Product Guide

LinuxShield™

version 1.5

McAfee®
System Protection

Industry-leading intrusion prevention solutions

McAfee®

Contents

1 Introducing LinuxShield 7

What is LinuxShield? . . . 7
How does LinuxShield work? . . . 8
How multiple LinuxShield installations interact . . . 8
Features . . . 10
What's new in this release . . . 11
Using this guide . . . 11
Audience . . . 11
Conventions . . . 12
Getting product information . . . 13
Contact information . . . 14

2 Scanning For Viruses 15

How does scanning work? . . . 15
What and when to scan . . . 16
Types of scanning . . . 16
On-access scanning . . . 16
On-demand scanning . . . 17

3 LinuxShield Interface 19

Opening the LinuxShield interface . . . 19
Retaining names in the Host Summary . . . 20
Introducing the LinuxShield interface . . . 21
Navigation pane . . . 22
Console . . . 23
Quick Help pane . . . 23
Links bar . . . 24
Using the interface . . . 25
Expanding and collapsing tables of information . . . 25
Sorting by table columns . . . 26
Navigating through long tables . . . 26
Changing the settings on a page . . . 27
Automatically refreshing information on pages . . . 27
Using wizards . . . 27
Understanding error messages . . . 28
Displaying dates and times . . . 28

4 Viewing LinuxShield Information 29

Host Summary . . . 29
Scanning Summary . . . 31
- Scanning statistics . . . 32
- Recently detected items . . . 32
- Recently scanned items . . . 33
- Obtaining a diagnostic report . . . 33

Detected items . . . 34
- Analyzing the detected items . . . 35
- Viewing the results . . . 36
- Exporting the results for analysis . . . 36

System events . . . 37
- Analyzing the system events . . . 37
- Exporting the results for analysis . . . 38

Scheduled tasks . . . 39
- Running a task immediately . . . 40
- Modifying an existing scheduled task . . . 40
- Deleting an existing scheduled task . . . 40
- Stopping a task . . . 41

Information about extra DAT files . . . 41

5 Setting Up Schedules 43

Using a wizard . . . 44
Updating the product . . . 44
- Creating a schedule to update the product . . . 45

Running on-demand scans . . . 47
- Creating a schedule to run an on-demand scan . . . 48

Running a task from the command line . . . 49

6 Configuring LinuxShield 51

Monitored hosts . . . 52
- Adding a new host . . . 53
- Stopping the monitoring of a host . . . 53
- Reconnecting a host . . . 53

General settings . . . 54
- Browser interface . . . 55
- Logging . . . 55
- Clearing statistics . . . 56
- Resetting configuration settings . . . 56

On-access settings . . . 57
- Scanning options . . . 58
- Paths excluded from scanning . . . 59
- Extension-based scanning . . . 60
- Anti-virus actions . . . 62

On-demand settings . . . 63
Notifications . . . 64
- SMTP notifications . . . 64
- SMTP settings . . . 65

7 Advanced Features 67

Substituting variables in notification templates . . . 67
Configuring features from a file . . . 69
Controlling LinuxShield from the command line . . . 70
- Controlling the processes . . . 70
- Controlling LinuxShield . . . 71

How the quarantine action works . . . 72

8 Troubleshooting 73
Frequently asked questions 73
Installation 73
Scanning 74
Viruses and detection 75
General information 77
Error messages 78

Glossary 79

Index 83

1 Introducing LinuxShield

LinuxShield detects and removes viruses and other potentially unwanted software on Linux-based systems. This section describes:

- What is LinuxShield?
- How does LinuxShield work?
- What's new in this release
- Using this guide
- Getting product information
- Contact information

What is LinuxShield?

LinuxShield detects and removes viruses and other potentially unwanted software on Linux-based systems. LinuxShield uses the powerful McAfee scanning engine — the engine common to all our anti-virus products.

Although a few years ago, the Linux operating system was considered a secure environment, it is now seeing more occurrences of software specifically written to attack or exploit security weaknesses in Linux-based systems. Increasingly, Linux-based systems interact with Windows-based computers. Although viruses written to attack Windows-based systems do not directly attack Linux systems, a Linux server can harbor these viruses, ready to infect any client that connects to it.

When installed on your Linux systems, LinuxShield provides protection against viruses, Trojan horses, and other types of potentially unwanted software.

LinuxShield scans files as they are opened and closed — a technique known as *on-access* scanning. LinuxShield also incorporates an *on-demand* scanner that enables you to scan any directory or file in your host at any time.

When kept up-to-date with the latest virus-definition (DAT) files, LinuxShield is an important part of your network security. We recommend that you set up an anti-virus security policy for your network, incorporating as many protective measures as possible.

LinuxShield uses a web-browser interface, and a large number of LinuxShield installations can be centrally controlled by ePolicy Orchestrator.

How does LinuxShield work?

Once LinuxShield software has been correctly installed and configured on your Linux host, it provides two functions:

- LinuxShield runs as a daemon (which is similar to a service in Microsoft Windows).

  As files are accessed via the Linux kernel, LinuxShield intercepts the files and scans them for viruses and other potentially unwanted software. (See *Events that trigger LinuxShield scanning* for more information.) This form of protection is called *on-access scanning*. LinuxShield also maintains a record of files that it has recently scanned to avoid any unnecessary repeated scanning.

- LinuxShield runs an HTTPS-based monitoring service.

  LinuxShield activities can be monitored and configured through an HTTPS interface. For example, you can configure which types of files LinuxShield will scan, and actions that LinuxShield will take against infected files, such as cleaning, deletion or quarantining. Using the simple and secure web-browser interface, you can monitor and control virus detection on several Linux hosts. Using ePolicy Orchestrator, you can control a large number of Linux hosts from a single point.

The LinuxShield software runs under a user called *nails*.

Events that trigger LinuxShield scanning

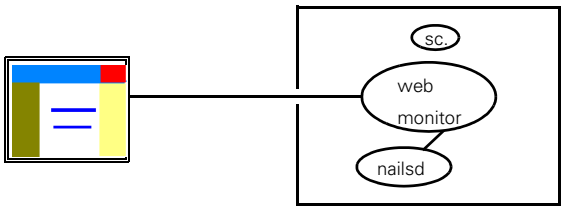
LinuxShield begins to scan files on the following events:

- File open — When a file is opened.
- File release — In the simple case, this is when a file is closed. If a process has multiple references to a file, for example, via dup or a memory mapping, this is when the last reference is released.

How multiple LinuxShield installations interact

LinuxShield requires a web browser to monitor and control virus scanning on a host. The diagram shows a web browser connected via a secure HTTPS link to a web monitor service that we supply as a component of the LinuxShield software.

Figure 1-1 Single LinuxShield installation



The next table explains how the components operate in this simple set up.

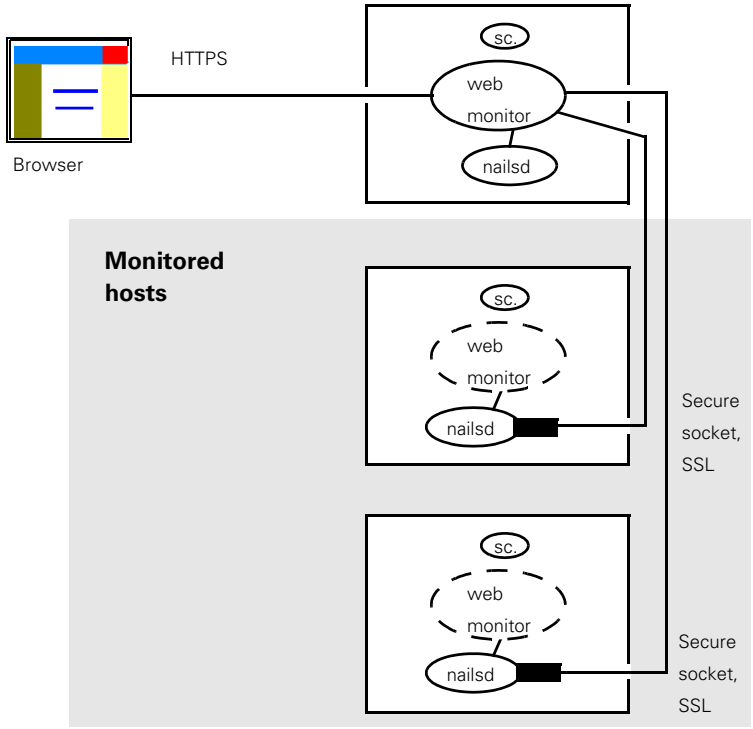
Table 1-1 Process names and functions

Process	Function
scanner	This component provides anti-virus protection, scanning files as instructed by nailsd. This is marked as **sc.** in the diagram.
nailsd	This component communicates between the web monitoring service and the scanner, passing information about the anti-virus scans and configuration details.
mon	This component of the web monitor examines LinuxShield activity on the host, and can configure the anti-virus activity.
nailswebd	This component of the web monitor communicates with a web browser such as Konqueror, using a secure HTTPS link. A name and password is required for user authentication.

Monitoring several hosts

You can monitor anti-virus activity on *several* hosts from this one location. The web monitor can communicate securely with up to 20 other hosts concurrently. The next diagram shows how the web monitor communicates with other hosts.

Figure 1-2 Monitoring several hosts



The web monitor service is required on only *one* host. All the other hosts with which the web monitor communicates are called *monitored hosts*. (Information is exchanged using Secure Socket Links (SSL.) Furthermore, the link needs to be authenticated using the same name and password that are entered by the user during log-on. The web monitor process does not need to be started on any host where you do not plan to connect a browser directly to the host.

By default, the browser shows the LinuxShield activity of the host to which it is directly connected.

Controlling multiple LinuxShield hosts from a single browser

To control multiple LinuxShield hosts from the single browser interface:

- LinuxShield must be running as the *same* user on each of the hosts. The default user during installation is *nails*.
- The *nails* user must have the *same* password on each of the hosts.

If this is not done, you can see only a summary of anti-virus activity from all the monitored hosts; you will see an *authentication failure* message if you try to configure the hosts (as through the pages described in *Configuring LinuxShield* on page 51).

Features

LinuxShield software has the following features:

- Kernel hooking modules (KHMs).
- Support for AMD 64 / EM64T (64-bit) platforms.
- Scanning
  - Comprehensive on-access anti-virus scanning and cleaning using the McAfee scanning engine.
  - On-access scanning for local file systems, NFS and Samba.
  - Kernel-level scan cache for improved performance.
  - Scheduling of on-demand scans.
  - Scheduling of updates for scanning engine and virus definition files.
- Administration
  - Remote administration using browser-based user interface.
  - Monitoring and configuring of multiple LinuxShield installations from the browser interface.
  - Secure browser interface with authentication and HTTPS (SSL) support.
  - Remote administration and reporting using ePolicy Orchestrator.
- Reporting
  - Real-time statistics.
  - Detailed database for detected items and system events.
  - Ability to query the database by date range or individual field values, for example, virus name. Results of query can be exported to a CSV file.
  - Configurable email notification for detected items, out-of-date virus-definition files, configuration changes, and system events.
  - Diagnostic report for use when reporting a problem with the product.

What's new in this release

This release of LinuxShield includes the following new enhancements:

- Redhat Enterprise Linux 5 (32-bit).
- Redhat Enterprise Linux 5 (AMD 64/EM64T).
- Global File System (GFS) on Redhat Enterprise Linux 5.
- Novell Open Enterprise Server 2 (32-bit).
- Novell Open Enterprise Server 2 (AMD 64/EM64T).
- Kernel module versioning which provides on-access scanning on new kernels without having to recompile modules.
- The latest version (5200) of the McAfee anti-virus engine.
- Incremental Virus Signature (DAT) updates.

Using this guide

This guide provides information on configuring and using your product. For system requirements and installation instructions, refer to the Installation Guide. These topics are included:

- *What is LinuxShield?* on page 7
  An overview of the product, including a description of new or changed features; an overview of this guide; McAfee contact information.
- *Scanning For Viruses* on page 15
- *LinuxShield Interface* on page 19
- *Viewing LinuxShield Information* on page 29
- *Setting Up Schedules* on page 43
- *Configuring LinuxShield* on page 51
- *Advanced Features* on page 67
- *Troubleshooting* on page 73
- *Glossary* of terms.

Audience

This information is intended for network administrators who are responsible for their company's anti-virus and security program.

Conventions

This guide uses the following conventions:

Bold Condensed	All words from the interface, including options, menus, buttons, and dialog box names. **Example:** Type the **User** name and **Password** of the appropriate 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).
	Examples:
	The default location for the program is:
	`C:\Program Files\McAfee\EPO\3.5.0`
	Run this command on the client computer:
	`scan --help`

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. **Example:** 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, another 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 using a hardware product.

Getting product information

Unless otherwise noted, product documentation comes as 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 — Introduction to the product and its 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.

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

Release Notes — *ReadMe*. Product information, resolved issues, any known issues, and last-minute additions or changes to the product or its documentation.

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

Contacts — Contact information for McAfee services and resources: technical support, customer service, Security Headquarters (AVERT), beta program, and training.

Contact information

Threat Center: McAfee Avert® Labs http://www.mcafee.com/us/threat_center/default.asp

Avert Labs Threat Library
http://vil.nai.com

Avert Labs WebImmune & Submit a Sample *(Logon credentials required)*
https://www.webimmune.net/default.asp

Avert Labs DAT Notification Service
http://vil.nai.com/vil/signup_DAT_notification.aspx

Download Site http://www.mcafee.com/us/downloads/

Product Upgrades *(Valid grant number required)*

Security Updates (DATs, engine)

HotFix and Patch Releases

- **For Security Vulnerabilities** *(Available to the public)*
- **For Products** *(ServicePortal account and valid grant number required)*

Product Evaluation

McAfee Beta Program

Technical Support http://www.mcafee.com/us/support/

KnowledgeBase Search
http://knowledge.mcafee.com/

McAfee Technical Support ServicePortal *(Logon credentials required)*
https://mysupport.mcafee.com/eservice_enu/start.swe

Customer Service

Web
http://www.mcafee.com/us/support/index.html
http://www.mcafee.com/us/about/contact/index.html

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

Professional Services

Enterprise: http://www.mcafee.com/us/enterprise/services/index.html

Small and Medium Business: http://www.mcafee.com/us/smb/services/index.html

2 Scanning For Viruses

and other potentially unwanted software

McAfee LinuxShield software can perform several types of scanning on your computers in order to provide as much anti-virus protection as possible. You can configure a number of these scanning features, the type of scan, which objects (for example archive files) to scan, and when to run the scan.

This section describes briefly how scanning works and the types of scanning that are available.

How does scanning work?

Your McAfee anti-virus software contains the McAfee scanning engine and the virus definition (DAT) files. The engine is a complex data analyzer. The DAT files contain a great deal of information, including thousands of different *drivers,* each of which contains detailed instructions on how to identify a virus or type of virus.

The McAfee scanning engine works together with the DAT files. It identifies the type of object being scanned (often a file) and decodes the contents of that object. The engine then uses the information in the DAT files to search for known viruses. Many viruses have a distinctive *signature* — a sequence of characters unique to that virus.

The engine uses a technique called *heuristic analysis* to search for unknown viruses. This involves analysis of some of the object's program code and searching for distinctive features typically found in viruses.

Once the engine has confirmed the identity of a virus, it cleans the object as far as possible. For example, the anti-virus software can remove an infected macro from a document or delete the virus code in an executable file. If the virus has destroyed data, and the file cannot be fixed, the anti-virus software must make the file safe so that it cannot be activated and infect other files.

What and when to scan

The threat from viruses can come from many directions, including infected macros, shared program files, files shared across a network, email, floppy disks, and files downloaded from the Internet. Each McAfee anti-virus software product targets a specific area of vulnerability. We recommend a multi-tiered approach to provide the full range of virus detection, security and cleaning capability.

You can configure your LinuxShield software according to the demands of your system. These demands depend on when and how the parts of your system operate and how they interact with each other and with the outside world, particularly through email and Internet access.

A variety of options can be configured or enabled which allow you to determine how your anti-virus software deals with different types of file and what it does with infected or suspect items.

For further information about configuring the software, see *Configuring LinuxShield* on page 51.

Types of scanning

Scanning fall into these main groups — on-access scanning and on-demand scanning. The types of scanning detect the same viruses, but they work at different points on the network and on the desktop computer. The types of scanning can take place at different times, and at different stages in the handling of objects.

On-access scanning

On-access scanning (or *real-time scanning*) examines objects as they are accessed by the user or the system. For example, an on-access scanner examines a file when the user opens it.

