spyware and riskware

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

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

A.1.1 Setting up spyware control for the whole domain

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

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

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

In **Standard view**:

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

      Alternatively, you can launch a manual spyware scan on the hosts.
   e) Click the following icon to distribute the policy:

2. Check the reported spyware and riskware:

   A list of the spyware and riskware found during the scanning is displayed in the **Spyware and riskware reported by hosts** table. This table is shown on the **Spyware control** page.
   a) Check the list of reported spyware and riskware.
   b) If there are applications that are needed in your organization, select the application in the table and click **Exclude application**.
      A dialog asking you to confirm the action is opened.
   c) Check the information displayed in the dialog, and if you are sure you want to allow the spyware or riskware to run on the host or domain, click **OK**.
      The selected application will be moved into the **Applications excluded from spyware scanning** table.

3. If you want to make sure that users cannot allow any spyware or riskware to run on their computers, set **Allow users to define the allowed spyware items** is set to **Not allowed**.
4. Check that the manual scanning settings are valid for the managed domain.
5. Click the following icon to distribute the policy:

A.1.2 Launching spyware scanning in the whole domain

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

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

In **Standard view**:

1. Select **Root** on the **Domain tree**.
2. As the manual scanning task also includes manual virus scanning, check the settings on the **Settings** > **Windows** > **Manual scanning** page, and modify them if necessary.
3. Go to the **Operations** tab and click the **Scan** button under **Virus and spyware scan**.

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

4. Click the following icon to distribute the policy:

A.1.3 Allowing the use of a spyware or riskware component

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

In **Standard view**:

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

A.2 Configuring alert sending

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

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

A.2.1 Sending virus alerts to an email address

In this example, all the security alerts that the managed hosts generate are forwarded to an email address.

In **Standard view**:

1. Select **Root** on the **Domain tree**.

2. Go to the **Settings** tab and select **Windows** > **Alert sending**.
3. Set up **Email alert sending**:

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

   a) Enter the address of the SMTP server in the **Email server address (SMTP)** field.

      Use the following format:

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

   b) Enter the sender's address for email alert messages in the **Email sender address (From):** field.

   c) Enter the email alert message subject in the **Email subject:** field.

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

4. Set up **Alert forwarding**:

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

   a) Select the **Email** check box on the **Security alert** row.
      This opens the **Email recipient addresses (To)** dialog box.

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

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

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

5. Click the following icon to distribute the policy:

A.2.2 Disabling alert pop-ups

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

In **Standard view**:

1. Select **Root** on the **Domain tree**.
2. Go to the **Settings** tab and select **Windows** > **Alert sending**.
3. Clear the check boxes for all products in the **Local user interface** column.
4. Click the following icon to distribute the policy:

A.3 Excluding a web site from HTTP scanning

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

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

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

In **Standard view**:

1. Select **Root** on the **Domain tree**.
2. Go to the **Settings** tab and select **Windows** > **Web traffic scanning**.
3. Exclude a domain from HTTP scanning:

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

   a) Click the **Add** button under the **Trusted sites** table.
      This creates a new line in the table.

   b) Click on the line you just created so that it becomes active, and enter `http://*.example.com/*`.
      This excludes all the sub-domains.

   c) Click the **Add** button under the **Trusted sites** table.

This creates another new line in the table.

d) Click on the line you just created so that it becomes active, and enter `http://example.com/*`.
This excludes the second-level domain.

4. Exclude a sub-directory from HTTP scanning:

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

   a) Click the **Add** button under the **Trusted sites** table.
   This creates a new line in the table.

   b) Click on the line you just created so that it becomes active, and enter `http://www.example2.com/news/*`.

5. Click the following icon to distribute the policy:

A.4 Firewall settings for Client Security 13 and older

This section describes the settings that you can configure for F-Secure's firewall.

Related concepts

Configuring firewall settings on page 80

This section provides an overview of the firewall settings and how you can configure them to suit your network.

