

---

# *DynaComm PointGuard*<sup>™</sup>

## **Administrator Guide**

---

2007 by FutureSoft, Inc. All rights reserved.

## DynaComm PointGuard Administrator 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 PointGuard 1.0.0.0

Document #E-AG-DCPG-P033007  
Revised 073107

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

Printed in the USA.

1.800.989.8908

[info@futuresoft.com](mailto:info@futuresoft.com)  
<http://www.futuresoft.com>

# Contents

## Chapter 1

### *Welcome*

This Guide .....	2
Technical Library .....	3
Technical Support .....	3

## Chapter 2

### *Understanding DynaComm PointGuard*

What DynaComm PointGuard Can Do .....	6
How DynaComm PointGuard Works .....	7
System Requirements .....	18

## Chapter 3

### *Installing DynaComm PointGuard*

Installation Procedure .....	20
Setup Maintenance .....	27

## Chapter 4

### *Basic Configuration*

Initial Configuration Tasks .....	32
Working with the Console .....	34
Managing Client Systems .....	39
Saving and Pushing Configuration Changes .....	42

## Chapter 5

### *Managing Files & Registry Content*

Categories .....	44
File Types .....	46
File Scans .....	47
Registry Scans .....	52
System Scans .....	56
Quarantine Management .....	59
Details .....	60

## Table of Contents

---

### Chapter 6

#### *Managing Client Activities*

System Policies .....	62
Policy Items .....	64
Time Intervals .....	71

### Chapter 7

#### *Protecting Client Systems*

Spyware Protection .....	74
--------------------------	----

### Chapter 8

#### *Alerting*

System Events .....	84
Server Alerts .....	85

### Chapter 9

#### *Reporting & Scheduling*

Reports .....	94
Scheduling .....	99

# Appendices

## Appendix A

### *Predefined Categories*

Table A.1 Predefined Categories .....	102
Table A.1 Predefined Categories, continued .....	104

## Appendix B

### *Predefined File Types*

Table B.1 Predefined File Types .....	106
---------------------------------------	-----

## Appendix C

### *Predefined Reports*

Table C.1 Details Reports .....	114
Table C.2 Drill-down Reports .....	115
Table C.3 Scan Errors Reports .....	117
Table C.4 Summary Reports .....	118
Table C.5 Files Reports .....	119
Table C.6 Machines Reports .....	124
Table C.7 Processes Reports .....	126
Table C.8 Users Reports .....	127
Table C.9 Details Reports .....	129
Table C.10 Drill-down Reports .....	130
Table C.11 Summary Reports .....	131

## Appendix D

### *Predefined Rules & Policy Items*

Table D.1 Block Malware Installations Via Browsers Rule Set .....	134
Table D.2 Sample Rules Rule Set .....	135

## Table of Contents

---

### Appendix E

#### *Predefined System Scans*

Application Inventory System Scan .....	146
Application Lockdown System Scan .....	146
Inappropriate Content System Scan .....	148
Instant Messaging System Scan .....	149
Internet Access Management	
System Scan .....	150
Network Shared Folders .....	151
P2P File Sharing System Scan .....	151
Suspected Pornographic Images	
System Scan .....	153
System Information System Scan .....	153
USB Devices System Scan .....	154

### Appendix F

#### *Predefined Time Intervals*

Table F.1 Predefined Time Intervals .....	156
---	-----

### Appendix G

#### *Sunbelt Threat Database Descriptions*

Table G.1 Sunbelt Threat Database Threat Level Descriptions .....	158
Table G.2 Sunbelt Threat Database Infection Type Descriptions .....	159

### Appendix H

#### *Active Directory Deployment of the DynaComm PointGuard Client*

Deploying the DynaComm PointGuard Client via Active Directory	162
---	-----

### Index

---

# Chapter 1

*Welcome*

---

### This Guide

DynaComm PointGuard is a member of the DynaComm i:series suite of products that supports activities used to ensure responsible use of corporate resources. This manual provides:

- General overview of how the product works with discussions of important considerations for installation and use of the product.  
(Chapter 2)
- Detailed procedures and notes for installation of this product.  
(Chapter 3)
- Review of configuration basics and basic client system management  
(Chapter 4)
- General procedures for creating file scans and registry scans to manage file and Registry contents  
(Chapter 5)
- General discussion of system policies, policy items and procedures for creating and implementing both.  
(Chapter 6)
- Review of spyware scan creation and the procedures for working with scans; includes a discussion of the Threat database and the procedure to update database contents.  
(Chapter 7)
- Detailed discussion of alerting concepts and procedures for file, device, spyware and active protection alerting set up.  
(Chapter 8)
- Review of the reporting and scheduling functions and list of considerations for producing both on-demand and scheduled reports.  
(Chapter 9)

### Other Documentation

For detailed information on all DynaComm PointGuard windows, dialogs, procedures and tasks, see the DynaComm PointGuard Online Reference (Help). For last minute changes to the current release of DynaComm PointGuard, see the Release Notes (readme.txt).

### More Help

For help with specific details of your installation, contact Technical Support.

## Technical Library

The DynaComm PointGuard technical documentation library includes both detailed information as well as overview literature. All electronic material is found in the /docs folder on the installation CD-ROM. The most current copies of all electronic material for DynaComm PointGuard are available 24 hours a day, seven days a week on the FutureSoft web site at:

<http://www.futuresoft.com/support/support.htm>

The DynaComm PointGuard technical library includes the following documents:

- ◆ DynaComm PointGuard Administrator Guide  
Designed for the individual responsible for installing, maintaining and administering DynaComm PointGuard. All overview concepts, software user-interface topics and procedural steps are discussed in detail.  
Document format: PDF file  
(AG\_PointGuard.pdf)
- ◆ DynaComm PointGuard Online Reference  
Designed for the individual who uses the DynaComm PointGuard console; provides detailed procedures and tasks for all administrative functions; includes detailed information for all windows and dialogs.  
Document format: Help system  
(appshell.cnt and appshell.hlp)
- ◆ Release Notes (Readme file)  
Includes last minute release information and items of particular significance for installing and running the product.  
Document format: Text file (readme.txt)

Send questions and comments about DynaComm PointGuard technical documentation to:

[docs@futuresoft.com](mailto:docs@futuresoft.com)

## Technical Support

Before contacting Technical Support, please collect all information regarding your question. This should include hardware and software configurations for all systems with DynaComm PointGuard components, the DynaComm PointGuard version number, any other software running when you experienced the problem, and the exact sequence of steps that preceded the problem.

For prompt and effective service, be sure to provide the following information when contacting us:

Your name  
Company name  
Company address  
Company phone/FAX numbers

Contact us at:

- ◆ Ground: FutureSoft, Inc.  
Technical Support Services  
12012 Wickchester Lane,  
Suite 600  
Houston, Texas 77079-1222
- ◆ E-mail: [support@futuresoft.com](mailto:support@futuresoft.com)
- ◆ Phone: Monday through Friday  
8:00 AM to 5:00 PM (CST)  
281.588.6868  
1.800.261.6357
- ◆ Fax: 1.281.496.1090
- ◆ Web Site: <http://www.futuresoft.com>



---

## Chapter 2

### *Understanding DynaComm PointGuard*

---

This chapter introduces you to the features and functions of DynaComm PointGuard beginning with an overview of components and processes.

Distributed versus non-distributed processing is reviewed. System requirements for both server and client systems are provided.

## What DynaComm PointGuard Can Do

DynaComm PointGuard performs these major functions:

- **Spyware Management**

Spyware scans determine if a client system is infected with adware/spyware parasites. When an infection is detected, the client system can be cleaned with use of the Sunbelt spyware scanner and Sunbelt Software Threat database which are licensed components.
- **File and Registry Scanning**
  - File scans will find files with a specific name or with specific attributes, files of a specific type, or files with questionable content or purpose. Target files can be copied, moved, quarantined or deleted, or file attributes can be modified. Processes associated with target files can be terminated or other scans can be started when a target file is found.
  - File scans include the ability to place matched files in a quarantine file on each client system. Quarantined items can be copied, moved, deleted or restored to their original location.
  - Registry scans will determine current Windows Registry settings, write new registry keys, or remove existing registry keys.
  - System scans take the work out of creating file and registry scans for the most commonly-requested end-point management functions. The New System Scan wizard walks you through the process of selecting the systems to scan and then choosing options for actions to perform. The individual file and registry scans created by the system scan are run by starting the system scan.

- **Policy Management**

Policies are rule sets that control the use of files and USB devices, and control changes to the Windows Registry.

- File Management Policies log file system activities, block access to files, send alerts and messages when a specified event occurs, stop file processes and more.
- Active Protection Policies alert, block or perform both when changes are attempted in selected protected areas of the Windows Registry. Users can be given override control or allowed no interaction with active protection functions.
- Device Management Policies log the addition or removal of a USB device, block or allow access to USB devices and send alerts and messages when a specified event occurs.

- **Reporting**

File scans, registry scans and policy management session log data (real-time) collected during the scan or session. Summary and detailed information for scans and real-time monitor sessions are available through reports displayed on the console, saved to a file or sent to a printer. Standard (predefined) reports are included in DynaComm PointGuard or custom reports can be set up.

- **Scheduling**

Scheduled jobs can include scans to run, reports to generate and database updates to retrieve. A single job can include multiple tasks and can be set to execute on any date and time or on a regular interval, such as, every week, month, etc.

## How DynaComm PointGuard Works

DynaComm PointGuard includes two components:

- Server component
  - Installed with Setup installation program.
  - Installed on Windows 2003 and higher systems. –Includes console interface used to:
    - Set up and maintain all configuration properties.
    - Manage quarantine files and file items.
    - Request and view reports.
    - Set up and maintain scheduled jobs.
  - Includes DynaComm PointGuard listening service which receives messages from client systems during scans, policy management sessions, and client maintenance functions.
  - Includes SQL Express databases that hold administrative and configuration data, scan and session data, and quarantine records.

### Notes

*During execution of a file scan, the console can be closed; the listening service remains active.*

*The console must be closed for scheduled jobs to run.*

- Client component
  - Installed through the console interface.
  - Deployed only to Windows 2003 or higher systems.
  - Includes client service (clientservice.exe).
  - Executes file scan, registry scan and real-time monitor configurations.

### Notes

- ❖ *If a file or registry scan includes a Windows 9.x or NT 4.0 machine, the client component is deployed to the DynaComm PointGuard server machine and non-distributed processing is used.*
- ❖ *NT 4.0 client systems do support file management policies.*
- ❖ *NT 4.0 client systems do not support spyware scans nor active protection policies.*
- ❖ *Installation of “clientservice.exe” is transparent to the client system user.*
- ❖ *The client executable remains on the client system until it is removed through the Client Management dialog (Tools > Client Management).*

## File Scan Processes

Scans run on Windows 2000 and higher systems (NTFS) are called *distributed* scans. The client component is deployed to the client machine. Scan processes run on the client system while the server system runs processes to collect log data.

Scans run against Windows 9.x and NT (FAT) client systems are called *non-distributed* scans. The client component is deployed to and all processes run on the DynaComm PointGuard server system.

When performing a file scan:

- All client systems must be powered on.
- Client Windows 9.x and NT 4.0 systems must have file writing and file sharing enabled.
- Distributed file scans, by default, use the processing power of the target machine (machine being scanned). The Distribute Processing option on the File Scan tab in the *file scan properties* dialog can be cleared to enable use of the processing power of the DynaComm PointGuard server system rather than the client system for Windows 2000 and higher client systems.
- When a file scan configuration includes both Windows 9.x files and Windows NT files:
  - Scans against Windows 9.x and NT 4.0 files run consecutively.
  - Scans against Windows 2000 and higher files run concurrently.
- The time required to complete a scan depends on the number and type of systems that are scanned and the volume of network traffic experienced during the scan.

## Registry Scan Processes

Registry scans are run against Windows 2000 and higher file systems (NTFS), *only*, and run in distributed mode. The client component is deployed to the client machine. Scan processes run on the client system while the server system runs processes to collect log data.

When performing a registry scan:

- All client systems must be powered on.
- Only the predefined keys HKEY\_USERS and HKEY\_LOCAL\_MACHINE, and sub keys can be scanned on a client system.
- If a problem occurs during a registry scan such that the registry should be restored, contact Technical Support Services for help.

## Spyware Scan Processes

Spyware scans are run only in distributed mode and only against Windows 2000 and higher file systems (NTFS). Spyware scans deploy the DynaComm PointGuard client component to the client system. Scan processes run on the client system while the server system runs processes to collect spyware scan log data.

## Policy Management Sessions

Policy management processes monitor Windows 2000 and higher file systems only. These processes deploy the DynaComm PointGuard client component to the client system. Monitor processes run on the client system while the server system runs processes to collect log data.

When performing system policy sessions:

- All client systems must be powered on.
- Only shares on Windows 2000, XP and 2003 systems can be monitored.
- By default, the client service starts automatically when the client component is installed. Monitoring processes begin on machine start up.
- Please be patient! Depending on the number of systems, selected session properties (i.e., volume of logged data), and the volume of network traffic experienced during the log file retrieval, it may take some time for all monitor-session log files to be retrieved and merged.

### Distributed processing on Windows 2000 and higher file systems

In Figure 2.1, the DynaComm PointGuard server component is installed on a Windows 2003 system.

Scans and policy management sessions run on the client Windows XP file system. Quarantined files are stored in the Quarantine folder on the client system. Reports are created with data stored on the server system in various databases.

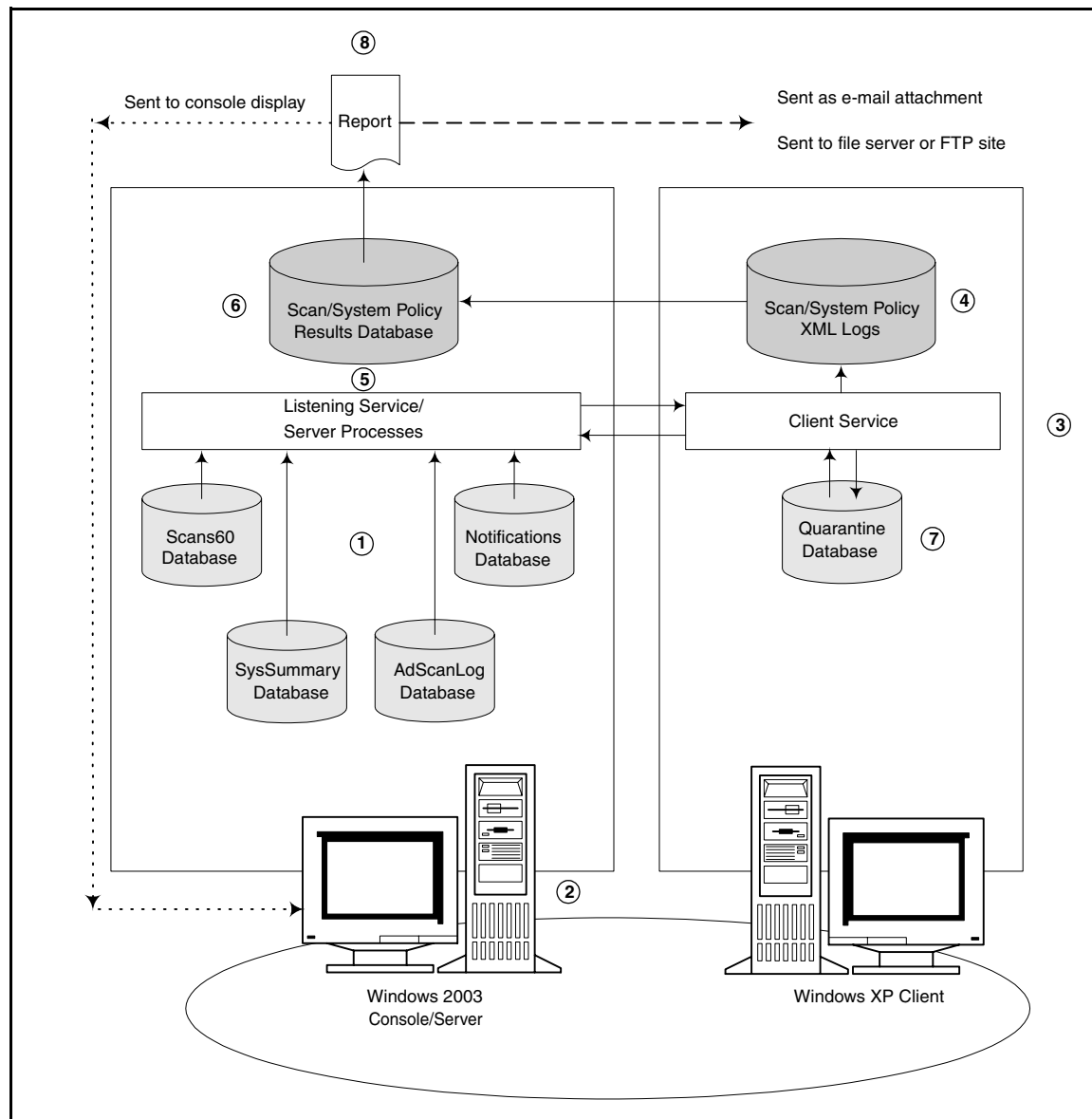


Figure 2.1  
Distributed processes example

Table 2.1 DynaComm PointGuard Distributed Processes Described

Step	Description
①	Scan and real-time configurations are created through the following topics and saved to the respective database on the Windows 2003 console/server system.
②	<p>A scan is started through the console in the File Scans, Registry Scans, System Scans or Spyware Scans topic.</p> <p>A file or device policy session, or active protection session start when the client real-time driver becomes active.</p>
③	<p>The DynaComm PointGuard client service logs on to the client system with the account name that started DynaComm PointGuard on the console. The client component is deployed to the client machine (Windows XP system) and includes:</p> <ul style="list-style-type: none"> <li>• Install of client service.</li> <li>• Copy of scan or session configuration.</li> </ul>
④	<p>The DynaComm PointGuard client service starts the scan or policy management session. Scan or policy processes take place on the client system.</p> <p>Scan data is logged to a corresponding XML file at: \Program Files\Futuresoft\PointGuard\Client\PointGuardShare</p>
⑤	<p>Policy management alert data is sent immediately to the DynaComm PointGuard server system as events occur.</p> <p>Policy management session logs are stored at: \Program Files\Futuresoft\DynaComm PointGuard\RTM.</p> <p>Active protection policy alerts are stored at: \Program Files\Futuresoft\DynaComm PointGuard\RTTP</p>
⑥	When scan processes finish, the client service notifies the listening service on the server.
⑦	The server retrieves XML log files from the client system, converts them to SQL databases, and stores them on the server system.
⑧	When a file scan includes moving or copying files to quarantine, the files are moved or copied from their original location to the client quarantine location on the client system at: \Program Files\Futuresoft\PointGuard\Client\PointGuardShare\Quarantine

Non-distributed processing on Windows 95/98/ME and NT 4.0 file systems

In Figure 2.2, the DynaComm PointGuard server component is installed on a Windows 2003 system. File scans are run against a Windows 95 client file system.

