

---

# *DynaComm PointGuard*<sup>®</sup>

## **Quick Start Guide**

---

2008 by FutureSoft, Inc. All rights reserved.

## DynaComm PointGuard® Quick Start Guide

This manual, and the software described in it, is furnished under a license agreement. Information in this document is subject to change without notice and does not represent a commitment on the part of FutureSoft. FutureSoft assumes no responsibility or liability for any errors or inaccuracies that may appear in this manual.

No part of this manual may be produced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, or otherwise, without the prior, written permission of FutureSoft, Inc.

DynaComm, DynaComm PointGuard and FutureSoft are registered trademarks of Futuresoft, Incorporated in the United States and/or other countries.

DynaComm PointGuard 8.0.0.0

Document #E-QS-DCPG  
Edition 2-2008 (e2-121508)

Written and designed at:  
FutureSoft, Inc.  
12012 Wickchester Lane, Suite 600  
Houston, Texas 77079-1221 USA

1.800.989.8908

info@futuresoft.com  
<http://www.futuresoft.com>

---

# Table of Contents

Quick View of DynaComm PointGuard .....	1
Components .....	1
System Requirements .....	3
Quick Install—Server .....	4
Before You Install... .....	4
Server Installation .....	5
Quick Configure — Server .....	7
Quick Configure — New Clients .....	8
Options Dialog Settings .....	8
Plug-in Manager Settings .....	8
Quick Install — Client Systems .....	9
Using the PointGuard Server .....	9
Using Alternate Deployment Methods .....	10
User Installation Methods .....	10
Quick Steps for Content Management .....	11
Content Management: Categories .....	12
Content Management: File Types .....	13
Content Management: File Scans .....	14
Content Management: Registry Scans .....	15
Content Management: Spyware/Virus Scans .....	16
Content Management: (Spyware/Virus) Definitions .....	17
Quick Steps for Quarantine Management .....	18
Quick Steps for Policy Management .....	19
Policy Management: Time Intervals .....	20
Policy Management: Policy Items - File Management .....	21
Policy Management: Policy Items - Device Management .....	22
Policy Management: Policy Items - Active Protection .....	23
Policy Management: Policy Items - Eventlog Monitoring .....	24
Policy Management: Policy Items - Spyware/Virus Protection .....	25
Policy Management: System Policies .....	26

Quick Steps for System Events .....	28
Quick Steps for Reports .....	29
Quick Steps for Scheduling .....	30
Index .....	31

## Contacting FutureSoft

### FutureSoft in the US

Corporate Headquarters  
12012 Wickchester Lane  
Suite 600  
Houston, TX 77079  
USA  
Tel: 281.496.9400  
Sales: 800.989.8908  
Fax: 281.496.1090  
[info@futuresoft.com](mailto:info@futuresoft.com)

### FutureSoft in Europe

FutureSoft UK, Ltd.  
Shepherds Mill  
Worrall Street  
Congleton  
Cheshire  
CW12 1DT  
United Kingdom  
Tel: +44 (0) 1260 292222  
Fax: +44 (0) 1260 292224  
[info@futuresoftuk.com](mailto:info@futuresoftuk.com)







---

## Quick View of DynaComm PointGuard

DynaComm PointGuard is an IT administrative tool used to manage, monitor and secure computer systems in the corporate enterprise. PointGuard provides on-demand and real-time functions. On-demand functions include file, registry and spyware/virus scans used to find and modify information on individual client systems. Real-time functions include file management sessions, active-registry protection, removable-device management, Windows Event log alerting, and spyware/virus protection.

### Components

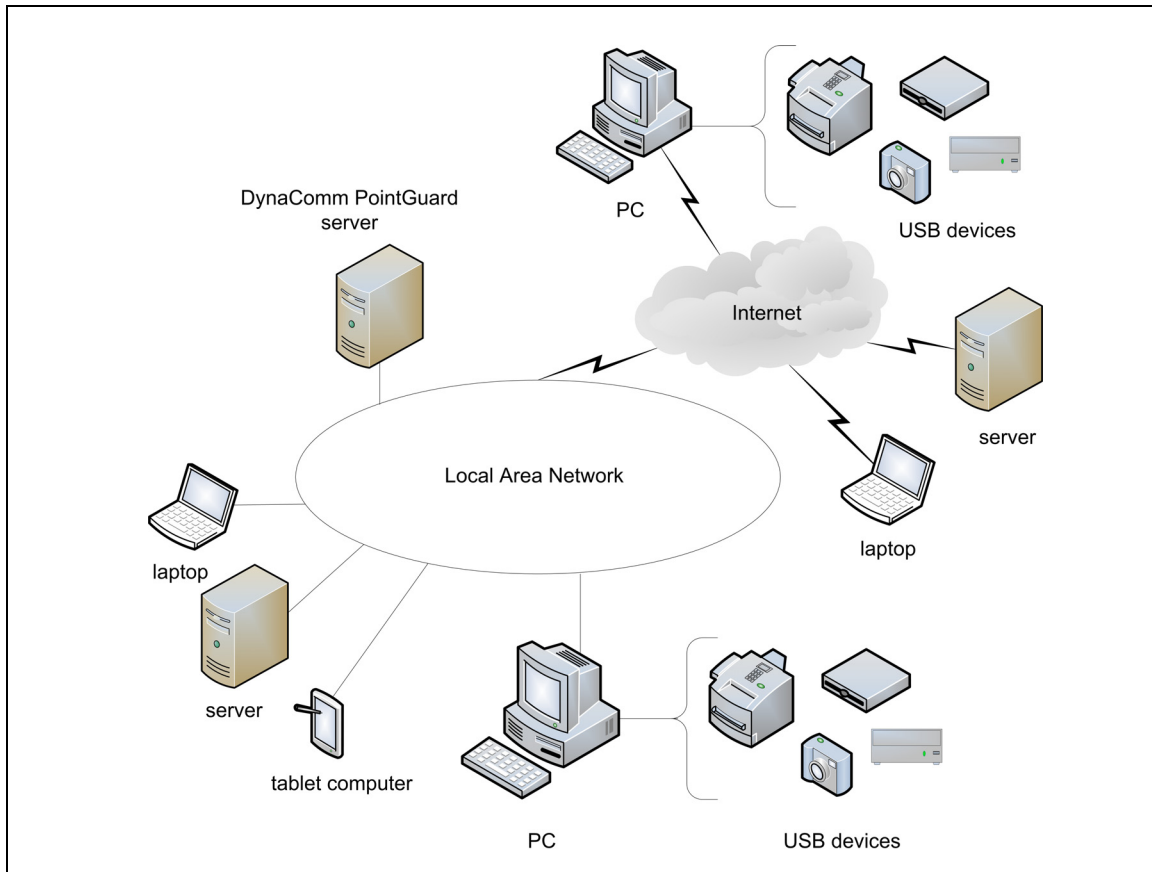
A PointGuard configuration includes a console component installed on a server system and one or more client systems on local or remote networks. On the server system, the console collects and stores all configuration data into the following areas (configuration topics):

- **System Events** — Displays function alerts and Windows Event log entries from client systems. Report Manager offers reports for spyware/virus histories and alerts, and a report for all system events that occurred within a specified date range.
- **Plug-In Management** — Manages functional modules installed on client systems that are used to perform on-demand and real-time functions, such as, running scans and policy management sessions. Installed plug-ins are set for automatic installation, or manual installation for a customized level of control. Manual installation is performed through the Client Management dialog and monitored through a system events window.
- **Content Management** — Collects configuration data and manages spyware/virus components, file and registry scans and elements used by scans, such as, keywords and file types. Summary and detailed scan results are viewed from result listings.
- **Quarantine Management** — Manages data quarantined through file, registry, and spyware/virus scans. Quarantine data can be retrieved, removed, or restored. By default, quarantine data “lives” for 7 days before being permanently removed. This default can be changed as needed.
- **Policy Management** — Manages sets of policies (rules) applied to groups of client systems that control the use of files and removable devices, changes to the Windows Registry, alert on selected Windows Event log entries, and alert on and block infection attempts by spyware/virus components.
- **Reports** — Manages pre-defined and custom report configurations for scans and file management policies. Reports are run on-demand or through a scheduled job. Report results are either displayed on the console or, exported to one of seven file formats and then saved to a file system or sent as an e-mail attachment.
- **Scheduling** — Creates and manages scheduled jobs which include re-occurring tasks, such as running scans and reports.

