Desktop Firewall™ software
version 8.5

McAfee®
System Protection
Industry-leading intrusion prevention solutions
# Contents

## 1 Introducing Desktop Firewall

- What Desktop Firewall does ............................................. 4
- Desktop Firewall components ........................................ 4
  - Stand-alone version ................................................. 5
  - ePolicy Orchestrator version .................................... 5
- Using this book ....................................................... 6
  - Audience ........................................................................ 6
  - Conventions .................................................................. 7
- Resources ....................................................................... 8
  - Getting product information ....................................... 8
  - Links from within the product .................................... 9
  - Contact information .................................................. 11

## 2 Installing the Software (Stand-Alone Version)

- Installation overview .................................................. 12
  - Upgrading from a previous version of Desktop Firewall .... 12
- Before you install ....................................................... 13
  - Incompatible software .............................................. 13
  - System requirements ................................................ 13
- Installing the software ................................................ 15
- Removing the software ................................................. 15

## 3 Installing the Software via ePolicy Orchestrator

- Installation overview .................................................. 16
  - Deployment recommendations .................................... 17
- System requirements .................................................. 18
  - Console and server requirements ................................. 19
  - Client requirements .................................................. 19
- Installing the software ................................................ 20
  - Running the McAfee Desktop Firewall ePolicy Orchestrator Update software ........................................ 20
  - Adding the Desktop Firewall client software to ePolicy Orchestrator ..................................................... 21
  - Deploying Desktop Firewall to other computers ............ 22
  - Removing Desktop Firewall ......................................... 24
  - Removing Desktop Firewall from client computers ......... 24
  - Removing the Desktop Firewall .NAP file from the Repository ...................................................... 25
  - Removing the Desktop Firewall package file from the Repository ...................................................... 25
  - Uninstalling the McAfee Desktop Firewall ePolicy Orchestrator Update software .............................. 26
Introducing Desktop Firewall

This section introduces the Desktop Firewall software, including:

- What Desktop Firewall does
- Desktop Firewall components

It also contains information about this document, including:

- Using this book
- Resources

What Desktop Firewall does

The Desktop Firewall software provides security for individual computers. It protects computers from external threats (like hackers) and from internal threats (like some viruses). It secures computers using several features, including:

- **A firewall** that inspects incoming and outgoing network traffic, and either blocks it or allows it based on rules that you set up.

- **An application monitoring system**, which monitors the applications you use and prevents those you specify from starting, or from binding themselves to other programs.

- **An intrusion detection system (IDS)** that scans traffic destined for your computer and identifies any potential attacks on your system.

- **An activity log** that records information about Desktop Firewall actions. You can use this log to troubleshoot problems, or review past activities.

You can use all of these features together, or just those features that you need.

Desktop Firewall components

The Desktop Firewall software comes in two versions — a stand-alone version and an ePolicy Orchestrator version.
**Stand-alone version**

The stand-alone version of Desktop Firewall runs on a single computer. You configure the software directly. This version is ideal for individual users or small corporate networks.

For more information on the stand-alone version of Desktop Firewall and its features, see the Desktop Firewall Product Guide.

**ePolicy Orchestrator version**

The ePolicy Orchestrator version of Desktop Firewall is designed for enterprise users. McAfee ePolicy Orchestrator is a software management product that you purchase separately. Using ePolicy Orchestrator, you can store the Desktop Firewall software in a central Repository. Once the software is in the Repository, you can deploy it at any time to any number of ePolicy Orchestrator-managed computers.

ePolicy Orchestrator lets you configure, distribute, and manage Desktop Firewall for all your network users, from a single point — the ePolicy Orchestrator console. It also gives you access to more features. The ePolicy Orchestrator version of Desktop Firewall includes all the features of the stand-alone version, plus additional features such as the ability to:

- Quarantine systems that don’t have up-to-date ePolicy Orchestrator policies.
- Create reports.
- Monitor users’ firewall and application rules remotely.