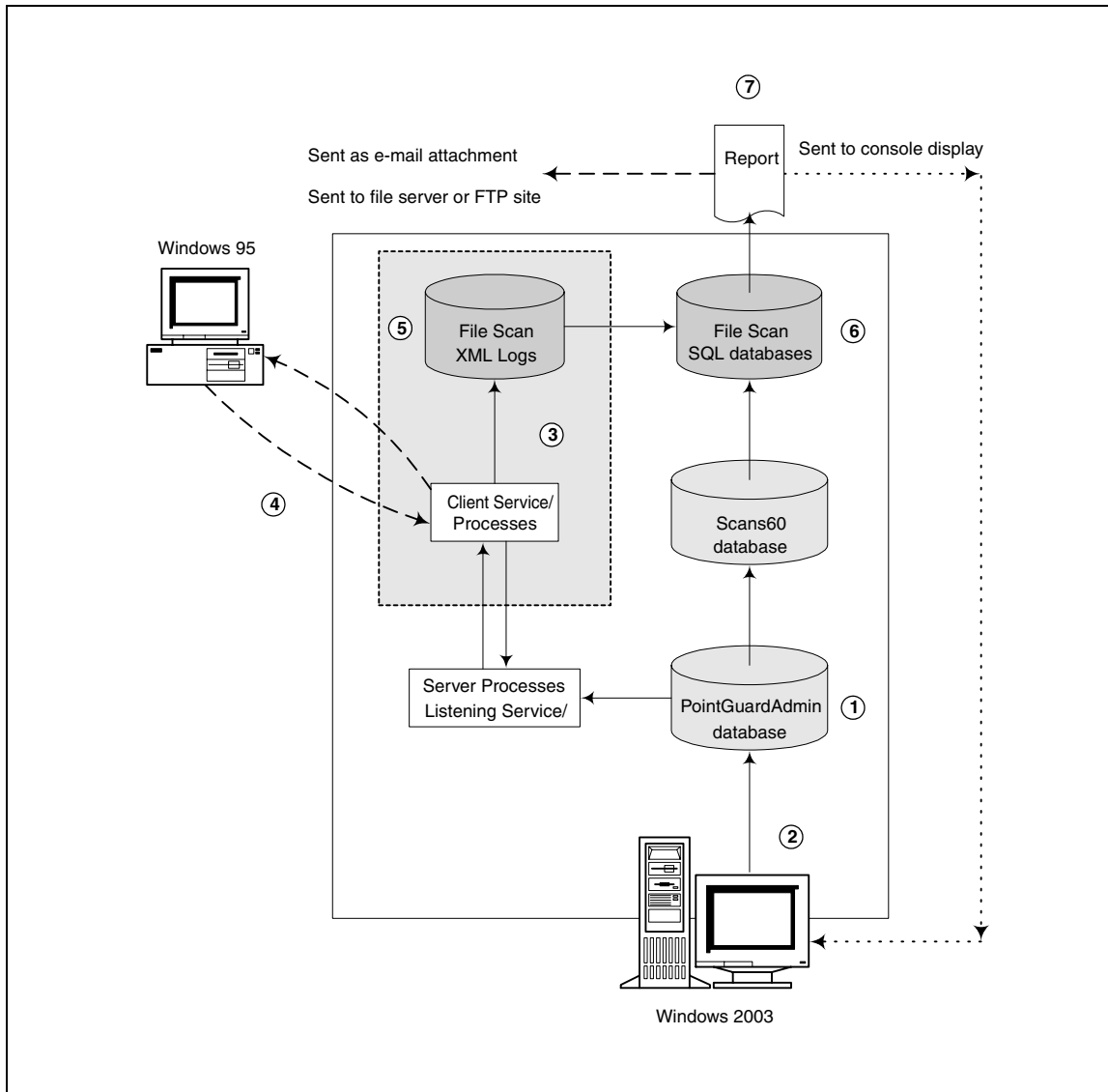


Figure 2.2  
Non-distributed processes example

Table 2.2 DynaComm PointGuard Non-distributed Processes Described

Step	Description
①	File scan configurations are created through the console and saved to the PointGuardAdmin database
②	The file scan is started through the File Scans topic in the console.
③	<p>The DynaComm PointGuard client component is deployed to the DynaComm PointGuard server system (installs PointGuard client service and PointGuard proxy service).</p> <p>A client area is created on the server system at:</p> <p style="padding-left: 40px;">\Program Files\Futuresoft\DynaComm PointGuard\Client\PointGuardShare</p>
④	File scan processes log on to the client system with the Log On As account established for the DynaComm PointGuard client service on the console. These processes traverse the target file system to locate specified files. Files selected for content scanning are retrieved from the remote system, placed into memory on the server system and scanned.
⑤	Scan data is logged to XML files in the client area set up on the server machine.
⑥	<p>When scan processes end, the client service notifies the listening service. The listening service retrieves the XML log file from the client area, converts it to an SQL database and saves it at:</p> <p style="padding-left: 40px;">\Program Files\Futuresoft\DynaComm PointGuard\File Scans</p> <p>When a file scan includes moving or copying files to a quarantine location, the files are moved or copied from the scanned system to the Quarantine folder in the client area on the server system.</p>
⑦	<p>Reports are created with data stored on the server system in the Scans60 and File Scans results databases at:</p> <p style="padding-left: 40px;">\Program Files\Futuresoft\DynaComm PointGuard\File Scans.</p>

### Notes

- ❖ *File scan configurations can include one or more scanned file systems.*
- ❖ *The client message discussed in step 5 is sent after all scan processes for all file systems is complete.*
- ❖ *The database file discussed in step 6 includes all data for all scanned file systems.*
- ❖ *See the Security section in this chapter for non-distributed file scanning considerations.*

### Databases

All DynaComm PointGuard databases reside on the server component system and are SQL Express databases which have a maximum size of 4GB.

If you open any database through Microsoft SQL Server 2005, do not modify the data or any data structures unless directed by FutureSoft Support. Doing so may cause unpredictable results that could damage the integrity of the database and DynaComm PointGuard functions.

The Admin database holds configuration data for scan and policy management configurations. Only one Admin database exists per DynaComm PointGuard server. However, two (or more) DynaComm PointGuard servers can include file scan and real-time monitor configurations for the same machine(s).

The Scans60 database stores current and past scan and monitor session configurations. The System Scans database stores current and past system scan configurations. Data is displayed from these databases to show configuration information as it existed when the scan was run or session was active. Configuration data is held until the associated log file is removed. Each time an existing configuration is updated, current configuration data is preserved in the Scans database while the new configuration data is saved to the Admin database.

The Spyware Scans database stores current and past system spyware scan configurations; used to display configuration information as it existed when the spyware scan was run.

Active Protection database stores all configuration and alert data. Active Protection configuration data is displayed in an individual system policy window. Alert data is shown in the Real-time Protection Client window (alert data).

The Quarantine database stores data about quarantine files and file items stored on each client system. Quarantine data is displayed in the Quarantine Management and Details windows, and is managed through the Quarantine Management topic.

Separate XML log files are created on each client system for scans and system policy sessions run against Windows 2000 and higher files for distributed processes. For non-distributed processes, XML log files are created on the server system. Log files are retrieved and merged into respective database files on the DynaComm PointGuard server.

For file and device policy sessions, session data is written to an XML file on the client system. A new log file is created when:

- A policy item configuration is updated and pushed to client systems with the Publish Policy function in an individual system policy window.
- The Retrieve all Logs right-click menu selection is used in the topics pane with the System Policies topic highlighted.
- The Retrieve Logs function in an individual system policy window is used.
- The Retrieve Logs right-click menu selection is used in the details pane with an individual system policy highlighted.

Retrievals of client logs create one database file per system policy group; retrievals merge data to the *same* log until either:

- Maximum size for the database file is reached (4GB), or
- Rule(s) in the assigned rule set change.

#### Note

*Adding or removing a client system to or from a system policy does not create a new log.*

### Log Data Encryption

DynaComm PointGuard uses data encryption when retrieving log data from the client to the server. Both scan and system policy session data is encrypted with a 64-bit RC4 symmetric stream encryption algorithm

## Network Traffic Considerations

Network traffic volume is affected by the operating system of the target system and properties of the file scan or real-time monitor configuration. File scans or system policy sessions generate network traffic when:

- The client service is deployed over the network to client systems that are Windows 2000 and higher.
- An updated configuration is sent over the network to client systems using Windows NT and higher file systems.
- File scan configuration properties include scanning file contents.

The Distributed Processing option on the File Scan tab of the *file scan properties* dialog offers the ability to run file scans on the DynaComm PointGuard server, overriding the default processing location for client systems using Windows 2000 and higher file systems. Enabling this option increases network traffic.

The File Filter tab of the *file scan properties* dialog offers four options for selecting files and two options for defining content scanning actions. Default settings for file selection include all files in the selected folders. Scan of file contents is not enabled by default.

When content scanning is not included, only the file system is traversed and target files are retrieved. Scans conducted on Windows 9.x systems that include content scanning must pass files over the network resulting in increased network traffic.

- Log files are retrieved from client systems (Windows 2000 and higher).

File scan logs are retrieved from client systems when the scan is complete. The log file size is dependent on the number of files that are scanned.

Policy management session activity (real-time) is logged on the client machine (or client area in the case of a monitored server system) and then retrieved to the DynaComm PointGuard server.

Recommendations for reducing network traffic for system policy sessions include retrieving logs during off-peak times. Recommendations for reducing network traffic during file scans include:

- Qualify files as much as possible to reduce the number of files to process and retrieve.
- Allow file content scanning to take place on client systems rather than the server system whenever possible.
- Schedule file scans that include non-distributed file scanning during off-peak hours.

### Security

Installation of the server component must be with a user account that has Administrator privileges. Installation includes installation and set up of the PointGuard service which requires Administrator privileges.

During installation the User Selector dialog is used to specify all user accounts that are allowed to start DynaComm PointGuard. The selected user accounts are added to the “DynaComm PointGuard Users” user group. After installation, user accounts can be added to or removed from this user group through the Windows Control Panel.

A second dialog, Service Run As Account Information, is used to specify one user account that is allowed to run scans and system policy sessions on all client systems. This user account must have full access rights on the client systems. After installation, this user account can be changed through the Windows Control Panel.

### Server Component

When upgrading DynaComm PointGuard with a patch file from FutureSoft, the logon account for the client service on the console is returned to the default, “Local System”. After upgrading you must change the user account to the previous account to allow non-distributed scans to run.

To create a new scheduled job, a user account and associated password are established with scheduled job properties. This user account is assigned to reports created in the scheduled job. When a scheduled report is saved to a file server or sent to an FTP site, the assigned user account must have access to the specified server.

### Client Systems

When a scan or system policy is created, the user account that you are logged on with must have access to the domains and systems that store the files to scan or monitor.

On Windows 9.x systems, a local share must be established before non-distributed file scans can be started.

When a scan or system policy session is started for the first time, the client service is installed on the client machine and uses the “Local System” account.

When non-distributed scans are used, the scan is run by the “PointGuard client” service on the console system. This service is installed by either adding the console as a client system through the Client Management dialog or by including the console system as a client in a file scan configuration. By default, this service is set up to log on and run under the “Local System” account. This account does not have the necessary rights to run scan functions on *other* systems. Therefore, a file scan run on systems other than the console will finish with file errors unless the logon account is changed. The logon account is changed through Windows Services properties. The new account must have the necessary rights to access folders and files on all systems that are included in the distributed scan.

### ForceGuest on XP systems

By default, all incoming connections on computers running Windows XP that are not joined to a domain are forced to use the Guest account. Even when a user account and password are provided, only Guest-level access is granted to the share. This is called ForceGuest and is established and controlled by the Windows XP operating system.

This situation affects access of the DynaComm client service installed on Windows XP systems that are to allow access from the DynaComm server to run a scan or system policy session. ForceGuest can be disabled by disabling the local security policy. See the DynaComm PointGuard Online Reference (Help) for detailed steps.

## Notification

DynaComm PointGuard includes several notification actions for error conditions, warnings and selected functions. All notification, at a minimum, requires establishing the following settings:

- SMTP server settings on the E-mail tab in the Options dialog. These settings are required for sending messages and alerts.
- The DynaComm PointGuard Administrator e-mail address. This data is required when “e-mail administrator” options are enabled.

When certain functions are selected, such as choosing to send an alert message in a real-time monitor session, and the E-mail tab in the Options dialog is not complete, you will be prompted to configure these settings. When the settings are saved, you are prompted to send the changes to all managed computers.

## Reports

Report notification can send report results to one or more users (on-demand or scheduled). For report notification to occur:

- The report file format is selected on the Notify tab of the Report Properties dialog. Default = PDF
- Report results are sent as message attachments to e-mail addresses set up on the Notify tab of the Report Properties dialog.
- Administrator receipt of report results is established by enabling the E-mail Administrator option on the Notification Options dialog. This dialog is accessed by clicking Modify on the Notification tab of the Job Scheduler dialog.

## Scheduled jobs

Scheduled Jobs can send an alert message to notify one or more users of the job completion status. For scheduled job notification to occur:

- E-mail addresses are added to the Notification tab of the Job Scheduler dialog.
- Administrator receipt of end of scheduled report results is established by enabling the Send an e-mail to the Administrator option on the Notification tab of the Job Scheduler dialog.

## System Policy Sessions

File system policy sessions can send an alert message to the DynaComm PointGuard server when selected files or media are accessed by processes, file owners or users. For this to occur, the Alert Server option on the Action tab in the Rule Properties dialog is enabled.

Device policy sessions can send messages when certain activities with USB devices occur. To send an alert message to the DynaComm PointGuard server, enable the Alert Server option on the Action tab of the Rule Properties dialog. To send the user a message, enable the Alert User option.

Active Protection policy sessions can send alert messages when attempts to change the Windows Registry are made. To send the user an alert, enable the Alert local user option in the Real-time Protection Settings dialog.

## Database alerts

When the current real-time monitor database file (server) reaches 4GB in size, a new database file is created and an alert message is automatically sent to the DynaComm PointGuard Administrator.

## System Requirements

System requirements vary according to the number and frequency of use of scans and system policy sessions, as well as the number of files included in the scan or session. Therefore, the following system requirements are beginning guidelines only.

### Server Component

During installation, only the server component is installed. Server system requirements include:

- Software
  - Microsoft Windows 2003 Server with SP1 (or higher) with IIS 6.0
- Hardware
  - 2.0 GHz or faster processor
  - 1 GB total RAM
  - 10 GB free hard drive space

### Client Component

The client component is installed either through the Client Management dialog or by running a scan or system policy session for the first time. Client system requirements include:

- Software
  - Microsoft Windows 2000 with SP4 (or higher), *or*  
  
Microsoft Windows XP with SP2 (or higher), *or*  
  
Microsoft Windows 2003 Server
- Hardware
  - 1.0 GHz or faster processor
  - 512 MB total RAM
  - 500 MB free hard drive space

---

# Chapter 3

## *Installing DynaComm PointGuard*

---

This chapter provides information for installing, maintaining and removing the server component of

DynaComm PointGuard. Upgrade and initial console opening procedures are also included.

## Installation Procedure

Before starting the installation procedure, be sure that you have reviewed the material in Chapter 2 Understanding DynaComm PointGuard. This chapter provides background information for the responses required for installation.

To install DynaComm PointGuard, you must be logged on with the system administrator account, or have administrator rights applied to your login. Otherwise, certain functions are not installed or not installed completely.

Installing DynaComm PointGuard includes the following steps:

Step 1: Start the Setup program.

More than one method can be used to start the Setup program.

Step 2: Respond to Setup dialog to install appropriate components.

The Setup program presents a series of screens that require a response for each. Details for each screen are provided.

## Rebooting

At the end of the installation, you may need to logoff or, in certain situations, may need to reboot your system. Before beginning the installation process, carefully evaluate the effects of rebooting your system, if it should be needed.

## Step 1: Start the Setup Program

The Setup Program guides you through the installation of DynaComm PointGuard. Setup uses two basic functions: Starting and Exiting.

### Starting Setup

If CD Autorun is enabled on the install machine, the DynaComm PointGuard Selection dialog appears when you insert the installation CD-ROM in the appropriate drive. In addition to installing the software, the DynaComm PointGuard Selection dialog offers other choices for viewing the documentation or simply seeing what's on the CD-ROM.

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.

To start the Setup program from the Windows Run dialog:

- 1 Place the installation CD-ROM in the appropriate drive.
- 2 On the Windows Taskbar, click Start and then select Run from the Start menu.
- 3 In the Run dialog, enter the CD-ROM drive name followed with "setup.exe".
- 4 Click OK.

The InstallShield Wizard dialog appears.

When Setup initialization is complete the Welcome dialog appears. Setup is ready to begin installation of DynaComm PointGuard.

### Exiting Setup

During the installation process, if you click Cancel on any dialog, the Exit Setup dialog appears with the message:

Are you sure you want to cancel the setup?

To respond to this dialog, click either:

- Yes to stop the installation and exit the Setup program.
- No to return to the previous screen and continue with Setup.

If you click Yes on the Exit Setup dialog, the InstallShield Wizard Complete dialog appears.

To respond to the InstallShield Wizard Complete screen

- Click Finish to close the Setup program.

## Step 2: Respond to Setup Program Screens

Setup presents a series of dialogs and messages to collect information about your installation of DynaComm PointGuard. Each Setup dialog and associated messages are described on the following pages.

### Internet Explorer Warning

One of the first tasks of the Setup program is to check for an installation of Internet Explorer (IE) 5.01 or higher. This version of IE includes MSTASK.EXE which is required by the Scheduling function. If this version of IE is not found, a warning message appears,

To continue

- Click OK.

The installation stops and the Windows desktop reappears. You must upgrade the installation before Setup can be used to install DynaComm PointGuard.

### Setup Dialog 1: Welcome

The Welcome dialog indicates that the Setup program is now ready to begin installation of DynaComm PointGuard and reminds you to stop any running applications. It also includes the copyright warning advising against illegal distribution of the software.

To respond to the Welcome dialog, click either:

- Next to continue the installation, or
- Cancel to exit Setup.

The Exit Setup dialog appears. See Exiting Setup in this chapter for help.

### Setup Dialog 2: License Agreement

Installation and use of DynaComm PointGuard is governed by the terms of the software License Agreement. You must accept the terms of the agreement before installation can continue. Use the scroll bar to view the entire agreement.

If you have any questions about the terms of the online Software License Agreement, contact your FutureSoft Account Manager or send an e-mail message to [info@futuresoft.com](mailto:info@futuresoft.com).

To respond to the Software License Agreement dialog

- 1 Select “I accept the terms of the license agreement”
- 2 Click one of the following:
  - Back to return to the Welcome dialog.
  - Next to accept the terms of the license agreement and to continue the installation.
  - Cancel to stop the installation and exit Setup.

The Exit Setup dialog appears. See Exiting Setup in this chapter for help.

### Setup Dialog 3: Enter User Information

The user information identifies you and your copy of DynaComm PointGuard to the Setup program.

To respond to the Enter User Information dialog

- 1 Enter:
  - a Your full name in User Name.
  - b Your company name in Company Name.
  - c Your DynaComm PointGuard serial number in Serial Number.
- 2 Click one of the following:
  - Back to return to the software License Agreement dialog.
  - Next to continue the installation.
  - Cancel to stop the installation and exit Setup.

The Exit Setup dialog appears. See Exiting Setup in this chapter for help.

#### Note

*Leaving Serial Number blank installs an evaluation version of DynaComm PointGuard.*

### Setup Dialog 4: Choose Destination Location

The Choose Destination Location dialog specifies the folder where the program files are to be installed. The default location (shown in Destination Folder) is:

C:\Program Files\Futuresoft\DynaComm PointGuard

To respond to the Choose Destination Location dialog

- 1 If a new folder needs to be specified, click **Browse** to select another location.

The Windows Choose Folder dialog appears. Use standard Windows navigation techniques to select a new location, and then click **OK**. Otherwise, click **Cancel** to return to the Choose Destination Location dialog.

- 2 Click one of the following:
  - **Back** to return to the Enter User Information dialog.
  - **Next** to continue the installation.
  - **Cancel** to stop the installation and exit Setup.

The Exit Setup dialog appears. See Exiting Setup in this chapter for help.

### Setup Dialog 5: Select Program Folder

By default, Setup creates the DynaComm PointGuard program group (folder) which is accessed through the Start menu. This program group contains shortcuts to the DynaComm PointGuard console and the DynaComm PointGuard Documentation folder that includes shortcuts to the Readme file, Online Reference (Help system) and Administrator Guide. The program group name can be changed on the Select Program Folder dialog.

To respond to the Select Program Folder dialog

- 1 If needed, enter a new folder name, or select a folder from the Existing Folders list.
- 2 Click one of the following:
  - **Back** to return to the Choose Destination Location dialog.
  - **Next** to continue the installation.
  - **Cancel** to stop the installation and exit Setup.

The Exit Setup dialog appears. See Exiting Setup in this chapter for help.

#### Caution!

*After installation, do not move any program files to another folder. Doing so may cause problems running DynaComm PointGuard.*

### Setup Dialog 6: Setup Status

During the file copy, the Setup Status dialog is displayed to show the status of the copy and updating processes. You do not need to respond to this screen. However, you can click **Cancel** to stop the installation and exit Setup. The Exit Setup dialog appears. See Exiting Setup in this chapter for help.

#### Caution!

*Depending on when you click **Cancel** during the install procedure, some files or registry entries may have been installed. To ensure complete removal of any files and registry entries, you must restart the Setup Program and choose **Remove** from the selection menu.*

### Setup Dialog 7: Authorized Access

After Setup has copied all files, the first of two dialogs used to create the security settings for DynaComm PointGuard appears. During installation the Setup program creates the “DynaComm PointGuard Users” local group. User accounts placed in this group are allowed to open and work with DynaComm PointGuard.

The Authorized Access dialog (Figure 3.1) informs you that your current logon account has automatically been added to the “DynaComm PointGuard Users” group. Users added to this group are allowed to open and run the DynaComm PointGuard console. Use the Windows User Manager function after installation to add additional accounts to the “DynaComm PointGuard Users” group.