## Quick Start Guide

Client systems are identified and managed through the console. Client components:

- Have the client software installed on them.
- Query the server at predefined intervals for new tasks (scans, policy updates, etc.) and scheduled jobs.
- Send result data to the server for scans and real-time policy sessions.



**Figure 1**

*DynaComm PointGuard server with local and remote client systems; USB devices attached to local or remote clients can be protected.*

## System Requirements

The following system specifications are recommended minimums for PointGuard installations serving 500 or fewer clients. Suggestions for system specifications for more than 500 clients are available upon request.

### DynaComm PointGuard Server

- Windows 2003 Server with SP2
- Microsoft Internet Information Services (IIS)
- Pentium 4–2 GHz or equivalent
- 2 GB memory
- 150 MB disk storage for application files
- 50 GB disk storage for data
- Network connectivity

### DynaComm PointGuard Clients

- Windows VISTA Business (64-bit), *or* Windows VISTA Ultimate (32-bit), *or* Windows 2003 SP2, *or* Windows XP SP2, *or* Windows 2000 SP4 v2 with Update Rollup 1
- 200 MB disk storage for client files
- 35 MB memory for client services
- Network connectivity

### Notes

- *If client systems are not on the same network as the server system, the server must have a public IP address or host name to which clients outside the network can connect to over port 80.*
- *We recommend that the PointGuard server be dedicated only to PointGuard functionality. Additional functionality may restrict or interfere with PointGuard functions.*

### Quick Install—Server

Installation of PointGuard begins with installation of the console component. Client systems are then installed either all at the same time or in organized groups using one of two methods or a mix of the two.

#### Before You Install...

Before installation, carefully evaluate the following points with respect to how they will affect your users and network.

#### Server Installation

- Microsoft Internet Information Services (IIS) and the Web Services component must be installed on the server system before installing PointGuard.
  - To test scanning capabilities for client machines that are not on an internal private network, make sure that the PointGuard server system has a public network interface and IP address.
  - If a firewall is enabled on the system that the PointGuard console is to be installed to, it must be configured to allow incoming and outgoing traffic on TCP port 80. If you have changed the port used by IIS Web Service, then an exception must be made for this port on the firewall.
- Clients can be installed at anytime with any deployment method that allows the .MSI client installation package to be copied to the client system and then run. This includes deployment through the PointGuard console, with any other Systems Management Server method, such as, Active Directory, or by downloading and installing the client installation package from a web site or FTP server. If you choose to install client systems through the PointGuard console, the following must be in place:
    - PointGuard server listening service must be configured to log on with an account that has local Admin privileges on the client system.
    - Windows Networking Client must be enabled.
    - Windows Print & File Sharing must be enabled.

#### Client Installation

- Create a limited and highly controlled initial environment before deploying PointGuard to all client systems. This allows you to evaluate which approach to use for client deployment based on your user needs, security policies, network environment, and software deployment policy.
- If you ***ever*** choose to deploy the client package through the PointGuard console for any client, you must use a logon during server installation ***that has local admin privileges on all client systems***.
- If you ***always plan to deploy all clients with a tool or method other than through the PointGuard console***, then you only need to ensure that the logon used during server installation has local admin privileges.

## Server Installation

Perform the following steps in the order listed. More information and details for each step are in the DynaComm PointGuard Administrator Guide.

### Step 1: Log on.

#### Note

*You must read the previous section on Client Installation to understand the effects of the logon used at installation time. Failure to do so may result in client system installation failure.*

Log on to the system on which the PointGuard server is to be installed. Log on with an account that has local administrator privileges.

### Step 2: Start the Setup program.

If you have downloaded the software from the FutureSoft web site, the download process asks if you want to run the program. Click “Run” to start the Setup program.

If you are installing from CD-ROM and CD Autorun is enabled, the Setup program starts automatically. If CD Autorun is disabled, the Setup program can be started from either the Windows Run dialog or the Control Panel Add/Remove Programs selection.

## Quick Start Guide

---

### Step 3: Respond to each installation dialog.

Nine dialogs are displayed during server installation. Several dialogs require a considered response. Review the following before proceeding with installation.

- **Welcome dialog**
- **License Agreement dialog**  
You must accept the terms of the license agreement to install PointGuard.
- **Enter User Information dialog**  
To install an evaluation version, leave the **Serial Number** field blank on this dialog. The evaluation period is 15 days. Otherwise, enter the number provided by FutureSoft for a licensed installation.
- **Choose Destination Location dialog**  
Make changes if needed.
- **Select Program Folder dialog**  
Make changes if needed.
- **Setup Status dialog**  
Informational.
- **Authorized Access dialog**  
This is the first of two dialogs used to create security settings for PointGuard. During the install process, the “DynaComm PointGuard Users” local group is created. Users in this group have rights to open and use PointGuard and its functions. The **Authorized Access** dialog informs you that the logon you used when you logged onto the server system and started the installation has been placed in this group.
- **Listening Service Account dialog**  
This is the second dialog used to create security settings for PointGuard. Enter a logon account and associated password that PointGuard will use to access client systems and run functions, such as, scans, policy management sessions, etc. By default, the installation program places the account in this field that started the Setup program.
- **InstallShield Wizard Complete dialog**  
Reboot the system, if prompted, to complete the installation.

You are now ready to configure the PointGuard server. ***This must be performed before any client systems are installed.***

## Quick Configure — Server

After installation of the server component you must perform an initial server configuration which adds network path information to the client package. Read through the following first before configuring the PointGuard server.

### To perform initial server configuration

- 1 From the DynaComm PointGuard program group, select DynaComm PointGuard Console to open PointGuard.
- 2 Click OK in the server endpoints message dialog.
- 3 On the Server tab of the Options dialog, verify or enter the internal and external server endpoints in the Server Endpoints group.

Server endpoints are the “server connection addresses” that client systems use to communicate with the PointGuard server and take the form of:

*http:[host name or IP address]/[web server folder]/webpage.aspx*

where:

*[host name or IP address]* is the name or IP address of the PointGuard server system

*[web server folder]* is the name of the folder in c:/inetpub/wwwroot that is used by the PointGuard server

Client systems in the internal network use the internal server endpoint. Clients outside the internal network, such as users in the field using laptops or other mobile systems, use the external server endpoint to communicate with PointGuard. We recommend using a public IP address. A complete path must be provided for both endpoints.

After initial configuration set up is complete and you click OK, the client.MSI installation package is created. This package includes the specified server endpoints.

- 4 On the E-mail tab of the Options dialog,
  - Enter the mail server name or IP address that handles messages for PointGuard.
  - Change the mail server port number, if necessary.
  - Enter the e-mail address of the PointGuard administrator.
- 5 Click OK in the Options dialog.

### Quick Configure — New Clients

Before installing client systems, you have a couple of decisions to make. These decisions affect default settings made in PointGuard regarding client installations.

#### Options Dialog Settings

By default, the Automatically push new installations to clients option is enabled. This option is on the Settings tab of the Options dialog.

When a new client is added through inclusion in a scan or system policy, all files are sent to the client, including the spyware/virus database when the scan is started or the policy is activated. If you add a *group* of systems, this may create an unacceptable load on your network. To off set the load to a later time when network traffic is lower, you may choose to delay installation by using a manual install. Before installing any clients, clear the option on the Settings tab to prevent automatic installation.

#### To clear the new client auto-install option

- 1 On the Tools menu, select Options.
- 2 In the Options dialog, click the Settings tab.
- 3 In the New Client Settings group, clear the Automatically push new installations to clients option.
- 4 Click OK.

#### Plug-in Manager Settings

The second step in configuring client systems is to determine:

- Are all or selected functions to be run on each client system?

By default all client plug-ins are installed on new client systems. This is controlled with the Automatically install this plug-in on all clients option in the Plug-in Settings dialog.

If you have determined that selected client systems should only have a selected set of functions installed, you will need to manually install the desired plug-in(s) on each client system. Before installing any clients you will clear this option for each plug-in that is to be installed manually.

#### To clear the plug-in auto-install option

- 1 In the left pane, select Plug-in Manager.
- 2 In the right pane, select a plug-in and click Edit.
- 3 In the Plug-in Settings dialog, clear the Automatically install this plug-in on all clients option.
- 4 Click Update.

If an individual function will never be used on client systems, you may choose to remove the plug-in from the plug-in management system.

#### To remove a plug-in from the Plug-in Manager

- 1 In the left pane, select Plug-in Manager.
- 2 In the right pane, select a plug-in and click Remove.
- 3 In the message dialog, click Yes.