When you first install LinuxShield, on-access scanning defaults are set but you can configure these to suit your system. You can set global options that determine how scanning is carried out, including how the scanner deals with different types of object, specifying what is to be done with infected items, and how quarantine and notification is handled.

For further details of how to configure on-access scanning, see *Configuring LinuxShield* on page 51.

On-demand scanning

The types of on-demand scan are:

- Standard on-demand scan - the user instructs the scanning software to perform a scan, this is launched manually.
- Scheduled on-demand scan - this is scheduled to run automatically at predetermined intervals or times. You may choose to schedule a scan of this type to run after the regular DAT update.

You may run an on-demand scan for many reasons, for example:

- To check a file that has been downloaded from the Internet or obtained from an external source.
- To check that a PC is virus-free, possibly following DAT update, in case new viruses can be detected.
- To check that your entire computer is completely clean, following a recent single detection.

For further details of how to configure on-demand scanning, see *Configuring LinuxShield* on page 51.

3 LinuxShield Interface

After LinuxShield has been correctly installed and configured on your Linux host, it runs as a daemon. To make changes to your LinuxShield software configuration, or to view information about your software, you use the LinuxShield interface.

This section describes the interface in detail:

- *Opening the LinuxShield interface* on page 19.
- *Introducing the LinuxShield interface* on page 21.
- *Using the interface* on page 25.

To start using LinuxShield straightaway, see page 29 to page 51.

We strongly recommend that you use the browser-based interface to manage LinuxShield features. Although some features can be configured using text-based files (described on *Configuring features from a file* on page 69), we do not recommend this.

Some actions can also be controlled from the command line. For more information, see *Controlling LinuxShield from the command line* on page 70.

Opening the LinuxShield interface

To open the LinuxShield interface:

1. Open a web browser, such as Internet Explorer, Mozilla or Konqueror. See the *Installation Guide* for a list of supported browser versions.
2. In the address bar, type:

   `https://<hostname>:<port>`

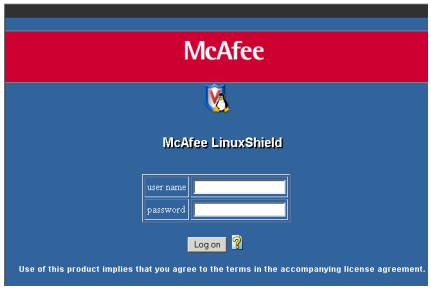
   For example: `https://192.168.200.200:55443` or `https://server1:55443`.

   Letter case is not important. LinuxShield regards `server1` and `SERVER1` as similar.

   The browser tries to connect to the port on the Linux host where the LinuxShield web-monitoring service runs, and displays the logon page.

   If your browser or its version are not supported, you see a warning message. You may continue to log on, but you might experience problems later with the display and operation of features of the interface.

Figure 3-1 Logon page



3 For help with logon, click the symbol: "**?**"

4 Enter the user name and password, then click **Log On**.

After a short time, the LinuxShield homepage is displayed.

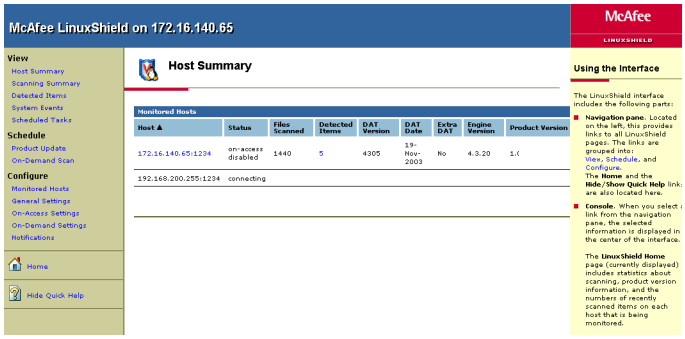
On Konqueror browsers, the following message appears in a dialog box:

```
Server certificate failed the authenticity test . . .
```

This happens because the certificate is self-signed. You may ignore this message and click **Continue**.

The **Host Summary** page is displayed. To return to this page at any time, click **Home** from the navigation pane (on the left side).

Figure 3-2 LinuxShield homepage



The **Host Summary** page lists all the hosts that are currently monitored and provides some brief information about them. See *Host Summary* on page 29 for more information about this page.

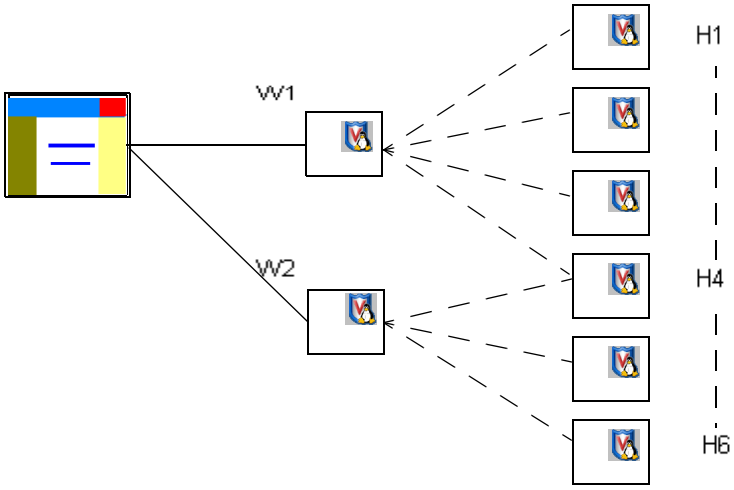
When the product is first started, the list contains only one host, as specified during installation. To add other hosts, see *Monitored hosts* on page 52. As you add more hosts to the list, their names are retained, so that you will see them again when you next run LinuxShield. This feature is explained further in *Retaining names in the Host Summary*.

Retaining names in the Host Summary

The following example shows how LinuxShield retains the names of the hosts that you see in the **Host Summary** page.

In the figure, *Connections through multiple web servers*, a LinuxShield web server is installed on the W1 host and the W2 host. While the browser was connected to the W1 host, the user added four other hosts, H1 - H4 to the list. While the browser was connected to the W2 host, the user added three hosts, H4 - H6 to the list.

Figure 3-3 Connections through multiple web servers

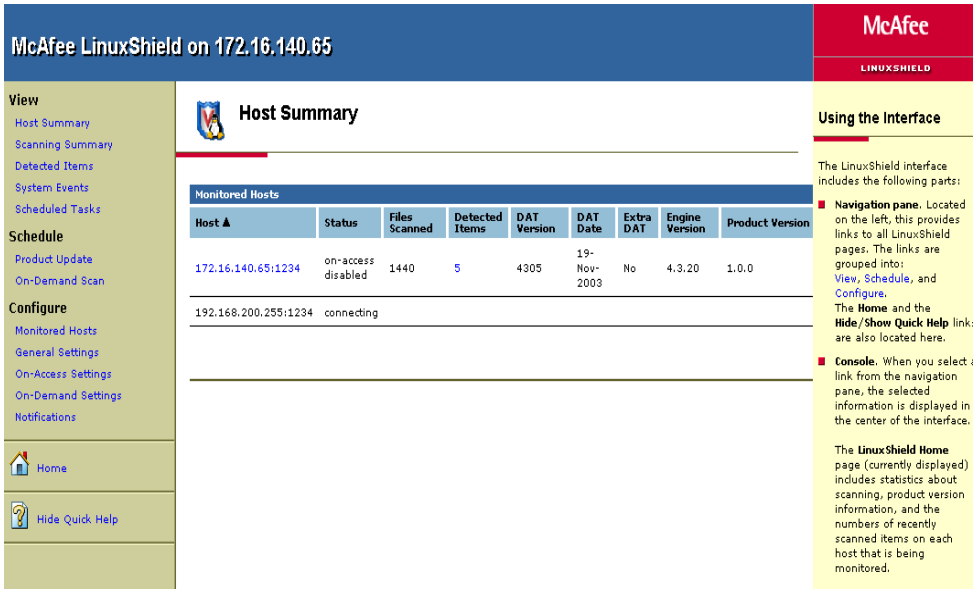


A host with a LinuxShield web server installed, such as W1 or W2, maintains a simple list of only the other hosts to which it has been connected. For example, when you connect your browser to W1, H6 does not appear in the **Host Summary** page. Similarly, when you connect your browser to W2, H1 does not appear in the **Host Summary** page.

Introducing the LinuxShield interface

The LinuxShield interface has the following layout.

Figure 3-4 LinuxShield interface



The interface has the following main areas:

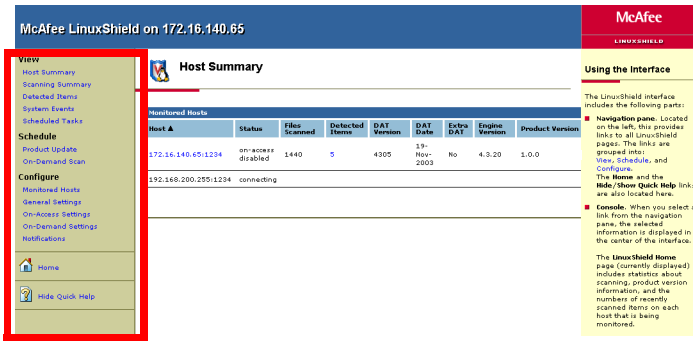
- Left — *Navigation pane* on page 22.
- Middle — *Console* on page 23.
- Right — *Quick Help pane* on page 23.

See also *Links bar* on page 24 and *Using the interface* on page 25.

Navigation pane

The navigation pane, on the left side of the LinuxShield interface, provides links to each page. Similar links are grouped together.

Figure 3-5 Navigation pane



The name of the currently selected Linux host appears above the navigation pane as a host name and port number, for example: **server1:1234**

The groups of items in the menu (**View**, **Schedule** and **Configure**) refer to this host.

- **View**

  These options display pages of information about the selected host:

  Host Summary. See *Host Summary* on page 29.

  Scanning Summary. See *Scanning Summary* on page 31

  Detected Items. See *Detected items* on page 34.

  System Events. See *System events* on page 37.

  Scheduled Tasks. See *Scheduled tasks* on page 39.

- **Schedule**

  These options display pages where you can set up schedules for running on-demand scans and updating the virus definition (DAT) files:

  - **Product Update**. *Updating the product* on page 44.
  - **On-Demand Scan**. *Running on-demand scans* on page 47.

- **Configure**

These options display pages where you can configure LinuxShield on the selected host:

- **Monitored Hosts**. See *Monitored hosts* on page 52.
- **General Settings**. See *General settings* on page 54.
- **On-Access Settings**. See *On-access settings* on page 57.
- **On-Demand Settings**. See *On-demand settings* on page 63.
- **Notifications**. See *Notifications* on page 64.

The navigation pane also includes the following links:

- **Home**

  The LinuxShield **Home** page displays summary information about the hosts that are being monitored.

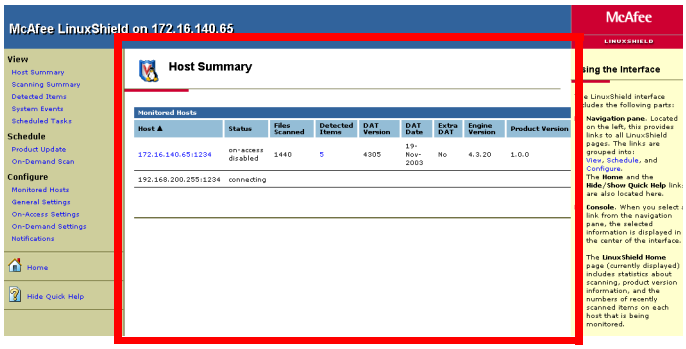
- **Show/Hide Quick Help**

  The LinuxShield interface includes the **Quick Help** pane, which is usually displayed on the right of the LinuxShield interface.

Console

The console, in the middle of the LinuxShield interface, displays each page that is selected from the navigation pane.

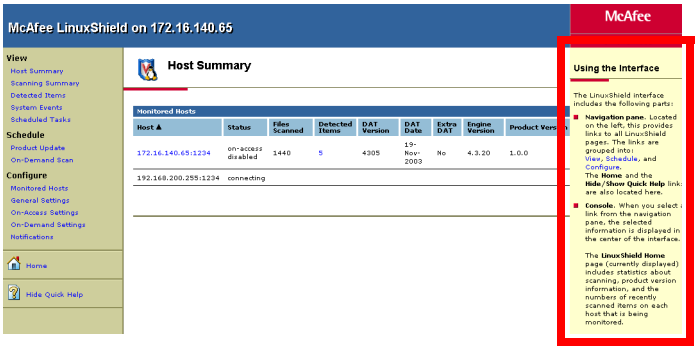
Figure 3-6 Console



Quick Help pane

The **Quick Help** pane, on the right side of the window, displays basic information about each page displayed within the console area of the interface. Quick Help includes links to the online Help system, to our web site and to other sources of product information.

Figure 3-7 Quick Help pane



You can show or hide **Quick Help**, using the **Show Quick Help** or **Hide Quick Help** menu options from the navigation pane. See also **Hide quick help on startup** under *General settings* on page 54.

Links bar

The links bar, at the top of the LinuxShield interface, contains links to useful resources such as the Virus Information Library and the **Help Topics**. This black bar contains the following links:

Table 3-1 Links bar

Log off	Return to the LinuxShield logon screen.
Technical Support	Frequently asked questions on our Technical Support web site.
Submit a Sample	Instructions for submitting a virus sample to us.
Virus Information	Links to the Virus information Library, which provides full information about every virus and other potentially unwanted software that our products can detect and clean.
About LinuxShield	Product and licensing information.
Resources	Contact information.
Help Topics	Online help.

The web addresses of the links are listed under *Contact information* on page 14.

Depending on the configuration that your organization requires, some of these links may not be available or they may redirect to other locations. See *Advanced Features* on page 67.

Using the interface

This section describes the features of the LinuxShield interface.

- *Expanding and collapsing tables of information*.
- *Sorting by table columns* on page 26.
- *Navigating through long tables* on page 26
- *Changing the settings on a page* on page 27.
- *Automatically refreshing information on pages* on page 27.
- *Using wizards* on page 27.
- *Understanding error messages* on page 28.
- *Displaying dates and times* on page 28.

We recommend that you use the navigation pane and the **Refresh** button on the LinuxShield interface, because in some browsers, the **Back** and **Refresh** buttons do not function as expected.

Expanding and collapsing tables of information

The interface contains several tables of information. For convenience, you can expand or collapse some tables.

Example of an expanded table:

[-] Recently Scanned	
Time	**File name**
May 5, 2004 12:01:05	file1
May 5, 2004 12:02:35	file2
May 5, 2004 12:10:00	file3
May 5, 2004 12:21:55	file4

Example of a collapsed table:

[+] Recently Scanned

To expand or collapse tables, click the following buttons.

Click to hide the information. (Collapse)

Click to show the information. (Expand)

Sorting by table columns

The interface contains several tables. For convenience, you can sort the information. For example, to sort rows into time order, click on the column heading, **Time**. An arrow on the right side of a column heading appears and indicates the order of the sorting.

^ — The information is displayed in ascending ordering (0-9, A-Z).

V — The information is displayed in descending ordering (9-0, Z-A).

To reverse the order of sorting, click the column heading again.

Table 3-2 Sorting information in tables

Time ^	File Name
May 5, 2004 12:01:05	foo1
May 5, 2004 12:02:35	foo2
May 5, 2004 12:10:00	foo3
May 5, 2004 12:21:55	foo4

This action does not refresh or update the contents of a table. The action does not sort all the information; it changes the order of the *currently displayed* rows of information only.

Navigating through long tables

If LinuxShield has too much information to display normally within a page, LinuxShield displays just a few rows at a time. Navigation arrows and numbers appear at the foot of the table to enable you to access the rest of the information. For example:

<< 1 **2** 3 4 5 >>

The symbols have the following meanings:

<< Click to go to the previous section of the table.

2 You are currently viewing section 2 of the table. The number is displayed larger than the others.

4 Click to go to section 4 of the table.

>> Click to go to the next section of the table.

To increase the number of rows of information that you can view in one page, see **Results per page** under *General settings* on page 54.

LinuxShield applies a limit to the amount of information that can be viewed over several pages. For example, on the **Detected Items** page (on page 34) and the **System Events** page (on page 37), you can view up to 20 pages each containing up to 50 rows. You can effectively view more results by using a query to filter the information.

Changing the settings on a page

From several pages within the interface, you can change settings, such as which types of file to scan. These pages have a button marked **Edit** at the top right of the page.

