Best Practices Guide

McAfee Endpoint Protection for Mac 1.0.0

Contents

Preface

This section provides information on the organization of this guide and its related product documentation details.

Contents

About this guide

This information describes the guide's target audience, the typographical conventions and icons used in this guide, and how the guide is organized.

Audience

McAfee documentation is carefully researched and written for the target audience.

The information in this guide is intended primarily for:

- **Administrators** — People who implement and enforce the company's security program.

Conventions

This guide uses the following typographical conventions and icons.

Book title or *Emphasis*	Title of a book, chapter, or topic; introduction of a new term; emphasis.
Bold	Text that is strongly emphasized.
`User input` or `Path`	Commands and other text that the user types; the path of a folder or program.
`Code`	A code sample.
User interface	Words in the user interface including options, menus, buttons, and dialog boxes.
Hypertext blue	A live link to a topic or to a website.
	**Note**: Additional information, like an alternate method of accessing an option.
	**Tip**: Suggestions and recommendations.
	**Important/Caution**: Valuable advice to protect your computer system, software installation, network, business, or data.
	**Warning**: Critical advice to prevent bodily harm when using a hardware product.

Finding product documentation

McAfee provides the information you need during each phase of product implementation, from installation to daily use and troubleshooting. After a product is released, information about the product is entered into the McAfee online KnowledgeBase.

Task

1 Go to the McAfee Technical Support ServicePortal at http://mysupport.mcafee.com.

2 Under **Self Service**, access the type of information you need:

To access...	Do this...
User documentation	1 Click **Product Documentation**. 2 Select a **Product**, then select a **Version**. 3 Select a product document.
KnowledgeBase	• Click **Search the KnowledgeBase** for answers to your product questions. • Click **Browse the KnowledgeBase** for articles listed by product and version.

1 Overview

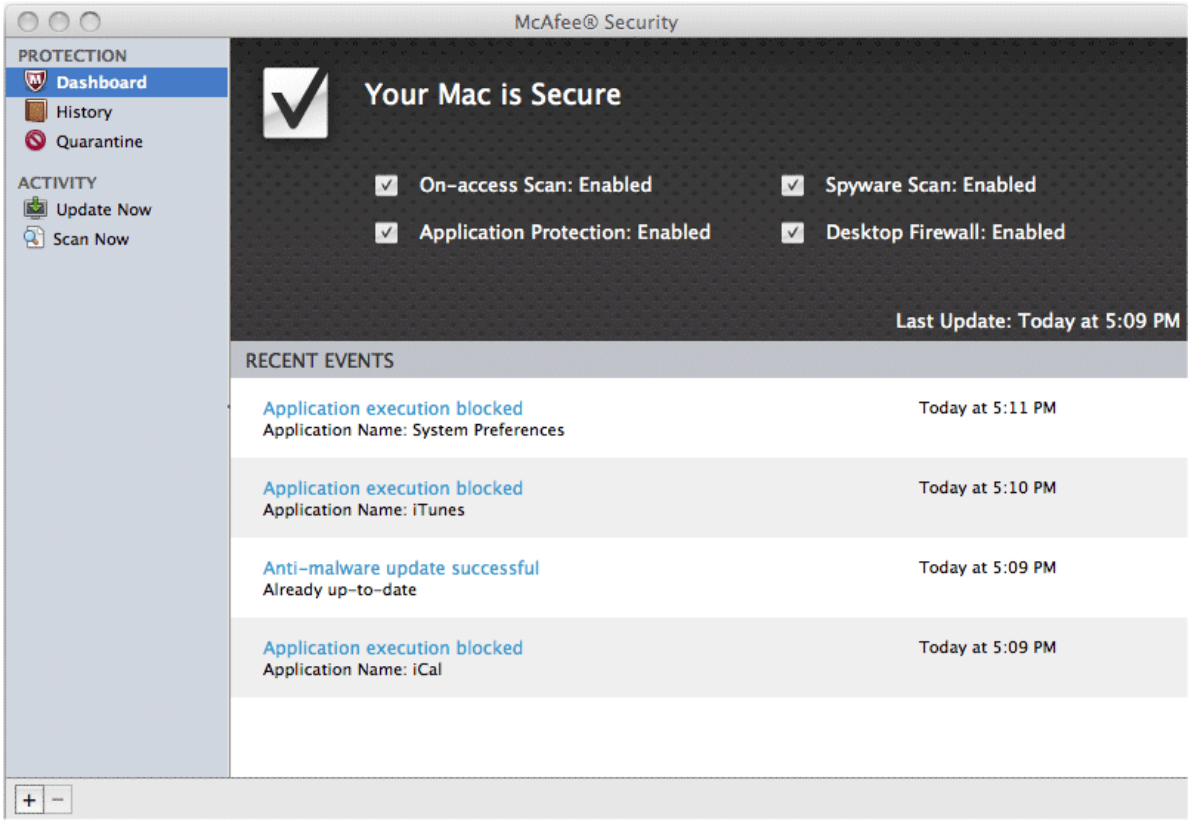
This chapter introduces McAfee Endpoint Protection for Mac 1.0, its protection features and gives you an overview of the Best Practices Guide.