## Quick Install — Client Systems

You are now ready to establish the method(s) for installing client systems. Two methods are available:

- Automatically or manually using the PointGuard server.
- Using a software deployment tool, such as Active Directory, or any other method that allows you to run the client installation package.

One method can be used exclusively for all clients, or both methods can be used, such as using the first method for internal clients and the second method for external clients. What is important is that you have set up the correct internal and external server endpoints (Quick Configure - Server: Step 3) before clicking OK in the Options dialog during initial configuration.

### Using the PointGuard Server

Using the PointGuard server to install the client package can be accomplished:

- Automatically, by including the client system in a scan configuration or system policy.
- Manually, by adding the client system to the client list in the Client Management dialog.

#### **To automatically install a client system with a scan**

- 1 On the toolbar, select Options from the Tools menu and verify that the Automatically push new installations to clients option on the Settings tab is enabled and click OK.
- 2 Create a file, registry or spyware/virus scan that includes one or more target systems.
- 3 Run the scan.

When the scan is run, the .MSI package is copied to the client system and executed which installs the client software.

### To manually install a client system

- 1 On the toolbar, select Client Management from the Tools menu.
- 2 In the Client Management dialog, do one of the following:
  - Method One
    - a In the left pane, expand a network node.
    - b In the right pane, select one or more systems and right-click on one of the selected systems.
    - c On the right-click menu, select Install Client Software.
  - Method Two
    - a In the left pane, select All Clients.
    - b In the right pane, right-click and select Add New Client.
    - c In the Enter New Client Name dialog, enter the client system name and click OK.

The new client system is added to the right-pane listing.
    - d In the right pane, right-click the newly added client system and select Install Client Software.

### Using Alternate Deployment Methods

The .MSI client installation package is updated during initial configuration (first time that console is opened) when server endpoints are set up on the Settings tab in the Options dialog. By default this package is placed in:

C:/Program Files/Futuresoft/Dynacomm PointGuard/clientinstall

This package can be used for client installation with other deployment tools, such as Active Directory.

#### To use Active Directory to deploy client systems

- 1 In the Active Directory Users and Computer window, do the following:
  - a In the right pane, right-click the Domain name and select Properties.
  - b In the *DomainName* Properties dialog, select the Group Policy tab.
- 2 On the Group Policy tab, do the following:
  - a In the Group Policy Object Links list, highlight the domain policy.
  - b Click Edit.
- 3 On the Group Policy Object window, do the following:
  - a In the left pane, expand Software Settings and select Software Installation.
  - b In the right pane, right-click and highlight New.
  - c Select Package.
  - d In the Open dialog, navigate to and select the “clientinstall.msi” package.
  - e Click OK.

4 Deploy the client package using one of the following:

- Wait for policy refresh time to elapse.
- Force a policy refresh.
- Reboot (the client system must be rebooted twice for installation to occur).

When the client installation is complete, the system attempts to communicate with the PointGuard server. When a connection is established, the client posts its status, checks for available file updates, and retrieves queued jobs.

### User Installation Methods

Other options for deploying the client .MSI package include placing the file on a file server or web site for download, or include the file as an attachment in an e-mail message. These methods are dependent on the user taking the required action to retrieve and install the package.

## **Quick Steps for Content Management**

Now that you have completed installation and initial configuration steps, you are ready to begin using PointGuard functions. Content Management includes those functions for:

- Scanning files for selected keywords in content and/or file name (file scans).
- Scanning the Windows Registry for selected entries (registry scans).
- Managing the Categories and File Types database which is used in scanning files and the Windows Registry.
- Scanning and removing spyware/virus components.
- Managing the Threat database which is used in scanning for spyware/virus elements.

Use the following quick steps to create and run file, registry and spyware/virus scans, and to manage databases used by these functions.

If you need more information on any of these functions, see the DynaComm PointGuard Online Help system or the DynaComm PointGuard Administrator Guide for details.

### Content Management: Categories

Keywords and file signatures are stored in categories. One or more categories can be selected in a file scan configuration to search for files that contain the category keyword(s) in file contents or file name, or to search for files with matching file signatures.

Registry entries are also stored in categories. One or more categories must be selected in a Registry scan configuration. The Registry scan searches through the Windows Registry for entries that match those stored in the selected categories.

Updates to the Categories and File Types database are available from the FutureSoft web site with either a manual retrieve or through a scheduled job.

#### To add a new category

- 1 In the left pane, expand Content Management and right-click Categories.
- 2 In the New Category dialog, enter a name and short description to identify the new category.
- 3 Click OK.

#### To add a keyword/keyword phrase

- 1 In the left pane, expand Content Management and then expand Categories.
- 2 Expand one category and select Keywords and Phrases below the category name.
- 3 In the right pane, click Add.
- 4 In the Keyword/Phrase for dialog, enter a keyword or keyword phrase, and select a keyword weight.
- 5 Click OK.
- 6 For each keyword or keyword phrase to add, repeat steps 3 through 5.

#### To manually retrieve Categories and File Types database updates

- On the Tools menu, select Update.

#### To add a file signature

- 1 In the left pane, expand Content Management and then expand Categories.
- 2 Expand one category and select File Signatures below the category name.
- 3 Do one or both of the following:
  - To select individual files
    - a In the File Signatures dialog, click Browse.
    - b In the Open dialog, navigate to a file and select Open.
    - c Repeat steps a and b for each file signature to create.
  - To select files in a file scan results log
    - a In the File Signatures dialog, click Import to display the Log Import dialog.
    - b In the Available Scans list, select one file scan.
    - c In the Available Logs list, pick one result log.
- 4 In the Log Import dialog, click OK.
- 5 In the File Signatures dialog, click OK.

## Content Management: File Types

File Types can be selected in a file scan configuration to refine the files to search. File Types contain one or more file type extensions. Over 160 file type extensions included in 17 file type groups are included at installation time. The Categories and File Types database can be updated manually or through a scheduled job.

### To view all file type groups

- In the left pane, expand Content Management and then expand File Types.  
All file type groups are listed in the left pane below File Types.

### To view all file type extensions included in a file type

- 1 In the left pane, expand Content Management and then expand File Types.
- 2 In the left pane, select one file type.  
All file type extensions included in the file type are listed in the right pane.

### To manually retrieve Category and File Types database updates

- On the Tools menu, select Update.

### To add a custom file type group

- 1 In the left pane, expand Content Management.
- 2 In the left pane, right-click File Types and select New File Type Group.
- 3 In the File Type Group dialog, enter a name for the new file type group and click OK.

### To add a custom file type extension

- 1 In the left pane, expand Content Management and then expand File Types.
- 2 In the left pane, right-click a file type and select Add File Type.
- 3 In the File Type dialog, click New.
- 4 In the File Type dialog:
  - a In File Type Name, enter a name to identify the new file type.
  - b In Extensions, and enter the file extension(s) to include in the file type group.
  - c Click OK.
- 5 In the File Type dialog, click OK.

### To move an existing file type to a different file type group.

- 1 In the left pane, expand Content Management and then expand File Types.
- 2 In the left pane, right-click a file type and select Add File Type.
- 3 In the File Type dialog, select one or more file type names and click OK.
- 4 In the message dialog, click Yes.

### Content Management: File Scans

#### To add a file scan configuration

- 1 In the left pane, expand Content Management and then right-click File Scans.
- 2 Select New File Scan.  
The New File Scan wizard opens the *file scan properties* dialog.
- 3 In the *file scan properties* dialog:
  - a On the File Scan tab:
    - (1) Enter a name and brief description to identify the scan.
    - (2) Select one or more client systems to scan.
    - (3) Click Add.
    - (4) Select client systems and click Add Checked Items.
    - (5) Click OK.
  - b Click Next.
  - c On the File Filter tab, select file and/or file-content properties to identify the files to scan.
  - d Click Next.
  - e On the Actions tab and select actions to perform on scanned files.
- 4 Click OK.

#### To run a file scan

- 1 In the left pane, expand Content Management and then expand File Scans to list all defined file scans.
- 2 Right-click a file scan name and select Run.

#### To stop a running file scan

- 1 In the left pane, expand Content Management and then expand File Scans to list all defined file scans.
- 2 Right-click a file scan name and select Stop.

#### To view all run results for a defined file scan

- 1 In the left pane, expand Content Management and then expand File Scans.
- 2 Select a file scan name to display a listing of all run results for the scan in the right pane.