1 To enable any changes to the settings, click **Edit**.

The **Edit** button is replaced by other buttons — **Apply** and **Cancel**, and in some cases, **Defaults** or **Reset**.

2 To change any settings, update the fields, then click **Apply**.

3 If while making the changes, you decide not to proceed, click **Cancel**.

4 To reset the settings on the page to the defaults that were in effect when LinuxShield was first installed, click **Reset**.

When you click **Cancel** or **Defaults**, you are prompted to confirm that you want to do this.

Automatically refreshing information on pages

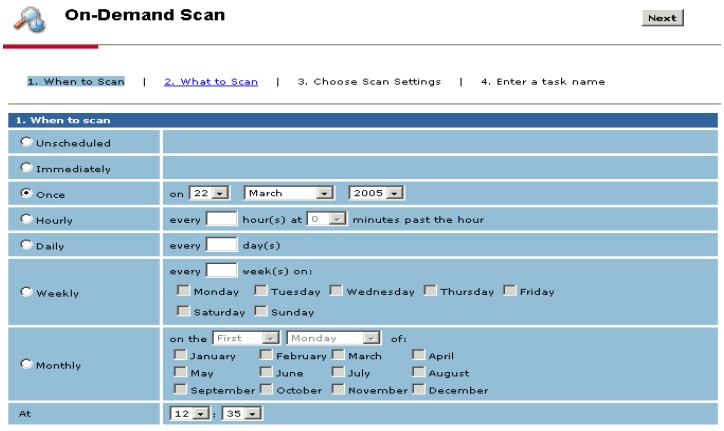
The information on some pages (such as the **Scanning Summary**) is automatically refreshed every 10 seconds by default. You can change the refresh interval from the LinuxShield interface. See *General settings* on page 54.

To manually refresh these pages at any time, click **Refresh** at the top of the page.

Using wizards

The LinuxShield interface uses a form of *wizard* to help you complete some complex tasks by specifying required settings in a sequence of panes.

Figure 3-8 Typical wizard pane



This example is taken from an option in the **Schedule** menu. The **Next** and **Back** buttons in the top right corner enable you to move from pane to pane. You can also move to any pane by clicking the tabs labelled **1. ...** and **2. ...** and so on.

To close the wizard and complete the task, click **Finish**.

Understanding error messages

If a fault occurs with the interface, LinuxShield displays a message on the current page. The message typically has the format:

Error Code	Description
25	Connection failed to host 192.168.255.200

For more information, click the error code. Other types of errors are logged as system events. See *System events* on page 37.

Displaying dates and times

Dates and times in the interface are expressed as the local time on the host. Time is displayed in 24-hour format, and includes a UTC (Universal Time Co-ordinates) offset. For example:

May 30, 2004 12:35:00 (-8:00 UTC)

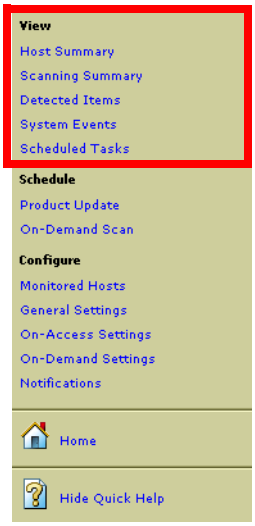
To prevent the display of the UTC offset, see **Display time UTC offset** in *General settings* on page 54.

4 Viewing LinuxShield Information

From the **View** area of the navigation pane, you can view the following information about LinuxShield:

- *Host Summary*.
- *Scanning Summary* on page 31.
- *Detected items* on page 34.
- *System events* on page 37.
- *Scheduled tasks* on page 39.

Figure 4-1 View menu

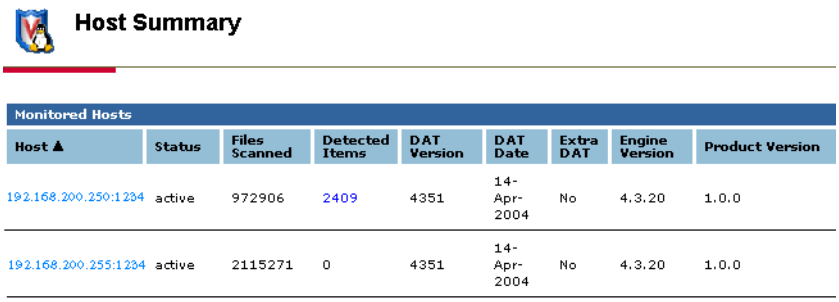


Host Summary

The **Host Summary** page shows information collected from a number of hosts (up to 20) that are running LinuxShield. The information includes the number of files that have been scanned and any detections. You can also check that the scanning engine and virus definition (DAT) files are consistent and current throughout your network.

To view this page, click **Host Summary** under **View** in the navigation pane.

Figure 4-2 Host Summary page



Host Summary

Monitored Hosts

Host ▲	Status	Files Scanned	Detected Items	DAT Version	DAT Date	Extra DAT	Engine Version	Product Version
192.168.200.250:1234	active	972906	2409	4351	14-Apr-2004	No	4.3.20	1.0.0
192.168.200.255:1234	active	2115271	0	4351	14-Apr-2004	No	4.3.20	1.0.0

To add or remove hosts, use the **Configure Monitored Hosts** page. See *Configuring LinuxShield* on page 51. For more information about the scanning activity on each active host, click its name in the **Host** column. The table contains the following information:

Table 4-1 Host Information

Host	Name of host being monitored. Click this address to view the **Scanning Summary** page for that host.
Status	Status of the host: ■ active — the host is being monitored. ■ connecting, disconnecting — brief changes of state. ■ disconnected — typically the host has been switched off, or its services are not running. ■ on-access disabled — on-access scanning has been disabled on the host. See *On-access settings* on page 57.
Files Scanned	Number of items that have been scanned since LinuxShield was installed, or since the statistics counters were last reset.
Detected Items	Number of detected items since LinuxShield was installed or since the statistics counters were reset. Click this number to see more details on the **Detected Items** page for that host.
DAT Version	The 4-digit version number for the DAT files.
DAT Date	Date when these DAT files were created. We regularly provide updated DAT files. If the date is more than a few days ago, your DAT files are probably out of date.
Extra DAT	We occasionally provide an 'extra DAT' file to counter specific threats. See *Glossary* on page 79. If an 'extra DAT' file is available, click **Yes** to view the details on the **Extra DAT** page.
Engine Version	Version of the scanning engine. Engines are updated less often than DAT files.
Product Version	Version of the product.

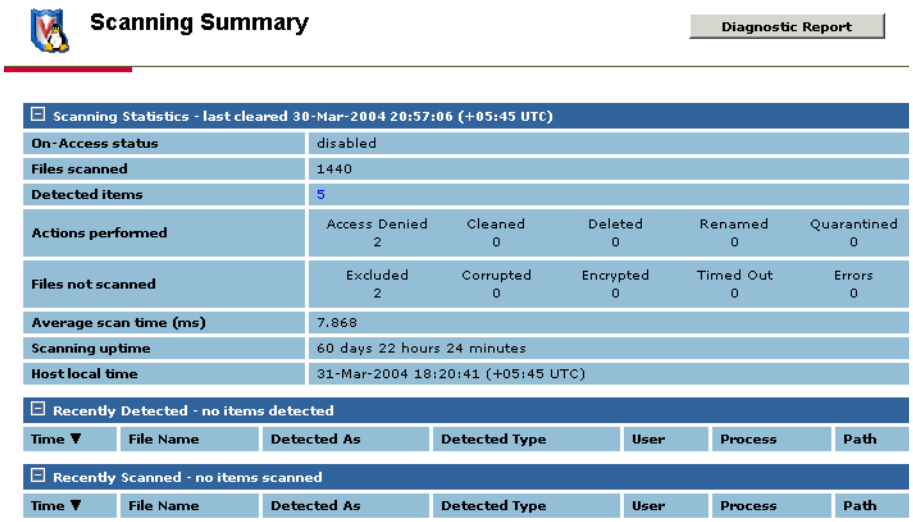
To reset the **Files Scanned** and **Detected Items** to zero, see the **General Settings** page. See *General settings* on page 54.

Scanning Summary

The **Scanning Summary** page shows details of on-access scanning activity on the host that you selected from the **Host Summary** page. See *Host Summary* on page 29. (Statistics about any on-demand scans are available from the **Detected Items** page. See *Detected items* on page 34.)

To view this page, click **Scanning Summary** under **View** in the navigation pane.

Figure 4-3 Scanning Summary page



The page includes the following information:

- *Scanning statistics* on page 32, which includes information such as the number of files that have been cleaned.
- *Recently scanned items* on page 33.
- *Recently detected items* on page 32.

Scanning statistics

The next table explains the information in each column. The statistics are collected from the time when LinuxShield was installed, or since the statistics counters were last reset on the **General Settings** page.

Table 4-2 Scanning statistics

On-Access status	Indicates whether on-access scanning is enabled.
Files scanned	Number of files scanned since the host started or the counters were reset.
Detected items	Number of items detected by on-access scanning since LinuxShield was installed or since the count was last cleared. To see more details, click this number to view the **Detected Items** page.
Actions performed	Actions that have been performed on files, in accordance with the settings on the **On-Access Settings** page. For on-access scans, **Access denied** means that all actions taken against the infection failed, or the action was set to deny access.
Files not scanned	Numbers of files that were not scanned for various reasons. For example, some items are excluded because they are on specified excluded paths, or because of the file name extension.
Average scan time (ms)	Measure of scan performance. Average time in milliseconds taken to scan an item.
Scanning uptime	Time since LinuxShield was last started. Statistics about average scanning time are based on this period.
Host local time	Time is expressed in 24-hour format as local time on the host, and with a UTC offset. See *Displaying dates and times* on page 28.

Recently detected items

This information is continuously updated as files are accessed, then scanned and any viruses are detected. Although a file name appears in the list, the file itself might no longer exist if LinuxShield has deleted the infected file. The following information is displayed under **Recently Detected**.

Table 4-3 Recently detected items

Time	Time when the detection occurred.
File Name	Name of the file, excluding its path.
Detected As	Name of any virus or other potentially unwanted software. For more information, click the name to visit the Virus Information Library.
Detected Type	Type of the detected item, such as: ■ Program — a program (application) such as spyware, remote-access software, or *password cracker*. ■ Joke — Joke program. ■ Test — Test virus such as EICAR. ■ Trojan — Trojan-horse program. ■ Virus — Virus, and other types of infection.
User	Name of the user who accessed the file.
Process	Process that accessed the file.
Path	Name of the file, including its full path. In the case of an archive or other file types that act as a container, this can include the name of an item within the archive.

Recently scanned items

This information is continuously updated as files are accessed and scanned. The following information is displayed under **Recently Scanned**.

Table 4-4 Recently scanned items

Time	Time when the scanning occurred.
File Name	Name of the file, excluding its full path.
Detected As	This column appears only if a recently scanned file was infected. Name of any virus or other potentially unwanted software. For more information, click the name to visit the Virus Information Library.
Detected Type	This column appears only if a recently scanned file was infected. Type of the detected item, such as: ■ Program — a program (application) such as spyware, remote-access software, or password 'cracker.' ■ Joke — Joke program. ■ Test — Test virus such as EICAR. ■ Trojan — Trojan-horse program ■ Virus — Virus, and other types of infection.
User	Name of the user who accessed the file.
Process	Process that accessed the file.
Path	Name of the file, including its full path. In the case of an archive or other file types that act as a container, this can include the name of an item within the archive. If the path name is very long, move the horizontal scroll bar to see it all clearly.

Obtaining a diagnostic report

A diagnostic report contains detailed information that is useful to our technical support staff if you need to contact them.

1 In the **Scanning Summary** page, click **Diagnostic Report**.

After a message such as `Loading`, the console displays a list of system events, configuration details, and other information.

2 Using the browser, you can copy the information for later analysis. Typically, you select **Select All** from a right-click menu (or Ctrl-a), copy then paste the text as required.

Detected items

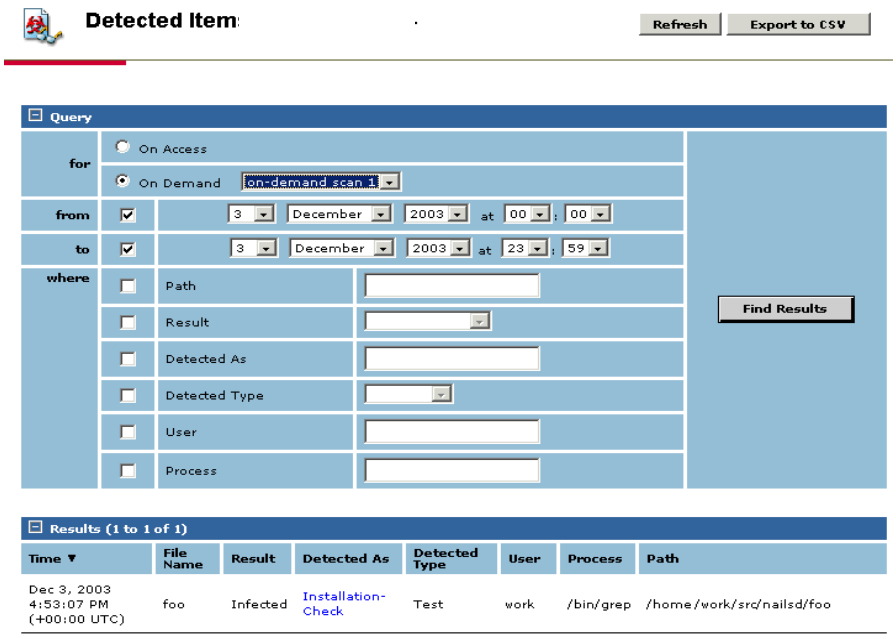
The **Detected Items** page shows a list of items that have been detected as containing a virus or other potentially unwanted software. The range of items that you see can vary because this depends on how you navigated to this page.

For example, if you navigated directly to this page from the left-hand navigation pane or you selected the count of **Detected Items** in the **Scanning Summary** page, you see items detected today by on-access scanning.

If you navigated to this page from a task in the **Scheduled Tasks** page for an on-demand task, then you see items detected during the last run of the task.

To view this page, click **Detected Items** under **View** in the navigation pane. From this page, you can modify the view to show information about items detected by on-access scanning or detected by an on-demand scan.

Figure 4-4 Detected Items page



The **Detected Items** page has two areas — **Query** and **Results**.

Analyzing the detected items

Under **Query**, you can refine the information that is displayed under **Results**.

You can examine entries made between, before or after specified dates and times, and you can filter the information further. For example, you can find all occurrences of a particular virus. This feature is useful if LinuxShield has detected a large number of viruses, and it enables you to analyze trends.

1 To view information about detections during on-access scanning, select **On-Access**, at **for**.

   To view information about detections during an on-demand scan, select **On-Demand**, at **for**. Then, select the name of the on-demand task.

2 To examine information after a specified date, select **from**. To examine information before a specified date, select **to**. Select the date and time.

   To examine information between two dates, select both **from** and **to**, then select the dates and times.

3 Click **Find Results**.

   After a short time, LinuxShield updates the information under **Results**.

Searching for files with known properties

1 At **where**, use the checkboxes on the right to select from items such as **Path** and **User**. For descriptions, see the table in *Recently detected items* on page 32

2 Enter or select the details to match. Enter any path names in the correct case.

3 Click **Find Results**.

   After a short time, LinuxShield updates the information under **Results**.

Viewing the results

The **Results** area of the page, below **Query**, has a table with several rows and columns. The number of rows is typically up to 10. To change the number, see *General settings* on page 54. The area contains the following information:

Table 4-5 Viewing the results

Time	Time when the detection occurred.
File Name	Name of the file, excluding its path.
Result	Result of the scan. This is one of the following: Cleaned, Deleted, Quarantined, or Renamed. Clean Failed, Delete Failed, Quarantine Failed, or Rename Failed. Access denied — no cleaning occurs but LinuxShield denies further access to the file. This option applies to on-access scans only.
Detected As	Name of any virus or other potentially unwanted software. For more information, click its name to view its details in our Virus Information Library.
Detected Type	Type of infection, such as Joke.
User	Name of the user who accessed the file. This field is not available in the results of on-demand scans.
Process	Process that accessed the file. This field is not available in the results of on-demand scans.
Path	Name of the file, including its full path. This field is not available in the results of on-demand scans.

To see more rows of information, use the navigation arrows and numbers below the table, for example: **<< 1 2 3 >>**.See *Navigating through long tables* on page 26.

To refine the information, use the **Query** filter. See *Analyzing the detected items* on page 35.