Contents

Introducing McAfee Endpoint Protection

McAfee Endpoint Protection safeguards your Mac from malware, prevents execution of unwanted applications, and denies unauthorized network access.

Following is the dashboard screen that is displayed on launching McAfee Endpoint Protection. Dashboard displays the security status of your Mac, on-access scan, spyware scan, application protection, and desktop firewall. It also displays five recent product events that occured from the time you installed the product and the instance of the last anti-malware update.



Protection Features

McAfee Endpoint Protection offers the following protection features:

Feature	Description
Anti-malware	Safeguards your Mac from viruses, spyware, Trojan horses, potentially unwanted programs, and other malware.
Application Protection	Prevents applications on your Mac from: • execution • accessing the incoming or outgoing network connection
Desktop Firewall	Allows or denies access from/to a specific network/IP/host based on the rules you configure.
Update	Downloads the latest DAT files (anti-malware signatures) from an FTP, HTTP, or a local repository (as per your configuration) when connected to the Internet keeping your Mac up-to-date.

For information on other core features of McAfee Endpoint Protection, refer the *McAfee Security 1.0 User Guide*.

About the Best Practices Guide

This guide highlights the best practices for using McAfee Endpoint Protection as a standalone product or when managed through McAfee ePolicy Orchestrator.

Benefits and risks of some of the product configurations that might not seem straight-forward are explained further in this guide. You can gauge which configuration best suits your environment.

If you are managing McAfee Endpoint Protection using ePolicy Orchestrator, we presume you are familiar with using ePolicy Orchestrator and are primarily focusing on safeguarding your managed Mac systems using our McAfee Endpoint Protection software.

2 Pre-installation instructions

This chapter describes the recommended actions to be performed before installing McAfee Endpoint Protection as a standalone product or when managing McAfee Endpoint Protection on your Mac clients using McAfee ePolicy Orchestrator server.

Contents

Standalone McAfee Endpoint Protection

This section provides list of actions you must perform before installing the standalone McAfee Endpoint Protection.

- Ensure your Mac meets the minimum hardware and software requirements. Refer the *Prerequisites* section in the *McAfee Security 1.0 User Guide*.
- Ensure you have administrator rights to install McAfee Endpoint Protection. This account must be a part of the administrator users and the credentials are required to authenticate the product installation.
- Remove any previous versions of the VirusScan for Mac product prior to the VirusScan for Mac version 8.5.
- Ensure you backup the firewall rules of your Mac to add it later from the product console.
- Ensure there are no third party anti-virus, firewall and application protection products are installed on your Mac.

McAfee Endpoint Protection managed using ePolicy Orchestrator

This section provides a list of actions you must perform before deploying McAfee Endpoint Protection using McAfee ePolicy Orchestrator 4.0 or 4.5.

- Use administrator credentials to log in to the ePolicy Orchestrator server.
- Ensure McAfee Agent 4.0 or later packages are checked in to the ePolicy Orchestrator repository.
- Ensure your Mac meets the minimum hardware and software requirements for installing McAfee Endpoint Protection. Refer the *Prerequisites* section in the *McAfee Security 1.0 User Guide*.
- Remove any previous versions of the VirusScan for Mac products from your Mac clients prior to VirusScan for Mac version 8.5.

- Ensure you backup the firewall rules of your Mac clients to add it later from the product console.
- Ensure McAfee Agent 4.0 or later extensions are installed on ePolicy Orchestrator.
- Copy the install.sh file from ePolicy Orchestrator to your Mac clients using SCP, FTP or download install.sh from a browser on your Mac clients. Please refer *McAfee Security 1.0 User Guide* for instructions.