#### To view run-result details for a defined file scan

- 1 In the left pane, expand Content Management and then expand File Scans.
- 2 Select a file scan name to display a listing of all run results for the scan in the right pane.
- 3 In the right pane, right-click a run-results listing and select Results.

#### To run a report with file scan results

- 1 In the left pane, expand Content Management and then expand File Scans.
- 2 Select a file scan name to display a listing of all run results for the scan in the right pane.
- 3 In the right pane, right-click a run-results listing and select Reports.
- 4 In the pop-up list of File Scan reports, click one.

## Content Management: Registry Scans

### **To add a registry scan configuration**

- 1 In the left pane, expand Content Management and then right-click Registry Scans.
- 2 Select New Registry Scan.  
The Registry Scan Properties dialog opens.
- 3 In the Registry Scan Properties dialog:
  - a In Name, enter a name to identify scan contents.
  - b In the Search Here group:
    - (1) Click Add.
    - (2) In the Computer Selector dialog, select one or more client systems to scan and click Add to place the systems in the Selected Items group.
    - (3) When all client systems have been selected, click OK
  - c In the Look for group:
    - (1) Click Add.
    - (2) In the Categories dialog, select one or more categories that contain the registry entries to search for and click OK.
  - d In the Perform the following actions group, enable one or more actions to perform when a registry key match is made.
- 4 Click OK.

### **To run a registry scan**

- 1 In the left pane, expand Content Management and then expand Registry Scans to list all defined registry scans.
- 2 Right-click a registry scan name and select Run.

### **To stop a running registry scan**

- 1 In the left pane, expand Content Management and then expand Registry Scans to list all defined registry scans.
- 2 Right-click a registry scan name and select Stop.

### **To view all run results for a defined registry scan**

- 1 In the left pane, expand Content Management and then expand Registry Scans.
- 2 Select a registry scan name to display a listing of all run results for the scan in the right pane.

### **To view run-result details for a defined registry scan**

- 1 In the left pane, expand Content Management and then expand Registry Scans.
- 2 Select a registry scan name to display a listing of all run results for the scan in the right pane.
- 3 In the right pane, right-click a run-results listing and select Results.

### **To run a report with registry scan results**

- 1 In the left pane, expand Content Management and then expand Registry Scans.
- 2 Select a registry scan name to display a listing of all run results for the scan in the right pane.
- 3 In the right pane, right-click a run-results listing and select Reports.
- 4 In the pop-up list of Registry Scan reports, click one.

### Content Management: Spyware/Virus Scans

Spyware/virus scans use the Threat database to look for spyware/virus components. The scan can simply look for infection components or can be directed to perform either a standard or deep clean that removes found components.

#### To add a spyware/virus scan configuration

- 1 In the left pane, expand Spyware/Virus Protection.
- 2 Right-click Spyware/Virus Scans and select New Spyware/Virus Scan.
- 3 In the Spyware/Virus Scan Properties dialog:
  - a In Name, enter a name to identify scan contents.
  - b In the Spyware/Virus Scan clients group,
    - (1) Click Add.
    - (2) In the Computer Selector dialog, select one or more client systems to scan and click Add Checked Items to place the systems in the Selected Items group.
    - (3) When all client systems appear in the Selected Items group, click OK.
  - c In the Spyware/Virus scan options group,
    - (1) In the Scan Type group, choose either Standard scan (searches selected file areas and limited portions of the Registry) or Deep scan (searches the entire file system and Registry).
    - (2) To remove found spyware/virus components, select Perform Clean in the Cleaning Options group and one or more actions to include in the cleaning process.
    - (3) If a client shutdown is needed, select Force the client to shutdown at and choose a shutdown time.
- 4 Click OK.

#### To run a spyware/virus scan

- 1 In the left pane, expand Spyware/Virus Protection.
- 2 Expand Spyware/Virus Scans to list all defined spyware scans.
- 3 Right-click a spyware/virus scan name and select Run.

#### To view all run results for a defined spyware/virus scan

- 1 In the left pane, expand Content Management and then expand Spyware/Virus Protection.
- 2 Expand Spyware/Virus Scans to list all defined spyware/virus scans.
- 3 Select a spyware/virus scan name to display a listing of all run results for the selected scan in the right pane.

#### To view run-result details for a defined spyware/virus scan

- 1 In the left pane, expand Content Management and then expand Spyware/Virus Protection.
- 2 Expand Spyware/Virus Scans to list all defined spyware/virus scans.
- 3 Select a spyware/virus scan name to display a listing of all run results for the scan in the right pane.
- 4 In the right pane, right-click a run-results listing and select Results.

## Content Management: (Spyware/Virus) Definitions

The Threat database contains spyware/virus definitions which include file signatures, file names, folders, registry entries, and domains of known spyware/virus software. Spyware/virus definitions are used by spyware/virus scans to search client systems for possible infections. The Threat database can be updated manually or through a task in a scheduled job.

### To view a list of spyware/virus definitions

- 1 In the left pane, expand Content Management and then expand Spyware/Virus Protection.
- 2 In the left pane, select Definitions.

The list of definitions appears in the right pane. The last date and time that the Threat database was updated appears in Definitions File Date.

### To view details of a spyware/virus definition

- 1 In the left pane, expand Content Management and then expand Spyware/Virus Protection.
- 2 In the left pane, select Definitions.
- 3 In the right pane, select a spyware/virus definition.

Definition details appear in the Details pane.

### To inactivate a spyware/virus definition

- 1 In the left pane, expand Content Management and then expand Spyware/Virus Protection.
- 2 In the left pane, select Definitions.
- 3 In the right pane, select a spyware/virus definition and click Inactive.

“No” appears in the Active column in the list of Definitions.

### To manually retrieve Threat database updates

- On the Tools menu, select Update.

### To retrieve Threat database updates through a scheduled job

- 1 Either add a new scheduled job or open an existing scheduled job.
- 2 In the Job Scheduler dialog, click the Task List tab and then click Add.
- 3 In the Select Tasks to Schedule dialog, select the Update definitions, keywords and file types task (apply check mark) and click OK.
- 4 In the Job Scheduler dialog, click OK.
- 5 On the toolbar, click Save.

### To retrieve Threat database updates through an Options dialog setting

- 1 On the Tools menu, select Options.
- 2 In the Options dialog, click the Settings tab.
- 3 In the General Settings group:
  - a Select the Perform daily database update check at option (apply check mark).
  - b Either enter a time or use the arrow buttons to select a time in the time entry field to the right of the selected option.
- 4 In the Options dialog, click OK.
- 5 On the toolbar, click Save.

#### Note

*By default, this option is enabled to run at 12:00 AM each day.*

### Quick Steps for Quarantine Management

Quarantine files are created for file scans that include the quarantine action for matching files and when a spyware scan includes cleaning of spyware infection elements. By default, quarantined items remain in quarantine for 168 hours (17 days) before being permanently removed. Time to live before removal is changed on the Settings tab of the Options dialog.

#### To view all clients with quarantine files

- In the left pane, select Quarantine Management.

#### To view all quarantine files stored on a client system

- 1 In the left pane, select Quarantine Management.
- 2 In the right pane, select a client system in the upper pane.

#### To view all items in all quarantine files

- In the left pane, expand Quarantine Management and select Details.  
In the right pane, all items stored in all quarantine files are displayed.

#### To filter displayed quarantine items

- 1 In the left pane, expand Quarantine Management and select Details.
- 2 In the Filter pane, click the “+” button before Advanced Filter Options.
- 3 Do one or more of the following:
  - In Quarantine Time, select a quarantine status and dependent options when available.
  - In Display, select one or more item types and status.
  - In Item, enter a complete file path or use wildcards in the path name.
- 4 Click Refresh.

#### To retrieve one or more items from a quarantine file

- 1 In the left pane, expand Quarantine Management and select Details.
- 2 In the right pane, select one or more items and click Retrieve.
- 3 In the confirmation message dialog, click Yes.
- 4 In the Provide Name and Location dialog:
  - a Navigate to a folder.
  - b In File name, enter a name for the zip file that will hold the retrieved item(s).
  - c Click Save.

#### To restore one or more items from a quarantine file

- 1 In the left pane, expand Quarantine Management and select Details.
- 2 In the right pane, select one or more items and click Restore.

#### To remove one or more items from a quarantine file

- 1 In the left pane, expand Quarantine Management and select Details.
- 2 In the right pane, select one or more items and click Purge.