If the page is showing on-access scanning, or if LinuxShield is still running a scheduled scan, click **Refresh** to see the latest detections.

Exporting the results for analysis

You can save all the information under **Results** as a CSV (Comma-Separated Values) file, then import the information into a spreadsheet program, such as Microsoft Excel or Lotus 123, for further analysis.

1 Click **Export to CSV**.

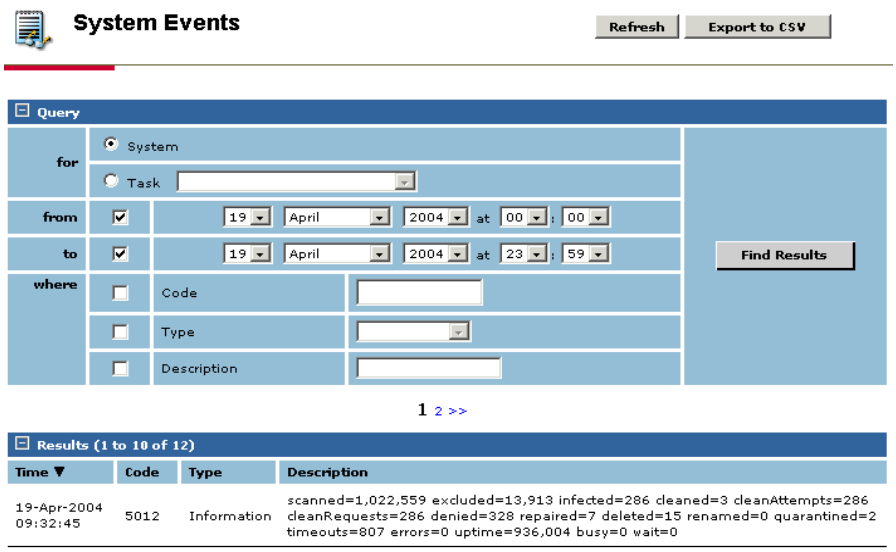
2 In the next dialog box, save the file. The default name is `detitems.csv`.

System events

The **System Events** page shows details of events such as system errors, updates to DAT files, and changes in configuration for the host that you selected from the **Host Summary** page. See *Host Summary* on page 29.

To view this page, click **System Events** under **View** in the navigation pane.

Figure 4-5 System Events page



The page has two areas — **Query** and **Results**.

The table under **Results** has several rows and columns. The number of rows is typically limited to 10. To change the number, see *General settings* on page 54. To see the latest events, click **Refresh**.

The columns contain the following information:

Table 4-6 System Events

Time	Time at which the event occurred. See *Displaying dates and times* on page 28.
Code	Event code (a number relating to the error or information event).
Type	Type of event — Error or Information.
Description	Details of the event or error.

Analyzing the system events

Under **Query** you can refine the information that is displayed under **Results**.

You can examine entries made between, before or after a specified date and time, and you can filter the information further, for example, you can find all occurrences of a particular error code. This feature is useful if LinuxShield has generated a large number of events, and enables you to analyze trends.

1 To examine information after a specified date, select **from**. To examine information before a specified date, select **to**. Select the date and time.

To examine information between two dates, select both **from** and **to**, then select the dates and times.

2 Click **Find Results**.

After a short time, LinuxShield updates information under **Results**.

Searching the information

1 At **where**, use the checkboxes on the right to select the properties — such as **Code**. See also *About code ranges*.

2 Enter or select the details to match.

3 Click **Find Results**.

After a short time, LinuxShield updates the information under **Results**.

About code ranges

LinuxShield uses ranges to categorize events to different parts of the product. For example, all engine-related errors are in the range 3000-3999. See the table *Error code ranges for System Events log* under *Error messages* on page 78.

At **Code**, you can specify a single code or a range of codes, for example:

3000	Only the 3000 code event.
3001	Only the 3001 code event.
3000-	All events above and including code event 3000,
-3000	All events up to and including code 3000.
1000-3000	All events between 1000 and 3000, including 1000 and 3000.

Exporting the results for analysis

You can save information under **Results** as a CSV (Comma-Separated Values) file, then import the information into a spreadsheet program such as Microsoft Excel or Lotus 123, for further analysis.

The **System Events** page shows only a few rows of information, typically 10 at a time. However the export will include *all* the events that match the query specification. The title line of the **Results** table shows the full number, for example: **(101 to 110 of 2359)**.

If the full number of rows is large, the export can take some time, during which the scanning performance is slower, and the host performance might also be affected.

1 Under **Query**, specify the information you want to see, as described in *Analyzing the system events* on page 37, and click **Find Results**.

2 Click **Export to CSV**.

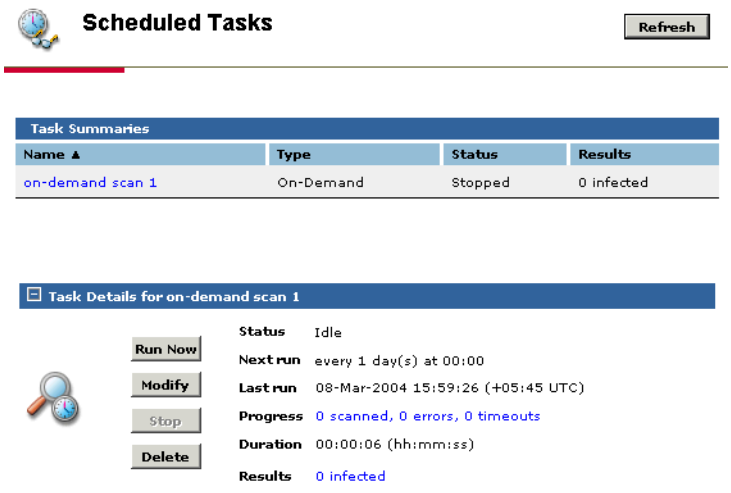
3 In the next dialog box, save the file. The default name is `sysevents.csv`.

Scheduled tasks

LinuxShield uses scheduled tasks to enable you to update the scanning engine and virus definition (DAT) files, or to run on-demand scans on your Linux host. You can choose these tasks to run immediately, to run once, or to run at regular times. To schedule a new task, see *Setting Up Schedules* on page 43.

The **Scheduled Tasks** page shows all tasks that you have scheduled under **Task Summaries**. To view this page, click **Scheduled Tasks** under **View** in the navigation pane.

Figure 4-6 Scheduled Tasks page



The page has two areas — **Task Summaries** and **Task Details**.

Task Summaries has the following information:

Table 4-7 Task Summaries

Name	Name of the task. To see the details for any task, click its name
Type	Type of task — Update or On-Demand scan.
Status	Status of the task, such as Idle, Completed, In Progress or Failed.
Results	Result of each task.

To see any more rows of information, use the navigation arrows and numbers, below the table. See *Navigating through long tables* on page 26.

To see extra information about any task, click its name under **Task Summaries**. The following information then appears under **Task Details**.

Table 4-8 Task Details

Status	Status of the task — Idle (not started), Completed, Failed, In Progress, or Stopped (by the user). (Stopping might appear briefly before Stopped.)
Next run	Scheduling information for the task. This applies to regular tasks only.
Last run	Date and time when the task was last run.

Table 4-8 Task Details (continued)

Progress	Progress of the task. During an on-demand scan, this field shows the number of files that have been scanned, and other information such as the number of files that were excluded from scanning. During an update, this field shows text messages about each stage. You can click any blue link here to see messages about this task in the **System Events** page.
Duration	The time taken for the last task, or the elapsed time on the current task.
Results	For an on-demand scan, a completed scan shows as the number of detected items. For more information, click the number to open the **Detected Items** page. If an update has completed, click here to open the **System Events** page and find more information. If a failure occurred, click here to open the **System Events** page and find the reason.

The buttons under **Task Details** enable you to run, stop, modify, or delete the task, as appropriate. To see the latest status of the tasks, click **Refresh**.

Running a task immediately

1 Under **Task Summaries**, click the task name to display its details under **Task Details**.

2 Under **Task Details**, click **Run Now**.

The task runs immediately. The results appear at **Results** under **Task Details**.

Modifying an existing scheduled task

If you no longer need a task but you want to set up a similar task, you can modify the existing task.

1 Under **Task Summaries**, select the existing task.

2 Under **Task Details**, click **Modify**.

3 Follow the procedures given in either:

- *Creating a schedule to update the product* on page 45.
- *Creating a schedule to run an on-demand scan* on page 48.

Deleting an existing scheduled task

If you no longer need a scheduled task, you can delete it.

1 Under **Task Summaries**, select the task name.

2 Under **Task Details**, click **Delete**.

Stopping a task

To stop a task that is already running:

1 Under **Task Summaries**, select the task name.

2 Under **Task Details**, click **Stop**.

The task status changes to **Stopping**, and later to **Stopped**. This can take a few seconds, and you will need to click **Refresh** to see the change of status.

In rare cases, **Task Details** can show the incorrect status. This can happen if a task is halted without its recorded status being updated, for example if a host is restarted while an on-demand scan is running.

To correct the status:

1 Click **Stop**. This will set the status to **Stopping**.

2 Click **Stop** again. This will set the status to **Stopped**.

You may now run or delete the task.

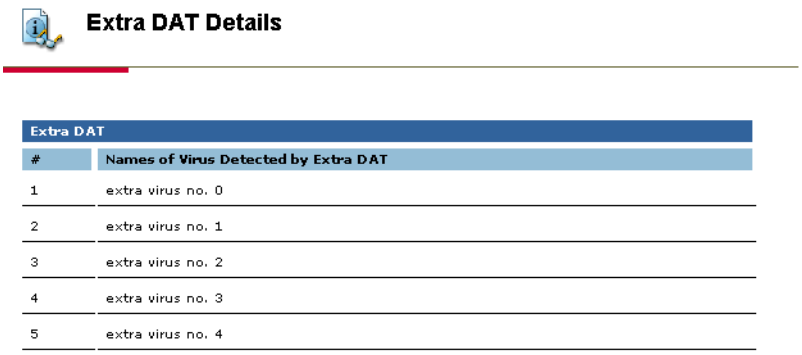
Information about extra DAT files

An extra.dat is a supplemental virus definition file that we occasionally create in response to an outbreak of some potentially unwanted software such as a new virus or a new variant of an existing virus.

The **Extra DAT** page shows information about any extra.dat file that is in use on the selected host. The information includes the names of viruses and other potentially unwanted software that the extra.dat file can detect.

To view this page, click on the text — for example **Yes(5)** — under the **Extra DAT** column on the **Host Summary** page. If the column contains **No**, no extra.dat file is available for the host, and LinuxShield does not display the page.

Figure 4-7 Extra DAT page



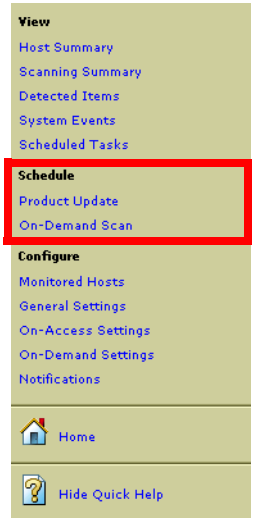
For information about any virus in the list, click on its name, to link to our Virus Information Library.

5 Setting Up Schedules

From the **Schedule** area of the navigation pane, you can protect your Linux hosts, by running the following tasks on a regular basis:

- Update the product. At least once per day, you must update virus definition (DAT) files to ensure that LinuxShield can recognize new viruses and other potentially unwanted software. See *Updating the product* on page 44.
- Run an on-demand scan. LinuxShield normally examines files as they are accessed, but for full security, scan other files occasionally. See *Running on-demand scans* on page 47.

Figure 5-1 Schedule menu



Product updating and on-demand scans are likely to be needed on a regular basis. LinuxShield enables you to create multiple schedules, for running these tasks at predetermined intervals.

You can also use the schedule options to create an immediate scan or update. These can be created in response to a suspected virus attack, where you want to use the latest available DAT files to counter any new viruses, then run the anti-virus software to ensure that your hosts are free from the new viruses.

You can also run these tasks from a command line. This can be useful at times when you do not want to use the browser interface, such as within a script.

Understanding time differences

It is important to understand how to set up times for scans and updates. Suppose you are in Los Angeles, using a browser to control a host that is running LinuxShield in New York. When you schedule the time and date, it will be the *local time* in New York. The time difference between these two locations is typically three hours. Therefore if you set an on-demand scan to run at midnight, the scan will run at midnight in New York, and you will see the results of the scan from 9 p.m. in Los Angeles.

Using a wizard

Each type of scheduling works in a similar way, using a wizard-like process to make the task easier. See *Using wizards* on page 27. The process leads you through a few pages where you enter the following information:

- When the scan or update will take place.
- How, where or what to scan or update.
- The name of the task.

Updating the product

The LinuxShield software depends on information in the virus definition (DAT) files to identify viruses. Without updated information on the latest virus threats, no anti-virus software can detect new virus strains or respond to them effectively. Software that is not using current DAT files can compromise your virus-protection program.

Hundreds of new viruses appear every month. To meet this challenge, we release new DAT files every day, incorporating the results of our ongoing research into the characteristics of new viruses and their variants. The update task that is provided with the LinuxShield software makes it easy to take advantage of this service.

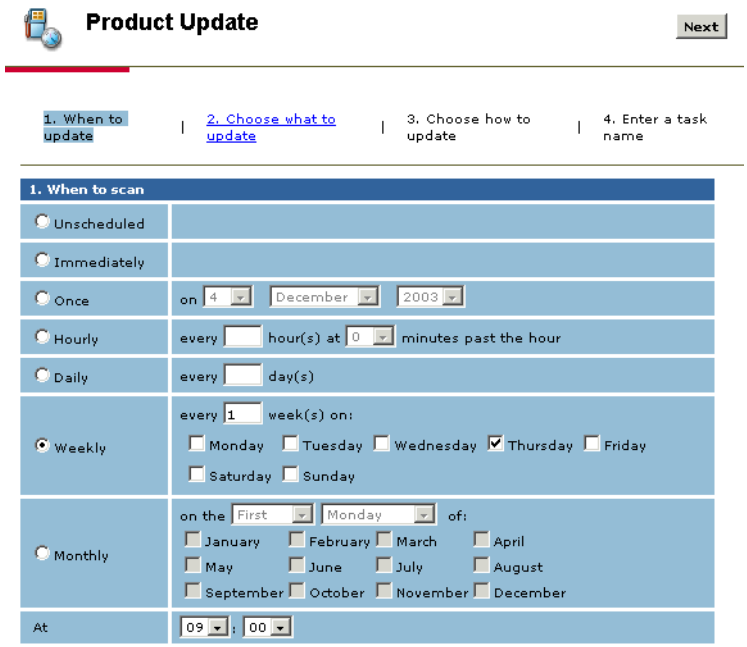
This feature allows you to download the latest DAT files or a new scanning engine, using an immediate update or a scheduled update.

You can also create an *unscheduled update*. Here, you provide information about an update but do not attach a schedule to it. You can then run the update at any time, or run it from a command line.

Within your network, you need at least one computer that can download the files from our FTP site. See details of the download site in *Contact information* on page 14. The LinuxShield software can then access the FTP site directly or via a proxy host, or it can copy files from that computer.

To use this feature, click **Product Update** under **Schedule** in the navigation pane.

Figure 5-2 Product Update page



Creating a schedule to update the product

To create a schedule to update the virus definition files or the scanning engine:

1 **Choose when to update**.

a Select how frequently you want the update to occur.

b If you select any option other than **Immediately** or **Unscheduled**, enter further details for the date, day, month and time (as appropriate) for the update to run. See *Understanding time differences* on page 44.

c Click **Next**.

2 **Choose what to update**.

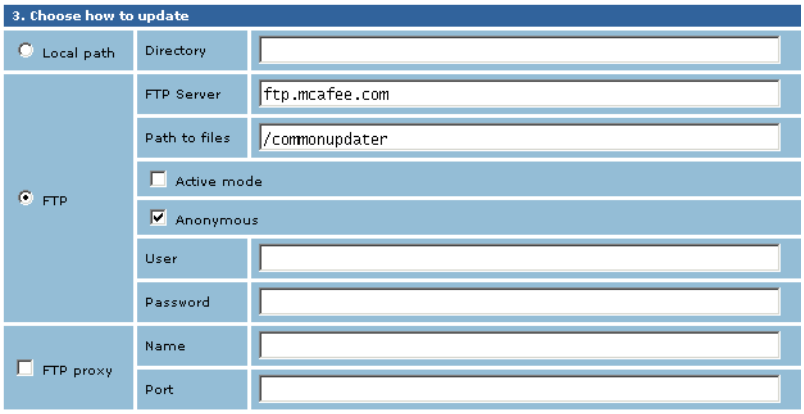
a Select what you want the update — DAT files or scanning engine.

b Click **Next**.