To respond to the Authorized Access dialog

- Click one of the following:
  - **Next** to continue the installation process.
  - **Cancel** to not add your current logon account to the “DynaComm PointGuard Users” group.

#### Note

*Membership in the “DynaComm PointGuard Users” group **does not** grant rights to run file scans or real-time monitor sessions.*

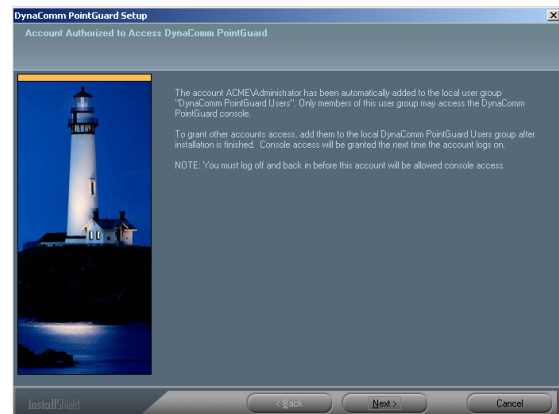


Figure 3.1  
Account Authorized to Access *dialog*

### Setup Dialog 8: Listening Service Account

The Listening Service Account dialog (Figure 3.2) collects information for the one account that is assigned to all scans and real-time monitor sessions. This account must have the proper rights and authority to allow it access to all machines on which scans and sessions are to be run. If the proper rights are not granted, an error message is shown that says that the Listening Service could not be started on the selected system(s).



Figure 3.2  
Listening Service Account *dialog*

To respond to the Listening Service Account dialog

- 1 In UserID, the account that you are logged in with is placed in this field by default. If needed, enter a new account name.
- 2 In Password, enter the associated account password.
- 3 In Confirm, re-enter the associated password.

#### Notes

- ❖ *The user account established in the Listening Service Account dialog must have administrator rights.*
- ❖ *For Windows 2003 Server system, the account used by Web Services must be added to the DynaComm Web Services group.*

- 4 Click one of the following:
  - Next to continue the installation.
  - Cancel to not set up the account.

When you click Next, the confirmation dialog appears.

- 5 Click OK.

The InstallShield Wizard Complete dialog appears.

### Setup Dialog 9: InstallShield Wizard Complete

The InstallShield Wizard Complete dialog is the last dialog displayed in the installation of DynaComm PointGuard. This dialog gives you the choice to restart your computer now or restart it later.

To respond to the InstallShield Wizard Complete dialog:

- 1 Select Yes, I want to restart my computer now.
- 2 Click Finish.

## Setup Maintenance

The Setup Maintenance Program is used to modify, repair or remove DynaComm PointGuard. To use Setup Maintenance with DynaComm PointGuard, you must be logged in as the system administrator or have administrator rights applied to your login.

Setup Maintenance will:

- **Modify** Add or remove individual components.
- **Repair** Reinstall all components that were installed by the previous setup.
- **Remove** Removes all installed components.

## Modify Procedure

Modifying DynaComm PointGuard includes the following steps:

- Step 1 Start the Setup Maintenance program.
- Step 2 Respond to Setup Maintenance dialogs.

On the Setup Maintenance Welcome dialog, choose Modify and follow the screen prompts.

## Repair Procedure

Repairing DynaComm PointGuard includes the following steps:

- Step 1 Start the Setup Maintenance program.
- Step 2 Respond to Setup Maintenance dialogs.

On the Setup Maintenance Welcome dialog, choose **Repair** and follow the screen prompts.

## Removal Procedure

Two different procedures are used to remove DynaComm PointGuard components:

- DynaComm PointGuard server
  - Removed through Setup program (includes the console, databases, reporting engine, scheduler and associated application files).
- DynaComm PointGuard client service
  - Removed through the Client Management dialog accessed with **Tools > Client Management**. See the DynaComm PointGuard Online Reference for the steps to remove the client service.

## Step 1: Start the Setup Maintenance Program

Setup Maintenance is started in the same manner as the Setup program (see Starting Setup in this chapter). Setup looks for an installed copy of DynaComm PointGuard. When the program is found, the Welcome dialog appears.

To respond to the Welcome dialog

- 1 Select one of the following:
  - **Modify**
  - **Repair**
  - **Remove**
- 2 Click one of the following:
  - **Next** to continue the Maintenance program.
  - **Cancel** to exit Setup.

The **Exit Setup** dialog appears. Refer to the **Exiting Setup** section in this chapter for instructions.

## Step 2: Respond to Setup Maintenance Dialogs

### Modify

After selecting **Modify** on the **Setup Maintenance Welcome** dialog and clicking **Next**, the **Select Components** dialog appears. All installed components on the current machine are listed. The total amount of space available is shown below the list of installed components.

To respond to the **Setup Maintenance Welcome** dialog

- 1 Add or remove check marks.
  - Remove check marks to remove component(s).
  - Add check mark(s) to install component(s).
- 2 Click one of the following:
  - **Back** to return to the **Welcome** screen.
  - **Next** to continue the **Maintenance** program.
  - **Cancel** to exit **Setup**.

The **Exit Setup** dialog appears. Refer to the **Exiting Setup** section in this chapter for instructions.

### Repair

After selecting **Repair** on the **Setup Maintenance Welcome** dialog and clicking **Next**, the **Setup Status** dialog appears. As the components are reinstalled, this dialog tracks the progress of the **Setup** program. When the repair is complete the **Setup Complete** dialog is displayed.

To respond to the **Setup Complete** dialog

- 1 Select **Yes, I want to restart my computer now**.
- 2 Click **Finish** to complete modify functions and restart the system.

The **Windows** desktop returns.

### Remove

The Setup Maintenance program removes only those items that have been installed by the Setup program. It will not remove a file that was not installed by Setup or an installed file that has been renamed or moved.

All client machines must have the client service removed before DynaComm PointGuard can be removed from the server system. If any client systems retain the client service, an error message appears.

The client service is removed through client management functions in the console. See the DynaComm PointGuard Online Reference for the steps to remove the client service.

To remove DynaComm PointGuard you must be logged on as the system administrator or have administrator rights applied to your login.

### To remove the server component

- 1 On the Setup Maintenance Welcome dialog, select **Remove** and click **Next**.

The **Confirm Uninstall** message appears.

- 2 Click **OK**.

The **Setup Status** dialog displays the progress of the program removal. The **InstallShield Wizard Complete** dialog appears when DynaComm PointGuard is uninstalled.

- 3 Select one options:

- Yes, I want to restart my computer now.
- No, I will restart my computer later.

- 4 Click **Finish**.

---

# Chapter 4

## *Basic Configuration*

---

4040 This chapter begins with a review of basic user interface particulars and proceeds with a discussion of initial configuration tasks. Certain configuration tasks, such as default client system settings, must be set up first because other functions use these configuration settings.

Basic management of client systems through the Client Management dialog is reviewed along with information on saving changes.

## Initial Configuration Tasks

Initial configuration tasks include those that establish settings that are used by DynaComm PointGuard to perform maintenance functions or when working with other configuration functions. Initial configuration tasks include:

- Establishing server endpoints.
- Establishing default client settings.
- Establishing e-mail settings.
- Establishing the database update connection method.
- Modifying daily database maintenance functions
- Establishing white-listed (allowed) processes

All of these tasks are performed through the Options dialog which is accessed from the Tools menu.

## Establishing Server Endpoints

For initial configuration of the DynaComm PointGuard server, establishing server endpoints is required. This setting is entered on the Server tab of the Options dialog.

### Step 1: Acknowledge Server Endpoints Message

When DynaComm PointGuard is opened for the first time after installation, the *Server Endpoints* message appears. This message prepares you for the appearance of the Server tab of the Options dialog.

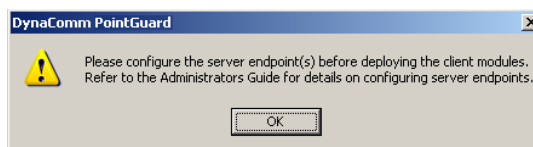


Figure 4.1  
*Server Endpoints message*

To respond to this dialog

- Click OK.

The Options dialog appears with the Server tab displayed.

## Step 2: Supply Server Endpoints

Server endpoints are the URLs that internal and external clients are to use to communicate with the DynaComm PointGuard server to collect configuration updates and to report the status of various functions, such as, active scans and monitor sessions. Server endpoints are established in the Server Endpoints group on the Server tab of the Options dialog. DynaComm PointGuard pre-fills the Internal path to this server field with a best guess. This URL is used by client systems that are to use private IP addresses to access the DynaComm PointGuard server. Access to the server is required to return scan results and configuration data. Make changes if needed.

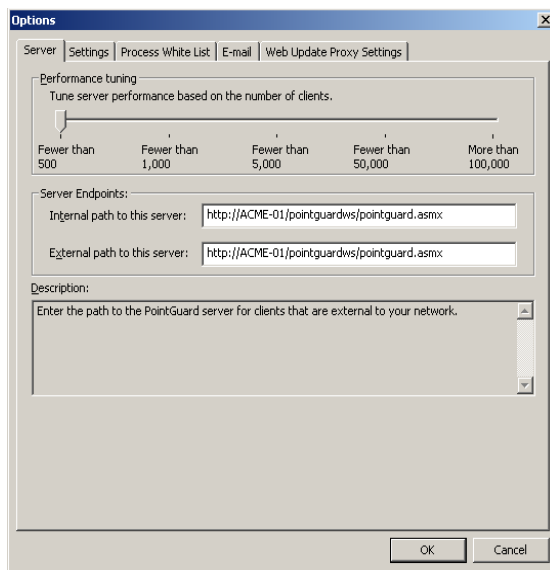


Figure 4.2  
Server tab of the Options dialog

The DynaComm PointGuard server machine can be exposed to outside networks to allow external clients, such as lap tops or other mobile computers, access capabilities. In this scenario you must include a complete URL in the External path to this server field for these clients.

To respond to this dialog

- 1 Enter new server endpoints or modify the supplied server endpoints (URLs).
- 2 Click OK.

DynaComm PointGuard verifies that the supplied internal URL is viable. This may take several minutes to complete. When the internal URL check is complete and if an external URL endpoint is supplied, a second message appears.

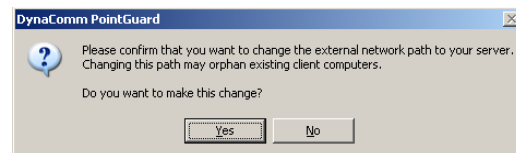


Figure 4.3  
External network path verification message

To respond to this dialog

- Click OK.

When the external URL check is complete, the console window appears. You are now ready to establish other default settings in the Options dialog. Reopen this dialog by selecting Options from the Tools menu on the menu bar.

## Working with the Console

The console provides the interface for configuring and managing all DynaComm PointGuard functions. Selecting DynaComm PointGuard Console in the DynaComm PointGuard program group opens the console window. Standard window manipulation techniques are used to customize the window size and placement.

Major components of the console window include:

- Title bar - displays DynaComm PointGuard application name.
- Menu bar - lists menu names.
- Toolbar - displays seven quick-access buttons for most commonly used functions.
- Topics pane - includes seven (7) first-level configuration topics; each topic provides access to a set of functions to configure

and manage selected topic elements. Selecting a topic in the topics pane displays the corresponding topic elements in the details pane.

- Details pane - displays topic elements, such as, defined file scans, categories, reports, etc., for the selected configuration topic. Lists are sorted by clicking on the column header; successive clicks alternate between ascending and descending sorts.

Topic functions are accessed by:

- Left-clicking on the function buttons in the details pane.
- Right-clicking in the topics pane to display popup menus.
- Double-clicking on a scan, rule or report name in either pane to display the corresponding properties dialog.

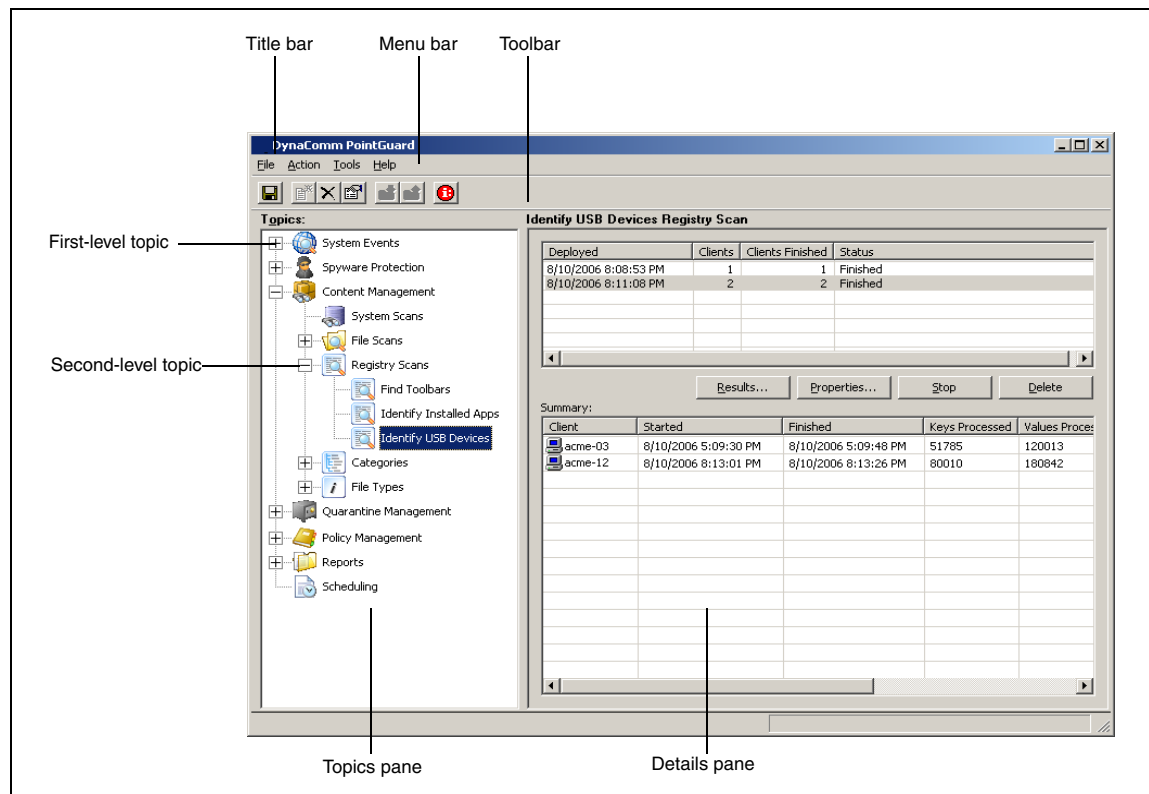


Figure 4.4  
DynaComm PointGuard console window

## Establishing Default New Client Settings

Two options in the New Client Settings option group on the Settings tab in the Options dialog are applied globally to all new clients. By default, these options are enabled:

- Automatically push new installations to clients

If the installation fails, installation retry attempts continue for 48 hours or until successful. This time limit can be changed, if needed.

Clients communicate with the server by initiating checks with the server for configuration updates and new scheduled jobs. Communication does not occur until the client service is installed. With this

option enabled, the communication begins immediately. With this option disabled, the client service must be installed manually through the Monitored Computers topic or through the Client Management dialog.

- Automatically add new clients to the 'Default' system policy

With this option enabled, new clients are automatically added to the group of client systems managed by the Default Policy in the System Policies configuration topic. This policy includes two policy items but no rules are included in either policy item.

Settings can be changed at any time and become effective when saved. To change existing client settings for system policy protection, open the individual policy items and make changes.

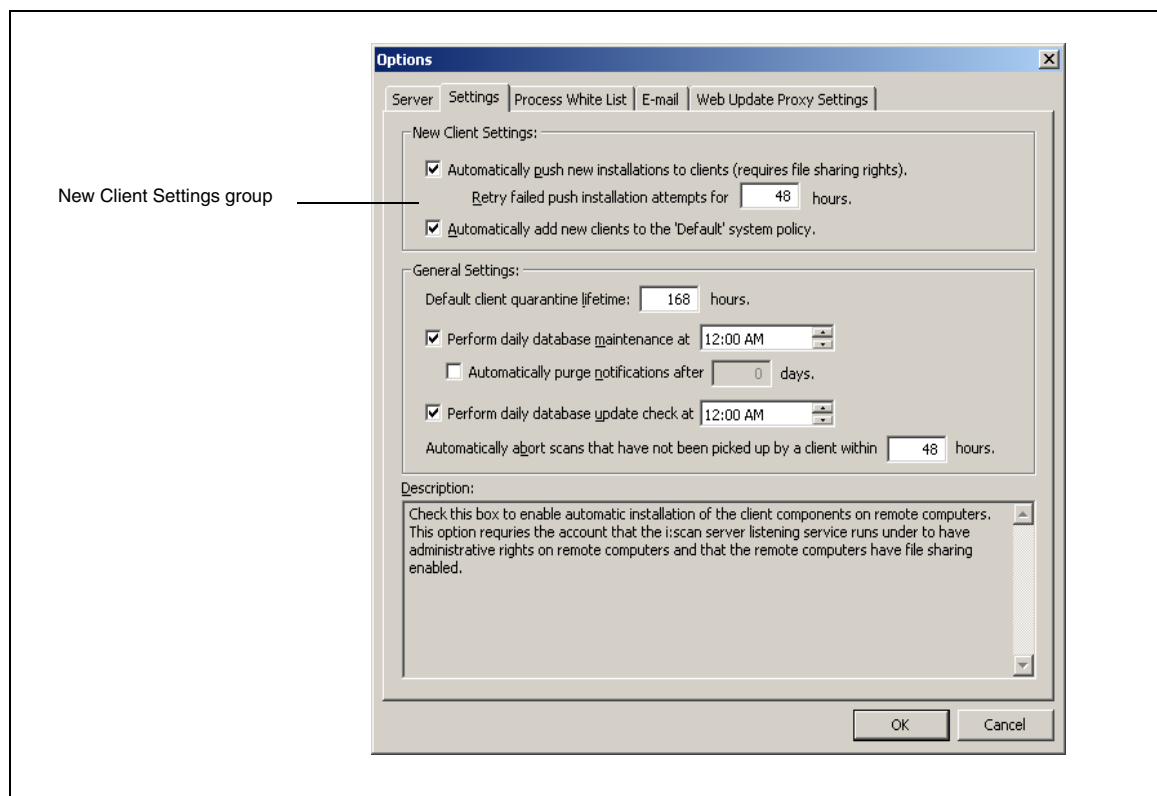


Figure 4.5  
Settings tab of the Options dialog

## Establishing E-mail Settings

Several DynaComm PointGuard features include notification functions. For notification to occur, a mail server name and the administrator e-mail address must be supplied on the E-mail tab of the Options dialog. When needed, the port used for e-mail can be changed.

These e-mail settings are used by reports, rules and scheduled jobs when notification is enabled in the Report Properties dialog, Rule Properties dialog and Job Scheduler dialog, respectively. See the Reports, Rule Sets and Scheduling sections in this chapter for information on configuring notification for these functions.