## Quick Steps for Policy Management

Policy management refers to the processes of:

- Monitoring and alerting on Windows Event log entries, and/or,
- Monitoring, blocking and alerting on file, registry and removable device use.
- Monitoring, blocking and alerting on registry and file changes associated with spyware/virus infection activities.

for a group of client systems. Policy management is a two step process where:

- 1 Individual policy items (rule sets) are created that specify:
  - What is to be monitored, and
  - Actions to perform when policy rule processing results in a TRUE condition.

Policy items are created for file management, active protection (registry management), device management, Windows Event log monitoring, and spyware/virus infection protection.

- 2 One or more policy items are added to a system policy that:
  - Defines the client systems to monitor, and
  - Includes one or more policy items.

One or more system policies can be created that include one or more client systems.

## Rule Processing

Rules are given a priority value which designates the processing order. Rules are processed within the set in a “top-down” order in this manner:

- 1 Rule with priority level of “1” (rule one) is processed first.
- 2 Monitored activity is matched to rule criteria.
  - If the monitored activity *meets* rule criteria (i.e., rule processing = TRUE), rule processing stops and selected actions are applied. No other rules are processed.
  - If the monitored activity *does not meet* rule criteria (i.e., rule processing = FALSE), rule processing proceeds to the next rule.
- 3 While rule processing = FALSE, rule processing continues to the next rule in priority order until all rules in the policy item are processed.

Upon installation, one system policy is created by default: Default Policy. This policy does not include any client systems or policy items.

By default, a new client system is automatically added to the Default Policy (system policy). This is controlled with the Automatically add new client to the 'Default' system policy option on the Settings tab of the Options dialog (Tools > Options). Clear this option if you want to manually add new client systems to system policies.

Use the following Quick Steps to set up policy items and system policies. Refer to the DynaComm PointGuard Online Help or DynaComm PointGuard Administrator Guide for more information on each of these procedures.

### Policy Management: Time Intervals

Time Intervals are used by a file management policy or device management policy to specify the days of the week and times of the day that policy actions are performed when rule processing results in a TRUE condition. Three standard time intervals are included at installation time.

#### To list all configured time intervals

- 1 In the left pane, expand Policy Management and then expand Policy Items.
- 2 Expand either File Management or Device Management.
- 3 Select Time Intervals to display all available time intervals in the right pane.

#### To list time interval properties

- 1 In the left pane, expand Policy Management and then expand Policy Items.
- 2 Expand either File Management or Device Management.
- 3 Select Time Intervals to display all available time intervals in the right pane.
- 4 In the right pane, select a time interval and click Edit.

#### To remove a custom time interval

- 1 In the left pane, expand Policy Management and then expand Policy Items.
- 2 Expand either File Management or Device Management.
- 3 Select Time Intervals to display all available time intervals in the right pane.
- 4 In the right pane, select a time interval and click Remove.

#### To add a custom time interval

- 1 In the left pane, expand Policy Management and then expand Policy Items.
- 2 Expand either File Management or Device Management.
- 3 In the left pane, right-click Time Intervals and select Add a New Time Interval.
- 4 In the New Time Interval dialog:
  - a In Name, enter a name for the time interval.
  - b In the day/time grid, clear or select (highlight) time blocks, as needed, using these techniques on an individual block:
    - Left-click to turn on/off whole hour blocks.
    - Use successive right-clicks to turn on/off half- and quarter-hour time periods.
    - Hold down the CTRL key and use successive left-clicks to turn on/off consecutive half- and quarter-hour time periods.

#### Note

*The selected time period is detailed below the grid as you move the cursor over the hour blocks or click inside an hour block.*

- c Click OK.

## Policy Management: Policy Items - File Management

File management policies monitor files, processes, users, file owners and media types with one or more rules. When rule processing results in a TRUE condition, possible actions include blocking access, preventing update, sending an alert to the PointGuard server, and logging session results.

### To add a file management policy

- 1 In the left pane, expand Policy Management and then expand Policy Items.
- 2 Expand File Management.
- 3 Right-click File Policies and select New Policy.
- 4 In the Properties dialog:
  - a In Name, enter a name for the new policy.
  - b In Description, enter a brief description to identify policy contents.
  - c Click OK.

The new policy appears in the right pane.

### To inactivate a rule in a file management policy

- 1 In the left pane below File Policies, select a file policy.
- 2 In the right pane, select a rule and click Edit.
- 3 In the Rule Properties dialog, clear the Active option and click OK.

### To reorder a rule in a file management policy

- 1 In the left pane below File Policies, select a file policy.
- 2 In the right pane, select a rule and click:
  - Up to move the rule up in the rule list and increase the priority level.
  - Down to move the rule down in the rule list and decrease the priority level.

### To add a rule to a file management policy

- 1 In the left pane below File Policies, select a file policy.
- 2 In the right pane, click Add.
- 3 In the Rule Properties dialog:
  - a In Name, enter a name for the rule.
  - b In Description, enter a brief description to identify rule contents.
  - c On the Files tab, select files to include and exclude in the monitoring activities.
  - d On the Processes tab, select processes to include and exclude in monitoring activities.
  - e On the Users tab, select users to include and exclude in monitoring activities.
  - f On the File Owners tab, select file owners to include and exclude in monitoring activities.
  - g On the Media tab, select media types to include in monitoring activities.
  - h On the Time tab, select a time interval to specify days and times to apply rule actions when rule processing results in a TRUE condition.
  - i On the Action tab, select actions to perform when rule processing results in a TRUE condition.
  - j Click OK.

The new rule appears in the right pane of the file management policy window.

### Policy Management: Policy Items - Device Management

Device management policies monitor the use of removable devices with one or more rules. When rule processing results in a TRUE condition, possible actions include blocking access to the device, sending an alert to the user using the device, and sending an alert to the PointGuard console.

#### To add a device management policy

- 1 In the left pane, expand Policy Management and then expand Policy Items.
- 2 Expand Device Management.
- 3 Right-click Device Policies and select New Policy.
- 4 In the Properties dialog:
  - a In Name, enter a name for the new policy.
  - b In Description, enter a brief description to identify policy contents.
  - c Click OK.

The new policy appears in the right pane.

#### To inactivate a rule in a device management policy

- 1 In the left pane below Device Policies, select a device policy.
- 2 In the right pane, select a rule and click Edit.
- 3 In the Rule Properties dialog, clear the Active option and click OK.

#### To reorder a rule in a device management policy

- 1 In the left pane below Device Policies, select a device policy.
- 2 In the right pane, select a rule and click:
  - Up to move the rule up in the rule list and increase the priority level.
  - Down to move the rule down in the rule list and decrease the priority level.

#### To add a new rule to a file management policy

- 1 In the left pane below Device Policies, select a device policy.
- 2 In the right pane, click Add.
- 3 In the Rule Properties dialog:
  - a In Name, enter a name for the rule.
  - b In Description, enter a brief description to identify rule contents.
  - c On the Devices tab, select devices to include and exclude in the monitoring activities.
  - d On the Users tab, select users to include and exclude in monitoring activities.
  - e On the Time tab, select a time interval to specify days and times to apply rule actions when rule processing results in a TRUE condition.
  - f On the Action tab, select actions to perform when rule processing results in a TRUE condition.
  - g Click OK.

The new rule appears in the list of rules in the right pane of the policy window.

#### To remove a rule from a device management policy

- 1 In the left pane below Device Policies, select a device policy.
- 2 In the right pane, select a rule and click Remove.
- 3 In the message confirmation dialog, click Yes.

## Policy Management: Policy Items - Active Protection

Active protection policies monitor 14 areas of the Windows Registry that are most often affected when programs are installed or removed. Creating Active Protection rules includes listing the Registry areas to monitor and choosing to block the changes, alert the user to the change attempts, or allow the user to override the blocking action when rule processing results in a TRUE condition.

### To add an Active Protection policy

- 1 In the left pane, expand Policy Management and then expand Policy Items.
- 2 Expand Active Protection.
- 3 Right-click Active Protection and select New Policy.
- 4 In the Properties dialog:
  - a In Name, enter a name for the policy item.
  - b In Description, enter a brief description to identify the policy contents.
  - c Click OK.
- 5 In the right pane, click Add.
- 6 In the Real-time Protection Settings dialog:
  - a Select all areas that are to be blocked.  
Use the Ctrl and Shift keys to select consecutive and contiguous protected areas, respectively.
  - b Clear the Block changes to selected items option if the policy is only to monitor activity.
  - c Clear the Alert local user option if the user is not to receive notification on the client of the attempted change.
  - d Click OK.