3 Choose how to update.

You can get the new files either directly from our FTP site, or indirectly from a local path where the files have been downloaded earlier.

Figure 5-3 Choosing how to update



a Select **Local path** or **FTP**.

For **FTP**, choose the connection mode by selecting or deselecting **Active mode**:

Active-mode FTP connections are sometimes referred to as *client-managed* because the client sends a `PORT` command to the server over the control connection. The server then establishes a data connection using the port specified by the client.

Passive-mode FTP connections are sometimes referred to as *server-managed* because after the client issues a `PASV`, `EPSV` or `LPSV` command, and the server responds with one of its transient ports used as the server-side port of the data connection. The client establishes a data connection to the server.

b For **FTP**, choose the user. To change the default, deselect **Anonymous**, and specify the user name and password for authentication.

c If required, type the details for an FTP proxy.

d Click **Next**.

4 Enter a task name.

a Enter a unique name for the update.

This will help you to locate the task later in the list of scheduled tasks.

b Click **Finish**.

LinuxShield displays the **Scheduled Tasks** page (see *Scheduled tasks* on page 39), and the update runs at the times you defined in the schedule.

Running on-demand scans

LinuxShield scans files as they are written to or read from disk. During these scans, LinuxShield uses the installed virus definition (DAT) files to check for any viruses or potentially unwanted software within the files.

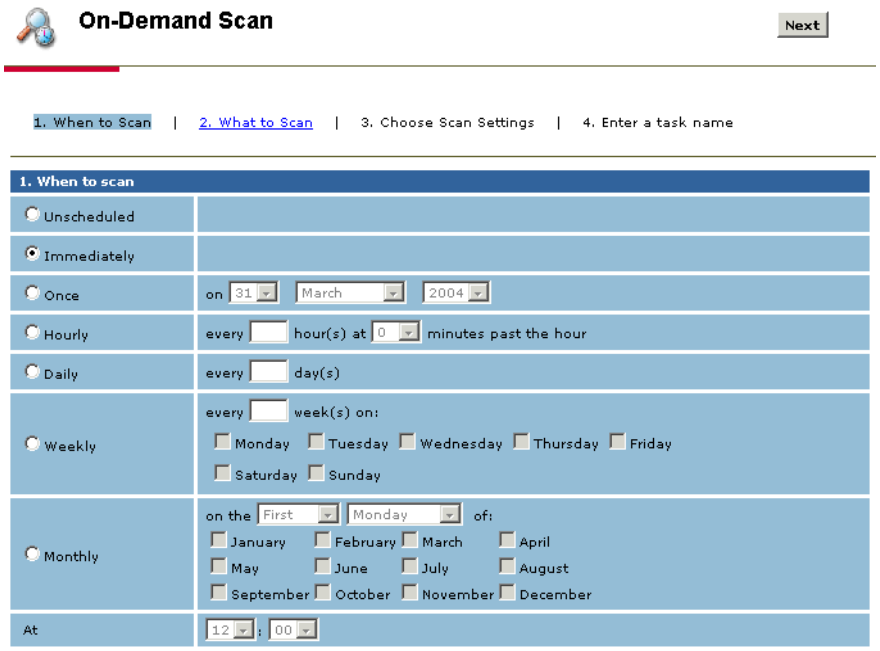
On-demand scanning provides a method for scanning all parts of your host at convenient times or at regular intervals. Use it to supplement the continuous protection that the on-access scanner offers, or to schedule regular scan operations when they will not interfere with your work.

You can perform a one-time on-demand scan when you want to scan a file or location that you believe is vulnerable or you suspect of containing a virus infection, or you can perform scheduled scanning activities at convenient times or at regular intervals.

You can also create an *unscheduled scan*. Here, you provide information about a scan but do not attach a schedule to it. You can then choose to run the scan at any time, or run it from a command line.

To use this feature, click **On-Demand Scan** under **Schedule** in the navigation pane.

Figure 5-4 On-Demand Scan page



Creating a schedule to run an on-demand scan

To create a schedule to run an on-demand scan:

1 **Choose when to scan**.

a Select how frequently you want the scan to run.

b If you select any option other than **Immediately** or **Unscheduled**, enter any further details for the date, day, month and time for the scan to run. See *Understanding time differences* on page 44.

c Click **Next**.

2 **Choose what to scan**.

Here, you can build a list of directories to scan.

a Under **Path**, type the name of a directory. Enter any path names in the correct case, and that the directory already exists.

b To scan its subdirectories, select **Scan Sub-Directories**.

c Click **Add**.

d Add any more directory names. To remove any directory name, click **Remove**.

e Click **Next**.

3 **Choose scan settings**.

Select the settings. They are organized into these main areas:

- *Scanning options* on page 58.
- *Paths excluded from scanning* on page 59.
- *Extension-based scanning* on page 60.
- *Anti-virus actions* on page 62.

4 **Enter a task name**.

a Enter a unique name for the on-demand scan.

This enables you to locate the task later in the list of scheduled tasks.

b Click **Finish**.

LinuxShield displays the **Scheduled Tasks** page (see page 39), and the scan runs at the times you defined in the schedule.

Running a task from the command line

You can run tasks from a command line. This can be useful at times when you do not want to use the browser interface, such as within a script. The task must already be set up from the **Product Update** page or the **On-Demand Scan** page.

Furthermore, you can define some tasks specifically to be run from a command line. Select **Unscheduled** from the **Product Update** page or the **On-Demand Scan** page and add the details as usual.

1 At the command line, type:

```
/opt/NAI/LinuxShield/bin/nails task --list
```

This provides the task number.

2 At the command line, type:

```
/opt/NAI/LinuxShield/bin/nails task --run task-number
```

The task runs immediately using the details previously entered at the **Product Update** page or the **On-Demand Scan** page.

Example

To run a task called **Daily scan** that you created earlier:

1 Find the number for the task by typing:

```
/opt/NAI/LinuxShield/bin/nails task --list
```

The output is:

```
LinuxShield configured tasks:
1  "Weekly scan”  (Stopped)
2  "Daily scan"   (Idle)
3  "Friday scan"   (Idle)
```

From the output, you can see that the task number is 2.

2 Run the task by typing:

```
/opt/NAI/LinuxShield/bin/nails task --run 2
```

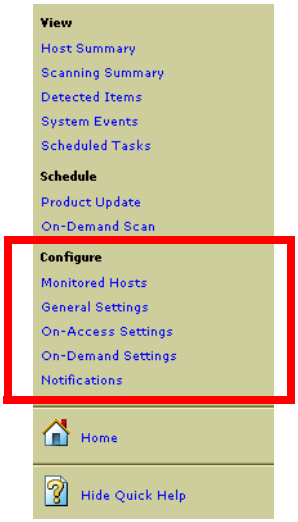
6 Configuring LinuxShield

When you first use LinuxShield, it provides optimum protection against viruses and other potentially unwanted software. However, you can modify these settings to suit your own computing environment.

From the **Configure** area of the navigation pane, you can configure the following areas within the LinuxShield software:

- Manage a list of hosts to monitor for attacks from viruses and other potentially unwanted software. See *Monitored hosts* on page 52.
- Configure some general settings. See *General settings* on page 54.
- Reset all the configuration settings to those at installation time. See *General settings* on page 54.
- Specify settings for on-access scanning. See *On-access settings* on page 57.
- Specify default settings for new on-demand tasks. See *On-demand settings* on page 63.
- Determine how to issue notifications of virus attacks and other events. See *Notifications* on page 64.

Figure 6-1 Configure menu



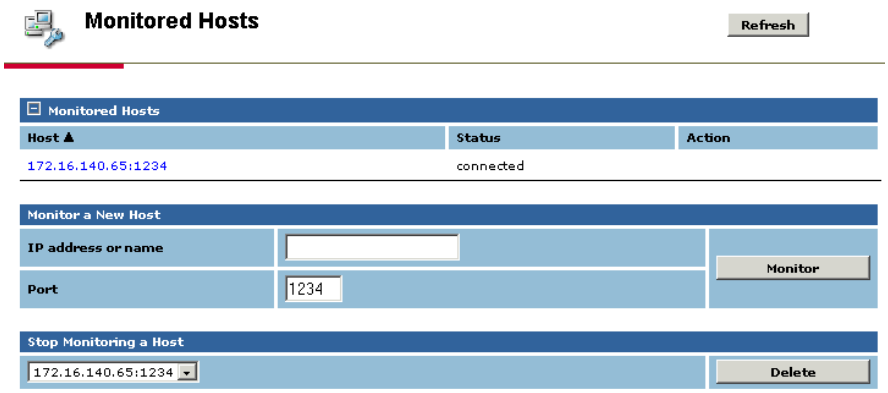
Monitored hosts

The **Monitored Hosts** page shows the list of hosts that are running LinuxShield. You can add Linux hosts to the list, in order to monitor them for virus activity. You can view up to 20 hosts in this list. Performance can suffer if you try to monitor a large number of hosts. For such purposes, we recommend using ePolicy Orchestrator. See the *Configuration Guide*.

LinuxShield software must already be installed on each host. In order that you can administer the other hosts, each host must have the same user name and password for accessing LinuxShield. If this is not the case, you can only view the scanning statistics.

To view this page, click **Monitored Hosts** under **Configure** in the navigation pane.

Figure 6-2 Monitored Hosts page



Under **Monitored Hosts**, you can see the following information:

Table 6-1 information about Monitored Hosts

Host	An IP address or the host name for a Linux host that is running LinuxShield, and a port number. To see more information about any host, click its name in the **Host** column to open its **Scanning Summary** page. See *Scanning Summary* on page 31. You can also sort the names in this column. See *Sorting by table columns* on page 26.
Status	The status is one of the following: active — Host is connected. connecting — This status message appears only briefly. disconnected — Host is disconnected. To reconnect, see *Reconnecting a host* on page 53.
Action	If any host becomes disconnected, this column contains a **Reconnect** button.

Adding a new host

To add a host to the list:

1 Under **Monitor a New Host**, enter the IP address or name of a host that is running LinuxShield, for example: `192.168.225.200` or `host1`.

2 Enter the port number, for example: `55443`.

By default, standard port for LinuxShield is 55443. You can change this default value by editing the configuration file.See page 69.

3 Click **Monitor**.

The host appears in the list of **Monitored Hosts**, and connection is attempted. You might briefly see the text, **connecting** in the **Status** column.

4 To see any change of status on this page, click **Refresh**.

You might see an error message if the host is not currently available, or if LinuxShield is not installed on the host, or if some other problem occurs.

Stopping the monitoring of a host

To stop monitoring a host:

1 Under **Stop Monitoring a Host**, select the host.

2 Click **Delete**.

The host name is removed from the list under **Monitored Hosts.**

Reconnecting a host

If a remote host is being monitored but LinuxShield stops running on that host or the network connection is lost, the status of the host is displayed as *disconnected*.

To reconnect a previously connected host, click **Reconnect** (in the same row).

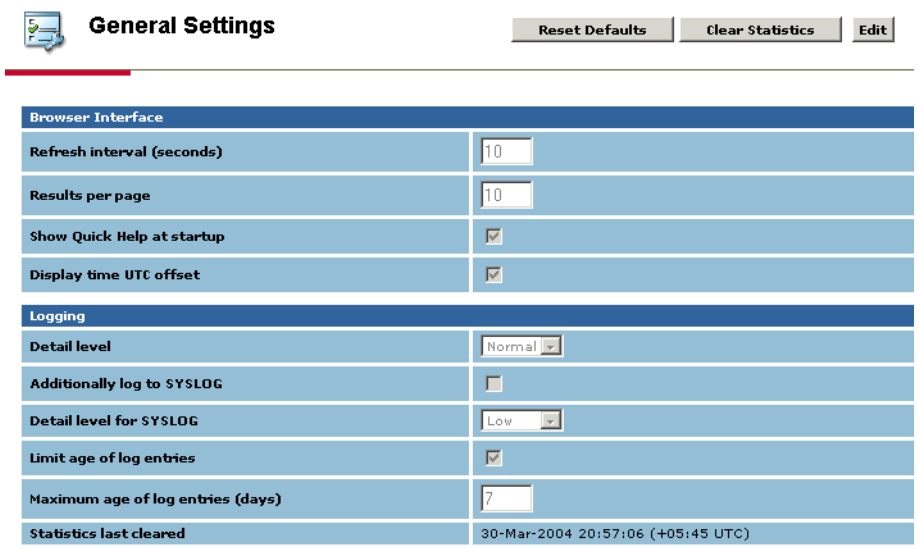
General settings

From the **General Settings** page, you can change the appearance of pages in the browser interface, the behavior of logging, and the collection of statistics.

To view this page, click **General Settings** under **Configure** in the navigation pane.

To make any changes to the settings, click **Edit**. To apply the new settings, click **Apply**. See *Changing the settings on a page* on page 27 for more information.

Figure 6-3 General Settings page



The page has two main areas. See:

- *Browser interface* on page 55.
- *Logging* on page 55.

This page also has two important buttons. See:

- *Clearing statistics* on page 56.
- *Resetting configuration settings* on page 56.

Browser interface

Under **Browser interface**, you can view and change settings such as the refresh interval. The next table explains the information in each column.

Table 6-2 Browser interface

Refresh interval (seconds)	The browser automatically updates the contents of pages such as the **Scanning Summary** page. By default, the page is refreshed every 10 seconds, but you can adjust the interval between 5 and 600 seconds.
Results per page	Number of rows of information shown in certain pages under **Results**, namely in the **Detected Items**, **Scheduled Tasks**, and **System Events** pages. By default, 10 rows are displayed at a time, but you can adjust the number between 1 and 50 rows.
Display time UTC offset	Wherever time values are displayed — as in scheduled tasks and detections — an offset value is displayed in UTC form to help you understand any time-zone differences.
Hide quick help on startup	Quick Help pane is not displayed when logging in to the browser interface.

Logging

Under **Logging**, you can view and change settings such as the level of detail that you require. The next table explains the information in each column.

Table 6-3 Logging

Detail level	Level of logging information that LinuxShield records in its database. A high level can affect performance and the size the database. By default, the level is Normal. Options are Low, Normal, and High.
Additionally log to SYSLOG	Indicates if information logged to the LinuxShield database is also logged to SYSLOG. By default, this is not required.
Detail level for SYSLOG	(This field is only available if **Additionally log to SYSLOG** is selected.) Level of detail of the information to be logged to SYSLOG. disabled if logging to SYSLOG is checked. By default, the level is Low. Options are Low, Normal, and High.
Limit age of log entries	Indicates if information in the log will be automatically removed later, based on the age of the log entries.
Maximum age of log entries	(This field is only available if **Limit age of log entries** is selected.) Limits to the age of entries in the LinuxShield database to the specified days. After the specified number of days, old entries are automatically removed. This helps to limit the size of the database. Maximum age of log entries (days) - By default, the limit is 28 days, but you can adjust the limit between 1 and 999 days.
Statistics last cleared	Indicates when statistics were removed by clicking **Clear statistics**.

Clearing statistics

To clear all the statistics, click **Clear statistics**. The values of **Files scanned** and **Detected items** in the **Scanning Summary** page are reset to zero, and current information in the **Recently scanned** and **Recently detected** areas is cleared.