For more information on the ePolicy Orchestrator version of Desktop Firewall and its features, see the Desktop Firewall Product Guide.
Using this book

This section contains information about using this Installation Guide, such as:

- Audience
- Conventions

Audience

This information is intended primarily for two audiences:

- Network administrators who are responsible for their company’s anti-virus and security program.
- Users who are responsible for updating virus definition (DAT) files on their workstation, or configuring the software’s detection options.
Conventions

This guide uses the following conventions:

**Bold Condensed**
All words from the user interface, including options, menus, buttons, and dialog box names.

**Example:**
Type the User name and Password of the desired account.

**Courier**
The path of a folder or program; text that represents something the user types exactly (for example, a command at the system prompt).

**Example:**
The default location for the program is:
`C:\Program Files\McAfee\EPO\3.5.0`
Run this command on the client computer:
`C:\SETUP.EXE`

**Italic**
For emphasis or when introducing a new term; for names of product documentation and topics (headings) within the material.

**Example:**
Refer to the VirusScan Enterprise Product Guide for more information.

**Blue**
A web address (URL) and/or a live link.

Visit the McAfee web site at:
http://www.mcafee.com

**<TERM>**
Angle brackets enclose a generic term.

**Example:**
In the console tree, right-click <SERVER>.

**Note:**
Supplemental information; for example, an alternate method of executing the same command.

**Tip:**
Suggestions for best practices and recommendations from McAfee for threat prevention, performance and efficiency.

**Caution:**
Important advice to protect your computer system, enterprise, software installation, or data.

**Warning:**
Important advice to protect a user from bodily harm when interacting with a hardware product.

**New:**
New or redesigned feature or option of this release of the product.
Resources

McAfee® products denote years of experience, and commitment to customer satisfaction. The McAfee PrimeSupport® team of responsive, highly skilled support technicians provides tailored solutions, delivering detailed technical assistance in managing the success of mission critical projects — all with service levels to meet the needs of every customer organization.

Refer to these sections for additional resources:

- Getting product information
- Links from within the product
- Contact information

Getting product information

Unless otherwise noted, the product documentation are Adobe Acrobat .PDF files available on the product CD or from the McAfee download site:

Installation Guide — System requirements and instructions for installing and starting the software.

Product Guide — Product introduction and features, detailed instructions for configuring the software, information on deployment, recurring tasks, and operating procedures.

Help — High-level and detailed information accessed from the software application: Help menu and/or Help button for page-level help; right-click option for What’s This? help.

Configuration Guide — For use with ePolicy Orchestrator®. Procedures for deploying and managing supported products through the ePolicy Orchestrator management software.

Quick Reference Card — A handy card with information on basic product features, routine tasks that you perform often, and critical tasks that you perform occasionally. (A printed card accompanies the product CD.)

Release Notes — ReadMe. Product information, resolved issues, any known issues, and last-minute additions or changes to the product or its documentation. (A text file is included with the software application and on the product CD.)

License — The McAfee License Agreement booklet that includes all of the license types you can purchase for your product. The License Agreement sets forth general terms and conditions for the use of the licensed product.

Contacts — Contact information for McAfee services and resources: technical support, customer service, Security Headquarters (AVERT), beta program, and training. (A text file is included with the software application and on the product CD.)
Links from within the product

The Help menu in the product provides links to some useful resources:

- Online Help
- Virus Information Library
- Submit a Sample
- Technical Support
- What can the current DAT file detect?

Online Help
Use this link to access the online Help topics for the product.

If the product’s built-in help system (accessed from within the software by clicking the Help menu) displays incorrectly on your system, your version of Microsoft® Internet Explorer may not be using ActiveX controls properly. These controls are required to display the help file. Make sure that you install the latest version of Internet Explorer.

Virus Information Library
Use the Virus Information link to access the McAfee Anti-Virus & Vulnerability Emergency Response Team (AVERT) Virus Information Library. This web site has detailed information on where viruses come from, how they infect your system, and how to remove them.