### To edit an Active Protection policy

- 1 In the left pane, expand Policy Management and then expand Policy Items.
- 2 Expand Active Protection and then expand Active Protection Policies.
- 3 In the left pane, select an active protection policy to list protected areas and actions included in the policy in the right pane.
- 4 In the right pane, select a protected area and click Edit.
- 5 In the Real-time Protection Settings dialog:
  - a Select or clear the Block changes to selected items option, as needed.
  - b Select or clear the Alert local user option, as needed.
  - c When all changes are complete, click OK.

### To remove an Active Protection policy

- 1 In the left pane, expand Policy Management and then expand Policy Items.
- 2 Expand Active Protection and then expand Active Protection Policies.
- 3 In the left pane, right-click an active protection policy and select Remove.
- 4 In the right pane, select a protected area and click Edit.
- 5 In the verification message dialog, click Yes.

### Policy Management: Policy Items - Eventlog Monitoring

Eventlog Monitoring policies monitor for selected entries made to the various Windows Event logs. Possible actions include ignoring the entry occurrence, or sending an alert to the server when the selected entry occurs.

#### To add an Eventlog Monitoring policy

- 1 In the left pane, expand Policy Management and then expand Policy Items.
- 2 Select Eventlog Monitoring.
- 3 In the right pane, click Add.
- 4 In the General Properties dialog:
  - a In Event Filter Name, enter a name for the policy item.
  - b In Description, enter a brief description to identify the policy contents.
  - c Click OK.
  - d In the Start From an Existing Filter dialog, click No.
- 5 In the Event Filter Properties dialog:
  - Add filters (rules) with the New function.
  - Reorder filters with the Move Up and Move Down functions.
  - Remove filters with the Delete function.
- 6 When all filters have been set up, click OK.
- 7 In the Event Filter Properties dialog, click Save.

#### To reorder a filter (rule) in an Eventlog Monitoring policy

- 1 In the left pane, select Eventlog Monitoring.
- 2 In the right pane, select a policy and click Edit.
- 3 In the Event Filter Properties dialog, select a rule and click:
  - Move Up to move the rule up in the rule list and increase the priority level.
  - Move Down to move the rule down in the rule list and decrease the priority level.

#### To add a filter (rule) to an Eventlog Monitoring policy

- 1 In the left pane below Policy Items, select Eventlog Monitoring.
- 2 In the right pane, select a policy and click Edit.
- 3 In the Event Filter Properties dialog, click New.
- 4 In the Event Filter Criteria dialog:
  - a Select an action to perform when filter evaluation results in a TRUE condition.
  - b Set up filter criteria:
    - If all Event Log entries are to be monitored, click OK in the Event Filter Criteria dialog.
    - If specific Event Log entries are to be monitored:
      - (1) Clear the Match all events option.
      - (2) Click Add.
      - (3) In the Edit Selected Criterion group:
        - Select a Search Type.
        - Select a Search Element.
        - Enter a string in Search Pattern.
      - (4) Click Update.
  - c Click OK.
- 5 In the Event Filter Properties dialog, reorder the filter, if needed.
- 6 Click Save.

## Policy Management: Policy Items - Spyware/Virus Protection

Spyware/virus policies use definitions in the Threat database to monitor registry changes and file use for possible spyware/virus infection attempts. Policy actions can alert and/or block suspect activities.

### To add a spyware/virus protection policy

- 1 In the left pane, expand Policy Management and then expand Policy Items.
- 2 Select Spyware/Virus Protection.
- 3 In the right pane, click Add.
- 4 In the Sunbelt Protection Policy Settings dialog:
  - a In Item Name, enter a name for the policy item.
  - b In Comments, enter a brief description to identify the policy contents.
  - c In Settings:
    - (1) Enable (apply check mark) one or both of the following:
      - Enable Spyware/Virus Protection.
      - Enable System Settings Protection.
    - (2) Enable (apply check mark) one or both of the following:
      - Automatically clean infected items.
      - Alert user of threats.
  - d Click OK.
- 5 Click OK to respond to the warning message.

### To edit a spyware/virus protection policy item

- 1 In the left pane, expand Policy Management and then expand Policy Items.
- 2 Select Spyware/Virus Protection.
- 3 In the right pane, select a spyware/virus protection policy item and click Edit.
- 4 In the Sunbelt Protection Policy Settings dialog, do one or more of the following as needed:
  - In Item Name, modify policy item name.
  - In Comments, modify the policy item description.
  - Enable/disable settings and sub-settings.
- 5 In the Sunbelt Protection Policy Settings dialog, click OK.
- 6 Click OK to respond to the warning message.
- 7 Click Save on the toolbar.

If the policy item is included in a system policy, a message appears asking to publish the system policy when the save is complete.
- 8 To respond to the save message, do one of the following:
  - To make policy item changes immediately effective on client systems, click Yes.
  - To preserve system policy functions as is, click No.

#### Note

*Until the changed policy item is published, the save message appears each time Save is clicked.*

### Policy Management: System Policies

Now that you have created policy items to monitor selected files, registry entries, and more, you are ready to place the policy items into a system policy which you will then publish to a group of client systems. At this point, monitoring begins and actions are performed when a TRUE condition results from rule processing.

#### STOP!

*We strongly recommend that you **publish your first system policy to a small group of client systems**. This allows you the opportunity to observe the effects and results of your policy items on both client s and server, and to make changes before a larger installation is attempted.*

#### To add a system policy

- 1 In the left pane, expand Policy Management and select System Policies.
- 2 In the right pane, click Add.
- 3 In the System Policy dialog, enter a name for the new policy and click OK.
- 4 On the Policy Information tab below the Policy Items list, click Add.
- 5 In the Available Policy Items dialog, select a policy item and click OK.
- 6 For each policy item that is to be included in the system policy, repeat steps 4 and 5.
- 7 If an Active Protection policy item is included in the system policy, select or clear options in the Client User Interface Settings group, as needed.
  - a To display alerts on the client system, select Enable client user interface and choose an alert type from the drop-down list.  
Default: Enabled.
  - b To allow users to override the action taken on registry entries, select the Allow the user to override active protection option.  
Default: Disabled.  
  
If needed, set up a password that the user must supply before the override takes effect by enabling the Require a password to override protection option and entering the password in the supplied area.
  - c To include sound with the client alert, select the Enable sound notification option.  
Default: Enabled.
- 8 Click the Clients tab and click Add to display the Computer Selector dialog.
- 9 Using the upper left and right panes, select one or more client systems and then click Add Checked Items in the right pane to list all selected systems in the Selected Items list in the lower pane. Remove and add clients until the Selected Items list reflects all client systems that are to be included in the system policy client group.
- 10 In the Computer Selector dialog, click OK.

**Policy Management: System Policies, *continued***

**To publish a system policy**

- 1 In the left pane, expand Policy Management and then expand System Policies.
- 2 Below System Policies, select one policy.
- 3 In the right pane on the Policy Information tab, click Publish Policy.
- 4 If prompted, save policy changes by clicking Yes in the confirmation dialog.

**To retrieve all logs from all client systems included in a system policy**

- 1 In the left pane, expand Policy Management and then select System Policies.
- 2 In the right pane, right-click one policy and select Retrieve Logs.
- 3 In the right pane, click the Clients tab.
- 4 Select a client listing and click Retrieve Logs.

**To retrieve an individual log from a client system**

- 1 In the left pane, expand Policy Management and then expand System Policies.
- 2 In the left pane below System Policies, select one policy.
- 3 In the right pane, click the Clients tab.
- 4 Select a client listing and click Retrieve Logs.

**To add a policy item to a system policy**

- 1 In the left pane, expand Policy Management and then expand System Policies.
- 2 In the left pane below System Policies, select one policy.
- 3 In the right pane on the Policy Information tab, click Add.
- 4 In the Available Policy Items dialog, select a policy item and click OK.
- 5 To make the added policy item effective immediately, click Publish Policy.
- 6 In the confirmation dialog, click Yes to save changes to the system policy.

**To remove a policy item from a system policy**

- 1 In the left pane, expand Policy Management and then expand System Policies.
- 2 In the left pane below System Policies, select one policy.
- 3 In the right pane on the Policy Information tab, select a policy item from the Policy Items list and click Remove.
- 4 In the Available Policy Items dialog, select a policy item and click OK.
- 5 To make the system policy changes effective immediately, click Publish Policy.
- 6 In the confirmation dialog, click Yes to save changes to the system policy.