Resetting configuration settings

To reset all the configuration settings to those at installation time, click **Reset Defaults**. The settings include:

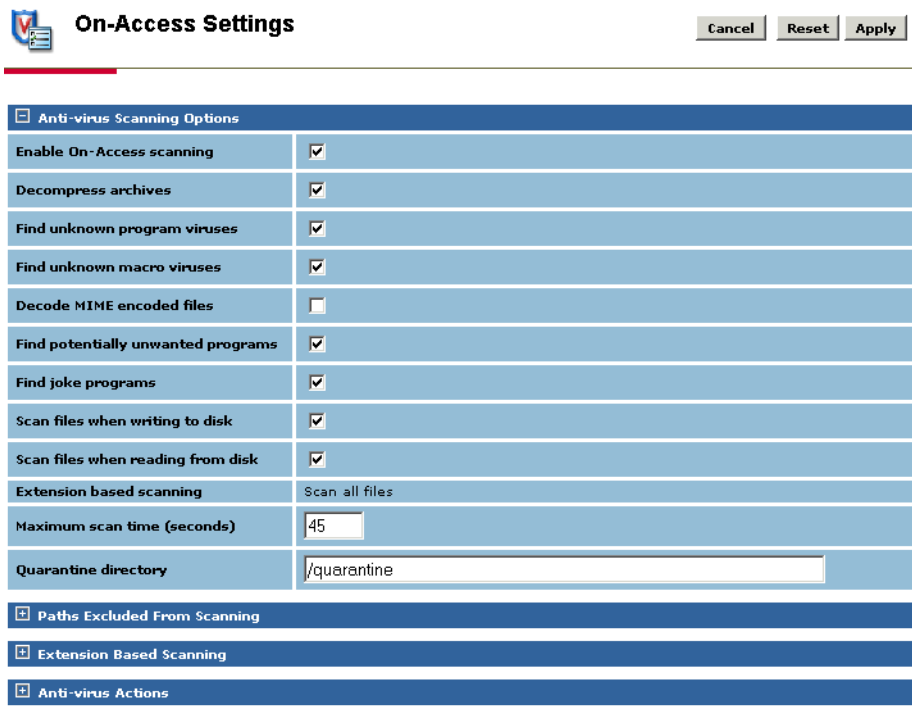
- On-access settings. (See *On-access settings* on page 57.)
- On-demand defaults. (See *On-demand settings* on page 63.)
- Notification settings. (See *Notifications* on page 64.)
- Settings for the browser interface and logging. (See *General settings* on page 54.)

On-access settings

The **On-Access Settings** page shows how LinuxShield will respond when a virus or other potentially unwanted software is detected whenever files are accessed. The available settings for on-access scanning and on-demand scanning are similar. To view this page, click **On-Access Settings** under **Configure** in the navigation pane.

To make any changes to the settings, click **Edit**. To apply the new settings, click **Apply**. See *Changing the settings on a page* on page 27 for more information.

Figure 6-4 On-Access Settings page



The **On-Access Settings** page has these main areas:

- *Scanning options* on page 58.
- *Paths excluded from scanning* on page 59.
- *Extension-based scanning* on page 60.
- *Anti-virus actions* on page 62.

Scanning options

The scanning options determine which types of file LinuxShield will scan. By default, all these scanning options are available, unless stated. The next table explains the options.

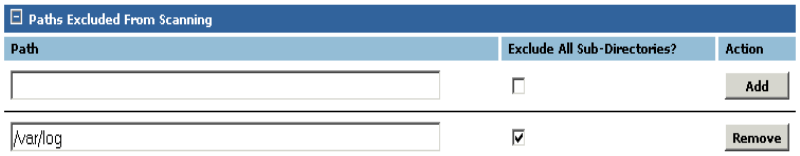
Table 6-4 Scanning options

Enable On-Access Scanning	This item appears for on-access scanning only.
Decompress archives	LinuxShield scans inside file archives such as `.tar` or `.tgz` files. The decompression can slow performance; any virus-infected file inside an archive cannot become active until it has been extracted.
Find unknown program viruses	LinuxShield uses heuristic analysis to identify potential new file viruses.
Find unknown macro viruses	LinuxShield uses heuristic analysis to identify any potential new macro viruses in files created by Microsoft Office products.
Decode MIME encoded files	Email messages are typically encoded in MIME format. Use of this option can affect performance. If your network has other anti-virus software for handling email, you might not require this option.
Find potentially unwanted programs	These programs might be dangerous but they are not viruses. They include programs such as spyware, remote-access utilities, and password crackers.
Find joke programs	Joke programs are not harmful. They play tricks such as displaying a hoax message. This feature only becomes available if you have selected **Find potentially unwanted programs.**
Scan files when writing to disk	Scan the contents of each file when it is closed.
Scan files when reading from disk	Scan the contents of each file when it is opened.
Extension-based Scanning	Indicates how LinuxShield will handle files that have extension names (for example, `.txt` and `.exe`). By default, LinuxShield scans all files regardless of the file name extension. See *Extension-based scanning* on page 60.
Maximum scan time (seconds)	Number of seconds after which scanning will stop. This feature prevents large files reducing overall performance, and protects against corrupted files and denial-of-service attacks. By default, this is 45 seconds but may be between 1 and 9999 seconds. On computers with low-specification hardware, LinuxShield might abandon scanning of some large files because of the length of time taken. In such cases, we recommend that you increase this number.
Quarantine directory	Directory for holding quarantined files. Do not use a symbolic link to refer to this directory. By default, this is called `/quarantine`, and should be on a local file system.

Paths excluded from scanning

This area of the page allows you to exclude some files from scanning.

Figure 6-5 Paths excluded from scanning



Some directories (or *paths*) might not require scanning, or you might prefer not to scan them frequently. For example:

- Directories that contain only plain text files or other file types that are not prone to infection.
- Directories that contain executable files that have file permissions that prevent them being modified.
- Directories that contain large archive files and compressed files.
- Directories that contain files already known to be infected (*quarantined*).

To exclude a directory (or *path*):

1 Click **Edit**.

2 Under **Paths excluded from Scanning**, enter the path name, for example:

`/directory1` or `/directory1/subdirectory2`

Enter path names in the correct case. Do not use symbolic links. For bind mounts (which appear in more than one place in the directory), add each path that you want to exclude.

You can use *wildcard* characters to represent missing characters within a directory name or a file name:

- ? represents any single character.
  For example, *d??* will match *day*, *dot*, and *dir*.
- * represents any number of characters including none at all.
  For example, *d*y* will match *day*, *diary*, and *directory*.

3 To exclude the subdirectories from scanning, select the checkbox in the **Exclude All Sub-Directories** column of that row.

4 Click **Add** in that row.

An extra row is added to the table. To remove any exclusion, click **Remove** in its row.

Extension-based scanning

This table only becomes visible when you click **Edit**. However, you can see the chosen setting at **Extension based scanning** in the first table.

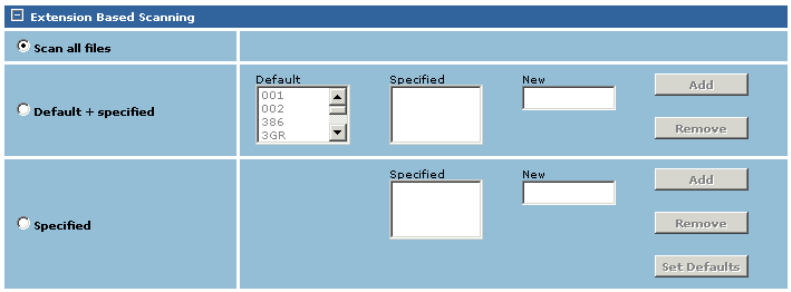
LinuxShield normally scans all files regardless of the file name extension. The virus definition files include a comprehensive list of file name extensions that are susceptible to attack. The list includes popular extensions such as `.doc` and `.exe`, and it is referred to here as the *default list*. The extension name is not case-sensitive.

If LinuxShield is running on a Samba file server that is accessed by Microsoft Windows users, it might be useful to specify the types of files to scan according to their file name extension. However, we recommend that all files are scanned where possible.

You can specify extension names that you want LinuxShield to scan, or you can specify extension names for LinuxShield to scan at the same time as it scans those in the default list. You cannot remove any extension names from the default list, although you can build your own list of extension names based on those in the current default list.

This area of the page allows you to limit scanning to certain types of file.

Figure 6-6 Extension-based scanning



The choices available in this area are as follows:

- *Scanning all files*.
- *Scanning default files and specific files* on page 61.
- *Scanning specific files* on page 61.

Scanning all files

To scan all files regardless of file name extension:

Under **Extension based scanning**, select **Scan all files**.

This is the default setting.

Scanning default files and specific files

To scan the default files and specific files:

1 Under **Extension based scanning**, select **Default + Specified**.

2 At **New**, type the file name extension, for example `AAA` or `aaa`.

3 Click **Add** to move the name to the **Specified** list.

To remove names from the **Specified** list, select each name, then click **Remove**:

- To select one name, just click the name.
- To select a range of names, click the first, then use Shift-Click to select the last.
- To select several names, use Ctrl-Click.

If a new file name extension is included in later virus definition files, files with that file name extension will also be scanned.

Scanning specific files

To scan specific files:

1 Under **Extension based scanning**, select **Specified**.

2 At **New**, type the file name extension, for example `AAA` or `aaa`.

3 Click **Add** to move the name to the **Specified** list.

4 To build a list quickly, click **Set Defaults** to copy all names from the virus definition files into the **Specified** list. You can then modify the **Specified** list.

The file name extensions in the **Specified** list do not change automatically. Therefore, if a new file name extension is included in later virus definition files, files with that file name extension will *not* be scanned.

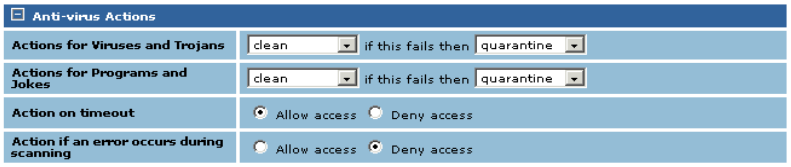
To remove names from the **Specified** list, select each name, then click **Remove**:

- To select one name, just click the name.
- To select a range of names, click the first, then use Shift-Click to select the last.
- To select several names, use Ctrl-Click.

Anti-virus actions

You can configure LinuxShield to take a variety of actions when it detects a virus or other potentially unwanted software. This area of the page allows you to choose the actions.

Figure 6-7 Anti-virus actions



The actions are:

- **clean** — Cleans the infected file by removing the virus code. LinuxShield cannot repair any damage that has occurred to the file. For example, some viruses can modify or erase data in spreadsheets.
- **continue** — Reports the detection and continues scanning. This action is only available for on-demand scanning.
- **delete** — Deletes the infected file.
- **deny access** — Prevents further access to the infected file. This action is only available for on-access scanning.
- **quarantine** — Moves the infected file to the area specified in **Quarantine directory**. To prevent the spread of infected files, LinuxShield will not move a file from a remote file system into this area.
- **rename** — Renames the extension of the infected file, to prevents its accidental use. Renaming is useful in cases where the file extension (such as `.exe` or `.txt`) determines the application that will open the file.

The next table explains the information in each column.

Table 6-5 Anti-virus actions

Action for viruses and Trojan horses	Actions to take when a virus or Trojan-horse program is detected. Your second choice of action is limited by your first choice. You cannot choose both actions to be the same.
Action for applications and joke programs	Actions to take when a potentially unwanted application or joke program is detected. Your second choice of action is limited by your first choice. You cannot choose both actions to be the same.
Action on time out	Action to take when the scanning takes too long to complete. You can choose to allow or deny access to the suspect file.
Action if an error occurs during scanning	Action to take if a fault occurs such as an internal fault in LinuxShield or the scanning engine, or a failure to complete the second choice of action. You can choose to allow or deny access to the suspect file.
Quarantine directory	Name of the quarantine file, as set up at installation time.

If any action fails to work, LinuxShield uses any secondary action. If that action fails, LinuxShield uses its *fallback* action. For on-access scanning, LinuxShield blocks access to the infected file. For on-demand scanning, LinuxShield reports that the file is infected.

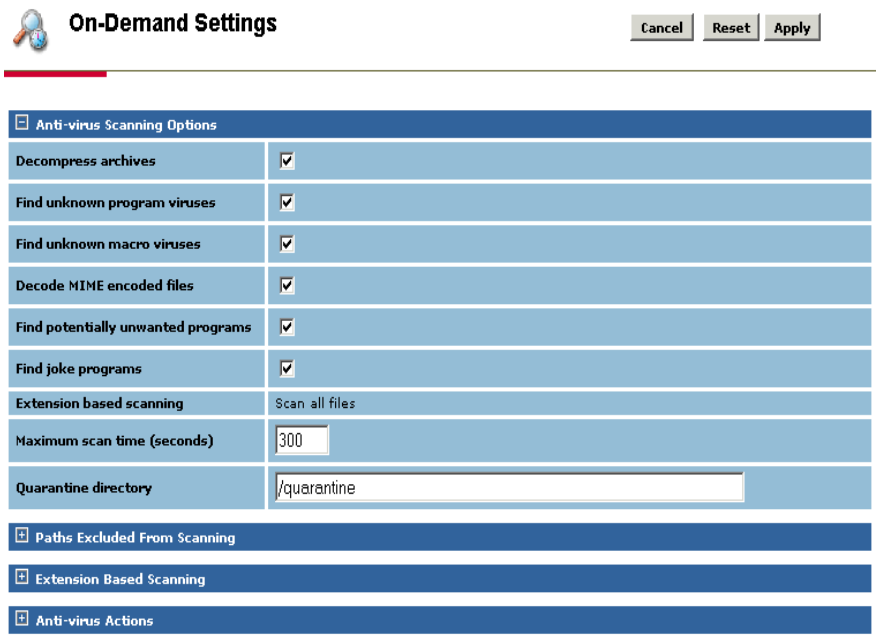
On-demand settings

The **On-Demand Settings** page shows how LinuxShield will respond when a virus or other potentially unwanted software is detected during an on-demand scan. See *Running on-demand scans* on page 47. Settings for on-access scans and on-demand scans are similar.

This page shows the default settings that will be applied to all new tasks. Any on-demand scanning tasks that you previously configured retain their own settings. To change any settings in an existing task, see *Modifying an existing scheduled task* on page 40.

To view this page, click **On-Demand Settings** under **Configure** in the navigation pane. To change any settings, click **Edit**. To apply the new settings, click **Apply**.See *Changing the settings on a page* on page 27 for more information.

Figure 6-8 On-Demand Settings page



The page has these main areas:

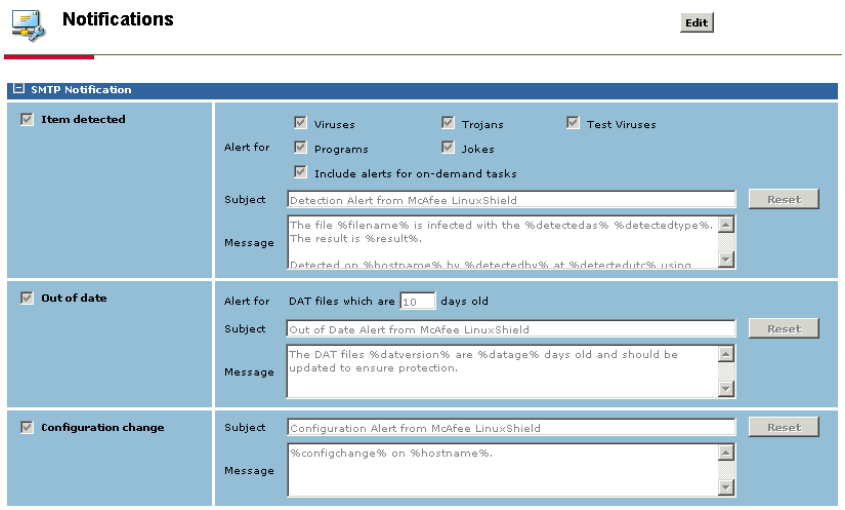
- *Scanning options* on page 58.
- *Paths excluded from scanning* on page 59.
- *Extension-based scanning* on page 60.
- *Anti-virus actions* on page 62.

Notifications

From the **Notifications** page, you can specify who will receive email notification of events such as virus detection and changes to the scanning options. LinuxShield sends the email messages using the SMTP email protocol.

To view this page, click **Notifications** under **Configure** in the navigation pane. To change any settings, click **Edit**. To apply the new settings, click **Apply**.See *Changing the settings on a page* on page 27 for more information.

Figure 6-9 Notifications page



The page has these main areas:

- *SMTP notifications*.
- *SMTP settings* on page 65.

SMTP notifications

From this area, you can define which events will be notified. The next table explains the available settings.

Table 6-6 SMTP notifications

Item detected	Details of a detection of a virus or other potentially unwanted software. Here, for example, you can decide whether to issue a notification if any joke programs are detected.
Out of date	Details of out-of-date DAT files. Here, for example, you can decide whether to notify if DAT files are more than 10 days old.
Configuration change	Details of changes to the settings for on-access scanning, notifications and general settings. Changes to the settings for on-demand scans are not notified. Here, for example, you can decide whether to notify if changes are made to the settings for on-access scanning.
System events	Details of any important events. Here, for example, you can specify the range of system events or event types to be forwarded by SMTP.

To enable any notification feature, select its checkbox in the left column under **SMTP Notification**.