In addition to genuine viruses, the Virus Information Library contains useful information on virus hoaxes, such as virus warnings that you receive via e-mail. A Virtual Card For You and SULFNBK are two of the best-known hoaxes, but there are many others. Next time you receive a well-meaning virus warning, view our hoax page before you pass the message on to your friends.

To access the Virus Information Library:

1. Open the product interface.
2. Select Virus Information from the Help menu.

Submit a Sample
Use the Submit a Sample link to access the McAfee AVERT WebImmune web site. If you have a suspicious file that you believe contains a virus, or experience a system condition that might result from an infection, McAfee recommends that you send a sample to its anti-virus research team for analysis. Submission not only initiates an analysis, but a real-time fix, if warranted.

To submit a sample virus to AVERT:

1. Open the product interface.
2. From the Help menu, select Submit a Sample.
3. Follow the directions on the web site.

Technical Support
Use the Technical Support link to access the McAfee PrimeSupport KnowledgeCenter Service Portal web site. Browse this site to view frequently asked questions (FAQs), documentation, and perform a guided knowledge search.
What can the current DAT file detect?
Use this link to view the list of items that are included in the current DAT file. This link is also available from the About dialog box.

- **Under Viruses, trojans, and unwanted programs that DAT version XXXX can detect**, the list shows all the files that can be detected using the current DAT file. Use the scroll bar to view the entire list.

- **Under Filter List**, search for a specific item by entering the substring. When you use this feature, the list displays only the names containing the specified string.

- **Click Cancel** when finished.
Contact information

Security Headquarters: AVERT

Home Page

Virus Information Library
http://vil.mcafeesecurity.com

AVERT WebImmune, Submitting a Sample (Logon credentials required)
https://www.webimmune.net/default.asp

AVERT DAT Notification Service

Download Site

Home Page

Anti-Virus DAT File and Engine Updates

Anti-Spam Rules File and Engine Updates
ftp://ftp.nai.com/spamdefs/1.x/

Product Upgrades (Logon credentials required)

HotFix and Patch Releases for Security Vulnerabilities (Available to the public)

HotFix and Patch Releases for Security Vulnerabilities (ServicePortal account and McAfee PrimeSupport grant number required)
https://mysupport.nai.com/products/products.asp

Product End-of-Life Support

Technical Support

Home Page
http://www.mcafeesecurity.com/us/support/technical_support

KnowledgeBase Search
https://knowledgemap.nai.com/phpclient/homepage.aspx

PrimeSupport Service Portal (Logon credentials required)
https://mysupport.mcafeesecurity.com

PSVANS — PrimeSupport Vulnerability Alert Notification Service

Customer Service

E-mail
https://secure.nai.com/us/forms/support/request_form.asp

Web

Phone — US, Canada, and Latin America toll-free:
+1-888-VIRUS NO or +1-888-847-8766 Monday – Friday, 8 a.m. – 8 p.m., Central Time

For information on contacting McAfee worldwide offices:
http://www.mcafeesecurity.com/us/contact/home.htm

McAfee Beta Program


Training: McAfee University

Installing the Software (Stand-Alone Version)

This section provides:

- An overview of how to install and deploy the stand-alone version of Desktop Firewall.
- A list of system requirements.
- Instructions for installing the software.
- Instructions for removing the software.

**Installation overview**

To install the Desktop Firewall software, you must:

1. Check to see if your computer uses PGP software, specifically PGPadmin or PGPvpn components.
   
   See *Incompatible software on page 13.*

2. Verify that your computer meets the minimum system requirements for running Desktop Firewall.
   
   See *System requirements on page 13.*

3. Download the Desktop Firewall files from the McAfee web site, or insert the product CD into your computer’s CD-ROM drive.