  While using FTP to copy install.sh file, ensure you copy it in binary mode.

- Ensure there are no third party anti-virus, firewall and application protection products installed on your Mac clients.

3 Post-installation instructions

This chapter provides instructions on verifying and maintaining the McAfee Endpoint Protection installation.

Contents

Standalone McAfee Endpoint Protection

After installing McAfee Endpoint Protection, you can verify if the following features of McAfee Endpoint Protection work properly.

- On-access scanning
- On-demand scanning
- Application launch
- Application network access
- System network access

To verify on-access scan and on-demand scan, we will use EICAR test file which is NOT a virus.

Tasks

- *Testing the on-access scan* on page 11
  This section provides instructions on testing the on-access scan to ensure McAfee Endpoint Protection is installed properly and can detect malware.
- *Testing the on-demand scan* on page 12
  This section provides instructions on testing the on-demand scan after testing on-access scanning.
- *Testing application launch and network access* on page 12
  This section provides instructions to test if all the third party applications launch successfully and if they can access network.

Testing the on-access scan

This section provides instructions on testing the on-access scan to ensure McAfee Endpoint Protection is installed properly and can detect malware.

Before you begin

Update McAfee Endpoint Protection with the latest DATs.

Task

1 Launch Safari and go to eicar.org.

2 Click the **Anti-Malware Testfile** link at the top-right corner of the webpage.

3 Click the **eicar.com** link.

The McAfee Notification dialog box pops up with a detection message. Click the caret for detection details.

You can view the results on the product console too.

Testing the on-demand scan

This section provides instructions on testing the on-demand scan after testing on-access scanning.

Task

1 Disable on-access scan by clicking the McAfee menulet on the menubar and selecting **McAfee Security Preferences**. Click the lock and type your administrator password. Then click **OFF** for **On-access Scan**.

2 Launch Safari and go to eicar.org.

3 Click the **Anti-Malware Testfile** link.

4 Click the **eicar.com** link to download an eicar file to a temporary location on your Mac.

5 Click McAfee menulet and select **McAfee Security Console**.

6 Click **Scan Now**, then click **Choose** in **What to scan**.

7 Select the downloaded eicar file, then click **Open**.

8 Click **Start Scan**.

The eicar test virus is detected in the scan results.

You can also view these results in the **Recent Events** pane on the dashboard or in the **History** page.

Testing application launch and network access

This section provides instructions to test if all the third party applications launch successfully and if they can access network.

Task

1 Launch applications like Safari, iTunes, Firefox or any third party application. All applications must start successfully.

2 From Safari, browse to www.mcafee.com. You should be able to browse to McAfee website.

Ensure www.mcafee.com is allowed by your firewall administrator.

McAfee Endpoint Protection managed using ePolicy Orchestrator

After deploying McAfee Endpoint Protection on Mac clients, you can verify the on-demand scanning and the details of managed nodes. You can also enforce policies to verify the reports on ePolicy Orchestrator server or theMac clients.

Testing the on-demand scan

We recommend you to test the on-demand scan when McAfee Endpoint Protection is managed using ePolicy Orchestrator.

Task

1 Disable on-access scan.

2 Download an eicar test file to a temporary location on your computer from eicar.org.

3 In **Client Tasks**, schedule an on-demand scan to run immediately.

Refer the *McAfee Security 1.0 User Guide* for instructions on scheduling on-demand scan tasks using ePolicy Orchestrator versions 4.0 and 4.5.

Details of managed nodes

Click a Mac client (managed node) in **System Tree** to view its details.

Configuring Policies

For instructions on configuring and enforcing policies, refer the *McAfee Security 1.0 User Guide*. To verify the on-access, application protection and on-demand scanning events, you can check in reports for which you need to install report extensions of McAfee Endpoint Protection 1.0 on ePolicy Orchestrator.

4 Product configurations

This chapter provides recommendations for configuring the on-access and on-demand scan, Application Protection, and Desktop Firewall policies.

Contents

Anti-malware configurations

This section provides recommendations for on-access preferences, on-demand scan preferences, and anti-malware exclusions.

On-access scan preferences

This section lists the best practices for configuring on-access scan preferences.

The following configuration identifies and eliminates viruses and other malicious programs from being copied or written to your Mac machines in real-time.