A.4.1 Configuring security levels and rules

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

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

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

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

Selecting an active security level for a workstation

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

In **Standard view**:

1. Select the **Desktops/Eng.** subdomain on the **Domain tree**.
2. Go to the **Settings** tab and select **Windows** > **Firewall**.
3. Click **13.x clients**.
4. Select **Office** from the **Host security level** drop-down list.
5. To restrict users from changing the setting, click the lock symbol beside it.
6. Click the following icon to distribute the policy:

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

Note: If the selected security level cannot be used for some reason, the default security level is used instead.

Configuring a default security level for the managed hosts

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

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

In **Advanced view**:

1. Select the **Laptops/Eng.** domain on the **Policy domains** tab.
2. Go to the **F-Secure Internet Shield** > **Settings** > **Security Level** > **Default Security Level** page.
3. Select the security level to use as a default from the drop-down list.
4. Click the following icon to distribute the policy:

Adding a new security level for a certain domain only

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

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

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

Create the new security level

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

In **Advanced view**:

1. Select **Root** on the **Domain tree**.
2. Go to the **F-Secure Internet Shield** > **Settings** > **Security Level** > **Security Levels** page.
3. Click **Add** to add a new security level.
   This opens the **Security Level Wizard**.
4. Enter an ID, name, and description for the new security level.

   For this example, enter `BrowserSecurity` as the name.
5. Click **Next**.
6. Select the filtering mode for the security level.

   For this example, select **Normal**.
7. Click **Finish**.
8. Click the following icon to distribute the policy:

Create rules for the new security level

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

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

1. Go to the **F-Secure Internet Shield** > **Settings** > **Rules** page.
2. From the **Security level being edited** drop-down list, select the **BrowserSecurity** security level that you just created.

   The **Firewall rules** table is empty when this security level is selected, because there are no associated rules yet.
3. Click **Add before** to add a rule that allows outbound HTTP traffic as the first one on the list.
   This opens the **Firewall rule** wizard.
4. Complete the **Firewall rule** wizard:
   a) On the **Rule type** page select **Allow** as the rule type.
   b) On the **Remote hosts** page select **Any remote host** to apply the rule to all Internet connections.
   c) On the **Services** page select **HTTP** in the **Service** column to apply the rule to HTTP traffic.
   d) On the **Services** page select **=>** in the **Direction** column to apply the rule to outbound connections only.

e) On the **Advanced settings** page you can accept the default values.

f) Verify the new rule on the **Summary** page.

You can also add a descriptive comment for the rule; for example, `Allow outbound HTTP traffic for browsing.`.

g) Click **Finish**.

5. Click **Add after** to add a rule that denies all other traffic both ways as the last one on the list.
6. Complete the **Firewall rule** wizard:

a) On the **Rule type** page select **Deny** as the rule type.

b) On the **Remote hosts** page select **Any remote host** to apply the rule to all connections.

c) On the **Services** page select **All traffic** in the **Service** column to apply the rule to all traffic.

d) On the **Services** page select **Both** in the **Direction** column to apply the rule to inbound and outbound connections.

e) On the **Advanced settings** page you can accept the default values.

f) Verify the new rule on the **Summary** page.

You can also add a descriptive comment for the rule. For example, `Deny rest`.

g) Click **Finish**.

Take the new security level into use

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

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

1. Select **Root** on the **Domain tree**.
2. Go to the **F-Secure Internet Shield** > **Settings** > **Security Level** > **Security Levels** page.
3. Turn off the **BrowserSecurity** security level by clearing the **Enabled** check box beside it on the **Security Levels** table.
4. On the **Policy domains** tab, select the subdomain where you want to use this security level.
5. Turn on the **BrowserSecurity** security level by selecting the **Enabled** check box beside it on the **Security Levels** table.
6. Go to the **F-Secure Internet Shield** > **Settings** > **Security Level** > **Active Security Level** page.
7. Set the new security level as the active security level by selecting it from the drop-down list.
8. Click the following icon to distribute the policy:

A.4.2 Configuring rule alerts

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

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

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

Adding a new rule with alerting

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

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

Select the rule type and denied service

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

In **Standard view**:

1. Select the subdomain for which you want to create the rule on the **Domain tree**.
2. Go to the **Settings** tab and select **Windows** > **Firewall**.
3. Click **13.x clients**.
4. Select the firewall security level for which you want to add the new rule from the **Security level being edited** drop-down menu.
   Now all the rules that have been defined for this firewall security level are displayed on the table.
5. Click **Add before** to add the new rule as the first one on the list.
   This opens the **Firewall rule** wizard.
6. Select **Deny** to deny the inbound ICMP connections.
7. Specify affected hosts.