### Quick Steps for System Events

Several PointGuard functions include, by default or by manual set up, system alerts which are displayed in system event windows in the console. For example, plug-in installations and removals are shown in the Administration system event window by default. To send alerts to the File Management window for activities that match file management policy criteria, the Alert Server option on the Action tab of the Rule Properties dialog must be enabled for a file policy rule.

#### To display a real-time view of all system events for the last 5 minutes

- In the left pane, select System Events.

#### To view details for all system events

- 1 In the left pane, select System Events.
- 2 In the right pane, click Details.

#### To view details for a system event by day range

- 1 In the left pane, expand System Events and then select a system event window.
- 2 In the right pane, select a day range in the Range drop-down list.

#### To view details for a system event by date range

- 1 In the left pane, expand System Events and then select a system event window.
- 2 In the right pane:
  - a In the Range drop-down list, select Between.
  - b In From, enter a beginning range date or use the drop-down calendar to choose a date.
  - c In To, enter an ending range date or use the drop-down calendar to choose a date.

#### To run a Summary of Notifications report

- 1 In the left pane, expand System Events and then select a system event window.
- 2 In the right pane, use the display filter controls to display the data that is to be included in the report.
- 3 Click Run Report.

#### To purge alert records

- 1 In the left pane, expand System Events and then select a system event window.
- 2 In the right pane, click Purge.
- 3 In the Purge dialog, select one alert type and specify a day range, if available.
- 4 Click OK.

## Quick Steps for Reports

After running scans and retrieving logs from system policy sessions, data is available for reporting on file, registry, and spyware scans, and on system policies that include a file management policy item. Over 80 standard reports are included in PointGuard. These reports can be used as is, modified, or copied and then modified. Each standard report is based on a report type which is simply a set of select data. Custom reports can also be created using a report type as a template.

Standard reports are run on-demand through Reports in the left pane of the console interface or with a right-click selection in the right-pane of a spyware scan, file scan or registry scan window. On-demand reports can be exported to a file and then saved to a file server or sent as an e-mail attachment. A report can also be run as a task in a scheduled job.

### To add a custom report

- 1 In the left pane, expand Reports and then expand one of the four report classes.
- 2 In the left pane, right-click a report group and select Add Report.
- 3 In the Add New Report dialog:
  - a In Report, enter a name for the report.
  - b In the Scan Name/Computer Groups list, select a file scan/computer group.
  - c To specify the log file to use, either accept the default (most recent log file) or clear the Use Most Recent Log File option and select a log in the Logs list.
  - d In Report Type, select a standard report type.
  - e Click OK.
- 4 In the Report Properties dialog, click each tab and:
  - Select or clear options.
  - Enter required information.
  - Make one or more selections on provided lists.
- 5 In the Report Properties dialog, click OK.

### To run a report on demand

#### Note

*The first time a report is run, a file scan or system policy log file must be associated with the report.*

- 1 In the left pane, expand Reports and then expand one of the four report classes.
- 2 In the left pane, select a report group below a report classification.
- 3 In the right pane, select a report and click Run.
- 4 If this is the first time that the report is run:
  - a Click OK to respond to the displayed message.
  - b In the Report Properties dialog on the General tab:
    - (1) Select a file scan/computer group and a log file, if needed.
    - (2) Make other changes on the other tabs, if needed.
    - (3) Click OK.
- 5 Preview the report in the report viewer window using viewer functions and then choose one of the following:
  - Close the report viewer window.
  - Print the report.
  - Export the report to a file.

### Quick Steps for Scheduling

Scheduled jobs include one or more tasks for running reports, running scans, performing database updates (Spyware and Categories), and removing scan result logs. Jobs can be scheduled to run once, daily, weekly or monthly.

#### To add a new scheduled job

- 1 In the left pane, select Scheduling.
- 2 In the right pane, click Add.
- 3 In the Run as User Account dialog:
  - a In Enter User Account, enter the user account to run the task under.
  - b In Password, enter the associated password.
  - c In Password to Confirm, re-enter the password and click OK.
- 4 In the Job Scheduler dialog:
  - a On the General tab, enter a name for the job and select or disable options, as needed.
  - b On the Schedule tab:
    - (1) Select the job occurrence frequency, job start time and start date.
    - (2) Select a job end date, and weekly and monthly options when appropriate.
  - c On the Task List tab:
    - (1) Click Add to display all available tasks, enable tasks and click OK.
    - (2) Rearrange task order with Move Up and Move Down.
  - d On the Notification tab:
    - (1) Enable the E-mail option and enter all e-mail addresses to receive job end notification.
    - (2) Enable the Event Log option and select the job end status to record.
  - e Click OK.

#### To change task priority in a scheduled job

- 1 In the left pane, select Scheduling.
- 2 In the right pane, select a scheduled job and click Edit.
- 3 In the Job Scheduler dialog, click the Task List tab.
- 4 In the list of tasks, select a task and:
  - Click Move Up to move the selected task up in the order of execution.
  - Click Move Down to move the selected task down in the order of execution.
- 5 Click OK.

#### To disable a scheduled job

- 1 In the left pane, select Scheduling.
- 2 In the right pane, select a scheduled job and click Edit.
- 3 On the General tab, select Disable (apply check mark).
- 4 Click OK.

## Index

### Symbols

.MSI client package 4, 7, 9, 10

### A

Active Directory 4, 9, 10  
 policy refresh 10

Active Directory Users and Computer window 10

Add New Report dialog 29

Add/Remove Programs selection (Control Panel) 5

administrator privileges, local 4, 5

administrator, PointGuard 7

alerting 1, 19, 21, 22, 23, 24, 26, 28

authorization

for PointGuard 6

logon used 6

to use PointGuard 6

Authorized Access dialog (Setup) 6

Available Policy Items dialog 27

### C

Choose Destination Location dialog (Setup) 6

cleaning spyware/virus infections 16

client communications 2, 7, 10

client deployment 9–10

Active Directory 4, 9, 10

FTP server 4

methods 4, 9, 10

PointGuard console 4

web site 4

Client Management dialog 1, 9

client systems 2, 4, 7, 8, 9, 10, 27

configure 8

deployment 9–10

requirements 3

components, PointGuard 1

client systems 3

server 3

Computer Selector dialog 16, 26

configuration

Active Protection policies 23

device management policies 19, 20, 22

event log monitoring policies 19, 24, 25

file management policies 19, 20, 21

file scan 12, 14

policy items 1, 21–24

registry scan 12, 15

reports 29

scheduled jobs 30

spyware/virus scan 16

system policies 26

configuration topic

Active Protection (Policy Items) 23

Categories 12

Definitions 17

Device Management (Policy Items) 22

Eventlog Monitoring (Policy Items) 24

File Management (Policy Items) 21

File Scans 14

File Types 13

Plug-in Manager 8

Policy Management 19

Quarantine Management 18

Registry Scans 15

Reports 29

Scheduling 30, 31

Spyware/Virus Protection (Policy Items) 25

Spyware/Virus Scans 16

System Events 28

System Policies 26

Time Intervals 20

configuration, PointGuard

initial, client systems 8

initial, server 7

topics 1

Control Panel, Windows 5

## Quick Start

---

- D**
  - database updates
    - scheduled job task 12, 13, 17, 30
  - databases
    - Categories and File Types 11, 12, 13
    - Threat (spyware/virus) 11, 16, 17, 25
  - Default Policy (system) 19
  - deployment, client package 4, 9
    - methods 10
  - disk storage requirements 3
  - DomainName Properties dialog (Active Directory) 10
- E**
  - e-mail message
    - client deployment 10
    - sending reports 29
  - endpoints, server 7, 9
  - Enter New Client Name dialog 9
  - Enter User Information dialog (Setup) 6
  - evaluation version 6
  - Event Filter Criteria dialog 24
  - Event Filter Properties dialog 24
  - Event log, Windows 1, 19, 24
- F**
  - file scan properties dialog 14
    - Actions tab 14
    - File Filter tab 14
    - File Scan tab 14
  - file scans
    - configuration 12
    - quarantining 18
    - reporting 29
    - reports 29
    - run results 14
    - scheduled job tasks 30
  - file signatures 12, 17
  - File Signatures dialog 12
  - File Type dialog 13
  - file type extensions 13
  - File Type Group dialog 13
  - file types 13
  - FutureSoft web site 5, 12
- G**
  - General Properties dialog 24
- I**
  - installation
    - CD Auto-run 5
    - client 4, 9–10
      - automatic 9
      - manual 8, 9
    - evaluation version 6
    - licensed version 6
    - logon 5
    - server 4–6
    - Setup program 5
  - InstallShield Wizard Complete dialog (Setup) 6
  - IP address
    - public 3
    - server 7
- J**
  - Job Scheduler dialog 17, 30
- K**
  - Keyword/Phrase for dialog 12
  - keywords 12, 14
- L**
  - License Agreement dialog (Setup) 6
  - Listening Service Account dialog (Setup) 6
  - Listening service, PointGuard 4
  - Log Import dialog 12
  - logon, installation 5
  - logs, retrieving 27
- M**
  - mail server 7
  - memory requirements 3
  - menu, Tools 8, 9, 12, 13, 17
  - Microsoft IIS 3
    - Web Services 4
  - mobile systems, using 7