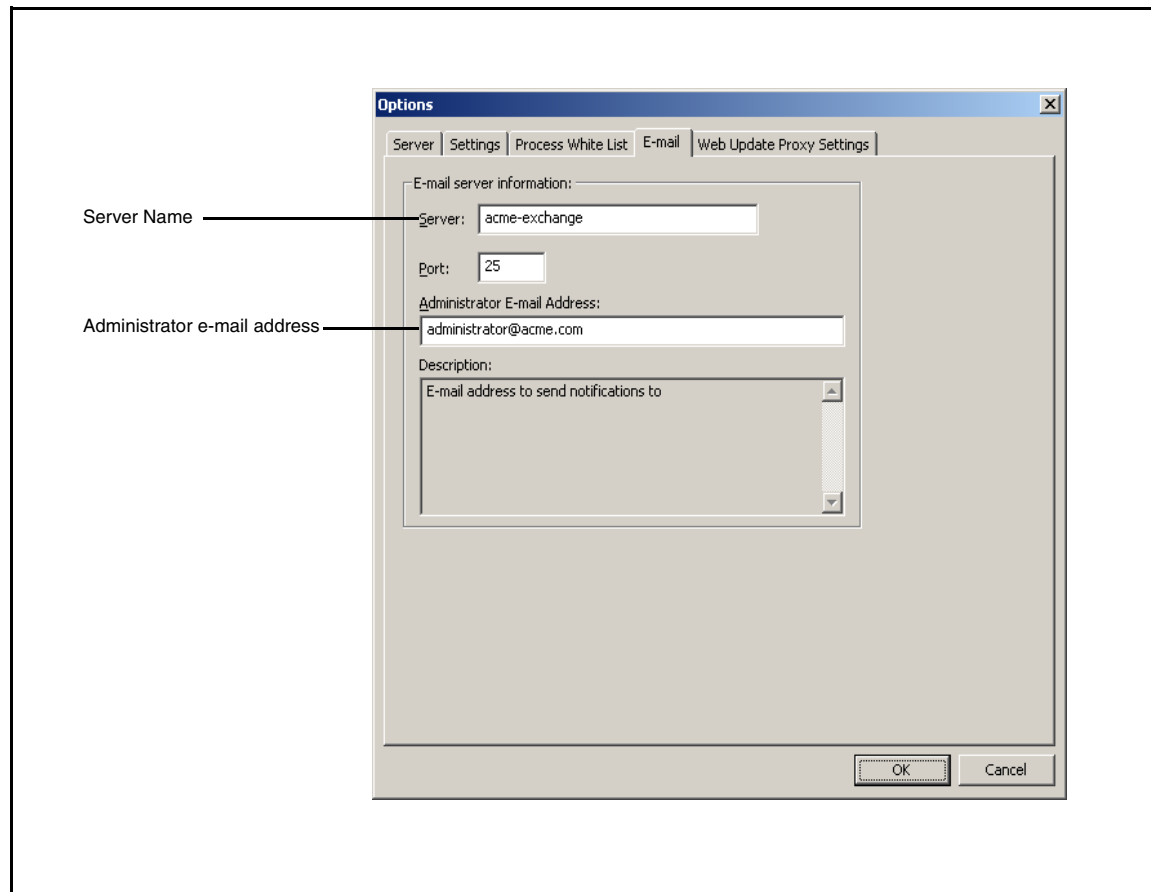


Figure 4.6  
E-mail tab of the Options dialog

## Establishing Database Update-Connection Method

FutureSoft performs daily research and maintenance on file types and file type extensions, keywords and keyword phrases for predefined categories. Adware/spyware updates for the threat database are received from Sunbelt Software. All updates are provided on the FutureSoft web site. A valid serial number and a current Support and Maintenance contract is required for a successful update.

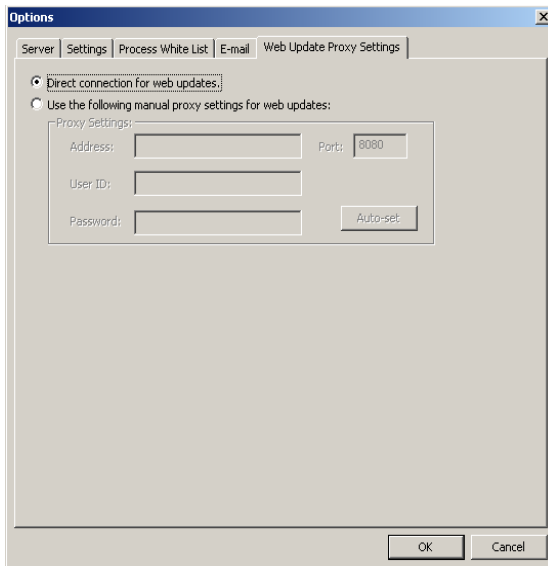


Figure 4.7  
Web Update Proxy Settings tab of the Options dialog

By default, a direct connection method is established for performing the updates. If a proxy server is used for web communications, the Use the following manual proxy settings for web updates option must be enabled and the Proxy Settings option group on Web Update Proxy Settings tab of the Options dialog must be completed. The required settings can be entered manually or use the Auto-set function to pre-fill with settings established in Internet Explorer (IE).

The database update is performed by:

- Clicking Update on the Tools menu.
- Including the Update spyware definitions, keywords and file types task in a scheduled job.
- Enable the Perform daily database update check in the Options dialog.

## Modifying Default Database Settings

Two settings in the General Settings option group on the Settings tab of the Options dialog establish automatic daily database maintenance:

- Perform daily database maintenance (compact data).
- Perform daily database update check (determine if updates are available for the Threat database and/or the Categories and File Types database; if yes, then perform update).

By default these two options are enabled and both are set to occur at 12:00 AM (midnight).

## Establishing White-Listed Processes

Selected processes may be terminated when:

- A change request is generated by a process associated with a blocked protected area.
- A file scan terminates a process that uses an executable file that has been logged by the file scan. This occurs when the Terminate processes that use any of the logged executable files option is enabled in the Actions tab (*File Scan Properties*).

So, for example, automatic updates from Microsoft or other similar procedures would not be completed. To avoid this problem, processes that are to be ignored (allowed) are listed on the Process White List tab of the Options dialog. Processes can be added or removed at any time.

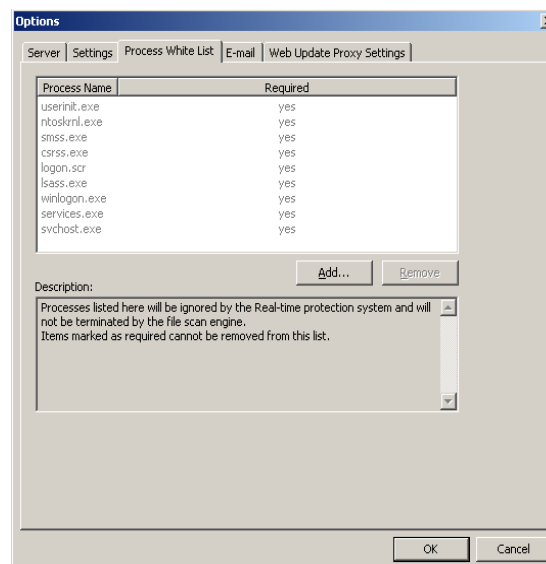


Figure 4.8  
Process White List tab of the Options dialog

## Managing Client Systems

Client Management on the Tools menu provides management functions for the DynaComm PointGuard client service. The client service is automatically deployed to a client system when a scan or real-time monitor session is started. To control deployment, the client service software can be installed, upgraded and removed independently of a scan or system policy session.

## Viewing Client Systems

When the Client Management dialog is requested, you see a brief message that DynaComm PointGuard is querying for information. By default, Active Directory Discovery is enabled. However, if Active Directory is not used on your network or your logon account does not have the appropriate rights to use Active Directory, Microsoft Windows Networking is used.

Two networking levels are available:

- Active Directory/Microsoft Windows Network

All network objects included in the respective network are listed.

- All Clients

All systems that have had the client software installed from the server system are shown. In other words, in installations with multiple DynaComm PointGuard console components, each console system displays only those client systems that had the client service installed as a function of a scan, system policy session or client management function performed by the respective console.

### Note

*For functions accessed through the Client Management dialog, it may take several minutes for update of the dialog display depending on the number of systems to update and network traffic requirements at the time of update.*

## Adding Client Systems

Computers are added to the list of managed client systems:

- By using Add New Client in the Client Management dialog (right-click menu).  
  
The client service is installed as each system is added to the list.
- Adding a computer to a system policy group (System Policiestopic).  
  
The client service is not installed but the computer is added to the list of managed client systems.
- Running a scan or system policy session on the computer.  
  
The computer is added to the list of managed clients. The client service and real-time driver is installed.

The Client Management dialog displays a one-line entry for each managed client system in the clients pane. Each entry lists the operating system installed on the client and the DynaComm PointGuard client service version, installation date and status.

Communication between the server and the client service is established by:

- Installing the client system.
- Pushing a configuration (saving or running a configuration).
- Retrieving a log.
- Requesting client details.
- Automatic run of “Health Check” routine (runs every 30 minutes).

When communications between the client and server are broken, the client listing in the Last Communications column appears in red. This typically occurs when the client machine is removed from the network, turned off or the client installation becomes damaged. Removing and then re-installing the client corrects most situations.

## Removing Client Systems

One or more client systems can be selected for uninstall or removal. With the Uninstall Client Software command the client service is removed but the client system remains in the list of managed clients. With the Remove Client menu selection the client service is removed and the client system is removed from the list of managed clients. A confirmation message appears before completing the selected action.

Client systems removed from a system policy are not removed from the managed client list. These systems must be removed through the Client Management dialog in a second step.

## Managing Client Systems

Client management functions are accessed from the right-click menu shown in Figure 4.11. The menu is accessed from the Client Management dialog and available functions depend on the item that is highlighted when the menu is accessed.

The client service can be installed and upgraded on all client systems or on selected client systems. After installing or upgrading the client service, rebooting the client system is required to start the real-time driver. When the client service is installed, the service is automatically started. Client system details can then be shown for a selected computer in the client details pane. Details include the installed operating system and all DynaComm PointGuard module names with the current product version and file version for each.

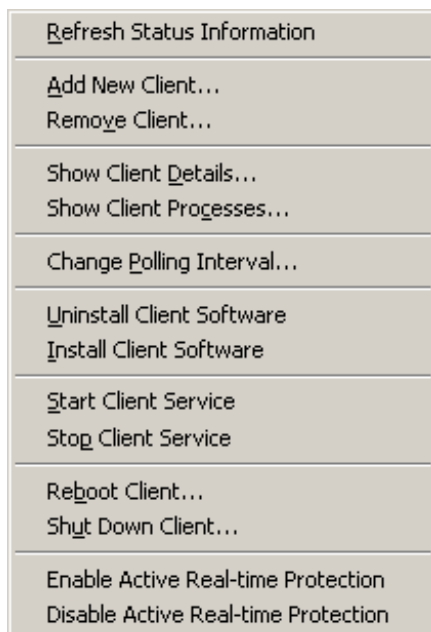


Figure 4.9  
*Right-click menu of Client Management dialog*

A snapshot of current processes for a selected client system are viewed through the Client Processes dialog by clicking Show Client Processes from the right-click menu. Detailed information accessed from the Client Processes dialog includes:

- System information (click System Info)

System information includes domain and client names, operating system particulars, all logged on users and CPU, memory and hard drive information.

- Client details (click Client Details)

Client details include product and version numbers for all DynaComm PointGuard client service installations.

The client service on any selected client system can be stopped and re-started through the Client Management dialog at any time to perform other maintenance functions or simply discontinue a scan or system policy session.

## Saving and Pushing Configuration Changes

Configuration changes are saved to the Admin database by either:

- Clicking Save on the toolbar, or
- Using the File > Save menu command, or
- If you close the console with unsaved changes, a confirmation message appears:

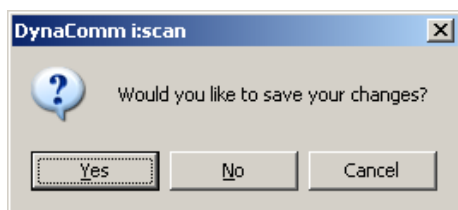


Figure 4.10  
*Save changes confirmation message*

To respond to the confirmation message, do one of the following:

- To save changes to the Admin database, click Yes.
- To discard changes, click No.
- To continue working with the console, click Cancel. Changes are not saved.

## System Policy Changes

When you ask to close the DynaComm PointGuard console with *unsaved system policy* changes, a question dialog appears:

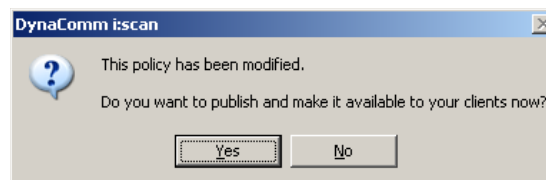


Figure 4.11  
*Push changes confirmation message*

To respond to the confirmation message, do one of the following:

- To push changes to the affected client systems, click Yes.
- To save changes to the Admin database only, click No.

## System Policy Item Changes

When you ask to close the DynaComm PointGuard console with *unsaved policy item* changes, a question dialog appears:

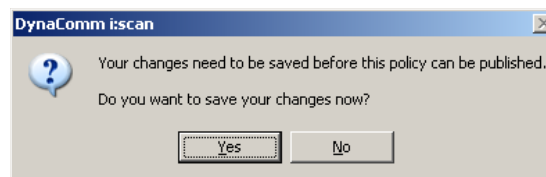


Figure 4.12  
*Push changes confirmation message*

Changes can be pushed to client systems at any time with the Update function in the individual system policy window.

---

# Chapter 5

## *Managing Files & Registry Content*

---

The Content Management topic includes subtopics used to manage file and Windows Registry contents. The File Scans topic includes structures to create and manage scans that scan file contents, copy and move files to the quarantine area or some other location, or completely remove files. The Registry Scans topic includes structures to create and manage scans that scan Windows Registry key entries and can write or remove selected keys.

Two supporting topics, Categories and File Types, include elements used in file and registry scans. In this chapter, Categories and File Types are discussed before reviewing the File Scans and Registry Scans topics.

System scans can include both file and registry scans. The System Scans topic is discussed last.

## Categories

A category is a group of elements commonly associated with major classifications, such as, adult material, instant messaging, games and so forth.

Key elements of categories include:

- Keywords and Keyword Phrases

Keywords are composed of alphanumeric characters. A keyword phrase consists of two or more words or a single word with a delimiter which is any non-alphanumeric character.

- Keyword Weight

Each keyword or keyword phrase is assigned a *weight* value that indicates the importance of the keyword in identifying the category. The higher the keyword weight value, the more closely the keyword identifies the category.

- Category Threshold

Each category is assigned a *threshold* value. The threshold value is the accumulated keyword weight value that triggers assignment of the category to a scanned file. As a scan progresses through a file, a running total of keyword weight is kept as keywords and keyword phrases are found. A scan reviews the entire file and may result in assignment of multiple categories.

- File Signatures

File Signatures have been included for commonly distributed files, such as, porn dialers, instant messaging executables, games, file sharing programs (P2P) and more. File signatures can be created manually or through a scan and then imported into a category. Categories do not always include file signatures.

- Registry Keys

Windows registry keys are placed in either the **Removable Registry Entries** or **Writable Registry Entries** subgroups. A registry scan logs all registry keys that are included in either subgroup when the category is selected in registry scan properties.

Registry keys included in the **Removable Registry Entries** subgroup are removed from the Windows Registry when the **Delete removable keys** option is enabled in registry scan properties. Registry keys included in the **Writable Registry Entries** subgroup are written to the Windows Registry when the **Add writable keys** option is enabled in registry scan properties.

Categories are used in a file scan to identify file contents. Categories are used in a registry scan to identify registry entries. Categories are used in reports to provide data on files with a specific content

## Special Operators

More complex filters can be performed with the use of special characters and operators in keyword phrases. Operator precedence is from left to right. However, precedence can be changed through the use of brackets. Nested brackets can also be used.

Special operators cannot be used with registry key entries; however, special characters can be used.

### Note

*See the DynaComm PointGuard Online Reference for detailed information on using special operators and characters with keywords and registry keys.*

## Predefined Categories

Predefined categories of commonly used keiretsu, phrases, file signatures and registry keys are included in DynaComm PointGuard for quick set up of file scans, registry scans and reports. Predefined categories included with DynaComm PointGuard are shown in Table 4.3.

Predefined categories can be customized by adding or removing keywords, file signatures and registry keys and changing keyword weights and category thresholds. Predefined categories can be renamed but cannot be removed.

### Note

*See Appendix A Predefined Categories for a complete description of each predefined category.*

## Custom Categories

Custom categories can be created to reflect a particular area of interest and can include any combination of keywords, keyword phrases, file signatures and/or registry keys. Custom category contents can be modified at any time as well as renamed or removed.

## Categories & File Types Database Update

FutureSoft continually updates predefined category contents. A subscription service to receive updates from the FutureSoft web site is available. Retrieval is performed with the Update selection on the Tools menu, through a scheduled job task or by enabling the Perform daily database update check at option on the Settings tab of the Options dialog.

## File Types

File types are groups of file type extensions with associated file formats. DynaComm PointGuard includes predefined file types that contain over 160 commonly used file type extensions. Predefined file types are listed in Appendix B Predefined File Types.

Predefined file types can be modified by adding or removing file extensions but cannot be removed. Custom file types can be created to include any file extension and can be modified or removed.

## Using File Types

File types are used in file scan configurations and reports. The File Filter tab of the *file scan properties* dialog offers the option to scan for file type. Reports can be set up to provide information on data logged for selected file types. The Report Properties dialog includes the File Types tab where file types are selected.

## Processing File Types

When processing files for tile type, target file format is compared first with known file formats. When a match is made, the file extension is then checked against all file type extensions to verify file classification. This is the preferred method for identifying file type to circumvent changing file extensions in an attempt to disguise files.

## Categories & File Types Database Update

FutureSoft continually updates file type extensions and file types. A subscription service to receive updates from the FutureSoft database update web site is available. Retrieval is performed with the Update selection on the Tools menu, through a scheduled job task or by enabling the Perform daily database update check at option on the Settings tab of the Options dialog.

## File Scans

A file scan configuration is a collection of properties that:

- Define the client systems to scan.
- Define the properties of files to scan.
- Specifies one or more actions to perform on target files, if needed.

## File Scan Procedure

The general steps to create and implement a file scan and then evaluate scan result data includes:

- 1 Plan the file scan.

Determine the purpose of the file scan, which systems to include in the scan and what files or types of files the scan is to locate. Try to narrow the file criteria as much as possible.

- 2 Set up supporting structures.

- If needed, create new or modify existing categories through the **Categories** topic.
- If needed, create new or modify existing file types through the **File Types** topic.

- 3 Add a new file scan configuration.

In the **File Scans** topic window, add a new file scan. In the file scan properties dialog, enter a name and a description of the scan, select or clear options and make entries to specify the files to scan and actions to take on files that meet scan properties.

- 4 Save the new file scan configuration.

- 5 Run the file scan.

Use **Run** in the **File Scans** window or **Run** on the right-click menu (select the file scan name). The file scan can also be added as a task in a scheduled job.

### Note

*A default setting on the **Settings** tab of the **Options** dialog is set to abort scans that have not been picked up by a client within 48 hours. This can be changed, if necessary.*

- 6 Run on-demand or scheduled report(s) using the log file produced in step 5. By default, the report uses the most recent log file.

- Run an on-demand report through the **Reports** topic. After viewing the report online, choose to release the report or export it to a file.
- Set up report properties through the **Reports** topic. Create a scheduled job through the **Scheduling** topic that includes the report in the list of tasks. Either select a save location for the report file or include one or more addresses to send the report to.

### Note

*See **Chapter 9 Reporting and Scheduling** for reporting considerations.*

## Configuring File Scans

A file scan configuration is created with the New File Scan wizard. This wizard walks through the creation process by displaying the three tabs of the *file scan properties* dialog on which file scan properties are set.

- File Scan *tab*

The File Scan tab includes the file scan name and a brief description to identify the scan. This information is displayed in the individual file scan window when the file scan name is highlighted in the topics pane.

The File Scan tab offers five sub tabs. An entire file system or individual folders and files are selected on any sub tab. Each file system is listed separately and can be customized for:

- File system exceptions (default: none)

Select a sub folder or file that is not to be scanned.

- CPU Usage (default: Below Normal)

By default, file scans run at lowest processor priority. This allows other system or application functions to perform with the least amount of interruption. Available selections include: System Idle, Low, Below Normal, Normal, High.

- Search NTFS Streams (default: No)

Alternate data streams store additional file data that can be used for unapproved purposes. Choose “Yes” to search all existing data streams for a file. This option is valid only for Windows 2000 and later file system.

- Search of sub folders (default: Yes)

Choose “NO” to search only the files in the selected folders and to ignore files in any sub folders.

- Distribute Processing (default: Yes)

Select “No” to specify a non-distributed scan. Remote scan processes run on the DynaComm PointGuard server. This is automatically performed for Windows 9.x and NT clients. Choose “Yes” to perform remote scan processes for Windows 2000 and later clients.

- Search of compressed files (default: No)

When scanning of compressed files is enabled, the following options are available:

- Number of levels (deep) of compressed files (default=3)
- File size limit (default=10MB)

- File Filter tab

The File Filter tab offers five option groups for:

Filtering files to scan by:

- File mask (default=\*.\*)
- File date (default=8/23/2004)
- File size (default=0KB)
- File attribute (default=none)

Scanning file content for

- File type (default=all file types)
- Keywords and file signatures (default=all keywords and file signatures in all categories)

#### Note

*The pornographic image scanner is automatically invoked when all of the following is true on the File Filter tab of the file scan properties dialog:*

- ❖ Scan content for keywords and file signatures option group is enabled.
- ❖ Calculate file signatures option is enabled.
- ❖ Filter search by categories option is enabled.
- ❖ Either all categories are included in the Selected Categories list (list is "blank") or the Adult Material/Offensive Language category is included in the list of selected categories.