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

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

   For this rule, select **Any remote host**.
8. Choose the denied service and direction for the rule.

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

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

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

   For this rule, select:

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

Define the advanced options

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

To do this:

1. Define whether the rule is applied only when a dial-up link is open by selecting or clearing the check box.
   a) Define whether the rule is applied only when a dial-up link is open by selecting or clearing the check box.
   b) Select the alert type in the **Send alert** drop-down list.

      For this rule select **Security alert**.
   c) Select the alert trap to be sent in the **Alert trap** drop-down list.
   d) Enter a descriptive comment for the alert in the **Alert comment:** field.
   e) You can accept the default values for the rest of the fields in this window.
2. Select the alert type in the **Send alert** drop-down list.
3. Select the alert trap to be sent in the **Alert trap** drop-down list.

   For this rule select **Network event: inbound service denied**.

4. Enter a descriptive comment for the alert in the **Alert comment:** field.

   This comment is displayed in the Client Security local user interface.

5. You can accept the default values for the rest of the fields in this window.
6. Review and accept the rule.

   You can review your rule now. You can also add a descriptive comment for the rule to help you understand the rule when it is displayed in the **Firewall rules** table. If you need to make any changes to the rule, click **Back** through the rule.

7. If you are satisfied with your new rule, click **Finish**.
   Your new rule will be added to the top of the list in the active set of rules on the **Firewall rules** page.

Configure alert forwarding

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

To do this:

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

Apply and test the new rule

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

To do this:

1. Make sure that you have the correct subdomain selected on the **Domain tree**.
2. Go to the **Settings** tab and select **Windows** > **Firewall**.
3. Click **13.x clients**.
4. Set the security level for which you created the rule as the active security level by selecting it from the **Host security level** drop-down list.
5. Click the following icon to distribute the policy:

6. Test the rule you created.

   You can test the rule you just created by pinging one of the managed hosts in the subdomain from a computer outside of that domain. When you have done this, you can check that the rule works as follows:

   a) Select the subdomain for which you created the rule on the **Domain tree**.
   b) Go to the **Dashboard** tab, and check if any new security alerts are displayed for the domain.
   c) To see the alert details, click **Summary** > **View alerts by severity**.
      This takes you to the **Alerts** tab that displays a detailed list of security alerts.

A.4.3 Using alerts to check that the firewall works

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

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

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

In **Standard view**:

1. Go to the **Settings** tab and select **Windows** > **Firewall**.
2. Click **13.x clients**.
3. Select the security level you want to use for testing purposes.
4. To start the creation of the new rule, click **Add before**.

This starts the **Firewall rule** wizard.

5. Select **Allow** on the **Rule type** page.
6. Select **Any remote host** on the **Remote hosts** page.
7. On the **Services** page, select **Ping** from the **Service** drop-down list, and **Both** from the **Directions** drop-down list.
8. On the **Advanced options** page, select the following options:
   - **Security alert** from the **Send alert** drop-down list
   - **Network event: Potentially dangerous service allowed** from the **Alert trap** drop-down list
   - You can also enter a comment for the alert in the **Alert comment** field.
9. On the **Summary** page you can verify that the rule is correct and enter a descriptive comment for the rule.
10. Click the following icon to distribute the policy:

11. You can now test the rule by pinging one of the managed hosts and checking that an alert is created and displayed on the **Alerts** tab.

A.5 Configuring Network access control

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

Note: Network access control is only available for F-Secure Client Security versions 13 and older.

Note: Network access control was named Application control in previous versions of Policy Manager.