4. Review the Desktop Firewall Readme file for additional installation information.

5. Run the Desktop Firewall installation program.
   
   See *Installing the software on page 15.*

If you need to remove the Desktop Firewall software from your computer, follow the instructions in *Removing the software on page 15.*

**Upgrading from a previous version of Desktop Firewall**

When upgrading from a previous version of Desktop Firewall:

- If you are running Desktop Firewall version 8.0, the recommended upgrade path is to install Desktop Firewall 8.5 over your current install and then restart your computer.
If you are running a version of Desktop Firewall prior to 8.0, the recommended upgrade path is to remove the existing version of Desktop Firewall before installing Desktop Firewall 8.5.

## Before you install

Before you install Desktop Firewall, make certain that:

- Your computer does not use products that are incompatible with Desktop Firewall (see **Incompatible software**).
- Your computer meets the minimum system requirements for running Desktop Firewall (see **System requirements**).
- You remove any third-party firewall software.

Before installation on Windows XP Service Pack 2, you must ensure that the Windows Firewall is turned off.

## Incompatible software

The Desktop Firewall software is not compatible with the PGPadmin and PGPvpn components of the following software suites:

- PGP Desktop Security, version 7.0 or later.
- PGP Corporate Desktop, version 7.1 or later.
- PGPfire Personal Firewall/IDS, version 7.1 or later.

You must remove the PGPadmin and PGPvpn components if you plan to install and use Desktop Firewall.

## System requirements

Before you install Desktop Firewall, verify that your computer satisfies the software’s minimum system requirements:

- An Intel Pentium 166MHz processor, or faster.
- A monitor offering a minimum display resolution of 800 X 600 (1024 X 768 recommended).
- One of the following amounts of RAM (depending on your operating system):
  - A minimum of 32MB of RAM for Windows 98 SE or Windows Me.
  - A minimum of 64MB of RAM for Windows NT and later.
  - No minimum requirement of RAM for Windows 2003 or Windows XP Tablet PC.
  - A minimum of 32MB hard disk space.
Before you install

- One of the following Microsoft operating systems:
  - Windows 98 SE (Second Edition), with Service Pack 1 or later.
  - Windows NT Workstation 4.0, with Service Pack 6a or later.
  - Windows NT Server 4.0, with Service Pack 6a or later.
  - Windows NT Enterprise Server 4.0, with Service Pack 6a or later.
  - Windows 2000 Professional, with Service Pack 3 or later.
  - Windows 2000 Server, with Service Pack 3 or later.
  - Windows 2000 Advanced Server, with Service Pack 3 or later.
  - Windows Me (Millennium Edition).
  - Windows XP Home, with Service Pack 1 or later.
  - Windows XP Professional, with Service Pack 1 or later.
  - Windows XP Tablet PC, with Service Pack 1 or later.
  - Microsoft Internet Explorer version 5.5, with Service Pack 2 or later.

These are the minimum system requirements. McAfee recommends that you always use the latest service packs, and that you install all available security HotFixes before installing Desktop Firewall.
Installing the software

See Before you install on page 13 for software compatibility information before you install Desktop Firewall.

1. Do one of the following:
   - If installing from the product CD, insert it into the CD-ROM drive of your computer.
   - If using files downloaded from the McAfee download site, continue to Step 2.

2. In Windows, click Start, then select Run.
   
   The Run dialog box appears.

3. Browse to the location of your Desktop Firewall SETUP.EXE file, then click OK.
   
   The default location for this file is \PRODUCTS\DESKTOP FIREWALL\SETUP.EXE, either on your installation CD or in the folder where you saved your download files.

   Your Desktop Firewall software installation begins.

4. Follow the installation wizard’s prompts to continue installing the product.

5. When the installation finishes, click Finish.

Removing the software

1. In Windows, click Start, then select Settings.

2. Select Control Panel, then select Add/Remove Programs.
   
   The Add/Remove Programs dialog box appears.

3. Select McAfee Desktop Firewall 8.5 from the list, then click Change/Remove.
   
   A welcome dialog box appears.

