Policy Manager Proxy

Administrator's Guide

Contents

Chapter 1: Policy Manager Proxy 3

1.1 System requirements.....4

1.2 Overview.....4

1.2.1 When should you use Policy Manager Proxy?.....5

1.3 Setting up Policy Manager Proxy.....5

1.4 Setting up Policy Manager Proxy in silent mode.....7

1.4.1 Upgrading Policy Manager Proxy in silent mode.....8

1.5 Centralized management of Policy Manager Proxy.....8

Chapter
1

Policy Manager Proxy

Topics:

- System requirements
- Overview
- Setting up Policy Manager Proxy
- Setting up Policy Manager Proxy in silent mode
- Centralized management of Policy Manager Proxy

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

1.1 System requirements

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

Operating system:	• Microsoft Windows:
	  • 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)
	  • Windows Server 2022; Essentials, Standard or Datacenter editions (Server Core is supported)
	  •
	• Linux (only 64-bit versions of all distributions listed are supported):
	  • AlmaLinux 8
	  • CentOS 7, 8
	  • Debian GNU Linux 10, 11, 12
	  • openSUSE Leap 15
	  • Oracle Linux 8
	  • Red Hat Enterprise Linux 7, 8
	  • Rocky Linux 8
	  • SUSE Linux Enterprise Desktop 12, 15
	  • SUSE Linux Enterprise Server 12, 15
	  • Ubuntu 20.04, 22.04, 24.04 LTS

Processor:	2 CPU cores
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.

1.2 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.

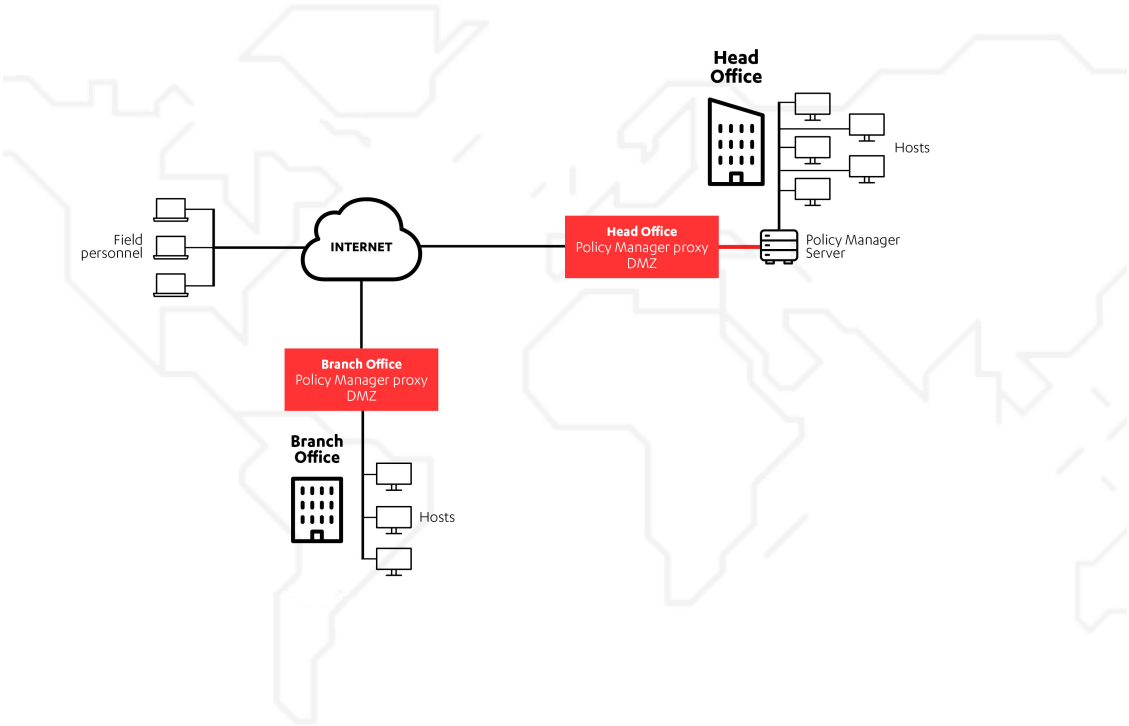
Secure connections are used both between hosts and proxy, and proxy and master server. This means that the proxy node certificates must be pre-configured. Managed hosts connect to the configured proxy nodes using the Policy Manager Proxies table.