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

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

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

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

How Network access control and DeepGuard work together

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

An example:

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

A.5.1 Setting up Network access control for the first time

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

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

1. Create a list of known applications:
   a) Create a test environment with, for example, two computers, that have the programs normally used in your company installed.
   b) Import these hosts to the centrally managed domain.
   c) Select **Report new unknown applications**, so that the new applications will appear on the **Unknown applications reported by hosts** list.
   d) Define the allow rules for these applications.
   e) When you have existing rules for all the necessary applications, this set of rules can be distributed as a policy to the entire managed domain.
2. Configure the basic settings that will be used when Network access control is running:
   a) Select the default action to take when an unknown application tries to make an outbound connection from the **Default action for client applications** drop-down list.
   b) Select the default action to take when an unknown application tries to make an inbound connection **Default action for server applications** drop-down list.
   c) Set the new applications to be reported to the administrator by selecting **Report new unknown applications**. This way you can see what kind of applications the end users are trying to launch, and you can define new rules for them if necessary.
   d) Define whether the default messages are displayed to users when an unknown application tries to make an inbound or an outbound connection by selecting or clearing **Show default messages for unknown applications**.
3. Verify the settings and take them into use.

   Network access control can be enabled for the whole domain as follows:
   a) Select **Root** on the **Domain tree**.
   b) Go to the **Settings** tab and select **Windows** > **Network access control**.
   c) Make sure that **Enable network access control** is selected.
   d) Click the following icon to distribute the policy:

A.5.2 Creating a rule for an unknown application on root level

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

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

In **Standard view**:

1. Select the application(s) for the rule:
   a) Go to the **Settings** tab and select **Windows** > **Network access control**.
   b) Select **Internet Explorer 4.01** in the **Unknown applications reported by hosts** table.
   c) Click **Create rule(s)** to start the application control rule wizard.
2. Select application rule type:
   a) Select **Deny** as the action to take when the application acts as a client and tries to make an outbound connection.
   b) Select **Deny** as the action to take when the application acts as a server and an inbound connection attempt is made.
3. Select the message shown to users:
   a) Select whether a message is shown to users when a connection attempt is made.

      The options are: **No message**, **Default message** or **Customized message**.

      If you selected **Default message**, you can check what the currently defined default messages are by clicking **Define default messages...**.

b) If you selected **Customized message**, the customized message text box is activated and you can enter the message there.

In this case you could use a customized message, for example: `The use of Internet Explorer 4 is prohibited by company security policy. Please use some other browser instead.`

4. Select the rule target:
   a) Select the domain or host that the rule affects from the domains and hosts displayed in the window.

      If the target host or domain already has a rule defined for any of the applications affected by the rule, you are prompted to select whether to proceed and overwrite the existing rule at the host.

      In this example select **Root**.

   b) When the rule is ready, click **Finish**.
      The new rule is now displayed in the **Application rules for known applications** table. The **Unknown applications reported by hosts** table has been refreshed.
5. Click the following icon to distribute the policy:

A.5.3 Editing an existing Network access control rule

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

In **Standard view**:

1. Select the rule to be edited:
   a) Go to the **Settings** tab and select **Windows** > **Network access control**.
   b) Select the rule which you want to edit in **Rules for known applications**.
   c) Click **Edit** to start the Network access control rule wizard.
2. Edit the application rule type:
   a) Select the action to take when the application acts as a client and tries to make an outbound connection.

      In this case select **Allow** for **Act as client (out)**.

   b) Select the action to take when the application acts as a server and an inbound connection attempt is made.
3. Select the message shown to users.

   Select whether a message is shown to users when a connection attempt is made.
4. Select the new rule target:
   a) Select the domain or host that the rule affects.

      In this case select **Engineering/Testing**.

      If the target host or domain already has a rule for any of the applications affected by the rule, you are prompted to select whether to proceed and overwrite the existing rule at the host.

   b) When the rule is ready, click **Finish**.
      The modified rule is now displayed in the **Application rules for known applications** table. It is a copy of the original rule with the changes you just made.
5. Click the following icon to distribute the policy:

A.5.4 Turning off Network access control pop-ups

When you want to configure Network access control so that it is totally transparent to the end users, all pop-ups have to be turned off.