- Actions tab

The Actions tab offers seven option groups for performing selected actions on target files. These options include:

- Perform file operations (move/copy to quarantine, or delete)
- Terminate processes
- Set file attributes (archive, hidden, read-only and system)
- Set file ownership (NTFS only - select one user account)
- Set file permissions (NTFS only)
- Set file auditing options (NTFS only)
- Start a selected registry scan
- Choose a shutdown time for the client system

File scan properties are modified through the file scan properties dialog. Changes become effective after saving.

## Viewing File Scan Properties and Logs

Two windows are used to work with file scans and scan run results:

- **File Scans**  
(Select the File Scans topic in the topics pane)  
  
File scan maintenance functions (Add, Edit and Remove) as well as starting and stopping a file scan (Run, Stop) are performed through this window. All currently defined file scan configurations are listed in the details pane with status information about the last run of the configuration.
- *File Scan Run Results*  
(Select an individual file scan name in the topics pane)

The details split pane shows:

- **Scan Runs**

Lists one line of data for individual file scan runs. Data includes date and time of scan instance, client statistics and run status.

Scan result information is manipulated by:

- Selecting a scan run in this list displays run details in the Summary pane.
- Displaying a list of files logged during the file scan through the View Files function.

- Viewing file scan configuration properties (File Scan Properties viewer) that were in effect for the selected scan instance through the Properties function.
- Removing the file scan log and associated configuration information through the Delete function.

A running scan can be stopped by selecting the scan and clicking Stop in the function area.

- **Summary**

Lists scan run instance details, by file system, for scan start and end, number of folders and files processed, and number of files and errors logged.

### Note

*When scanning file contents with categories, using keywords (categories) produces fewer false positive results but requires the greatest load on processing resources.*

## File Scan Considerations

Creating and running file scans and producing reports on file scan results should take the following into consideration:

- File scans only work with files. Folders cannot be removed with a file scan.
- As much as possible, narrow the number of files to scan or the amount of file content scanning to perform in a file scan. Choosing default file filtering options scans all files of any size with any date and with any file attributes.

Narrowing the files to scan or file items to evaluate helps to:

- Reduce data to be evaluated.
- Require less resources to store log data.
- Avoid exceeding Access database size limits which stops the merge process of log data. Unmerged log file data is not accessible.
- Reduce processing time required to merge log data to database file.
- Reduce CPU utilization on the target machine.
- Set the CPU Usage option on the File Scan tab in the file scan properties dialog as low as possible to reduce impact on user and system functions.

- When working with the file scan properties dialog, the systems shown on the Computer and File Selector tab is dependent on the access rights granted to the user account that you logged on with to the DynaComm PointGuard server. If the user account has access to Active Directory, then that structure is shown. Otherwise, Microsoft Networking structures are shown.
- File scans can be run on-demand or placed in a scheduled job.
- File scans that include two or more computers produce a single database file on the DynaComm PointGuard server system that contains all data from all systems included in the file scan.
- The XML log file created on target systems (distributed Scan) is removed when the log file is retrieved by the DynaComm PointGuard server.
- A file can be run concurrently with a file or device system policy session on the same system with no impact to the file scan. However, this scenario may impact the system policy session. See Topic: System Policies in Chapter 6 for detailed information.
- By default, a file scan run against a Windows NT file system uses the processing functions of the client machine. However, this feature can be disabled by changing the Distribute processing option on the File Scan tab in the file scan properties dialog to “No”. When this feature is disabled, the file scan uses the processing functions of the server machine. Therefore the Terminate processes that use any of the logged executable files option is not available on the Actions tab in the file scan properties dialog.

## Registry Scans

Registry scans search through the Windows Registry and perform selected actions. A registry scan configuration is a collection of properties that:

- Define one or more computer systems to scan.
- Define the categories that include the target registry keys.
- One or more actions to perform when a registry key match is made.

### Registry Scan Procedure

The general steps to create and implement a registry scan and then evaluate scan result data includes:

#### 1 Plan the registry scan.

Determine the purpose of the registry scan, which systems to include in the scan, the registry keys to search for and the action to take when target keys are found. Try to narrow the criteria as much as possible, such as, scanning only the necessary systems and only the required predefined key. Less time and resource overhead is required to run a scan with narrow scan properties than one with broadly-defined properties.

#### 2 Set up supporting structures.

Add the target registry key(s) to a category through the **Categories** topic in the console. Target keys that are only to be logged can be placed in either the **Removable Registry Entries** or **Writable Registry Entries** subgroups in a category. Keys to be removed or written must be established in the corresponding category subtopic.

#### 3 Add a new registry scan configuration.

In the **Registry Scans** topic window, add a new registry scan with the **Add** function or select **Add** from the right-click menu. In the **Registry Scan Properties** dialog, enter a name and a brief description for the scan. Select systems and folders to scan. Select categories that include the target registry keys. Select the action(s) to take when target registry keys are found.

#### 4 Save the new registry scan configuration.

Use the **Save** selection on the **File** menu or the **Save** toolbar function.

#### 5 Run the registry scan.

Use **Run** in the **Registry Scans** window or **Run** on the right-click menu (select the registry scan name). The registry scan can also be added as a task in a scheduled job.

#### 6 Run on-demand or scheduled report(s) using the log file produced in step 5. By default, the report uses the most recent log file.

- Run an on-demand report through the **Reports** topic after viewing the report online, choose to release the report or export it to a file.
- Set up report properties through the **Reports** topic. Create a scheduled job through the **Scheduling** topic that includes the report in the list of tasks. Either select a save location for the report file or include one or more addresses to send the report to.

## Configuring Registry Scans

A registry scan configuration includes:

- Client system(s) to scan  
Windows NT and later systems can be selected.
- Categories to include in the scan  
Target registry keys are included in any category in either the Removable Registry Entries or Writable Registry Entries subgroup.
- Actions to perform when a match is made.

### Registry Entries

Registry entries for scans performed on the *console* client can include the following predefined keys:

- HKEY\_CLASSES\_ROOT
- HKEY\_CURRENT\_CONFIG
- HKEY\_CURRENT\_USER
- HKEY\_LOCAL\_MACHINE
- HKEY\_USERS

Registry entries for scans performed on *remote* clients can include the following predefined keys:

- HKEY\_LOCAL\_MACHINE
- HKEY\_USERS

The complete registry key path must be included, for example:

```
HKEY_CURRENT_CONFIG\Software\Fonts
HKEY_LOCAL_MACHINE\SOFTWARE\Adobe
```

Abbreviations can be used for:

- HKLM for HKEY\_LOCAL\_MACHINE
- HKEU for HKEY\_USERS

When scanning for users that are currently logged into a computer, the HKEY\_CURRENT\_USER key is used. To find keys for all users that have access to the computer, the HKEY\_EACHUSER key is used (only for use with DynaComm PointGuard).

## Registry Key Actions

If no action options are enabled in the Registry Scan Properties dialog, all registry keys listed in the Writable Registry Entries or Removable Registry Entries category subgroups are logged, only.

When the Delete removable keys option is enabled, registry keys to be removed must be included in the Removable Registry Entries subgroup. Any entries in the Writable Registry Entries subgroup are ignored.

When the Add writable keys option is enabled, registry keys to be written to the registry must be included in the Writable Registry Entries subgroup. Any entries in the Removable Registry Entries subgroup are ignored.

If both options are enabled, removal is performed before the write function. This has implications when the same key is listed in both subgroups for a single category. Scan run results only reflect that the key has been added.

The Lock Keys and Unlock Keys options changes registry key security to block others from changing key values or allow others to change key values, respectively.

Enabling the Shutdown Client option starts the Windows shutdown process. The default shutdown time is 12:00 am.

## Viewing Registry Scan Properties and Logs

Two windows are used to work with registry scans and scan run results:

- **Registry Scans**  
(Select the Registry Scans topic in the topics pane)

Registry scan maintenance functions (**Add**, **Edit**, **Remove**) as well as starting and stopping a registry scan (**Run**, **Stop**) are performed through this window. All currently defined registry scan configurations are listed in the details pane with status information for the last scan run.

- **Registry scan run results**  
(Select an individual registry scan name in the topics pane)

The details split pane shows:

- *Scan run instances* pane

Lists one line of data for each registry scan run. Data includes date and time of scan run instance, client statistics and run status.

Scans and scan result information is manipulated by:

- Selecting a scan run in this list; displays run details in the Summary pane.
- Clicking **View Results**; displays list of registry entries logged during the file scan in the Registry Scan Log Viewer.

- Clicking **Properties**; displays registry scan configuration properties (**Registry Scan Properties** viewer) that were in effect for the selected scan.
- Clicking **Stop** during an active scan run; aborts a running scan.
- Clicking **Delete**; removes the registry scan log and associated configuration information.

- **Summary** pane

Lists run details, by client computer, for scan start and end, number of keys and values processed and number of items and errors logged.

## Registry Scan Considerations

When creating and running registry scans and producing reports on scan results consider the following:

- As much as possible, narrow the number of target registry keys. Choosing the defaults in a registry scan is choosing to scan all registry keys.
- Narrowing target registry keys help to:
  - Reduce data to be evaluated.
  - Require less resources to store log data.
  - Avoid exceeding database size limits which stops the merge process of log data. Unmerged log file data is not accessible.
  - Reduce processing time required to merge log data to database file.
  - Reduce CPU utilization on the target machine.
- When working with the Registry Scan Properties dialog, the systems shown for selection in the Computer and File Selector dialog is dependent on the access rights granted to the user account that you logged on with to the DynaComm PointGuard server. If the user account has access to Active Directory, then that structure is shown. Otherwise, the Microsoft Networking structure is shown.
- Registry scans can be run on-demand or placed in a scheduled job.
- Registry scans that include two or more computers produce a single database file on the DynaComm PointGuard server system that contains all data from all systems included in the scan.
- The .XML log file created on target systems (distributed scan) is removed when the log file is retrieved by the DynaComm PointGuard server.
- A registry scan can be run concurrently with a file scan or system policy session on the same system with no impact to the registry scan. However, this scenario may impact the system policy session. See Topic: System Policies in this Chapter 6 for detailed information.

## System Scans

System scans are designed to quickly set up file and registry scans for frequently-requested scan functions. A system scan may include one or more file scans, registry scans or both.

By default, the majority of system scans look through *all* folders on each selected system. After the system scan is saved, individual file scans created by the system scan can be modified to include selected folders.

### System Scan Procedure

The general steps to create and implement a system scan and then evaluate scan result data includes:

- 1 Start the New System Scan wizard.

The wizard is started by either:

- Double-clicking a system scan icon in the Content Management window.
- Right-clicking the System Scans topic and selecting New System Scan from the popup menu.

- 2 Complete each wizard dialog.
- 3 Start or save the new system scan configuration.

Click one choice in the Scan Summary dialog.

- 4 After running the scan, view individual scan instance results.
  - Use the File Scan results viewer for file scans. Double-click the result listing in the Summary pane.
  - Use the Registry Scan results viewer for registry scans. Double-click the result listing in the Summary pane.
  - Use the System Scan Properties viewer for system scan properties.
  - Run on-demand or scheduled report(s) using the log files produced in step 3.

Set up report properties through the Reports topic.

- By default, the most recent log file is used to generate report data. This can be changed in the report properties.
- For a scheduled report, select either a save location for the report file or include one or more addresses to send the report to.

A scheduled report is created by including the report as a task in a scheduled job. Create the scheduled job through the Scheduling topic.

After viewing an on-demand report, you can close or print the report or export it to a file.

#### Note

*See Appendix D System Scans for detailed information on file or registry scans included in a system scan.*

## New System Scan Wizard

The New System Scan wizard collects information about the machines to scan and, for selected scans, the actions to perform. To use the New System Scan wizard

- 1 In the System Scans window, double-click the wizard name.
- 2 In the System Scan Name dialog,
  - a In Name, key in a name for the system scan and click Next.
  - b In Description, update the scan description with a custom description, if needed.
- 3 In the System Scan Clients dialog,
  - a Do one or both of the following:
    - Enable the Scan this computer option to include the DynaComm PointGuard console system in the scan (apply check mark).
    - Click Add to select one or more systems.
  - b Click Next.
- 4 On the Scan Actions dialog, select one action option and click Next.
- 5 On the System Scan Summary dialog, verify the scan name and review the file and/or registry scans that will be created for the system scan.
- 6 Choose one of the following:
  - Run Now to start the system scan immediately.
  - Schedule . . . to create a scheduled job that includes the system scan as a task.
  - Done to save the system scan for later execution.

### Note

*Windows 9.x systems cannot be included in a system scan.*

## Working with System Scans

Saved system scans are started with the Run function from the right-click menu in the topics pane of the System Scans window. A one-line listing for the scan run appears in the upper details split-pane that includes the date and time of deployment and the current or last status of the scan run instance.

System scans are modified with the Edit function selected from the right-click menu in the topics pane. Client systems can be added to- or removed from the system scan, and the scan name can be changed.

Selecting one run instance in the details pane and clicking Results in the details pane displays system scan results. Detailed summary information for each client included in the system scan is shown in the system scan results viewer.

A currently running scan is aborted with the Stop function. The Last Status column will reflect “Aborted.” All running scan instances can be aborted with Stop All selected from the right-click menu in the topics pane.

One or more scan instances are removed with the Delete function in the details pane or with the Delete function selected from the right-click menu in the topics pane. You are asked to confirm the deletion.

The Summary (lower-split) pane lists all file and registry scans that were run in the selected system scan. Individual file or registry scan results are displayed by either double-clicking the one-line scan listing or by selecting Results from the right-click menu. On-demand reports are generated with the Reports function from the right-click menu.

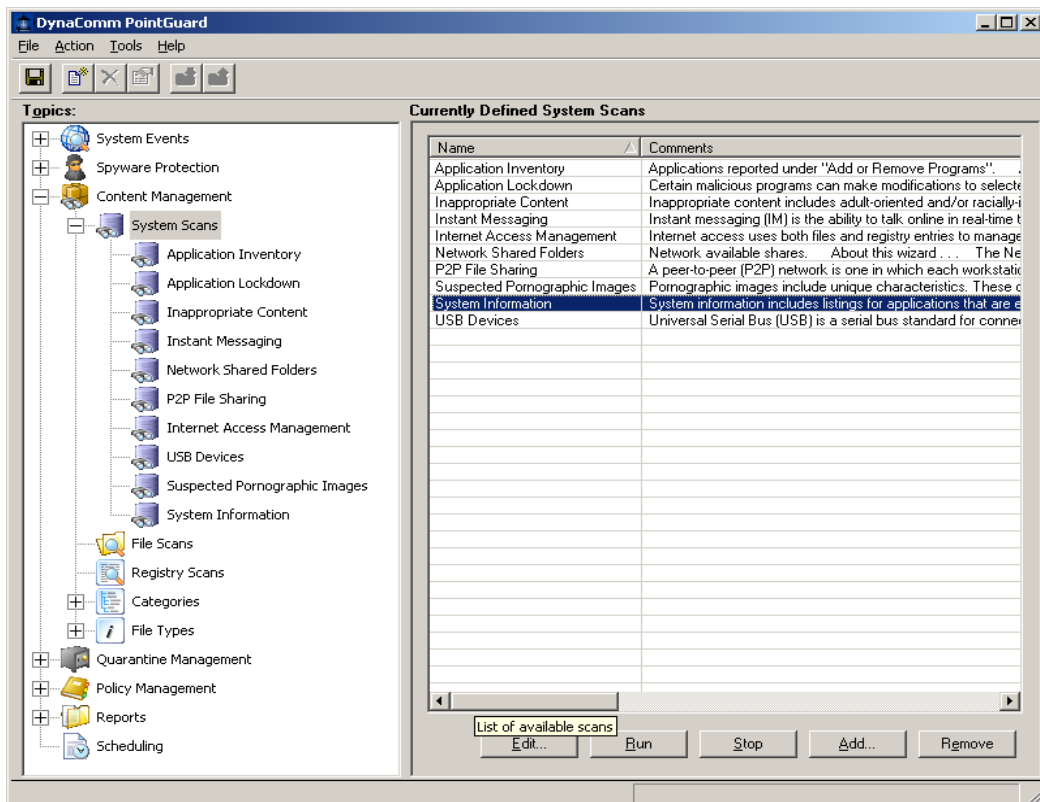


Figure 5.1  
System Scans window

## Quarantine Management

One quarantine file is created for each file scan run instance that includes quarantining or for each spyware scan that includes cleaning of detected infections. Each quarantine file may contain one or more quarantine items. The items that are quarantined depend on scan type and scan properties. Spyware scans can include files, cookies and registry entries as quarantine file items.

Quarantine files are stored on each client system. Records of each quarantine file and file items are stored in the Quarantine database on the console system. The Quarantine Management window displays the records stored in the Quarantine database.

The Quarantine Management window displays quarantine file information by client in the details panes.

- ◆ Upper pane

Lists each client and the number of quarantine items stored for all scans that have been run on the client.

Total size for all quarantined items is shown.

- ◆ Lower pane

Provides detailed quarantine file information for a client selected in the upper pane. One line is listed for each scan run instance and displays:

- Number of items quarantined in the scan run instance.
- Date and time that the items were placed in quarantine.
- Date that quarantined items will be purged from the quarantine file.
- Scan name
- Scan type
- Current status of the quarantined items.
- Total size for all quarantined items.

## Working with Quarantine Files

Quarantine files can be:

- ◆ Removed (purged) through the Purge function or the Purge All right-click menu selection.

All items in the quarantine file are removed along with the quarantine file.

- ◆ Restored through the Restore function or the Restore All right-click menu function.

A restored item is returned to its original location and removed from the quarantine file.

The Status column reflects the status *Purged* or *Restored* when the corresponding function is used.

## Default Quarantine Settings

When DynaComm PointGuard is installed, one default setting is created for the length of time that items remain in quarantine before they are automatically removed. The Default client quarantine lifetime option on the Settings tab of the Options dialog in the New Client Settings option group specifies a default of 168 hours (7 days). This can be changed at anytime and takes effect with the next save of DynaComm PointGuard.

## Details

The Details topic provides functions for working with quarantine file items. Selecting Details in the topics pane displays the Details window. The details pane of the Details topic window is divided into:

- ◆ *Filter group*  
  
Provides controls for refining the display of quarantine items. By default, all quarantined items are shown sorted by client name.
- ◆ *Quarantine Items list*  
  
Displays one listing for each quarantined item. Each listing provides quarantine details about the item.

## Filtering the Quarantine Items Display

Advanced filter options are accessed by expanding the Filter group (toggle Advanced Filter Options in the Filter group). Items are filtered with the following controls:

Quarantine Time	Specify a date and time range based on a quarantine or auto-purge time.
Display	Select one or more item types.
Item	Supply a character string that matches item name, path, registry entry, etc.
Scan Name	Enter a scan name.

Filter options can be used in any combination. Wild card characters can be used in the Item or Scan Name controls.

- “\*” - represents unlimited number of characters
- “?” - represents a single character

When multiple parameters are entered in Item or Scan Name, separate each parameter with a semi-colon.

## Working with Quarantine Items

Quarantine items are selected in the Client Items list using standard window selection techniques. The following window functions are used to work with quarantine items:

Retrieve	Quarantine item(s) are moved from the quarantine file to a specified location; item(s) are stored at the new location in a zip file with a new name.
Restore	Retrieved or quarantined item(s) are returned to their original location.
Purge	Selected item(s) are permanently removed from the quarantine file; purged items cannot be restored.

---

# Chapter 6

## *Managing Client Activities*

---

Client activities are managed through the use of system policies. A system policy includes selected client systems policy items that direct allowed or blocked activities on the client systems.

System policies are created and managed through the System Policies topic. Policy items are created and managed through the Policy Items topic. Both topics are accessed through the Policy Management topic

## System Policies

System policies are used to monitor and control actions performed on client systems with files, USB devices and Windows Registry changes. A system policy includes one or more client systems and one or more policy items. A policy item is a set of rules that manage file, device or Windows Registry activities.

### System Policy Procedure

The general steps to create and implement a system policy and then evaluate logged data includes:

1 Plan the system policy.

Determine policy properties which includes:

- System policy purpose.
- Client systems to include.
- Policy items to include.
- Action(s) to take when a policy rule makes a match.
- Time(s) that policy item rules will perform selected actions.

2 Set up supporting structures for the system policy.

- Create a new time interval or modify an existing time interval.

A time interval is used in rules in either file management or device management policy items to specify when selected actions are performed.

- Create one or more policy items.

In the Policy Items window, either use the “Default” policy item or add a new policy item. Add one or more rules to the policy item that specifies the elements to monitor and the actions to take. Set the priority for each rule.

3 Add the new system policy.

In the System Policies window, create a new system policy, add at least one client system, and add one or more policy items.

4 Save changes.

Use the Save command on the File menu or the Save toolbar command.