- Always enable the scan for **Network Volumes** to scan files copied from or written to any network volumes.
- In case you are using Apple Mail as your mail client, enable scan for **Apple Mail Messages** for on-access policy.
- Select the **Quarantine** option always as the secondary action for virus and spyware detections so that you can retrieve the files from the quarantine database from product console later if required.

On-demand scan preferences

Here are the best practices for configuring on-demand scan preferences.

The following configuration identifies and eliminates viruses and other malicious programs on your Mac through scheduled on-demand scans.

- Always enable the scan for **Archives & Compressed Files** to scan files copied from or written to any network volumes.
- If you are using Apple Mail as your mail client, enable scan for **Apple Mail Messages** for on-demand policy.
- Select the **Quarantine** option always as the secondary action for virus and spyware detections so that you can retrieve the files from the quarantine database from product console if required later.

On-demand scanning

This section describes the best practices for scheduling on-demand scans to obtain high performance.

- Schedule on-demand scans during non-peak hours (For example, during weekends or maintenance period).
- When scheduling an on-demand scan for the first time, schedule a full on-demand scan. Subsequently, you can scan only the new or modified items on your Mac rather than re-scanning the entire server. For example, you can scan the user's home folder or Documents and Download folder where documents are saved or downloaded by default. You can also add the folders where the files are frequently saved.

Anti-malware exclusions

This section provides recommendations for Anti-malware exclusions.

This version supports regular expression based exclusions for Anti-malware. You can add regular expressions that matches required pattern to exclude multiple files and folders from being scanned.

Some of the recommended exclusions include:

- Microsoft Entourage database files
- Thunderbird database files
- Encrypted files
- Generic plist files such as (Info.plist, version.plist and so on) for on-access scanning

The recommended exclusions will be available as an article at McAfee KnowledgeBase.

Following are few examples of regular expressions you can use for different patterns.

- To exclude files with extension "mdb", use **.*\.mdb**
- To exclude files with extension either "mdb" or "odc", use **.*\.(mdb|odc)**
- To exclude each user's Entourage/outlook Database files of different Microsoft Office versions, use **/Users/.*/Documents/Microsoft\ User\ Data/Office\ \d+\ Identities/.*Identity/Database**
- To exclude all Info.plist, version.plist under /Applications, use **/Applications/.*/Contents/(version|Info).plist**
- To exclude files with extension "jar" or "rar" or "war" under /private/var/tmp, use **/private/var/tmp/.*\..+ar**
- To exclude files under /private/var/tmp starting with an alphabet and ending with a number, use **/private/var/tmp/([A-Z]|[a-z]).*[0-9]$**

Application Protection configurations

This section provides recommendations for Application Protection configurations.

After McAfee Endpoint Protection is successfully deployed, we recommend that you follow the strategies described in this section. By following them, you will be ready to focus on activating application protection function that match your system and business needs.

You can follow the instructions in this section and perform these steps by yourselves. However, you can also contact McAfee Technical Support professionals to assist you.

Stages

- Strategy and Planning
- Initial configuration
- Continuous tuning and learn mode
- Enhanced protection

Strategy and Planning

Firstly, think about your system protection, set realistic goals, and create a pilot and deployment plan to match.

Define the priorities for pilot

Ensure you understand your security goals and align to the pilot process. You must identify applications to be blocked immediately, allow certain applications to launch, block network access to specific applications and so on. Every organization maintains its unique balance between protection and productivity.

Ask yourself questions like:

- Which applications have specific security incidents flagged in audits in the recent times?
- Which applications are most vulnerable?
- Which applications you do not want the users to use in an environment?

Answers to these questions will help you prioritize systems where you want to deploy the pilot.

Define the pilot environment

We recommend you to choose a small set of pilot systems to run a test adoption. Select various systems like mobile computers (MacBook, MacBook Pro), Intel Macs, PowerPCs (if your environment includes PowerPCs) and so on. Ensure, these systems have combinations of operating systems used in your environment.

During pilot phase, we suggest you to run the tests in your Labs with real-time applications. You can also include a few real-time users and systems as part of your pilot environment.

Categorize the applications

While defining the pilot environment, you must also categorize the applications in your environment. Prepare a checklist of the applications you want to allow, block, restrict network access and so on. We recommend you to go with basic protection in the initial stages of the roll out; the checklist will help you in further tuning process.