In **Standard view**:

1. Select **Root** on the **Domain tree**.

2. Go to the **Settings** tab and select **Windows** > **Network access control**.

   On this page select:

   - **Allow** from the **Default action for server applications** drop-down list.
   - **Allow** from the **Default action for client applications** drop-down list.

3. When creating any rules with the **Network access control rule** wizard, select:

   - Either **Allow** or **Deny** as the action on incoming and outgoing connection attempts in the **Application rule type** dialog box.
   - **No message** in the **Message shown to users** dialog box.

4. Click the following icon to distribute the policy:

A.6 Advanced features: firewall

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

Note: The topics in this section only apply to F-Secure Client Security versions 13.x and older.

A.6.1 Managing firewall properties remotely

This section describes how you can manage firewall properties remotely.

Using packet logging

Packet logging is a very useful debugging tool to find out what is happening on the local network.

Packet logging is also a powerful tool that can be abused by the end user to eavesdrop on the activities of other users on the LAN, and this means that in some corporate environments the administrator needs to disable the packet logging.

In **Advanced view**:

1. Select the target domain.
2. Select **F-Secure Internet Shield** > **Settings** > **Packet logging** > **Active**.
   This variable shows the status of the packet logging; **Disabled** means that it is not running, and **Enabled** that it is currently running on the host.
3. To turn off logging completely, make sure that it is set to **Disabled**, and select **Disallow user changes**.
4. Click the following icon to distribute the policy:
5. Check the packet logs on the target host.
   a) On the main page of Client Security, click **Settings**.
   b) Select **Network connections** > **Logging**.
   c) Select the packet log that you want to view and click **Details**.
   The default packet log viewer opens. The upper pane of the window shows all the logged connections.

To later undo this change, select **Allow user changes** and distribute the new policy.

Note: Use this with caution, as for example setting the variable to **Enabled** for the whole domain would start a logging session on every affected host.

Using the trusted interface

The trusted interface mechanism is used to allow use of the firewalled host as a connection-sharing server.

Firewall rules are not applied to traffic going through the trusted interface. If it is used wrongly it can open up the host to any kind of attack from the network, so it is a good security precaution to turn this mechanism off if it is not absolutely needed.

In **Advanced view**:

1. Select the subdomain where you want to enable the trusted interface in the **Policy domains** tree.
2. On the **Policy** tab, select **F-Secure Internet Shield** > **Settings** > **Firewall engine** > **Allow trusted interface**.
3. Select **Enabled** to turn on the trusted interface for the currently selected subdomain.
   This allows the end-users in the subdomain to configure a network interface as the trusted interface.
4. Click the following icon to distribute the policy:

Using packet filtering

This is one of the basic security mechanisms in the firewall; it filters all the IP network traffic based on information in the protocol headers of each packet.

Packet filtering can be turned on or off from the **Advanced** tab in the **Network protection** settings. Turning it off is sometimes needed for testing purposes, but will endanger the security. Because of this, most corporate environments should make sure that the packet filtering is always on.

In **Advanced view**:

1. Select **Root** on the **Domain tree**.
2. On the **Policy** tab, select **F-Secure Internet Shield** > **Settings** > **Firewall engine** > **Firewall engine enabled**.
3. To make sure packet filtering is always turned on, set this variable to **Yes** and select **Disallow user changes**.
4. Click the following icon to distribute the policy:

A.6.2 Configuring security level autoselection

In this example, security level autoselection is configured for a subdomain that contains only laptops in such a way that when the computers are connected to company LAN, the **Office** security level is used; when a dialup connection is used, the security level is changed to **Mobile**.

Before you start, you should know the DNS server IP address and the default gateway's address, as they are needed for defining the security level autoselection criteria. You can find out these addresses by issuing the `ipconfig -all` command in the command prompt.

In **Advanced view**:

1. Select the subdomain on the **Policy domains** tree.
2. On the **Policy** tab, select **F-Secure** > **F-Secure Internet Shield** > **Settings** > **Security level** > **Autoselect mode**.
3. Make sure that security level autoselection is turned on.