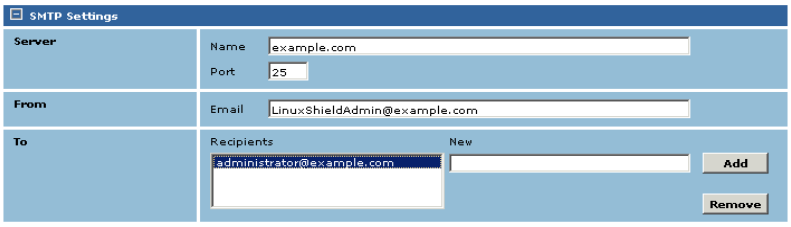
For each type of notification, LinuxShield provides a default subject and a message. You can change these messages to suit your organization. Messages can include substitution variables, such as **%hostname%** to indicate the host name. To include variables in any message, see *Substituting variables in notification templates* on page 67.

To restore the default message, click **Reset**.

SMTP settings

From this area, you can define who LinuxShield will notify about the events specified in *SMTP notifications*.

Figure 6-10 SMTP Settings



The next table explains the available settings.

Table 6-7 SMTP Settings

Server	Name and port of the server that sends the email message, This is set up at installation time.
From	Name of the sender. By default, this is the address that was given during installation.
To	Names of the recipient, for example: `user1@example.com`.

To add to the list of recipients:

1 At **To**, type the email address in **New**, for example: `user1@example.com`.

2 Click **Add** to move the name to the **Recipient** list.

To remove names from the **Recipient** list, select each name, then click **Remove**:

- To select one name, just click the name.
- To select a range of names, click the first, then use Shift-Click to select the last.
- To select several names, use Ctrl-Click.

Enhancing this feature

LinuxShield sends all messages to the same recipients. However if your email software includes some advanced features, you can enhance this feature. For example, you can send all messages about detections to one person, and all messages about out-of-date products to another person. See the following examples.

Example with Microsoft Outlook

1 Give each type of notification a different subject line:

Item detected	LinuxShield detection
Out of date	LinuxShield update is needed

2 Create a rule that checks for the specific words, **LinuxShield detection** in the subject line and forwards the message to the required person.

3 Create a rule that checks for the specific words, **LinuxShield update is needed** in the subject line and forwards the message to another person.

Example with procmail

Add the following recipe lines to the file .procmailrc:

```
:0:
  * ^Subject: LinuxShield detection
  |linuxshield-admin@example.com

:0:
  * ^Subject: LinuxShield update is needed
  |linuxshield-otheradmin@example.com
```

For more information, visit the web site, http://www.procmail.org.

7 Advanced Features

This section describes some advanced features of LinuxShield:

- *Substituting variables in notification templates*.
- *Configuring features from a file* on page 69.
- *Controlling LinuxShield from the command line* on page 70.
- *How the quarantine action works* on page 72.

Substituting variables in notification templates

The notification messages described in *Notifications* on page 64 can use variables that LinuxShield substitutes when sending a message. For example, the template message:

File, %filename% is infected on %hostname%.

becomes:

File, example.exe is infected on computer1.

The following table lists all the available variables. Some variables are valid only in particular instances.

Table 7-1 Substitution variables

Valid for ...	Variable	Equivalent field in the interface	Description
All alerts	%hostname%	<none>	Name of the host on which LinuxShield is installed.
All alerts	%hostip%	<none>	IP address of host on which LinuxShield is installed.
All alerts	%productversion%	Host Summary page — Product Version	Version of the product.

Table 7-1 Substitution variables (continued)

Valid for ...	Variable	Equivalent field in the interface	Description
Item detected	%detectedas%	Detected Items page — Detected As	Name of the virus.
Item detected	%detectedby%	Detected Items page — Task	"On-Access" if detected by the on-access process, or name of the On-Demand task which detected the infection.
Item detected	%detectedtime%	Detected Items page — Time	Date and time on the local host for detected item.
Item detected	%detectedtype%	Detected Items page — Detected Type	Type of the virus.
Item detected	%detectedutc%	Detected Items page — Time	Date and time on the local host, with UTC offset shown in brackets. For example: May 19 2004 12:30:12 (+5:30 UTC).
Item detected	%engineversion%	Host Summary page — Engine Version	Version number of the scanning engine.
Item detected	%extradatcount%	Host Summary page — Extra DAT	Number of signatures in the extra.dat file
Item detected	%extradatflag%	Host Summary page — Extra DAT	**Yes** or **No** to indicate if an extra.dat file is present
Item detected	%filename%	Detected Items page — File Name	Name of the file which was scanned (excluding path).
Item detected	%path%	Detected Items page — Path	Name of the file which was scanned (including path).
Item detected	%process%	Detected Items page — Process	Name of process resulting in the scan.
Item detected	%result%	Detected Items page — Result	Result of any action taken for the detected infection.
Item detected	%user%	Detected Items page — User	Name of user who caused the scan.
Out of date, and Item detected	%datage%	<none>	Age of the DAT files in days, from the LinuxShield host date and time.
Out of date, and Item detected	%datdate%	Host Summary page — DAT Date	Date when the current DAT files were created.
Out of date, and Item detected	%datversion%	Host Summary page — DAT Version	Version of the DAT files.

Table 7-1 Substitution variables (continued)

Valid for ...	Variable	Equivalent field in the interface	Description
Configuration change	%configchange%	<none>	Configuration change made — modified, on-access detection enabled, or on-access detection disabled.
System events	%eventcode%	System Events page — Code	Error code for the event.
System events	%eventdescription%	System Events page — Description	Error description for the event.
System events	%eventtime%	System Events page — Time	Date and time on the local host for event.
System events	%eventtype%	System Events page — Type	Error type for the event.
System events	%eventutc%	System Events page — Time	Date and time for the event on the local host, with UTC offset shown in brackets. For example: May 19 2004 12:30:12 (-5:00 UTC).

Configuring features from a file

You can configure features from a text-based configuration file, called `nailsd.cfg`. However, we strongly recommend that you control LinuxShield activities from the interface described in *LinuxShield Interface* on page 19. Do not edit this file unless instructed to do so by our technical support staff.

Controlling LinuxShield from the command line

We strongly recommend that you control LinuxShield activities from the interface described in *LinuxShield Interface* on page 19. However you can also control some features from a command line.

Controlling the processes

The following commands are available from the `/etc/init.d/` directory.

Table 7-2 Commands

Command	Description
nails start	Starts LinuxShield processes which include: ■ nailsd — Scan manager and scheduler. ■ scanner — Anti-virus software: scanner and cleaner. ■ mon — Interface communications. ■ nailswebd — Web server. ■ nailslogd — Configuration, log/alerting. ■ ods — On-demand scanner. ■ nails-update — Updater. The `lshook` and `linuxshield` kernel modules are also loaded.
nails stop	Stops all LinuxShield services.
nails restart	Performs a stop then start.
nails reload	Reloads the configuration information. This is only required if manual changes are made to configuration files rather than by using the browser interface.
nails status	Provides status on the running services.

Controlling LinuxShield

The following commands are available from the `/opt/NAI/LinuxShield/bin` directory.

Table 7-3 Commands

Command	Description
nails --help	Displays brief information about all nails commands.
nails --version	Displays information about the product version.
nails dump [--verbose]	Produces a diagnostic report. This is the same report that is produced by clicking **Diagnostic Report** on the **Scanning Summary** page of the browser interface. The `--verbose` flag provides more detail, however this greatly increases the size of the report and the time taken to generate the report. The output of the command should be re-directed to a file.
nails on-access --disable	Disables on-access scanning.
nails on-access --enable	Enables on-access scanning.
nails on-access --flush	Clears the cache of scanned files, forcing the on-access scanner to re-scan files when they are next accessed.
nails on-access --queue	Displays information about files currently being processed by the on-access scanner.
nails on-access --status	Displays the status of the on-access scanner, whether enabled or disabled.
nails passwd	Changes the password for the nails user.
nails quarantine --list [--verbose]	
	Displays information about the files in the on-access quarantine directory. The metafiles in the quarantine directory provide information that can be used to restore the file.
nails quarantine --recover <meta-file> [<destination-file>]	
	Uses information in the .metafile to recover a file, and move the file to its original location, or to the <destination-file>. Use this command only when a non-infected file has been incorrectly quarantined. The recovered file might be quarantined again when accessed unless an exclusion has been set up for the recovered file.

Scheduled tasks for updating and on-demand scans can normally be managed using the browser interface. The following commands allow basic control of tasks using the command line.

Table 7-4 Scheduling

Command	Description
nails task --list	Lists tasks created at the browser-based interface.
nails task --run *taskid*	Runs the specified task immediately.
nails task --stop *taskid*	Stops the specified task.

How the quarantine action works

As one of the anti-virus actions, you can configure LinuxShield to place infected files into a quarantine directory. The processes that LinuxShield uses depend on the relative locations of the infected file and the quarantine directory, and on the features of the file system. In some cases, moving the infected file by copying then deleting is not suitable. In every case, LinuxShield works to prevent loss of security and the further spread of viruses and other potentially unwanted software. LinuxShield uses the following techniques to quarantine infected files:

- If the file system supports *hard links* and the infected file is on the same file system, LinuxShield creates a hard link to the quarantine directory, then unlinks the infected file. If the unlink fails, LinuxShield unlinks the copy in the quarantine directory, so that only the original infected file remains.
- If the infected file is on a remote file system, LinuxShield copies the infected file into the quarantine directory *only if* the quarantine directory is also on that remote file system. This method prevents the spread of infection between hosts.
- LinuxShield verifies that it can copy the infected file into quarantine directory and that it can delete the file from the quarantine directory. This method prevents creation of a copy of an infected file that cannot be deleted.
- If LinuxShield cannot delete the original infected file, LinuxShield deletes the copy of the file in the quarantine directory so that only the original infected file remains.

If the quarantine action fails to work, LinuxShield uses any secondary action. If that action fails, LinuxShield uses its *fallback* action. For on-access scanning, LinuxShield blocks access to the infected file. For on-demand scanning, LinuxShield reports that the file is infected.

8 Troubleshooting

This section provides answers to common situations that you might encounter when installing or using LinuxShield.

The following topics are included:

- *Frequently asked questions* (FAQs)
- *Error messages* on page 78

Frequently asked questions

This topic contains troubleshooting information in the form of frequently asked questions, in these categories:

- *Installation*
- *Scanning* on page 74
- *Viruses and detection* on page 75
- *General information* on page 77

Installation

How do I start the anti-virus software running?
See *Opening the LinuxShield interface* on page 19 and *Controlling LinuxShield from the command line* on page 70.

My operating system or version does not appear in the list. How do I get a kernel hooking code that will work for me?
LinuxShield monitors accesses to file, so a component of its software (the *kernel hooking module*) is dependent on the Linux kernel that you are using. We provide components to suit a range of Linux operating systems. See the *Installation Guide* for information about the supported kernels.

Which versions of the program components are in use?

To display version numbers of components used by LinuxShield on a host, type the following at a command-line prompt:

```
/opt/NAI/LinuxShield/bin/nails --version
```

You can also click **About LinuxShield** in the Links bar.

Scanning

How can I disable on-access scanning from the command line?

Type the following on a command line:

```
/opt/NAI/LinuxShield/bin/nails on-access --disable
```

Why are some files being scanned and detected twice since the quarantine directory was changed?

LinuxShield maintains a cache to record details of files that have been scanned. Changing the quarantine directory flushes the cache, so LinuxShield must re-scan the file to ensure its information is up to date.

Why was an infected file removed from my KDE desktop before I even opened the file?

If LinuxShield has been configured to delete infected files, it does this when you access the file. However, scanning can also occur at other times depending on how your desktop is configured. For example, scanning may occur if the directory includes previews of file contents or if a pop-up appears when you move the cursor over a file name or icon.

Some large files are not being scanned.

On computers with low-specification hardware, LinuxShield abandons scanning of some large files because of the length of time taken. You can increase the time-out value at **Maximum scan time** on the **On-Access Settings** page and the **On-Demand Settings** page.

How can I use uvscan with LinuxShield?

Run uvscan as root to prevent double scanning.

Why does a file disappear or report "access denied" when an operation (such as cat) is performed on it?

The file is infected, and has been cleaned (or deleted or quarantined), or denied by the on-access scanner. View **Detected Items** in the browser interface to see if a virus was detected in that file.

How can I release a file where the on-access scanner has denied access?

Add the file to the list of paths excluded (on the **On-Access Settings** page), or create a directory on the same file system, and add that directory to the list. Use `mv` to move the file to the exclusion directory. Because `mv` is a meta-data change, it does not cause any on-access scanning.

If LinuxShield has blocked the file, the file is likely to be infected, and will not be scanned again when in an excluded directory.

How can I restore a file from quarantine?

Type the following on a command line:

```
/opt/NAI/LinuxShield/bin/nails quarantine --restore
```

How can I see which files LinuxShield is processing but has not yet completed scanning?

Type the following on a command line:

```
/opt/NAI/LinuxShield/bin/nails on-access --queue
```

Why can I see virus detections on other hosts but cannot control those hosts?

The **Host Summary** page can show the anti-virus activity of several monitored hosts. See *Host Summary* on page 29. If you click a host name, you can view further information about the selected host. However, in order for you to make changes to the configuration of the selected host, the selected host must have the same user name and password as the host to which your browser is connected.

Viruses and detection

How can I be sure that the anti-virus software is working?

You can test the operation of the anti-virus software by running a test file on any computer where you have installed the software. The EICAR Standard AntiVirus Test File was developed by the European Institute of Computer Anti-virus Research (EICAR), a coalition of anti-virus vendors, as a method for their customers to test any anti-virus software.

To test scanning:

1. Open a standard text editor, then type the following character string as *one line, with no spaces or line breaks*:

   ```
   X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
   ```

   The line shown above should appear as *one line* in your text editor window, so be sure to maximize your text editor window and delete any line breaks. Also, be sure to type the letter O, not the number 0, in the "X5O..." that begins the test message.

   If you are reading this manual on your computer, you can copy the line directly from the Acrobat PDF file and paste it into your text editor. If you copy the line, be sure to delete any carriage returns or spaces.

2. Save the file with the name EICAR.COM. The file size will be between 68 and 70 bytes (depending on end-of-line characters appended by the editor).

3. Start your anti-virus software and allow it to scan the folder or directory that contains EICAR.COM.

   If the scanner appears not to be working correctly, check that you have read permissions on the test file.

   This file is *not a virus* — it cannot spread or infect other files, or otherwise harm your computer. Delete the file when you have finished testing your scanner to avoid alarming other users.

How can I find out more about the effect of a virus?

Visit our web site. See *Contact information* on page 14.

What should I do if I find a new virus?

If you suspect you have a file that contains a virus and the scanning engine does not recognize it, please send us a sample. For information, click on the *Links bar*, described on page 24.

How do I prevent the quarantine area filling up?

When LinuxShield detects a virus or other potentially unwanted software, LinuxShield moves it to a quarantine area if you have configured this action. See **Anti-virus actions** in *On-access settings* on page 57 and *On-demand settings* on page 63.

However, the area must be monitored to prevent it becoming full. If the area fills too quickly in normal use, we recommend that you change the action. It is only worthwhile to keep quarantined items if you intend to examine them promptly.

The area can become full quickly during a virus outbreak, and many of the files in the area will then have identical contents, and are not worth keeping. We recommend that you create a `cron` job to perform housekeeping operations on the quarantine directory to ensure that the directory does not exhaust all the available disk space.

I believe that a quarantine file has been falsely identified as infected. What should I do?

To ensure that LinuxShield does not quarantine the file again, first see *How can I release a file where the on-access scanner has denied access?* on page 74.

Type the following on a command line:

```
/opt/NAI/LinuxShield/bin/nails quarantine --restore
```

See *What should I do if I find a new virus?*.

Where is information about LinuxShield recorded?

By default, LinuxShield records information about detections, system events, and events related to tasks. You can view the information at the **Detected Items** and **System Events** pages of the browser-based interface. In addition, you can configure logging to SYSLOG from the **General Settings** page.

What kind of information is recorded?

The recorded information includes the following:

- Detections of viruses and other potentially unwanted software, and the result of any action taken.
- Events such as scanning status and errors.
- Events for specific tasks such as updates to DAT files, and on-demand scanning tasks.

What happens to the log messages if the system logger is not working?

If SYSLOG logging is enabled (from the **General Settings** page) and syslogd has stopped due to a fault, all log messages are printed on the console.

General information

How do I contact Technical Support?

See *Contact information* on page 14 for the address.