Saving changes deploys the client component to all client systems in the system policy, pushes the system policy to all client systems and starts the client service. The system policy is in effect when the client service is active. Rule actions are applied during the “active” times set up in the time interval.

Allow some time to elapse to log activity data to the client logs. Individual log files are created on each client system

5 Retrieve log data through the System Policies or individual system policy window.

6 Run on-demand or scheduled report(s) with the log files produced in step 5.

Run an on-demand report through the Reports topic. After viewing the report online, choose to close the report or export it to a file.

Create a scheduled job through the Scheduling topic that includes the report in the list of tasks. Either select a save location for the report file or include one or more addresses to which the report is sent.

## Working with System Policies

System policies are managed through the System Policies window. All system policies are listed in the details pane when System Policies is selected in the topics pane or under System Policies when the topic is expanded.

In the System Policies window, a new policy is added with either the Add function in the details pane or with the Add New System Policy selection on the topics pane right-click menu. The System Policy dialog collects a name for the new policy.

Selecting an individual system policy in the topics pane shows policy details in the details pane. The Policy Information tab displays summary information about the total number of clients systems included in the selected policy, the number of client systems that received the last push of policy items, and last date and time that policy items were pushed to client systems. All policy items that are currently assigned to the system policy are listed in the Policy Items list. All current policy items are sent to client systems with the Publish function. New policy items are added with the Add function and removed with the Remove function.

The Clients tab lists all client systems included in the system policy and reports current client communication and policy status information. New client systems are added to the system policy with the Add function. One or more existing client systems are removed from the system policy with the Remove function. Client details are displayed in the Client Details dialog with the Details function.

Logs are retrieved for one or more individual client systems, all clients in a system policy or all clients in all system policies. Selecting one or more clients on the Clients tab and using the Retrieve Logs function retrieves individual client logs that are merged into one log file on the server system. To retrieve all client logs for selected system policies, use the Retrieve Logs function in the System Policies window or use the Retrieve Logs selection on the details pane right-click menu after highlighting one or more system policies. To retrieve all client logs for all system policies, use the Retrieve all logs selection on the topics pane right-click menu for the System Policy topic.

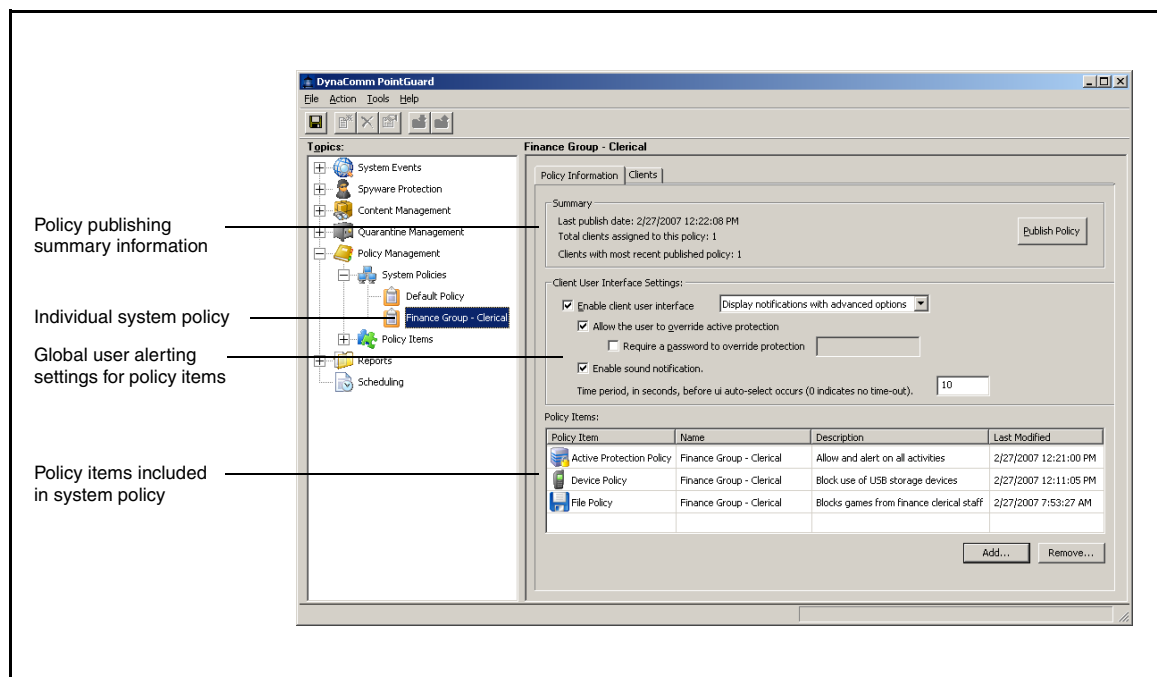


Figure 6.1  
Individual system policy window — Policy Information tab

## Policy Items

A policy item is a set of one or more rules. A rule is a statement that specifies the actions to perform when certain conditions for files, Registry keys or USB devices are true. A system-policy session compares the activities of client systems included in the system policy with rule properties.

When a new policy item is created, the policy is given a unique name and one or more rules are added. A system policy can share policy item(s) with other system policies, can include unique policy items, or can include a mix of both.

## Active Protection Policy Items

The Active Protection function, sometimes called real-time threat protection or RTP, monitors Windows Registry areas that are most frequently modified when new software components are installed.

Active Protection policy items are set up through the Policy Management configuration topic. An active protection policy item is then added to a system policy to activate active protection for a group of client systems. Active Protection becomes effective when the system policy is pushed to client systems. When system protection is active, a green shield appears in the user's system tray on the taskbar.

Active Protection monitors one to fourteen "protected areas" in the Registry. Figure 6.2 shows the Real-time Protection Settings dialog that lists fourteen Registry areas. One or more areas are added to an Active Protection policy item.

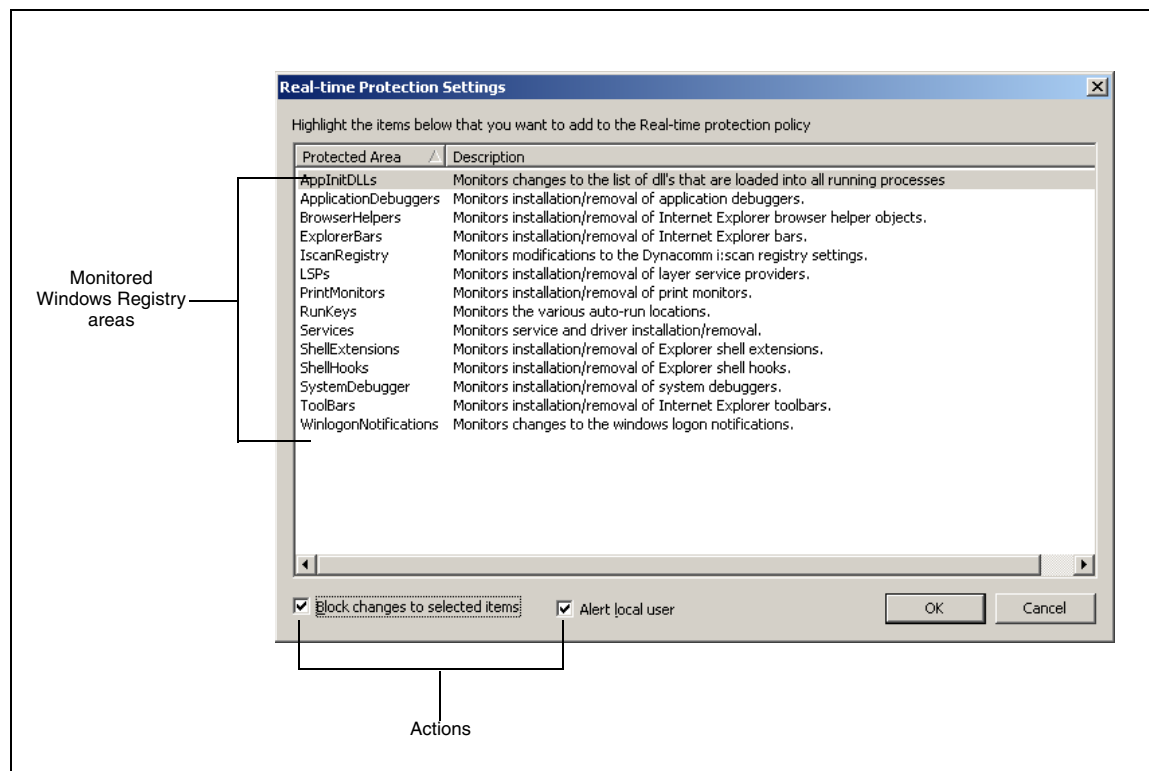


Figure 6.2  
Default settings on the Real-time Protection Settings dialog

## Active Protection Actions

By default, each protected area is set to have changes blocked and to send an alert message to the user about the requested change. An individual protected area can be set to one of the following action combinations:

- Allow changes and alert user
- Allow changes but do not alert user
- Block changes and alert user (default)
- Block changes and do not alert user

Each protected area selected for a policy item can have its own unique action combination by selecting or clearing the Block changes to selected items and Alert local user action options.

A range of options for user and server alerts is available for Active Protection. Users can be allowed to choose the action to take on requested Registry changes or given a visual alert only. User alerts can be set by individual or groups. See Chapter 8 Alerting for detailed information on Active Protection alerting.

## File & Device Management Policy Items

File and Device management rules are set up in the Rule Properties dialog. Each rule is identified with a name and short description which is shown in the individual policy item window. When a rule is added, it is automatically assigned the “active” status. The rule can be disabled by clearing the Active option in the Rule Properties dialog or can be completely removed through the individual policy item window.

Remaining rule properties are accessed through dialog tabs and include:

### Device Management Policy Item

- Devices - default: all devices
- Users - default: all users
- Time - default: all times time interval
- Action - default: all actions enabled

### File Management Policy Item

- Files - default: all files
- Processes - default: all processes
- Users - default: all users
- File Owners - default: all users
- Media - default: all media types
- Time - default: all times time interval
- Action - default: all actions enabled

### Note

*When selecting properties in a rule, file owners can be an individual user or a group of users. If the Administrators group is selected, you must also include each user name in the Administrator group as an individual user.*

### Rule Conditions

Selecting properties in the Rule Properties dialog sets up rule conditions. When all conditions are met, rule evaluation is equal to *true* and specified rule actions are performed. When at least one condition is not met, the rule evaluation equals to *false* and specified rule actions are not performed.

Rule conditions exist *between* and *within* properties selected on tabs in the Rule Properties dialog. These conditions are:

- **AND**   Exists *between* properties selected on separate tabs, i.e., selected files AND selected processes AND selected users, etc.
- **OR**     Exists *within* properties selected on the same tab, i.e., file A OR file B OR file C, etc.

For example, let's say that you want to create a rule that blocks everyone from playing the Windows computer games of Hearts, Solitaire and Minesweeper. You would establish these properties in the Rule Properties dialog for the Block Games rule with the conditions seen in Figure 6.3.

### Rule Priority and Processing

When a rule is added, it is automatically assigned the next priority order in the rule set. The priority order specifies the sequence that rules in the rule set are used to evaluate monitored activities of the system policy group. Rule order in the rule set is changed through the Rule Set window.

A monitored action is evaluated with the first rule in the policy item. If the rule evaluation results in a false condition, the processing proceeds to the next rule. This process continues until the rule evaluation of the monitored action results in a true condition. At this point, rule actions are applied and no further rule processing is performed.

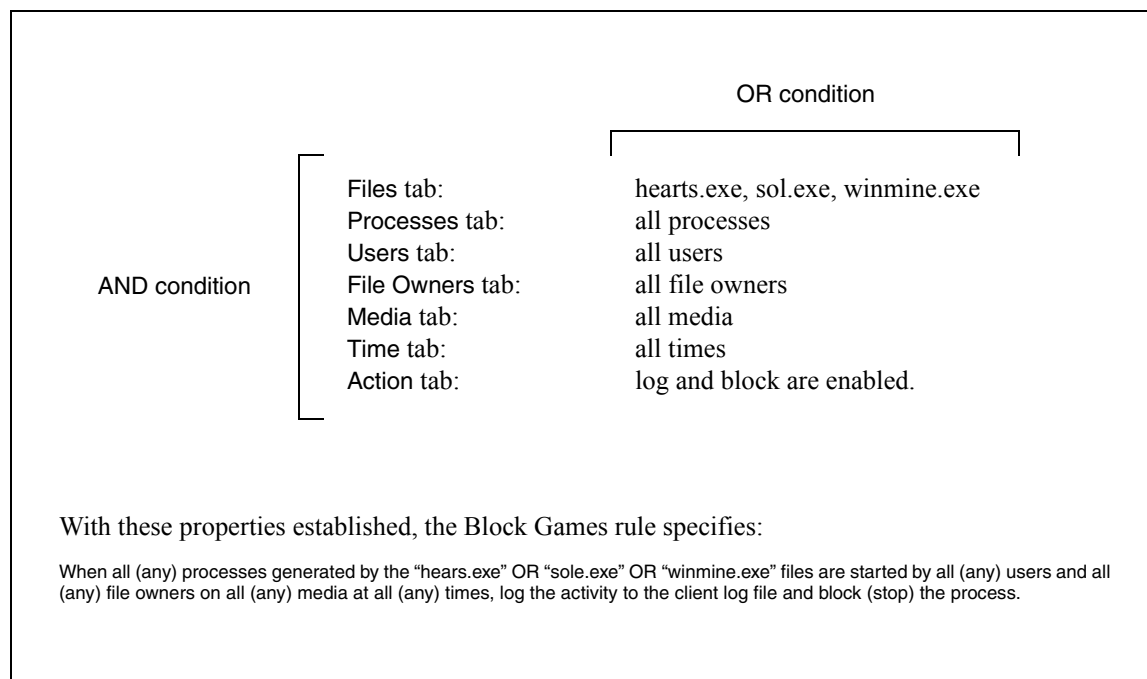


Figure 6.3  
*Rule conditions*

In Figure 6.4, two rules have been established to restrict access of payroll files and payroll processes to users in the Payroll user group. The third rule prevents access to games by members of the Payroll user group by blocking game processes. It also sends an alert message to the payroll supervisor

Priority	Name	Description	Active
1	Restrict Payroll Process Access	Prevent access to monthly pay...	Yes
2	Restrict Access to Payroll Files	Prevent access of payroll files ...	Yes
3	Block and Alert use of Games	Prevents playing games	Yes

Figure 6.4  
*Rule processing example*

when someone attempts to play games. John is a member of the Payroll user group. When he runs the monthly payroll application (Rule 1) or opens a payroll file (Rule 2), rule evaluation of his activities result in a true condition and he is allowed to run those processes. Remaining rules are not processed.

However, when John attempts to start Solitaire or Pinball, Rule 1 and Rule 2 processing evaluate to a *false* condition and rule processing continues to Rule 3. Rule 3 processing results in a *true* condition and rule actions are performed which block use of the game and send an alert message.

### Rule Actions

Rule actions are established on the Action tab of the Rule Properties dialog. Actions for file management can include enabling one or more of:

- Logging  
(Default: Enabled)
- Block access to the file  
(Default: Enabled)
- Prevent writing to the file
- Send an alert message to the DynaComm PointGuard server

Actions for USB device management can include enabling one or more of:

- Block access to the device
- Send an alert message to the DynaComm PointGuard server  
(Default: Enabled)
- Send an alert message to the user

Rule notification is sent when rule evaluation results in a true condition. Notification is enabled on the Action tab in the Rule Properties dialog. File policies send a message to the DynaComm PointGuard server. Device policies send a message to the DynaComm PointGuard server or the user.

Sending an alert message to the DynaComm PointGuard server displays a one-line entry in the respective System Event subtopic. See Chapter 8 Alerting for more information on sending alerts and the alerting process.

### Predefined Policy Items

DynaComm PointGuard includes two predefined rule sets which are described in Appendix D Predefined Rules & Rule Sets. The first rule set, Block Malware Installation Via Browsers, includes one rule that blocks and logs installation attempts of executable files. By default, this rule is active. This rule set can be assigned to a monitored computer group to begin immediate blocking of unwanted downloads of adware, spamware and more.

The second rule set includes nineteen rules that represent the most commonly established rules to block and/or log access to selected file types, storage devices or media. By default, none of these rules are active. These rules can be copied into a different rule set and then activated, or selected rules can be activated in the Sample Rules rule set. The rule set can then be added to a system policy.

Predefined rule properties can be modified to customize monitoring actions. However, original rule properties cannot be automatically restored but can be manually restored using the information provided in *Appendix D Predefined Rules & Rule Sets*.

## Working with Policy Items

Expanding Policy Items in the topics pane displays the File Management, Active Protection and Device Management policy item topics. Each policy item type is managed through the respective topic window. Expanding a policy item in the topics pane displays all current policies for the policy item.

### Policy Items Windows

The File Policies, Active Protection Policies and Device Policies windows list all existing policy rule sets in the respective policy management area. The date and time that the policy was changed is noted along with a short description of policy item contents or functions (if one was provided).

Right-clicking a policy item window name in the topics pane provides access to the New Policy function to add a new policy (displays the Properties dialog) or to the Paste Policy function to paste a copied policy rule set.

Three functions are accessible through the window details pane. A new policy item is added to the list with the Add function by completing the Properties dialog. The policy item name and description are entered through this dialog. If no data is entered a default name is automatically provided. Using the Edit function with a policy item name highlighted also causes the Properties dialog to appear. The policy item name or description can be changed before clicking OK.

The Remove function deletes the highlighted rule set(s). A confirmation message dialog appears to confirm the removal. The policy rule set is removed from the database and cannot be restored.

Right-clicking a policy rule set name in the details pane provides access to two more functions in addition to the three discussed above. The Copy function places a copy of the selected rule set onto the Windows clipboard. Paste places a copy of the selected policy rule set *in the same policy item type*. “Copy of” is automatically prefixed to the copied policy name.

### Individual File & Device Policy Item Windows

Individual file and device management policy windows list all current rules in the policy item. Each rule listing displays the rule priority, name, description, and the active/inactive status of the rule.

Five functions are accessible through the window details pane. The Add function displays the Rule Properties dialog to set up properties for a new rule. Edit displays the properties of the highlighted rule in the Rule Properties dialog. Changes on the various dialog tabs are made before clicking OK. Remove deletes the rule from the list of rules in the rule set. The remaining rule priorities are adjusted. The Up and Down function move the highlighted rule up or down in processing priority within the rule set.

Right-clicking a rule in the details pane provides access to additional functions. The Copy function places a copy of the selected rule onto the Windows clipboard. Paste places a copied rule into the same rule set or another rule set *of the same policy type*.

### Individual Active Protection Policy Item Window

An individual Active Protection policy window lists the protected areas included in the selected policy item. The current action(s) in effect for each protected area with a short description of the protected area are shown.

Three functions are accessible through the window details pane. The Add function displays the Real-time Protection Settings dialog. A new protected area is selected and actions chosen to set up a new monitored protected area. Edit displays current properties of the selected protected area in the Real-time Protection Settings dialog. Action changes are made before clicking OK. Remove deletes the selected protected area from the Active Protection policy item.

## System Policy Considerations

### Security

- A system policy is pushed to a client system with the user account/password that is entered during installation on the Service Run As Account Information dialog. However, the system policy session runs on the client system under the System Account which is not monitored, i.e., ignored.
- When working with the Rule Properties dialog, the elements shown on the various tabs are dependent on the access rights granted to the user account that you logged on with to the DynaComm PointGuard server.

### Concurrent Activities

- A system policy session can be run concurrently with a file scan on the same system with no impact to the file scan. However, this scenario does impact the system policy session:
  - If the file scan is distributed (runs on the client system), the system policy session ignores the file scan process and does not log session activity, does not send alerts or messages and does not block access or prevent update of target files, processes, etc.
  - If the file scan is non-distributed (runs on the DynaComm PointGuard server), system policy session activity is logged and all selected actions are performed.

### Alerts

- Enabling the Alert option on the Action tab in Rule Properties dialog may quickly overwhelm the specified e-mail boxes, even if you have narrowed the processes, users, files, etc., that you are monitoring. This is particularly true when asking for alerts on allowed and frequently performed activities, such as, accessing common files.

## Log Data

- Restrict system policy monitoring to only those files, users, processes, etc., of interest. Monitoring “\*.exe” processes or “\*.doc” files typically produces more data, and requires more resources, than needed.