   To turn on security level autoselection, select **User can change** or **Admin full control** from the **Autoselect mode** drop-down list.
4. Go to the **Autoselect** page and click **Add** to add the first security level, in this example **Office**.
5. You can enter the data in the cells by selecting a cell and clicking **Edit**.

   For the **Office** security level you should add the following data:

   - **Priority**: The rules are checked in the order defined by the priority numbers, starting from the smallest number.
   - **Security level**: Enter the ID (composed of number and name) of the security level here; for example: `40office`.
   - **Method 1**: Select **DNS server IP address** from the drop-down list.
   - **Argument 1**: Enter the IP address of your local DNS server here; for example: `10.128.129.1`.

- **Method 2**: Select **Default Gateway IP address** from the drop-down list.
- **Argument 2**: Enter the IP address of you default gateway; for example: `10.128.130.1`.

Note: You can only use one argument, for example one IP address, in the **Argument** field. If there are several default gateways in use in your company, and you want to use all of them in the security level autoselection, you can create a separate rule for each of them in the table.

The first security level is now ready.

6. Click **Add** to add the second security level, in this example **Mobile**.
7. Enter the data in the cells by selecting a cell and clicking **Edit**.

   For the **Mobile** security level you should add the following data:

   - **Priority**: The rules are checked in the order defined by the priority numbers, starting from the smallest number.
   - **Security level**: Enter the ID of the security level here; for example: `20mobile`.
   - **Method 1**: Select **Dialup** from the drop-down list.
   - **Argument 1**: You can leave this empty.
   - **Method 2**: Select **Always** from the drop-down list.
   - **Argument 2**: You can leave this empty.

   The configuration is now ready.
8. Click the following icon to distribute the policy:

A.6.3 Troubleshooting connection problems

If there are connection problems, for example a host cannot access the internet, and you suspect that the firewall might cause these problems, you can use the steps given here as a check list.

1. Check that the computer is properly connected.
2. Check that the problem is not in the network cable.
3. Check that ethernet is up and working properly.
4. Check that the DHCP address is valid.

   You can do this by giving the command `ipconfig` in the command prompt.
5. Next you should ping the default gateway.

   If you do not know the address, you can find it out by issuing the command `ipconfig -all` in the command prompt. Then ping the default gateway to see if it responds.
6. If normal Internet browsing does not work, you can try to ping a DNS server:

   - Run `nslookup` to make sure that the DNS service is running.
   - You can also try to ping a known web address to make sure that the computer at the other end is not down.
7. Next you should check whether something in the centrally managed domain has been changed; is there a new policy in use and does this policy contain some settings that might cause these problems?

   - Check from firewall rules that outbound HTTP connections are allowed.
   - Check from the local application control that the IP address the user tries to connect to has not accidentally been added to the list of denied addresses.
8. If nothing else helps, unload F-Secure products or set the firewall to allow all mode.

If even this does not help, it is likely that the problem is in routing or in some other component in the computer the user is trying to connect to.

A.6.4 Adding new services

Service, short for network service, means a service that is available on the network, e.g. file sharing, remote console access, or web browsing.

Services are most often described by what protocol and port they use.

Creating a new internet service based on the default HTTP

In this example, it is assumed that there is a web server running on a computer, and the web server is configured to use a non-standard web port.

Normally a web server would serve TCP/IP port 80, but in this example it has been configured to serve port 8000. To enable connections to this server from the workstations you will have to create a new service. The standard HTTP service does not work here because we are not using the standard HTTP port any more. This new service is `HTTP port 8000` and it is based on the default `HTTP` service.

In **Advanced view**:

1. Select the subdomain for which you want to create the new service in the **Policy domains** tab.
2. On the **Policy** tab, select **F-Secure** > **F-Secure Internet Shield** > **Settings** > **Services**.

   This page contains the **Firewall services** table.
3. Click the **Add** button to start the **Firewall services** wizard.
4. Enter a service name:
   a) Define a unique name for the service in the **Service name** field; you cannot have two services with the same name. For example, `HTTP port 8000`.
   b) Enter a descriptive comment for the service in the **Service comment** field.