4. Select Remove to uninstall the Desktop Firewall software, then click Next.

5. Click Yes to verify that you want to remove the application.

6. Click Finish.

You must restart the computer before you can reinstall the software.
This section provides:

- An overview of how to install and deploy Desktop Firewall using ePolicy Orchestrator.
- A suggested deployment scenario.
- A list of system requirements.
- Instructions for installing the software.
- Instructions for removing the software.

**Installation overview**

To deploy and manage Desktop Firewall software using ePolicy Orchestrator, follow these steps (each of which is a procedure described in this section or in the ePolicy Orchestrator documentation):

1. **Install ePolicy Orchestrator and a database.**
   
   Verify that your ePolicy Orchestrator server meets the minimum system requirements for running Desktop Firewall. See [Console and server requirements](#) on page 19.
   
   See the ePolicy Orchestrator documentation for installation instructions.

2. **Log on to ePolicy Orchestrator and set up its Repository.** You must add any sites, groups, or individual computers to which you plan to deploy Desktop Firewall.

3. **Deploy ePolicy Orchestrator agents to these computers.**
   
   You can skip this procedure if you already have ePolicy Orchestrator agents installed on these computers.
   
   See the ePolicy Orchestrator documentation for agent deployment instructions.

4. **On your ePolicy Orchestrator server, run the McAfee Desktop Firewall ePO Update software.**

   Before running the update, it is recommended that you close the ePolicy Orchestrator console. Otherwise, you must restart the ePolicy Orchestrator console after the firewall update.
5 Add the Desktop Firewall client software (.NAP files and packages) to the ePolicy Orchestrator Repository.

See Adding the Desktop Firewall client software to ePolicy Orchestrator on page 21.

6 Verify that your target Desktop Firewall computers meet the minimum system requirements for Desktop Firewall.

See Client requirements on page 19.

7 Configure the rules and other Desktop Firewall settings that you want to deploy.

See the Desktop Firewall Product Guide for information.

8 Deploy the Desktop Firewall client software to each of your target computers.

See Deploying Desktop Firewall to other computers on page 22.

---

### Deployment recommendations

Always develop a basic set of rules for Desktop Firewall before you deploy the product on a large scale. You can create a common rule set using the following approach, which involves working with a small test group before deploying the Desktop Firewall software to the rest of the network:

1 Using ePolicy Orchestrator, deploy the Desktop Firewall software to an administrator’s computer.

2 Put the deployed product in **Learn Mode** (for both the firewall and for application monitoring).

   Use **Audit Learn Mode** if you do not want to respond to regular **Learn Mode** alerts. See the Desktop Firewall Product Guide for more information.

3 Use this computer normally for at least a week.

   **Learn Mode** continually adds rules that are appropriate to your network.

4 After a week, review the new firewall rules, application monitoring rules, and blocked hosts in Desktop Firewall. If necessary:
   - Delete any rules that are not appropriate for general users.
   - Add any additional rules that you need.

5 Using ePolicy Orchestrator, define this configuration as the common configuration for all future Desktop Firewall software deployments. See the Desktop Firewall ePolicy Orchestrator Configuration Guide for more information on deployment.

6 Deploy Desktop Firewall to a larger test group (ten to twenty users is ideal), and put the products in **Learn Mode** or **Audit Learn Mode**.

   This group of users will test your new Desktop Firewall configuration. Check their rule lists regularly for any new learned rules, and add these to the common configuration if appropriate.
When the test group software operates for a week without learning any new and relevant rules, your common configuration is ready for general release.

7 Disable Learn Mode for all your test users, and for the common Desktop Firewall configuration.

8 Deploy the Desktop Firewall software to all your remaining network computers.

9 Using ePolicy Orchestrator, generate reports to confirm that Desktop Firewall was properly deployed to all the required computers.