Narrowing files or devices to monitor helps to:

- Reduce data to be evaluated.
- Require less resources to store log data.
- Avoid exceeding database size limits which stops the merge process of log data. Unmerged log file data is not accessible.
- Reduce processing time required to merge log data to database file.
- Reduce CPU utilization on the target machine.
- If you only want to monitor client activities, disable the Log option on the Actions tab of the Rule Properties dialog. When this option is enabled, a log file is not created and retrieving/merging data into a database file on the server machine is not performed.
- Weigh resource requirements for producing a single database or report versus the need to have all data in one database or report. For example, when monitoring ten machines, it may be advantageous to place the machines in two or more groups and then produce separate reports of the logged data. Two merge processes of data from five machines may take less time and require less CPU resources than merging data from ten machines into one file. However, the importance of having all data in one database or report may outweigh processing requirements.

### Log Files

- Client log retrieval for a system policy session occurs when:
  - The Retrieve Logs function in a window is used.
  - Retrieve Logs is selected on a right-click menu.
  - A new or updated system policy is pushed to client systems. The DynaComm PointGuard server retrieves the current log and a new log file is created on the client system.
- The client log file is removed when the file is retrieved by the DynaComm PointGuard server.
- A new client log file is *not* created when:
  - Adding or removing a client system to a system policy.
  - Modifying a time interval through the Time Intervals topic.

### Database Files

- Each retrieval produces a single database file that contains all data for all client systems that are members of the system policy. If two system policies share the same policy item, two separate log files are stored on the server system.
- A new database file is created on the DynaComm PointGuard server when:
  - An updated system policy is pushed to the client system.
  - The current database file on the server reaches a size of 4GB.

## Time Intervals

A time interval is a set of active and inactive minutes and hours in selected days of the week. Time intervals are used in file and device policy rules to specify those times during which the rule is *active* or *inactive*. During active times, a rule evaluates requests and performs rule actions when the rule evaluation equals TRUE. During inactive times, rule evaluation is performed but actions are not executed. Time intervals are also used in report properties to specify the times for which data is to be included in a report.

Time interval properties are shown in the Time Interval dialog. This dialog displays a grid of seven rows, one for each day of the week. Each row is divided into 24 one-hour blocks. The first block represents the hour from 12:00 am to 12:59 am, the second block represents the hour from 1:00 am to 1:59 am, and so forth. Selected (highlighted) blocks indicate an active time. Clear blocks indicate inactive times.

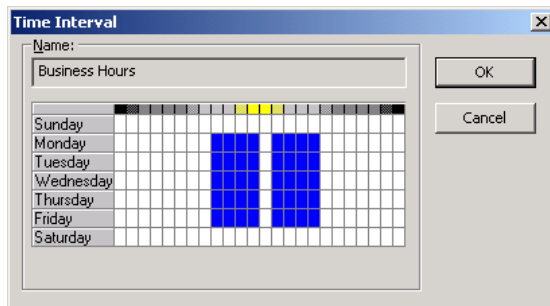


Figure 6.5  
*Predefined Business Hours time interval*

## Predefined Time Intervals

Three predefined time intervals with preset active and inactive days and times are included in DynaComm PointGuard. Predefined time intervals can be used as is, customized by changing active and inactive times or used as templates for creating custom time intervals. Predefined time intervals cannot be removed. Figure 6.5 shows the Business Hours time interval. See *Appendix F: Predefined Time Intervals* for a review of all predefined time intervals.

### Note

*Modified predefined time intervals cannot be automatically restored to their original settings.*

## Custom Time Intervals

Custom time intervals are created through the New Time Interval dialog which uses the All Times predefined time interval as a template. Establishing a new time interval includes entering a name for the interval and selecting active and inactive times. See the Online Help system for the mouse/keyboard techniques used to specify active and inactive times in a time interval.

### Notes

- ❖ *A custom time interval cannot be removed if it is referenced by a rule.*
- ❖ *Removed time intervals cannot be automatically restored. They can be manually re-added.*



---

# Chapter 7

## *Protecting Client Systems*

---

DynaComm PointGuard offers two solutions for managing spyware and other unwanted threats — active protection to control initial infection attempts of client systems, and spyware protection to locate and remove infections that have made their way onto client systems.

Active Protection policy items are reviewed in Chapter 6 and Chapter 8. This chapter reviews spyware configurations and the Sunbelt Threat database used by spyware scans to detect spyware infections on client systems.

## Spyware Protection

The Spyware Protection topic includes two configuration topics that work together to find and remove existing adware/spyware on client systems. The Definitions topic provides access to the Threat database that is used with spyware scans. The Definitions window offers functions to inactive and reactivate use of selected definitions for scans. The Spyware Scans topic provides access to creating modifying, running, stopping and removing spyware scans.

### Definitions

The Definitions topic provides functions to manage the Threat database. The Threat database holds infection definitions. Each definition includes all the elements associated with one infection. Elements can be any combination of file signatures, file names, folders, registry entries and domains.

All infection definitions are shown in the details pane when the Definitions topic is selected. The total number of infections in the Threat database and the last date of update of the database is shown at the top of the details pane. Each infection listing provides the infection type, threat level and short description of the infection. Refer to tables G.1 and G.2 in Appendix G Sunbelt Threat Database Threat Level & Infection Type Descriptions for descriptions of threat level and type. Selecting an infection in the listing displays more information about the infection in the lower pane of the details pane.

By default, each infection definition is “Active” meaning that it is actively used in spyware scans and in real-time threat protection. An infection can be made inactive such that it is not used by spyware scans.

### Updating the Threat Database

Updates to the Threat database are available for download from the FutureSoft web site 24 hours a day. Updating the Threat database requires a current, valid serial number established in the About dialog.

The update process can be initiated either on-demand with the Update selection on the Tools menu or through a scheduled job that includes the task: Update spyware definitions, keywords and file types.

### Working with Spyware Scans

An adware/spyware scan configuration is a collection of properties that includes a set of client systems to scan (required), the type of scan to perform (required), and how to clean infected client systems (optional).

Expanding Spyware Protection in the topics pane and selecting Spyware Scans displays all spyware scans in the details pane. The Add function displays the Spyware Scan Properties dialog to set up configuration properties for a new spyware scan.

Using the Edit function or double-clicking a scan in the details pane displays current properties in the Spyware Scan Properties dialog for the highlighted scan.

Run starts the highlighted scan(s). The Stop function stops the highlighted running scan(s). Remove deletes the selected scan(s). The right-click menu, accessed in the details pane offers these same functions.

## Spyware Scan Procedure

The general steps to create and implement a spyware scan and then evaluate scan result data includes:

- 1 Plan the spyware scan.
 

Determine what actions the scan is to perform, which systems to include in the scan and what level of scanning to perform (Standard or Deep).
- 2 Set up supporting structures.
 

Add client systems through the Client Management dialog. If needed, modify infection definitions to inactivate or activate selected definitions.
- 3 Add a new spyware scan configuration.
 

In the Spyware Scans topic window, click Add and select or enter scan properties in the Spyware Scan Properties dialog.
- 4 Save the new spyware scan configuration.
 

Use the Save selection on the File menu or the Save toolbar function.
- 5 Run the spyware scan.
 

Use Run in the Currently Defined Spyware Scans window or Run on the right-click menu (select the spyware scan name). The spyware scan can also be as a task to a scheduled job.

When the scan is complete, log file data is encrypted with a 64-bit RC4 symmetric stream encryption algorithm before being sent to the server.

- 6 Review results of the scan.

In the details pane of the individual spyware scan window:

- View summary information for the scan on the Summary tab.
- View summary information for the individual client machine on the Clients tab.
- View detailed information for an individual client machine by double-clicking the client listing on the Clients tab.

- 7 Run report(s).

Right-click a client listing on the Clients tab in the details pane of the individual spyware scan window and select one of the following reports:

- Summary by Threat Type and Level
- Summary by Client
- Summary by Infection

A spyware report can also be added as a task in a scheduled job.

## Configuring Spyware Scans

Spyware scan properties are set up in the Spyware Scan Properties dialog. This dialog includes three groups of option properties:

- **Spyware Scan clients *group***

Clients are selected through the Computer Selector dialog which is accessed by clicking Add in the Spyware Scan clients group. Client names are either manually entered or selected through a network tree. For new clients, the client software is installed the first time the spyware scan is started and options must be applied through the Client Management dialog.
- **Spyware scan options *group***

Spyware scans can be either:

  - **Standard**

Standard scans review cookie files, System folder, desktop files, selected registry entries and all running processes and modules.
  - **Deep**

Deep scans perform all functions of a standard scan as well as scanning all files in all folders on all drives, all registry entries and all running processes and modules.
- **Cleaning Options *group***

Cleaning detected infections is optional. Enabling clean removes detected files and registry entries. Two separate options allow for stopping infected processes and forcing a reboot to clear the processes.

To review or change current spyware scan properties, double-click the scan name in either the topics pane or in the Currently Defined Spyware Scans list in the details pane. The Spyware Scan Properties dialog appears to display the current set of defined properties for the scan.

## Spyware Scan Run Summaries

Spyware scan run summaries are displayed in the details pane. This pane is divided into three sub-panes which present summary information about the selected scan instance.

- **Deployments (*top pane*)**

Each run instance is listed with a run summary that includes client and infection data. Selecting an individual run instance updates the charts displayed in the middle pane
- **Deployment summary graphs (*middle pane*)**

Graphical summaries for the selected run instance are displayed for:

  - **Infection Statistics**

Ratio of infection states for all clients included in the scan.
  - **Threat Levels**

Ratio of infection threat levels for all scanned clients. Table G.1 provides descriptions for each of five threat levels used by the Threat database.
  - **Infection Types**

Ratio of the different types of infections found on all clients. Table G.2 in Appendix G provides descriptions for eleven infection types or categories used by the Threat database.

### Note

*For more information on threat levels and infection type descriptions, visit the Sunbelt Software Research Center web site at: <http://research.sunbelt-software.com/>*

- Infections summary (*bottom pane*)

- Summary tab

The Summary tab displays a list of individual infections found on all client systems. Selecting an infection listing displays the infection description below the infection list. Options for cleaning selected infections are offered from a right-click menu.

- Clients tab

The Clients tab provides summary information for each client included in the scan. Clean options, reports or detailed scan results for a selected client are offered from a right-click menu. Double-clicking a client name displays detailed scan results for the selected client in the Spyware Scan Results viewer.

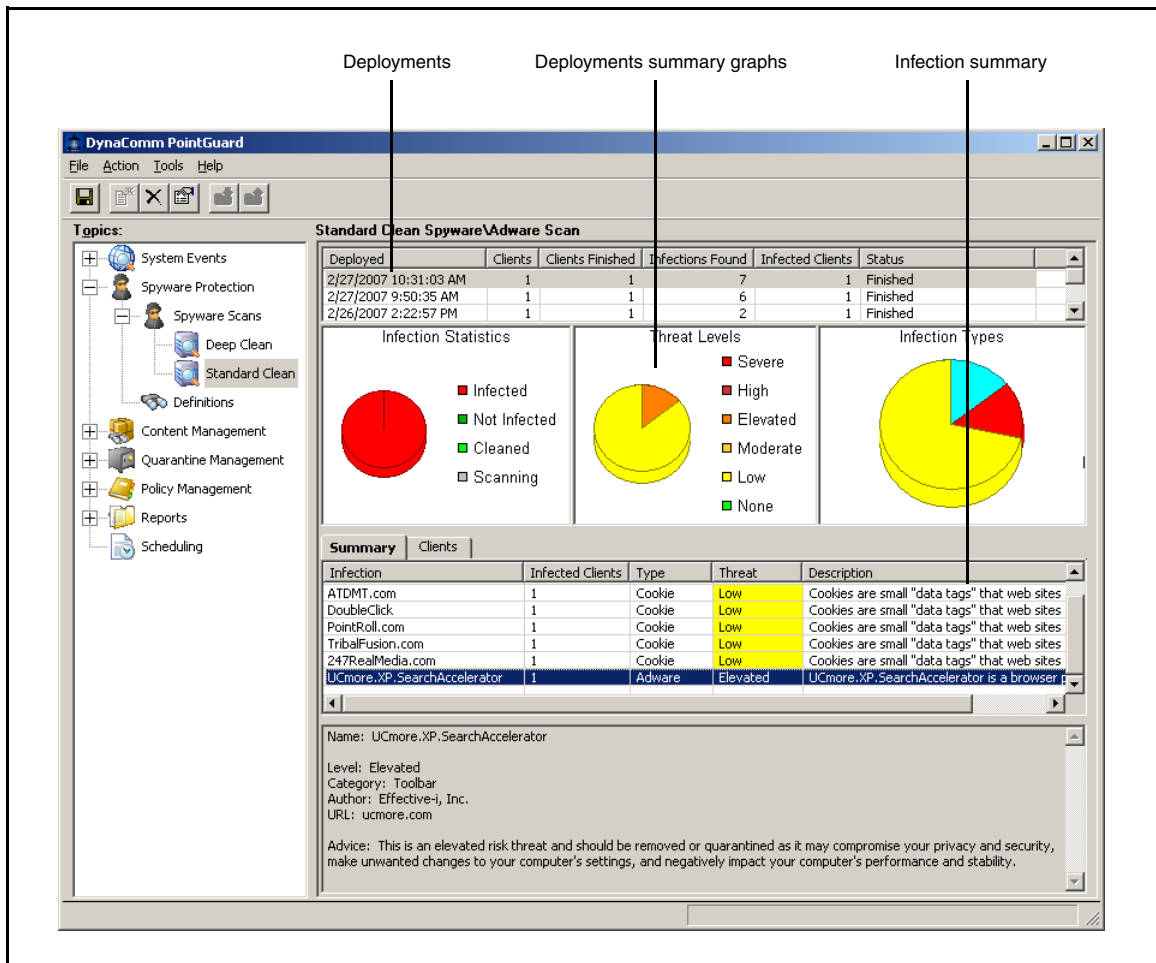


Figure 7.1  
Spyware scan run summaries window

## Spyware Scan Results Viewer

Figure 7.2 presents an example of detailed results for a spyware scan. The Spyware Scan Results viewer displays the information in three panes:

- Graphic summary (*top pane*)

Two pie charts are presented in the top pane. The first chart, Threat Level, illustrates the relative threat level for all infections found on the client system. Refer to Table G.1 in Appendix G for threat level descriptions.

The second chart, Infection Types, displays the ratio of the different infection types found on the client system. Refer to Table G.2 in Appendix G for infection type descriptions.

- Infection listing (*middle pane*)

All infections found on the client are listed in the middle pane. Each listing includes the total number of infection items and infection description summary.

- Infection item details (*bottom pane*)

Selecting an infection in the infection listing pane (middle) displays all items associated with the selected infection in the infection item details pane. Detailed information begins with descriptive information about the selected infection. Summary information follows that lists all individual infection items found in specific areas of the client file system and Registry file. This information can include one or more of the following:

- Cookies
- Toolbar Hooks
- Run Key Hooks
- LSP Entry Hooks
- Registry Infections
- Infected Processes
- File and folder infections
- Browser Helper Object Hooks

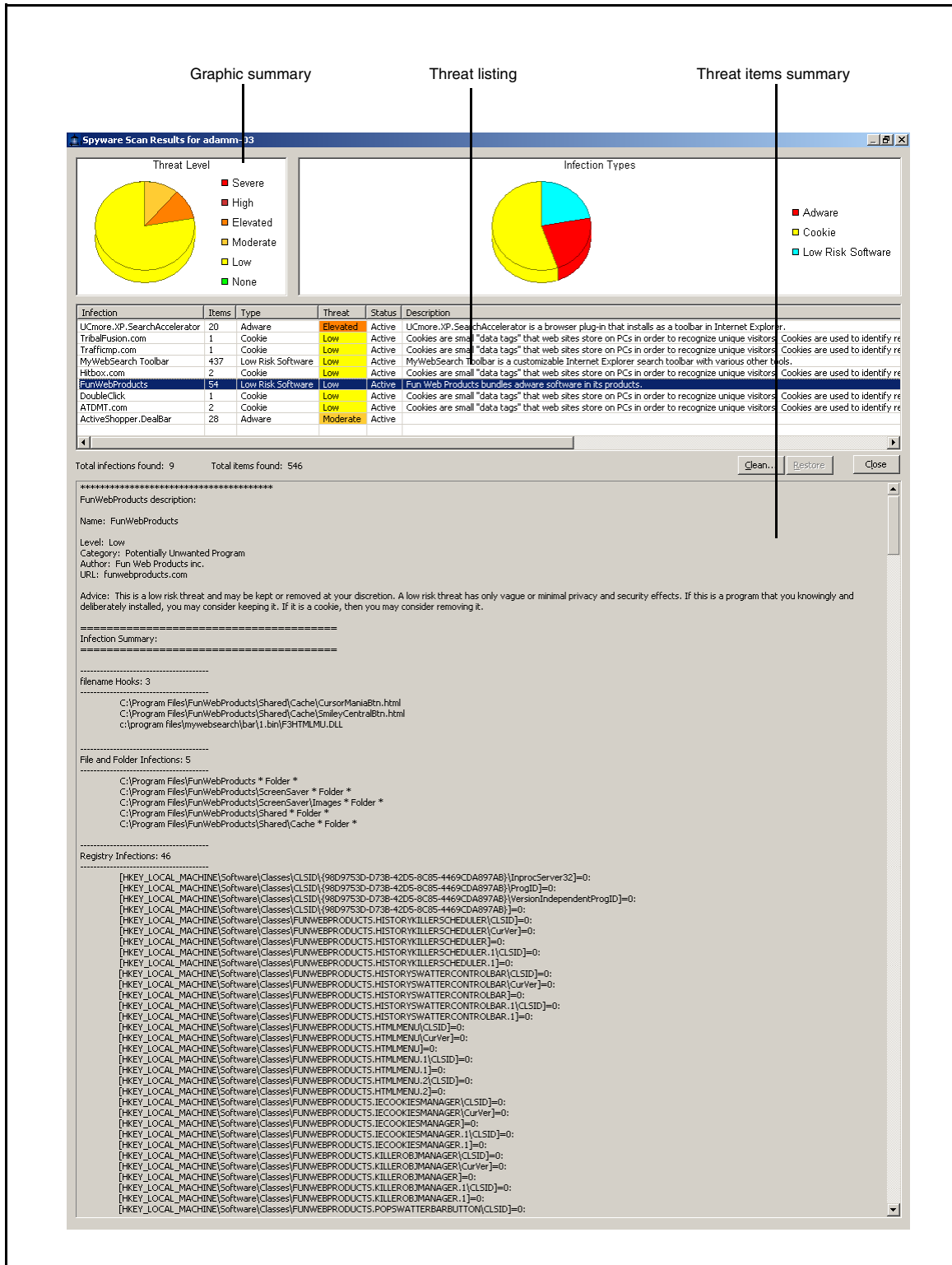


Figure 7.2 Detailed Spyware Scan Results window

## Spyware Scan Reports

Report: Summary by Client

Spyware scan reports are accessed from the Spyware Scans topic window. Right-click either a run instance in the list of deployments or a client name on the Clients tab to select one of the three available spyware reports.

This report presents a data table that groups data by individual client. For each client, all detected infections and infection details are listed. See Figure 7.3 for a sample Summary by Client report.