      The comment will be displayed on the **Firewall services** table.
5. Select an IP protocol number:
   a) Select a protocol number for this service from the **Protocol** drop-down list.

      It contains the most commonly used protocols (TCP, UDP, ICMP). If your service uses any other protocol, refer to the table below and enter the respective number.

      In this example, select **TCP (6)** from the **IP-protocol number:** drop-down list.

Protocol name	Protocol number	Full name
ICMP	1	Internet Control Message Protocol
IGMP	2	Internet Group Management Protocol
IPIP	4	IPIP Tunnels (IP in IP)
TCP	6	Transmission Control Protocol
EGP	8	Exterior Gateway Protocol
PUP	12	Xerox PUP routing protocol
UDP	17	User Datagram Protocol
IDP	22	Xerox NS Internet Datagram Protocol
IPV6	41	IP Version 6 encapsulation in IP version 4
RSVP	46	Resource Reservation Protocol
GRE	47	Cisco Generic Routing Encapsulation (GRE) Tunnel
ESP	50	Encapsulation Security Payload protocol
AH	51	Authentication Header protocol
PIM	103	Protocol Independent Multicast
COMP	108	Compression Header protocol

Protocol name	Protocol number	Full name
RAW	255	Raw IP packets

6. Select the initiator ports:

   If your service uses the TCP or UDP protocol, you need to define the initiator ports the service covers. The format for entering the ports and port ranges is as follows:

   - `>port`: all ports higher than `port`
   - `>=port`: all ports equal and higher than `port`
   - `<port`: all ports lower than `port`
   - `<=port`: all ports equal and lower than `port`
   - `port`: only the `port`
   - `minport-maxport`: `minport` and `maxport` plus all ports between them (notice that there are no spaces on either side of the dash).

   You can define comma-separated combinations of these items. For example ports 10, 11, 12, 100, 101, 200 and over 1023 can be defined as `10-12, 100-101, 200, >1023`.

   In this example, define the initiator port as `>1023`.

7. Select responder ports:

   If your service uses the TCP or UDP protocol, you need to define the responder ports the service covers.

   In this example, define the responder port as `8000`.

8. Select a classification number for the service from the drop down list.

   You can accept the default value.

9. Select whether any extra filtering is to be applied for the traffic allowed by the service you are creating, in addition to the normal packet and stateful filtering.
   In this example you can accept the default, **Disabled**.

   Note: When the service uses TCP protocol, and you do not have application control enabled, you can select **Active mode FTP** from the **Extra filtering** drop-down menu. **Active mode FTP** requires special handling from the firewall, as the information about the port that should be opened for the connection is included in the transferred data.

10. You can review your rule now.

    If you need to make any changes to the rule, click **Back** through the rule.

11. Click **Finish** to close the rule wizard.
    The rule you just created is now displayed on the **Firewall rules** table.

12. Take the new rule into use:

    To take this new service into use you will have to create a new firewall rule that allows the use of the **HTTP 8000** firewall service in the currently used firewall security level. In this case you can select the new service on the **Rule wizard** > **Service** page and you do not have to define any alerts on the **Rule Wizard** > **Advanced options** page.

Appendix B

Using Policy Manager with a MySQL database

Topics:

- Migrating H2 data to MySQL using the command line

As of version 12.30, you can use a MySQL database to store Policy Manager's data instead of the standard H2 database.

If you want to use MySQL with Policy Manager, you need to have MySQL installed either on the same machine as Policy Manager or on a different node that it can access.

You can migrate your Policy Manager database from H2 to MySQL by running the migration tool, which guides you through the required steps:

- On Windows, run `C:\Program Files (x86)\F-Secure\Management Server 5\bin\fspms-db-migrate-to-mysql.exe`
- On Linux, run `/opt/f-secure/fspms/bin/fspms-db-migrate-to-mysql`

Alternatively, you can follow the steps given under Migrating H2 data to MySQL using the command line on page 130 to run the migration from the command line.