Following is a sample checklist for your environment:

Application Name	Execution	Network Access
Safari	Yes	Full
iTunes	Yes	No
Messenger	No	No
Firefox	Yes	Full
iChat	Yes	Restricted (No external network)

Once you are ready with initial set of applications, you can proceed with the 'Initial Configuration' instructions. Ensure no third party application protection and firewall products are installed on the systems in pilot environment.

Initial Configuration

After planning and preparing the environment, now is the time to deploy the product and configure the initial settings for Application Protection. Follow the installation and deployment steps as provided in *McAfee Security 1.0 User Guide*. Remember to deploy the latest patches and hotfixes available at McAfee Service Portal.

Before Application Protection configuration, notify users that they are receiving a new protection and provide remediation steps for certain cases. This communication will reduce perceived risk to end-user productivity, specially for users who will be carrying the MacBooks (or MacBook Pros). During the pilot period, users can override Application Protection configuration in multiple ways. They can disable or remove specific configuration, or completely remove the product if necessary. For example, if a user needs to use a specific application for a critical presentation, he can add a whitelist rule for that particular application.

As part of pilot, we suggest you to install the product manually on portable systems (such as MacBook, MacBook Pro and so on) so the user can change the configuration accordingly. If these systems are managed through ePolicy Orchestrator, modified rules will be available until the next policy enforcement only.

After notifying the users and deployment of product, remember to perform the post installation instructions for verifying successful product installation. Also for every policy changes or configuration, ensure to test each system so users can perform their tasks successfully. The best practice is to deploy the product starting with few clients and expand to more systems as confidence grows.

Next step is to configure the baseline protection. We recommend configuring the following settings for Application Protection as base link protection.

- Enable **Allow All Apple Signed Binaries** on Mac OS X Leopard and Snow Leopard to allow the execution and network access for all Apple signed applications. This configuration does not apply for Mac OS X Tiger.
- For Mac OS X Tiger, add rules to allow or block specific Apple applications such as Safari, iTunes, iChat and so on.
- Add basic rules to allow or block certain applications based on the checklist prepared earlier. During this stage, do not add any rules for restricted network access or advanced rules for certain binaries.

Once the configuration is set, check the pilot systems for proper operation of the applications and monitor ePolicy Orchestrator and product logs. Product logs are available on the client systems and can be viewed from the product console. They are named as **McAfee Security.log** and available under /var/log.

Continuous tuning and learn mode

With your pilot up and running, you can watch the behavior for a while (for about a week). Administrators must monitor the events regularly (daily or twice a day) to examine the behavior and performance of the systems. This will also help the administrators to tweak their application rules.

Your monitoring must cover the behavior and impact on normal operations of a particular user due to the application protection rules, application updates and the new applications that the user has installed on his own. Till now, as per the configured rules, you are allowing the unknown/modified applications (applications/binaries for which the rules are not added), so any new application installed by the user will automatically be allowed. In this phase, let us configure the **Unknown/Modified Applications**

setting to **Prompt** which is called *Learn mode*. After this configuration, the Application Protection starts working in learn mode. For example, one user has installed a new application for which no rule exists and when user is trying to launch this application, he will be prompted with an alert to choose an action for that binary. Based on the action chosen, a particular rule will be applied. If the user chooses **Allow Execution with Full Network Access** and clicks **Always**, a new rule will be added for that binary automatically in Application Protection rules.

- Learn Mode works at a binary level. For example, you are trying to launch an application that requires certain dependent binaries to be allowed for execution. You will be prompted for each depended binary for that application.
- If the system is managed by ePolicy Orchestrator, any action chosen by the user will be applicable till next policy enforcement only.
- When the user is in learn mode, he will be alerted with prompt to choose an action for application launch only. For example, you already opened an application that requires network access, before configuring the learn mode and there is no rule already exists for that application, after configuring in learn mode, network access for that application will automatically be denied. So ensure all applications that are not associated with a rule are closed or add rules for all the applications before configuring to learn mode.

In learn mode, we recommend you to add rules for all applications that are not associated with any rule. Specially, in Mac OS X Tiger, ensure to add rules for each Apple native application such as (Safari, iTunes and so on).