---

**System requirements**

Before you install Desktop Firewall, make certain that your hardware meets the minimum requirements to run the software. Desktop Firewall consists of two main components, each with different system requirements:

- The ePolicy Orchestrator-based console and server.
- The deployed client(s).

You generally install both the console and server on a single ePolicy Orchestrator server. This ePolicy Orchestrator server must meet the minimum requirements specified in *Console and server requirements* on page 19.

Once you finish installing the ePolicy Orchestrator components, you can use the software to deploy Desktop Firewall clients to computers managed by ePolicy Orchestrator. Each of these target computers must meet the minimum system requirements specified in *Client requirements* on page 19.
Console and server requirements

Install the Desktop Firewall console and server components on an ePolicy Orchestrator server that:

- Runs ePolicy Orchestrator version 3.0.x, 3.1.x, or 3.5.x.

Client requirements

Before you use ePolicy Orchestrator to deploy Desktop Firewall clients, you must do the following:

- Make certain that each target computer meets the system requirements.
- Uninstall any incompatible software from each target computer. See Incompatible software on page 20.

Minimum system requirements

- An Intel Pentium 166MHz processor, or faster.
- A monitor offering a minimum display resolution of 800 X 600 (1024 X 768 recommended).
- A minimum of 64MB of RAM.
- A minimum of 32MB hard disk space.
- One of the following Microsoft operating systems:
  - Windows 98 SE (Second Edition), with Service Pack 1 or later.
  - Windows NT Workstation 4.0, with Service Pack 6a or later.
  - Windows NT Server 4.0, with Service Pack 6a or later.
  - Windows NT Enterprise Server 4.0, with Service Pack 6a or later.
  - Windows 2000 Professional, with Service Pack 3 or later.
  - Windows 2000 Server, with Service Pack 3 or later.
  - Windows 2000 Advanced Server, with Service Pack 3 or later.
  - Windows Me (Millennium Edition).
  - Windows XP Home, with Service Pack 1 or later.
  - Windows XP Professional, with Service Pack 1 or later.
  - Windows XP Tablet PC, with Service Pack 1 or later.
  - Microsoft Internet Explorer version 5.5, with Service Pack 2 or later.

These are the minimum system requirements. McAfee recommends that you always use the latest service packs, and that you install all available security HotFixes before installing Desktop Firewall.
Incompatible software
The Desktop Firewall software is not compatible with the PGAdmin and PGPvpn components of the following software suites:

- PGP Desktop Security, version 7.0 or later.
- PGP Corporate Desktop, version 7.1 or later.
- PGPfire Personal Firewall/IDS, version 7.1 or later.

You must remove the PGAdmin and PGPvpn components if you plan to install and use Desktop Firewall.

Installing the software
Once you verify that your computers meet the Desktop Firewall and ePolicy Orchestrator system requirements, you can install the software. To do this, you must:

1. Run the McAfee Desktop Firewall ePO Update application.
2. Add the Desktop Firewall .NAP file and package file to ePolicy Orchestrator.
3. Deploy the Desktop Firewall client software to the ePolicy Orchestrator-managed computers you have selected.

Running the McAfee Desktop Firewall ePolicy Orchestrator Update software
Before running an update, it is recommended that you close the ePolicy Orchestrator console. Otherwise, you must restart the ePolicy Orchestrator console after the firewall update.

1. Do one of the following:
   - Insert the Desktop Firewall CD into your CD-ROM drive.
   - Download Desktop Firewall from the McAfee web site following the instructions provided there, and unzip them to a folder on your hard disk.
2. Navigate to the McAfee Desktop Firewall ePO Update program file (MCAFEEFIREEPOUPDATE85.EXE) and double-click to launch it.
   - This file is located in the \PRODUCT\EPO UPDATE FOR FIREWALL\ folder.
3. When the Update wizard starts, accept the license agreement to continue.
4. Follow the remaining prompts to install the Update software.
5. Click Finish to complete the installation.