**N**

network  
 endpoints 7  
 internal 4  
 IP address 4  
 public interface 4  
 traffic 8  
 network connectivity 3  
 New Category dialog 12  
 New File Scan wizard 14  
 New Time Interval dialog 20

**O**

on-demand functions  
 database updates 12, 13, 17  
 file scans 1, 14  
 registry scans 1, 15  
 reports 29  
 spyware/virus scans 1, 16  
 Open dialog (Windows) 12  
 opening PointGuard 7  
 Options dialog 7, 8, 9, 10, 18, 19

**P**

Plug-in Settings dialog 8  
 plug-ins, client 1, 8  
 removal 8  
 policies 1  
 alerting in 19  
 blocking in 19  
 monitoring in 19  
 policy items  
 actions 19  
 Active Protection 23, 26  
 blocking changes 23, 25  
 blocking in 22  
 device management 20, 22  
 file management 21, 29  
 file policy 20  
 overriding blocking action 23, 26  
 rule processing 20, 22  
 sending alerts 21, 22, 23, 24, 25  
 spyware/virus protection 25  
 program group, DynaComm PointGuard 7  
 Properties dialog 21, 22, 23

**Q**

quarantine  
 data 1  
 files 18  
 items 18  
 quick steps  
 for Content Management 11–17, ??–17  
 for Policy Management 19–27  
 for Quarantine Management 18  
 for Reports 29  
 for Scheduling 30  
 for System Events 28  
 To add a custom file type extension 13  
 To add a custom file type group 13  
 To add a custom report 29  
 To add a custom time interval 20  
 To add a device management policy 22  
 To add a file management policy 21  
 To add a file scan configuration 14  
 To add a file signature 12  
 To add a filter (rule) to an Eventlog Monitoring policy 24  
 To add a keyword/keyword phrase 12  
 To add a new category 12  
 To add a new rule to a file management policy 22  
 To add a new scheduled job 30  
 To add a policy item to a system policy 27  
 To add a registry scan configuration 15  
 To add a rule to a file management policy 21  
 To add a spyware/virus protection policy 25  
 To add a spyware/virus scan configuration 16  
 To add a system policy 26  
 To add an Active Protection policy 23  
 To add an Eventlog Monitoring policy 24  
 To automatically install a client system with a scan 9  
 To change task priority in a scheduled job 30  
 To clear the new client auto-install option 8  
 To clear the plug-in auto-install option 8  
 To disable a scheduled job 30  
 To display a real-time view of all system events for the last 5 minutes 28  
 To edit a spyware/virus protection policy item 25  
 To edit an Active Protection policy 23  
 To filter displayed quarantine items 18  
 To inactivate a rule in a device management policy 22  
 To inactivate a rule in a file management policy 21

## Quick Start

---

- To inactivate a spyware/virus definition 17
  - To list all configured intervals 20
  - To list time interval properties 20
  - To manually install a client system 9
  - To manually retrieve Categories and File Types database updates 12, 13
  - To manually retrieve Threat database updates 17
  - To move an existing file type to a different file type group 13
  - To perform initial server configuration 7
  - To publish a system policy 27
  - To purge alert records 28
  - To remove a custom time interval 20
  - To remove a plug-in from the Plug-in Manager 8
  - To remove a policy item from a system policy 27
  - To remove a rule from a device management policy 22
  - To remove an Active Protection policy 23
  - To remove one or more items from a quarantine file 18
  - To reorder a filter (rule) in an Eventlog Monitoring policy 24
  - To reorder a rule in a device management policy 22
  - To reorder a rule in a file management policy 21
  - To restore one or more items from a quarantine file 18
  - To retrieve all logs from all client systems included in a system policy 27
  - To retrieve an individual log from a client system 27
  - To retrieve one or more items from a quarantine file 18
  - To retrieve Threat database updates through a scheduled job 17
  - To run a file scan 14
  - To run a registry scan 15
  - To run a report on demand 29
  - To run a report with file scan results 14
  - To run a report with registry scan results 15
  - To run a spyware/virus scan 16
  - To run a Summary of Notifications report 28
  - To stop a running file scan 14
  - To stop a running registry scan 15
  - To use Active Directory to deploy client systems 10
  - To view a list of spyware/virus definitions 17
  - To view all clients with quarantine files 18
  - To view all file type extensions included in a file type 13
  - To view all file type groups 13
  - To view all items in all quarantine files 18
  - To view all quarantine files stored on a client system 18
  - To view all run results for a defined file scan 14
  - To view all run results for a defined registry scan 15
  - To view all run results for a defined spyware/virus scan 16
  - To view details for a system event by date range 28
  - To view details for a system event by day range 28
  - To view details for all system events 28
  - To view details of a spyware/virus definition 17
  - To view run-result details for a defined file scan 14
  - To view run-result details for a defined registry scan 15
  - To view run-result details for a defined spyware/virus scan 16
- ## R
- real-time functions
    - Active Protection policies 1, 23
    - Device Management policies 1, 22
    - Eventlog Monitoring policies 1, 24
    - File Management policies 1, 21
    - Spyware/Virus Protection policies 25
  - rebooting 10
  - registry entries 17, 26
  - Registry Scan Properties dialog 15
  - registry scans
    - configuration 12, 15
    - reporting 29
    - run results 15
  - Registry, Windows 11, 23
    - entries 12
  - removable device monitoring 19
  - Report Properties dialog 29
  - reports
    - custom 29
    - exporting 29
    - file scan 14
    - on-demand 1
    - registry scan 15
    - report type 29
    - saving 29
    - scheduled 1, 30
    - sending 29
    - standard 29
  - Rule Properties dialog 21, 22, 28

## rules

- creating 21, 22, 23, 24
  - overview 1
  - reordering in policy 21, 22
  - rule processing 21, 23, 24, 26
- Run as User Account dialog 30
- Run dialog (Windows) 5

**S**

- scans, result listings 1, 14, 15, 16
- scheduled jobs 1, 12, 13, 17, 30
- reports 29
  - tasks 17
- security settings
- DynaComm PointGuard Users group 6
- Select Program Folder dialog (Setup) 6
- Serial Number field (Enter User Information) 6
- Server Endpoints group (Options dialog) 7
- server, PointGuard 1, 9, 21, 26
- endpoints 7, 10
  - firewall 4
- settings
- client systems 9, 19
  - e-mail 7
  - Plug-in Manager 8
  - quarantine time to live 18
  - server endpoints 7, 9, 10
- Setup Status dialog (Setup) 6
- spyware/virus definitions 17
- spyware/virus infection 18, 25
- Spyware/Virus Scan Properties dialog 16
- spyware/virus scans
- quarantining 18
  - reporting 29
  - run results 16
  - scheduled job tasks 30
- Sunbelt Protection Policy Settings dialog 25
- system alerts 28
- system policies 26
- adding client systems 19
  - policy items 19
  - publishing 26
  - reporting on 29
  - sending alerts 26
- System Policy dialog 26
- system policy session, retrieving logs 29
- system requirements 3
- Systems Management Server 4

**T**

- TCP port exception 4
- Threat database (spyware/virus) 11, 16, 17, 25
- time interval
- day/time grid 20
  - using 21, 22

**W**

- web site, deployment from 10
- Welcome dialog (Setup) 6
- window, system event 1
- Administration 28
  - File Management 28
- Windows 2000 3
- Windows 2003 3
- Windows 2003 Server 3
- Windows Event log entries 19
- Windows Event logs 24
- Windows Networking Client 4
- Windows Print and File Sharing 4
- Windows VISTA Business 3
- Windows VISTA Ultimate 3
- Windows XP 3
- wizard, New File Scan 14