Policy Manager supports Oracle MySQL 5.5, 5.6, 5.7, 8.

Note: If you are using MySQL version 8, you need to select **Use Legacy Authentication Method** on the **Authentication Method** page of the MySQL installer wizard.

Note: TLS connections are currently not supported.

B.1 Migrating H2 data to MySQL using the command line

Follow these steps to configure MySQL and migrate your Policy Manager data from H2 to MySQL from the command line.

Note: If your setup does not require you to run the migration on the command line, the easiest approach is to use the migration tool (run `C:\Program Files (x86)\F-Secure\Management Server 5\bin\fspms-db-migrate-to-mysql.exe` on Windows, `/opt/f-secure/fspms/bin/fspms-db-migrate-to-mysql` on Linux) and follow the instructions given there.

Note: Depending on the amount of data stored in the database, the migration process can take only a few minutes or up to an hour.

1. Stop the MySQL service.
2. Edit the `my.ini` configuration file.

   Change or add the following entry under the `[mysqld]` section: `max_allowed_packet=100M`

   Note: For MySQL version 8, you also need to define the following property in the configuration file: `default_authentication_plugin=mysql_native_password`
3. Start the MySQL service.
4. Open the MySQL Command Line Client and run the following commands to create the database schema and users:

   a) `CREATE SCHEMA <schema>;`

   `<schema>`: replace this with the database name to be used by Policy Manager to store all its data. The name can be anything distinguishable by the administrator and accepted as a valid database name by MySQL, for example `fspms` or `policy_manager`.

   b) `CREATE USER <pm_all> IDENTIFIED BY '<all_password>';`

   `<pm_all>`: replace this with the name of the MySQL user, which is used by Policy Manager to initialize the database schema, such as creating all the necessary tables. The user name can be any valid name accepted by MySQL.

   `<all_password>`: replace this with the password for the `<pm_all>` MySQL user.

   c) `CREATE USER <pm_rw> IDENTIFIED BY '<rw_password>';`

   `<pm_rw>`: replace this with the name of the MySQL user, which is used by Policy Manager to access the database while running. The user name can be any valid name accepted by MySQL.

   `<rw_password>`: replace this with the password for the `<pm_rw>` MySQL user.

   d) `GRANT ALTER, ALTER ROUTINE, CREATE, CREATE ROUTINE, CREATE TEMPORARY TABLES, CREATE VIEW, DELETE, DROP, EXECUTE, INDEX, INSERT, LOCK TABLES, REFERENCES, SELECT, UPDATE ON <schema>.* TO <pm_all>@'%';`

   e) `GRANT CREATE TEMPORARY TABLES, DELETE, EXECUTE, INSERT, LOCK TABLES, SELECT, UPDATE ON <schema>.* TO <pm_rw>@'%';`
5. Stop the Policy Manager service.
6. Run the following command to start the migration:

   - On Windows, run `C:\Program Files (x86)\F-Secure\Management Server 5\bin\fspms-db-migrate-to-mysql.exe`
   - On Linux, run `/opt/f-secure/fspms/bin/fspms-db-migrate-to-mysql`

   Note: If you are running the migration on Linux in headless mode, then you need to configure the MySQL configuration parameters manually using the `/var/opt/f-secure/fspms/data/fspms.db.config` config file.

```
active.db=mysql
mysql.type=mysql
mysql.host=<MySQL server address>
mysql.port=<MySQL server port>
mysql.schema=<schema>
mysql.init.user=<pm_all>
mysql.init.password=<all_password>
```

```
mysql.user=<pm_rw>
mysql.password=<rw_password>
```

If your MySQL setup supports replication and you want to take it into use, you need to grant additional permissions for the Policy Manager database users by running the following commands in the MySQL Command Line Client:

- `GRANT REPLICATION CLIENT, SUPER ON *.* TO <pm_all>@'%';`
- `GRANT REPLICATION CLIENT ON *.* TO <pm_rw>@'%';`

The `SUPER` privilege is required for the user changing the schema in order to replicate the stored routines.

Note: If `binlog` is enabled, only row-level replication is supported.