If you use more than one ePolicy Orchestrator server, or if you use ePolicy Orchestrator remote consoles, repeat this procedure to install the Update software on each one.
Adding the Desktop Firewall client software to ePolicy Orchestrator

To add the Desktop Firewall client software to ePolicy Orchestrator, you must add two files to the ePolicy Orchestrator Repository:

- A .NAP file (MCAFEEFIRE85.NAP).
- A package file (PKGCATALOG.Z).

If you use a remote ePolicy Orchestrator console, you must install the ePolicy Orchestrator Update for Firewall before installing Desktop Firewall. Follow the instructions in Running the McAfee Desktop Firewall ePolicy Orchestrator Update software on page 20 before installing the Desktop Firewall software.

Adding the .NAP file to ePolicy Orchestrator

1. Start ePolicy Orchestrator and log on to the server that you want to manage.
2. If necessary, expand this server’s icon (in the console tree) to see the Repository icon.
3. Right-click Repository and select Configure Repository.
4. When the configuration wizard starts, select Add new software to be managed.
5. Click Next.
6. Navigate to the MCAFEEFIRE85.NAP file and double-click it.
   This file is located in the \PRODUCTS\DESKTOP FIREWALL FOR EPO\ folder on your Desktop Firewall installation CD, or in the folder where you extracted your Desktop Firewall download files.
7. Click OK.
   ePolicy Orchestrator adds the Desktop Firewall software to the Repository.

Adding the package file to ePolicy Orchestrator

1. Start ePolicy Orchestrator and log on to the server that you want to manage.
2. If necessary, expand this server’s icon (in the console tree) to see the Repository icon.
3. Select Repository.
4. In the Details pane, locate the AutoUpdate Tasks area and click Check in package.
5. When the check-in wizard starts, click Next to continue.
6. Select Products or updates, then click Next.
7. When ePolicy Orchestrator prompts you for a path, click Browse.
8. Navigate to the package file (PKGCATALOG.Z) and double-click it.
   This file is located in the \PRODUCTS\DESKTOP FIREWALL FOR EPO\ folder on your Desktop Firewall installation CD, or in the folder where you extracted your Desktop Firewall download files.
9. Click Next, then click Finish to add the package file to the Repository.
Deploying Desktop Firewall to other computers

To deploy the Desktop Firewall software to other computers, you must configure and use the ePolicy Orchestrator Deployment task. ePolicy Orchestrator automatically creates this task for each user that you add to the Directory. To deploy Desktop Firewall using this task, you must:

1. Configure the task to send out the Desktop Firewall software.
2. Set up a deployment schedule for the task.

You can only deploy Desktop Firewall to computers that you have set up in the ePolicy Orchestrator Directory, and that have ePolicy Orchestrator agents installed. See the ePolicy Orchestrator documentation for more details.

Configuring the Deployment task for Desktop Firewall

1. Start ePolicy Orchestrator and log on to the server that you want to manage.
2. If necessary, expand this server’s icon (in the console tree) to see the Directory icon.
3. Expand the Directory icon and navigate to the site, group, or computer to which you want to deploy the Desktop Firewall software.
4. In the details pane, click Tasks to display that tab.
   ePolicy Orchestrator lists all the tasks for this site, group, or computer.
5. Right-click the Deployment task, then select Edit Task.
   The ePolicy Orchestrator Scheduler dialog box appears.
6. Click Task to display that tab.
7. Click Settings.
   The Task Settings dialog box appears.
8. Clear the Inherit checkbox.
9. In the Product deployment options list, locate McAfee Desktop Firewall.
10. Select Install from the Action list.
    If you installed more than one language version, select the language that you want to deploy from the Language list.
    Set any products that you do not want to remove to Ignore.
11. Click OK to return to the ePolicy Orchestrator Scheduler dialog box.
    Now that you have configured this task to deploy Desktop Firewall, create a deployment schedule for the task.

Creating a deployment schedule for the Deployment task

1. In the ePolicy Orchestrator Scheduler dialog box, click Task to display that tab.
2 In the Schedule Settings area, clear the Inherit checkbox.