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.

1.2.1 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.

1.3 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.

   Note: For available MSI parameters, see #unique_6.

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\WithSecure\Policy Manager\Policy Manager Server\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.

   - Linux: `/var/opt/f-secure/fspms/data/fspms.proxy.config`
   - Windows: `C:\ProgramData\WithSecure\NS\Policy Manager\Policy Manager Server\data\fspms.proxy.config`

   b) Add the proxy as a new line, using the following format:

   ```
   http_proxy=[http://][user[:password]@]<address>[:port].
   ```

   Note: Policy Manager only supports basic authentication for HTTP proxies.

   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.

1.4 Setting up Policy Manager Proxy in silent mode

If you want to install Policy Manager Proxy without any prompts during installation, you need to configure the required details separately for the installation package.

Note: Silent clean installation is not supported for Windows.

1. Open Policy Manager Console and create a temporary user with full access permissions to the root domain.
2. Download the Policy Manager Proxy installer.
3. 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.
4. Customize the installation package.

   Linux (Red Hat, CentOS, SuSE):

   a) Create a shell script named, for example, `pmp.sh` with the following content:

   ```
   yum -y update libstdc++
   yum -y install libstdc++.i686
   rpm -i fspmp-<installer_version>-1.x86_64.rpm
   /opt/f-secure/fspms/bin/fspms-config << PMPCONFIG
   PM address
   PM port (usually 443)
   ./admin.pub
   PMP http port to be used (usually 80)
   PMP httpS port to be used (usually 443)
   PM admin username (for the temporary user that you created)
   PM admin password (for the temporary user that you created)
   PMPCONFIG
   ```

   b) If you want to install Policy Manager Proxy in reverse mode, add the following command to `pmp.sh` between the installation and `fspms-config` commands:

   ```
   echo 'additional_java_args="-DreverseProxy=true"' >>
   /etc/opt/f-secure/fspms/fspms.conf
   ```

   Linux (Debian, Ubuntu):

   a) Create a shell script named, for example, `pmp.sh` with the following content:

   ```
   apt -y upgrade libstdc++6
   apt -y install libstdc++6:i386
   dpkg -i fspmp_<installer_version>_amd64.deb
   /opt/f-secure/fspms/bin/fspms-config << PMPCONFIG
   PM address
   PM port (usually 443)
   ./admin.pub
   PMP http port to be used (usually 80)
   PMP httpS port to be used (usually 443)
   PM admin username (for the temporary user that you created)
   PM admin password (for the temporary user that you created)
   PMPCONFIG
   ```

b) If you want to install Policy Manager Proxy in reverse mode, add the following command to `pmp.sh` between the installation and `fspms-config` commands:

```
echo 'additional_java_args="-DreverseProxy=true"' >>
/etc/opt/f-secure/fspms/fspms.conf
```

The Policy Manager Proxy distributable package is now ready.

5. Transfer the `rpm` package, `admin.pub` key, and `pmp.sh` script. Remember to set the execute bit for the `.sh` file.
6. Install the product by running the `./pmp.sh` script.
7. When the installation is complete on each target host, remove the temporary user that you created to avoid credentials being shared in plain text format.

1.4.1 Upgrading Policy Manager Proxy in silent mode

For upgrading the product, you do not have to configure Policy Manager Proxy or create certificates, you only need to upgrade the installation.

Follow these steps:

- Windows:
  1. Download the Policy Manager Proxy installer.
  2. Run the msiexec with the /quiet option: `msiexec /i wspmp-windows-msi-<installer_version>.msi /quiet`
- Linux (Red Hat, CentOS, SuSE):
  1. Download the Policy Manager Proxy installer.
  2. Run the following command: `rpm -U fspmp-<installer_version>-1.x86_64.rpm`
- Linux (Debian, Ubuntu):
  1. Download the Policy Manager Proxy installer.
  2. Run the following command: `dpkg -i fspmp_ <installer_version>_amd64.deb`

1.5 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.