The other feature we recommend you to check in this phase is update/upgrade of applications that are associated with application protection rules. For example, if there is a rule added for version 1 of an application, when you upgrade this application to the next version (major or minor), the updated version is treated as unknown/modified application. In this case, appropriate action takes place based on the settings configured for **Unknown/Modified application**. We recommend you to update your rules whenever an update/upgrade takes place for any application associated with a rule. Please refer the *McAfee Security 1.0 User Guide* on how to apply the rules when application update/upgrade happens.

- Application upgrade/update is automatically taken care for the users in ePolicy Orchestrator managed mode. In other words, the old rules are automatically applied when the next policy enforcement occur from ePolicy Orchestrator.
- For Apple signed binaries, upon update/upgrade from one version to another version you do not need to update your rules if the updated version is also signed by Apple.

Continue monitoring and tweak your rules as applicable and update the checklist created earlier. This checklist will be useful when you deploy McAfee Endpoint Protection on all your systems. We recommend you to try this phase for at least two weeks before you move to the next phase.

Enhanced protection with strict mode

In this phase, we recommend you to enforce strict mode where all applications not associated with a rule are automatically denied. So, before you enable strict mode, we request to verify against your checklist that the rule sets are updated as per the checklist from your monitoring and tweaks. Inform

the users before you move to strict mode because it denies execution of any new application they may install. You might even need to remind them with the remedy steps discussed earlier.

To enforce the strict mode, set the **Unknown/Modified Applications** to **Deny**. Once this is configured, execution and network access to any application that is not associated with a rule will be denied and an event is generated. For managed systems, these events can be monitored from ePolicy Orchestrator. Based on the events generated, administrator can add rules to allow/deny these applications and subsequently update the checklist.

After completing these phases, you can expand the product deployment to larger set of systems.

Following are some of the basic points to remember and recommended by McAfee:

- Always select **Enable Apple Signed Binaries** on Mac OS X Leopard and Snow Leopard.
- To deny/block execution and network access for any Apple specific applications/binaries, add customized rules for those applications.
- In Mac OS X Tiger, add rules to allow Apple native applications/binaries. You can also use Application Protection exclusions, if you want to allow execution and network access of applications under a specific directory or folder.
- If your systems are not managed by ePolicy Orchestrator, ensure to update your rules whenever application update/upgrade happens.
- Do not enable the strict mode unless each application in your environment is associated with any of the customized rules, exclusions, or Apple signed binaries.
- While adding rules for applications that are dependent on binaries in different folders, please ensure to add rules for dependent binaries too.

Desktop Firewall configurations

This section provides recommendations for Desktop Firewall configuration.

Recommended rules

Following are the rules recommended by McAfee. You can configure these rules in McAfee Endpoint Protection Preferences.

General

Enable stealth mode to block ICMP incoming ping.

Custom Rules

- Allow outgoing DNS port 53 to any.
- Allow bi-directional NTP port 123 to 123.
- Allow bi-directional NetBIOS name service port 137 to 137
- Allow bi-directional all high UDP port 1024-65535 to 1024-65535
- Allow outgoing ftp client port 1024-65535 to 21
- Allow outgoing https port any to 80, 443
- Allow bi-directional for POP3, IMAP, SMTP

- Allow RDP and SNMP
- Add rules for ldap and afp/smb

Trusted Networks

- Add ePolicy Orchestrator's server IP for agent - server communication
- Add any critical server IP/subnet to allow the incoming/outgoing communication to/from that server

5 Repairing McAfee Endpoint Protection

You can use the "repairMSC" utility to troubleshoot McAfee Endpoint Protection issues. It generates a diagnostic report, which can be uploaded to the McAfee server for the analysis of the issue.

Task

1. Open the Terminal window, type the following command and press **return**:
   /usr/local/McAfee/repairMSC
2. Type the administrator password when prompted and press **return**.
3. Type "y" to continue, then press return. A consolidated diagnostic report is generated for the analysis of the issue in your home directory. A list of general issues appear; each issue relating to a number beginning from 1 to 8.
4. Type a number that best describes your issue, then press **return**. The **repairMSC** utility runs a repair based on the selected number and offers a solution.
5. Type "y" or "n" based on whether your issue was resolved or not and follow the on-screen instructions accordingly.

If your issue is not related to the ones in the list, press 8, press **return** and follow the on-screen instructions.

The final report is in ZIP format and is available in your home directory. Contact McAfee Technical Support for further assistance.

Index