3 Select Enable to make the task active.

4 Click the Schedule tab.

5 Clear the Inherit checkbox, then set up the time when you want the Desktop Firewall software deployed.

To deploy the software immediately, select Run Immediately from the Schedule Task list.

For instructions, see the ePolicy Orchestrator Product Guide.

6 Click OK.

ePolicy Orchestrator deploys the Desktop Firewall client software to this site, group, or computer at the time you specified.
Removing Desktop Firewall

To completely uninstall the Desktop Firewall software, you must:

- Remove Desktop Firewall from all your ePolicy Orchestrator clients.
- Delete the Desktop Firewall .NAP file from the ePolicy Orchestrator Repository.
- Delete the Desktop Firewall package file from the Repository.
- Remove the McAfee Desktop Firewall ePO Update software from your ePolicy Orchestrator server.

If you have more than one ePolicy Orchestrator server, or if you use ePolicy Orchestrator remote consoles, you must uninstall the Update from each one separately.

Removing Desktop Firewall from client computers

1. Start ePolicy Orchestrator and log on to the server that you want to manage.
2. If necessary, expand this server’s icon (in the console tree) to see the Directory icon.
3. Expand the Directory icon and select the site, group, or computer that you want to remove Desktop Firewall from.
4. In ePolicy Orchestrator’s details pane, click Tasks to display that tab.
5. Right-click the Deployment task, then select Edit Task.
   The ePolicy Orchestrator Scheduler dialog box appears.
6. On the Task tab, click Settings.
   The Task Settings dialog box appears.
7. If necessary, clear the Inherit checkbox.
8. In the Product deployment options list, locate McAfee Desktop Firewall.
9. Select Remove from the Action list.
   If you installed more than one language version, select the language that you want to remove from the Language list.
   Set any products that you do not want to remove to Ignore.
10 Click OK to return to the ePolicy Orchestrator Scheduler dialog box.

11 Click OK to save your changes.

   ePolicy Orchestrator will remove the Desktop Firewall clients at the time specified in the task. To change the task’s schedule, use the procedure outlined in Creating a deployment schedule for the Deployment task on page 22.

Removing the Desktop Firewall .NAP file from the Repository

1 Start ePolicy Orchestrator and log on to the server that you want to manage.

2 If necessary, expand this server’s icon (in the console tree) to see the Repository icon.

3 Expand Repository to see its contents.

4 Expand Managed Products, and then Windows.

5 Right-click McAfee Desktop Firewall and select Remove.

6 Click Yes to verify that you want to remove the software.

7 Click OK to finish removing the Desktop Firewall software from the Repository.

Removing the Desktop Firewall package file from the Repository

1 Start ePolicy Orchestrator and log on to the server that you want to manage.

2 If necessary, expand this server’s icon (in the console tree) to see the Repository icon.

3 Select Repository.

4 Locate the AutoUpdate Tasks area and click Manage packages.
   ePolicy Orchestrator lists all of the package files in the Repository.

5 Select McAfee Desktop Firewall.

6 Click Delete.

7 Click OK when ePolicy Orchestrator asks whether to remove the package file.

8 Click OK again when ePolicy Orchestrator confirms that it made the change.
Uninstalling the McAfee Desktop Firewall ePolicy Orchestrator Update software

1. In Windows, click Start and then select Settings.

2. Select Control Panel, then select Add/Remove Programs.
   The Add/Remove Programs dialog box appears.

3. Select McAfee Desktop Firewall 8.5 ePO Update from the list, then click Change/Remove.

4. Click OK when Windows asks whether you want to remove the application.
   Windows uninstalls the Update and prompts you to restart your computer.

5. Select Yes and then click Finish.
   Your computer restarts, and Windows finishes removing the Update.

   If you select the No, I will restart my computer later checkbox, the Update will not be completely removed until you restart your computer.