Before speaking to Technical Support, try to have the following information ready:

- The version of the operating system, such as Red Hat 9 or SuSE 8.
- The type of computer on which LinuxShield is installed — manufacturer and model.
- Any additional hardware that is installed.
- The browser being used and its version.
- A diagnostic report. You can produce this in several ways:
  - In the **Scanning Summary** page, click **Diagnostic Report**. You can select all the text, and copy and paste it.
  - Enter the following command at the command-line prompt:

    ```
    /opt/NAI/LinuxShield/bin/nails dump > dumpfile
    ```

  - Enter the following command at the command-line prompt, to produce a fuller report:

    ```
    /opt/NAI/LinuxShield/bin/nails dump --verbose > dumpfile
    ```

Where can I obtain the open source code for third-party components?

Open source code is available on the product's download site (see *Contact information* on page 14) or on the product CD.

Problems with pid files

As with other processes, LinuxShield uses .pid files. Do not delete these files, because this may cause unpredictable effects.

Server certificate failed the authenticity test

This message appears on Konqueror browsers during logon, because the certificate is self-signed. You may ignore this message and click **Continue**.

Error messages

Error messages appear in several forms:

- Messages displayed in the browser, as shown in *Understanding error messages* on page 28. These are browser problems and errors reported by the web server.
- Messages logged in the system events log. For a list of categories of these messages, see the next table.

Table 8-1 Error code ranges for System Events log

Range	Error Categories	Description
3000 - 3999	Anti-virus Engine errors	Errors which occur during scanning or cleaning reported by the anti-virus engine.
5000 - 5999	Scan Manager	Errors reported by the nailsd process, which controls the scanners.
6000 - 6999	Logging errors	Errors reported by the logging subsystem. If the error logging system fails, errors will be redirected to syslog.
7000 - 7999	Configuration errors	Errors found when parsing values in the configuration files.
8000 - 8999	Exclusions and filtering errors	Errors found when processing the information about files excluded from scanning, or which extensions to scan.
9000 - 9999	Monitoring errors	Errors reported by the monitoring processes that provide administration of the product.
11000 - 11999	IPC errors	Errors reported during inter-process communication.
12000 - 12999	On-Demand scanner errors	Errors reported by the on-demand scanner.
13000 - 13999	Command processor errors	Internal errors with respect to the commands used during inter-process communication.
14000 - 14999	Anti-virus Engine scan errors	Errors reported by the anti-virus engine when processing a specific file.
15000 - 15999	Task Scheduler errors	Errors reported by the task scheduler.
16000 - 16999	SMTP Alerting errors	Errors reported by the SMTP alerting component.

Glossary

ABCDEFHIJKLMNOPQRSTUVWXYZ

A

action taken

How McAfee Security anti-virus or security products responded to detected infections; for example, "cleaning" indicates that the infection was successfully removed from the corresponding file.

alert

A message or notification regarding computer activity such as virus detection. It can be sent automatically according to a predefined configuration, to system administrators via email.

attack

An attempted breach of system security. Successful attacks range in severity from someone having an unauthorized view of data on your system, to destroying or stealing data, or shutting down your system.

AutoUpdate

The automatic program in the McAfee software that updates that software program with the latest virus definition (DAT) files and scanning engine.

C

clean, cleaning

An action taken by the scanner when it detects a *virus*, a *Trojan horse* or a *worm*. The cleaning action can include removing the virus from a file and restoring the file to usability; removing references to the virus from system files, system INI files, and the registry; ending the process generated by the virus; deleting a macro or a Microsoft Visual Basic script that is infecting a file; deleting a file if it is a Trojan horse or a worm; renaming a file that cannot be cleaned.

command-line scanner

The McAfee anti-virus software scanner that runs from the Command Prompt.

D

DAT files

Virus definition files, sometimes referred to as signature files, that allow the anti-virus software to recognize viruses and related potentially unwanted code embedded in files.

See also *extra.dat file*.

denial-of-service attack (DoS)

A means of attack, an intrusion, against a computer, server or network that disrupts the ability to respond to legitimate connection requests. A denial-of-service attack overwhelms its target with false connection requests, so that the target ignores legitimate requests.

download site

The McAfee web site from which you retrieve product or DAT updates.

E

EICAR test file
European Institute of Computer Anti-Virus Research has developed a file consisting of a string of characters that can be used to test the proper installation and operation of anti-virus software.

ePolicy Orchestrator agent
A program that performs background tasks on managed computers, mediates all requests between the ePolicy Orchestrator server and the anti-virus and security products on these computers, and reports back to the server to indicate the status of these tasks.

ePolicy Orchestrator console
The interface of the ePolicy Orchestrator software that is used to remotely control and monitor managed computers.

ePolicy Orchestrator server
The back-end component of the ePolicy Orchestrator software.

See also *ePolicy Orchestrator agent* and *ePolicy Orchestrator console*.

exit codes
The code a program returns when it exits. These codes identify any viruses or problems that were found during a scan operation.

extra.dat file
Supplemental virus definition file that is created in response to an outbreak of a new virus or a new variant of an existing virus.

See also *DAT files*.

H

heuristic analysis, heuristics
A method of scanning that looks for patterns or activities that are virus-like, to detect new or previously undetected viruses.

host, host computer
Any computer on a network.

J

joke program
A non-replicating program that may alarm or annoy an end user, but does not do any actual harm to files or data.

L

log
A record of the activities of a component of McAfee anti-virus software. The log records the actions taken during an installation or during the scanning or updating tasks.

M

macro virus
A malicious macro — a saved set of instructions created to automate tasks within certain applications or systems — that can be executed inadvertently, causing damage or replicating itself.

mass mailer virus
Viruses such as Melissa and Bubbleboy that propagate themselves rapidly using email services.

O

on-access scanning — An examination of files in use to determine if they contain a virus or other potentially unwanted code. It can take place whenever a file is read from the disk and/or written to the disk.

Compare to *on-demand scanning*.

on-demand scanning — A scheduled examination of selected files to determine if a virus or other potentially unwanted code is present. It can take place immediately, at a future scheduled time, or at regularly scheduled intervals.

Compare to *on-access scanning*.

P

packed executable — A file that, when run, extracts itself into memory only, never to disk.

potentially unwanted program — A programs that performs some unauthorized (and often harmful or undesirable) act such as viruses, worms, and Trojan horses.

properties — Attributes or characteristics of an object used to define its state, appearance, or value.

Q

quarantine folder or directory — The location on a computer system that stores files that may contain virus or other suspicious code; the messages are stored until the system administrator can review them and decide on a course of action.

quarantine — Enforced isolation of a file, folder or directory — for example, to prevent infection by a virus until action can be taken to clean or remove the item.

S

scan action — The action that takes place when an infected file is found.

scan task — A single scan event.

scan, scanning — An examination of files to determine if a virus or other potentially unwanted code is present.

See *on-access scanning* and *on-demand scanning*.

signature files — See *DAT files*.

T

task — An activity (both one-time such as *on-demand scanning*, and routine such as *updating*) that is scheduled to occur at a specific time, or at specified intervals.

Trojan horse — A program that either pretends to have, or is described as having, a set of useful or desirable features, but actually contains a damaging payload. Trojan horses are not technically viruses, because they do not replicate.

U

updating — The process of installing updates to existing products or upgrading to new versions of products.

UTC time — Coordinated Universal Time (UTC). This refers to time on the zero or Greenwich meridian.

V

virus definition (DAT) files — See *DAT files*.

virus — A program that is capable of replicating with little or no user intervention, and the replicated program(s) also replicate further.

W

worm — A virus that spreads by creating duplicates of itself on other drives, systems, or networks.

Index

A

action, fails to work 63
actions, against viruses 62
alerts, see email notification 64
analysis of events 33
anti-virus action, fails to work 63
anti-virus software, testing 75
Apply button 27
archives 58
arrows, in tables 26
audience for this guide 11
authentication 9
authenticity test, failed 77
Avert Labs Threat Center 14
Avert Labs Threat Library 14

B

Back button 27
  does not work! 25
beta program website 14
bind mounts 59
buttons
  Apply 27
  Back 27
  Cancel 27
  Defaults 27
  Edit 27
  Next 27
  Refresh 27
  Reset 27

C

Cancel button 27
certificate failed! 77
code event 38
code ranges 38, 78
code, open source 77
command line 49
  running scans from 47
  running updates from 44
compressed files, excluding from scan 59
configuration file, nailsd.cfg 69
Configure menu 51
configuring
  actions against viruses 62
  browser interface 55
  excluded paths 59
  general settings 54
  hosts 52
  logging details 55
  monitored hosts 52
  notifications 64, 66
  on-access settings 57
  on-demand settings 63
  scanning options 58
  SMTP 64, 65
connection, how to reconnect a lost 53
console 19, 23
contacting McAfee 14
controlled pattern release, see extra DAT files 41
CPR, see extra DAT files 41
CSV (Comma-Separated Values) 36, 38
  export slows scanning performance 38
customer service, contacting 14

D

daemon
  (like Microsoft Windows service) 8, 19
DAT files
  Avert Labs notification service for updates 14
  date, variable 68
  extra DAT 30
  information about extra DAT 41
  updates, website 14
  updating 45
  version, variable 68
  why they are important 44
dates, representation 28
Defaults button 27
definition of terms (*See* Glossary)
defs, see DAT files 44
Detected Items
  limit to information displayed 26
  querying 35
  viewing results 36, 37
detections, number of 30
detitems.csv file 36
diagnostic report 33
disinfect, same as clean 62
disinfection, same as cleaning
.doc 60
download website 14
dup 8

E

Edit button 27
EICAR 75
email messages, see email notification 64
email notification 64
error codes 28, 38
error messages
  display of 28
  troubleshooting 78
escalation report 33
evaluating McAfee products, download website 14
event codes 28
examples
  Microsoft Outlook 66
  procmail 66
  running tasks from command line 49
Excel, Microsoft 38
exclusion list 59
extension-based scanning 60
  not case sensitive 61
extra DAT files, information about 41
extradat, variable 68

F

FAQs 24, 73
features, described 10
features, overview 7
file name extensions 60
%filename% 67

files
large files not scanned 58
not being scanned 74
number scanned 30
releasing from quarantine 74
scanned and detected twice 74
still being scanned 75
frequently asked questions 24, 73
FTP site 44
see download web site (in Preface) 46
FTP, download new DAT files 46

G
glossary 79—82

H
hard links, effect on quarantine 72
heuristic analysis 58
hooking code 73
hooking module, kernel 73
%host% 67
hosts
adding a new host 53
connection is lost 53
controlling multiple 10
maximum to monitor 52
monitored 9
reconnect 53
stop monitoring 53
HotFix and Patch releases (for products and security vulnerabilities) 14
HTTPS, secure HTTP 8, 9

I
identities (virus), see DAT files 44
IDEs, see DAT files 44
installation
see Installation Guide 73
troubleshooting 73
installation (*See* the Installation Guide)
interface 19
console 23
Home page 20
Links bar 24
navigation pane 22
opening the 19
overview of 21
Quick Help pane 23
introducing LinuxShield 7

J
joke programs 58, 62

K
KDE desktop preview 74
KDE desktop, file removed! 74
kernel hooking code 73
kernel hooking module 73
KHM, kernel hooking module 73
KnowledgeBase search 14

L
large archive files, excluding from scan 59
links bar 24
Linux kernel, hooking module 73
Loading, message 33
log off 24
logon message, Server certificate failed 20
logon page 20
Lotus 123 38
lpt files, see DAT files 44
lshook, kernel hooking code 73

M
macro analysis 58
MacroTrap, (see macro analysis) 58
manual scan, use Immediately radio button 45
menus
Configure 51
Schedule 43
View 29
MER tool 33
messages
Loading 33
Microsoft Excel 38
Microsoft Outlook, example 66
Microsoft Windows, scanning of files for 60
MIME encoded files 58
minimum escalation report 33
module, kernel hooking 73
mon process 9
monitored hosts 9
mounts, bind 59

N
nails user 8
nailsd process 9
nailsd.cfg 69
nailswebd process 9
navigation pane 22
network, connection is lost 53
new features 11
Next button 27
notifications
configuring 64
configuring for different people 66

O
official pattern release, see DAT files 44
on-access scanning 7, 8
configuring 57
deny access 62
disabled 30
items detected 34
status 32
summary 31
on-demand scanning 47
configuring settings 63
open source code 77
OPR, see DAT files 44
options
configure 22
schedule 22, 43
view 22
Outlook, example 66
overview of features 7

P
password ‘cracker’ 33
pattern files, see DAT files 44
percent (%) variables 67
.pid files 77
potentially unwanted programs 58
processes 9
mon 9
nailsd 9
nailswebd 9
scanner 9
procmail, example 66
.procmailrc 66
product information, where to find 13
product overview 7
product update 44
product upgrades 14
professional services, McAfee resources 14
programs
jokes 58
potentially unwanted 58
ptn files, see DAT files 44

Q

quarantine
- did not move file 62
- directory does not work! 58
- file was falsely identified 76
- full 76

quarantine directory 58, 62
queries
- Detected Items 35
- limit to information displayed 26
- System Events 37

questions, frequently asked (FAQs) 73
Quick Help pane 23
- do not display 55

R

real-time scanning 16
- (see on-access scanning) 57

recipe, procmailrc 66
Refresh button 27
- does not work! 25

remote-access software 33
reports
- diagnostic 33
- minimum escalation 33
- verbose 77

Reset button 27
resources, for product information 13

S

Samba 60
samples, viruses 24
scan log, see recently scanned items 33
scan now, use Immediately radio button 45
scanner process 9
scanning
- all files 60
- at regular intervals 47
- based on extension 58
- default and specific files 61
- do not scan here 59
- elapsed time 40
- excluded paths 59
- extension-based 60
- fails on large files 58
- heuristics 58
- maximum time for 58
- slower during CSV export 38
- specific files 61
- testing 75
- troubleshooting 74
- unscheduled 47

scanning options
- enable program file heuristics 58

scans
- do not stop immediately 41
- stopping 41

Schedule menu 43
Schedule options 43, 44, 45
scheduled scans 47
Scheduled Tasks 39
- delete an existing 40
- modify an existing 40
- stopping a running 41

schedules 43
- DAT files 44
- on-demand scan 47
- using a wizard 44
- virus definition files 44

Secure Socket Links 9
Security Headquarters (*See* Avert Labs)
security updates, DAT files and engine 14
security vulnerabilities, releases for 14
Server certificate failed 77
- message at logon 20

ServicePortal, technical support 14
signature files, see DAT files 44
SMTP 64
sorting tables 26
spyware 33
SSL 9
statistics
- clearing 55, 56
- files scanned 30

submit a sample, Avert Labs WebImmune 14
symbolic links
- not as excluded paths 59
- not for quarantine directory 58

sysevents.csv file 38
syslog 55
syslogd
- log messages 76

System Events 37
- categories of errors 78
- limit to information displayed 26
- querying 37

T

tables
- arrows and numbers 26
- collapsing 25
- expanding 25
- hiding 25
- navigating long 26
- showing 25
- sorting 26

tar files 58
tasks
- names entered at browser interface 46
- running from command line 49

Technical Support, contacting 77
technical support, contacting 14
tgz files 58
Threat Center (*See* Avert Labs)
threat library 14
- 3000 38

time differences, understanding 44
time-out 62
- problems 58
- scanning large files 74

times, representation 28
training, McAfee resources 14
Trojan horses 62
troubleshooting
- error messages 78
- FAQs 73
- general information 77
- installation 73
- scanning 74

U

unscheduled scan 47
unscheduled update 44
unwanted programs 58
update now, see on-demand scan 22
updates
- does not stop immediately 41
- engine and DAT files 45
- stopping 41
- unscheduled 44

upgrade website 14
user, nails 8
using this guide 11
- audience 11
- typeface conventions and symbols 12

UTC, Universal Time Co-ordinates 28, 55

V

variables, % 67

–verbose, for fuller report 77
versions
component numbers 74
DAT, variable 68
virus-scanning engine, variable 68
View menu 29
virus identities, see DAT files 44
Virus Information Library 24, 75
Virus Information Library (*See* Avert Labs Threat Library)
virus log, see recently detected items 32
virus pattern files, see DAT files 44
virus patterns, see DAT files 22
viruses
effect of 75
EICAR, test virus 75
information about (VIL) 24
preventing spread across file systems 62
send a sample 24
what to do with new 76

W

warnings
Back button 25
CSV export slows scanning performance 38
letter case for excluded path names 59
letter case for path names 35, 48
no symbolic links for excluded paths 59
Refresh button 25
WebImmune, Avert Labs Threat Center 14
why use LinuxShield software? 7
wildcard 59
wizards 27
setting up schedules 44