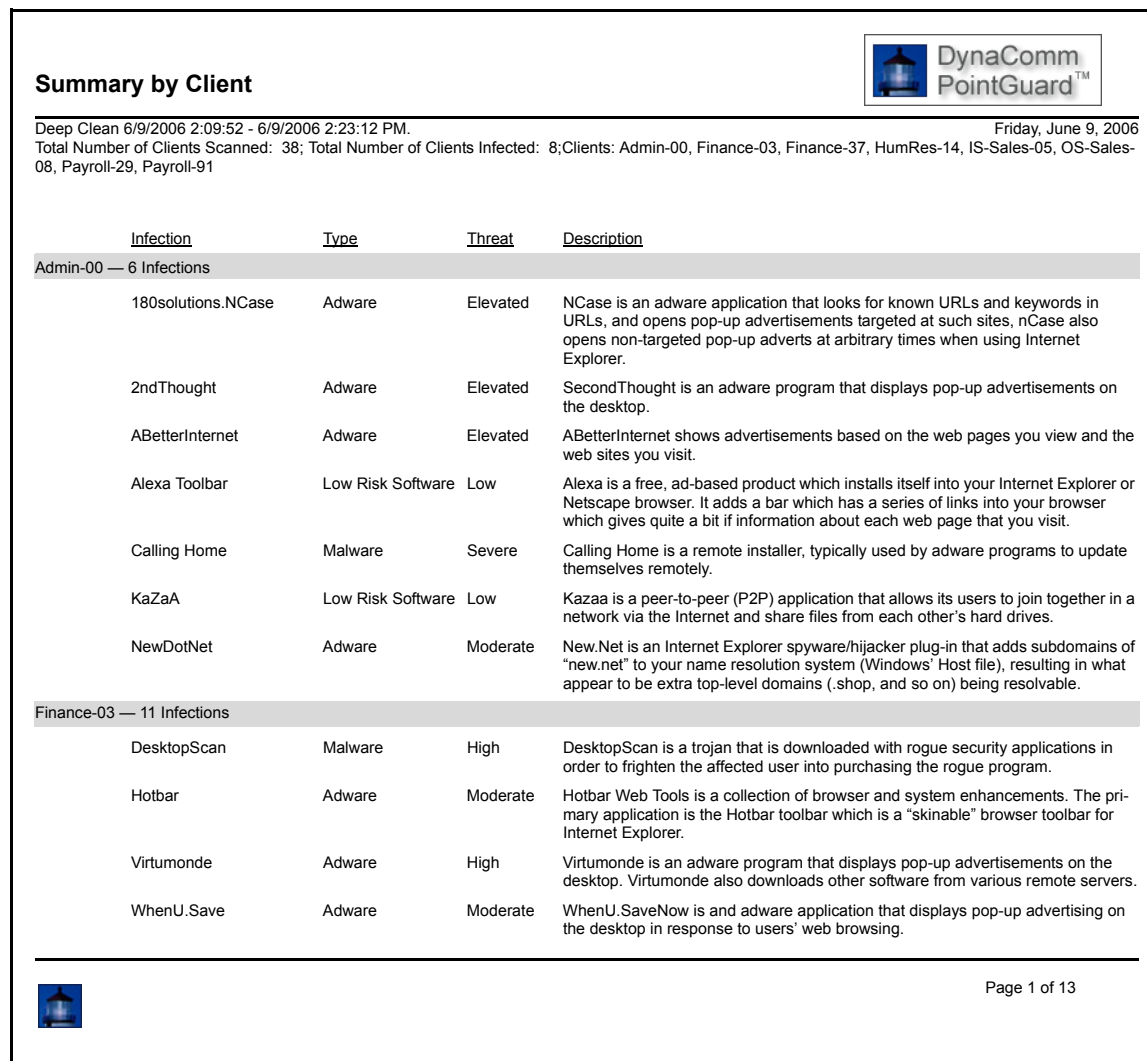


Figure 7.3  
Sample Report — Summary by Client

## Report: Summary by Infection

This report presents a data table that groups data by individual infection. For each infection found on a client included in the scan instance, infection details are listed and include infection type, threat level and a short description of the infection. All clients on which the infection was found are listed below the infection details. See Figure 7.4 for a sample Summary by Infection report.

## Report: Summary by Threat Type and Level

This report presents two charts with corresponding percentage legends and a data table. The first graph shows the top 5 infections found with a corresponding percentage legend. The second graph shows the ratio of infections found by threat level with a corresponding percentage legend.

The data table provides one listing for each infection that includes the number of clients on which the infection was found, the infection type, threat level and a short description of the infection.

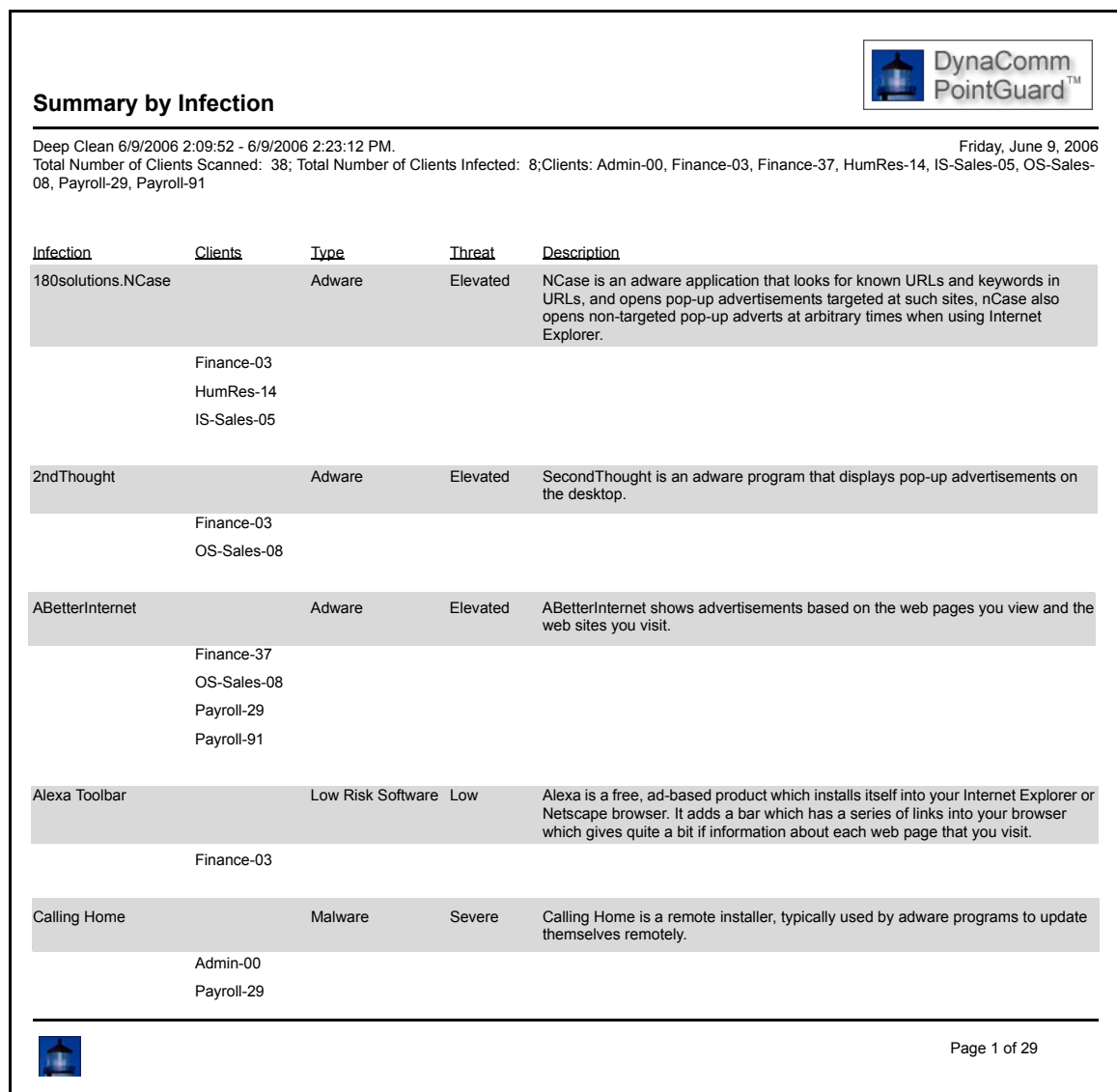
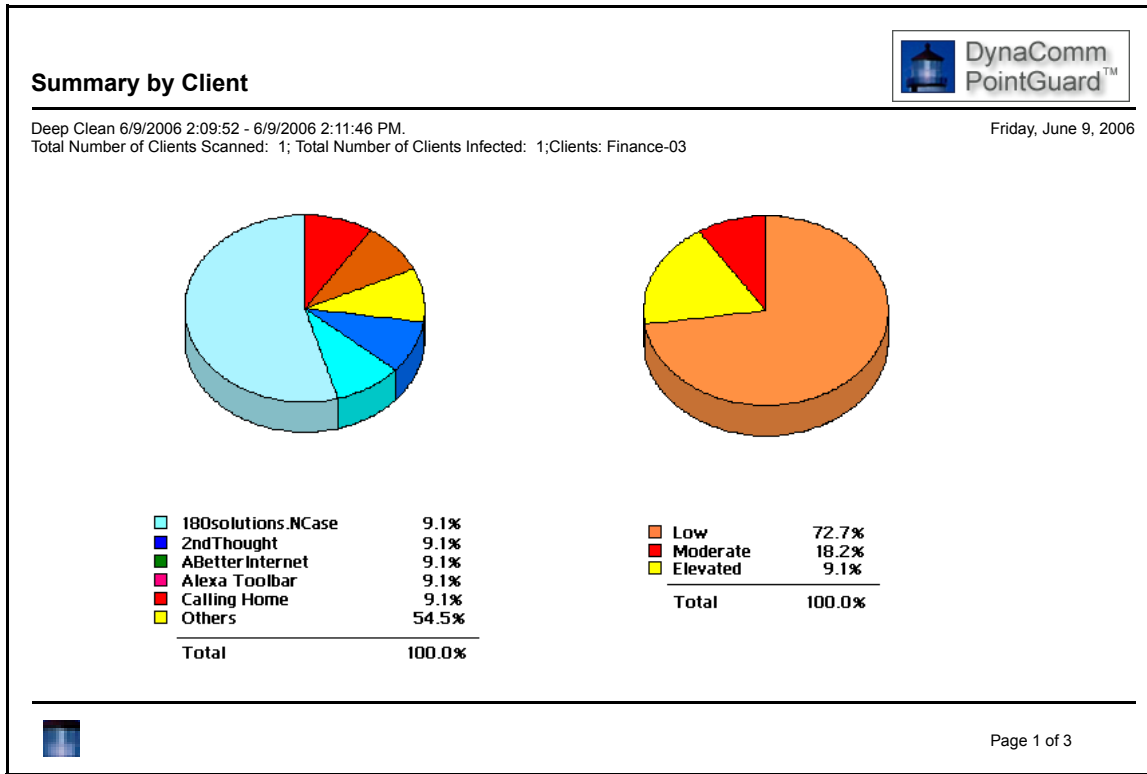



Figure 7.4  
Sample Report — Summary by Infection





### Finance-03 - Summary by Threat Type and Level

Friday, June 9, 2006

Infection	Clients	Type	Threat	Description
180solutions.NCase	1	Adware	Elevated	NCASE is an adware application that looks for known URLs and keywords in URLs, and opens pop-up advertisements targeted at such sites, nCase also opens non-targeted pop-up adverts at arbitrary times when using Internet Explorer.
2ndThought	1	Adware	Elevated	SecondThought is an adware program that displays pop-up advertisements on the desktop.
ABetterInternet	1	Adware	Elevated	ABetterInternet shows advertisements based on the web pages you view and the web sites you visit.
Alexa Toolbar	1	Low Risk Software	Low	Alexa is a free, ad-based product which installs itself into your Internet Explorer or Netscape browser. It adds a bar which has a series of links into your browser which gives quite a bit of information about each web page that you visit.
Calling Home	1	Malware	Severe	Calling Home is a remote installer, typically used by adware programs to update themselves remotely.
KaZaA	1	Low Risk Software	Low	Kazaa is a peer-to-peer (P2P) application that allows its users to join together in a network via the Internet and share files from each other's hard drives.
NewDotNet	1	Adware	Moderate	New.Net is an Internet Explorer spyware/hijacker plug-in that adds subdomains of "new.net" to your name resolution system (Windows' Host file), resulting in what appear to be extra top-level domains (.shop, and so on) being resolvable.



Page 2 of 3

Figure 7.5  
 Sample Report — Summary by Threat Type and Level

---

# Chapter 8

## *Alerting*

---

Several functions in DynaComm PointGuard send alerts to the server, to users or to both. Some functions automatically send alerts to the DynaComm PointGuard server while others require a particular set up to effect the desired alerting. This chapter reviews the four features that send alerts and details the required set up for each.

A review of the System Events topic includes a discussion of the topic window display, and how to filter and sort the display of event listings.

## System Events

System events are alerts sent from file, device and active protection policy sessions, and spyware scans to the DynaComm PointGuard server component. The details pane of the System Events window presents a continuous real-time view of all real-time alert events (file, device and active protection) received in the last five minutes. This display provides a quick view of the frequency of file, USB device and active protection functions occurring on monitored client systems. The relative importance-level of each event is identified by color.

Expanding the System Events topic displays sub-topics for each alert event type as well as one for All Events. These topics present one-line listings in the details pane for each server alert event that identifies the client system, the date and time the event occurred and was logged, the relative importance level of the event, and a short event description. Clicking Details in the System Events window displays the All Events window.

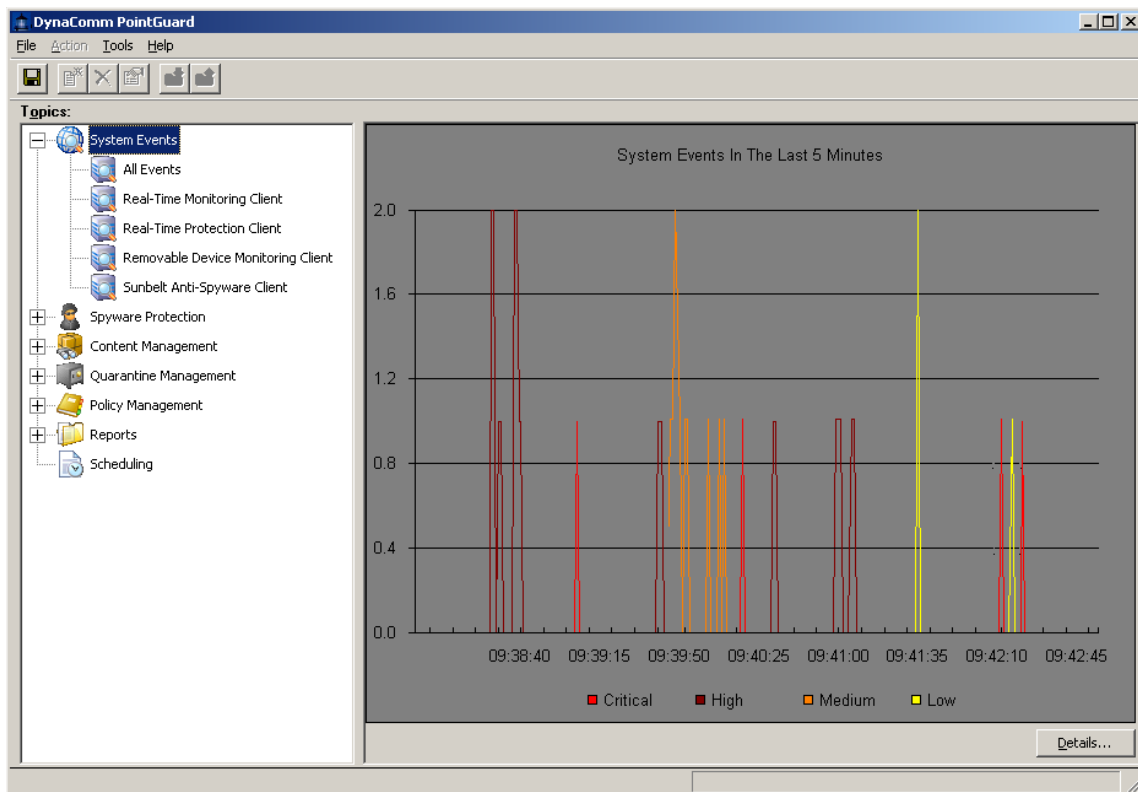


Figure 8.1 System Events window showing the frequency and relative-importance of real-time alerts for the past five minutes

## Server Alerts

One-line text listings for all event alerts appear in the details pane of the All Events topic window. Each alert listing identifies the client system, the time the event occurred on the client system and the time it was written to a log file, importance level of the event, a short description of the event, and an event type identifier. Selecting an alert listing displays more details about the event in the lower details pane.

## Spyware Server Alerts

Each time a spyware scan is run a one-line listing is placed in the details pane of the Sunbelt Anti-Spyware Client window for each infection found. This is a default function that cannot be changed or disabled. See *Chapter 7 Protecting Client Systems* for more information on creating and managing spyware scans.

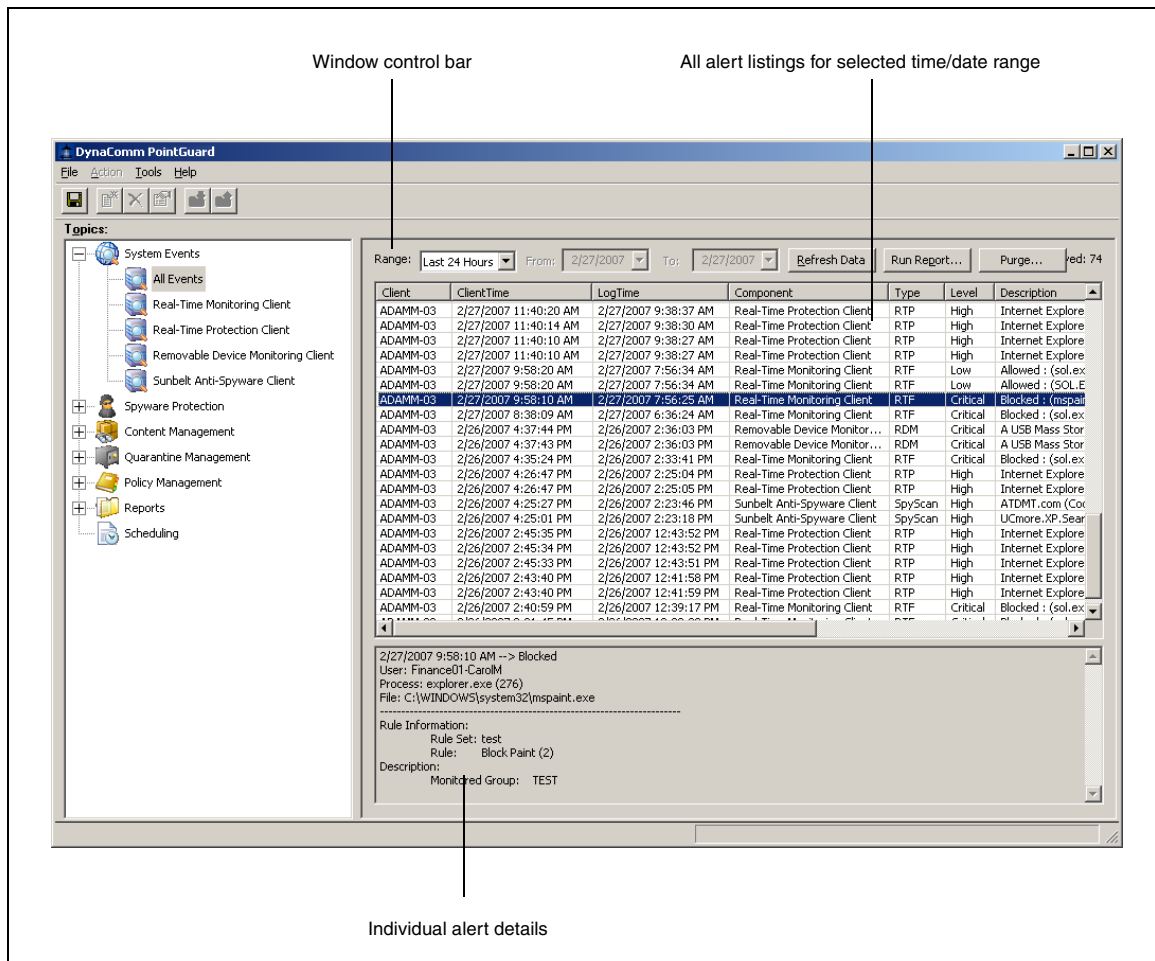


Figure 8.2  
All Events window

## File Management Server Alerts

File management policies include one or more rules for real-time monitoring file activities. This function is also referred to as “real-time monitoring.” When monitored file activities are evaluated with file policy rules and the evaluation-result condition is TRUE, actions specified in the rule are performed. See *Chapter 6 Managing Client Activities* for more information on file management policies.

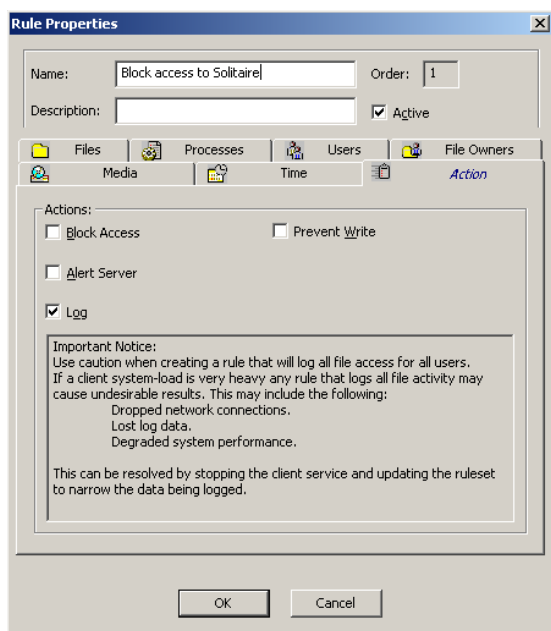


Figure 8.3  
Action tab of the Rule Properties dialog for a file management policy item

One alert option for file policies, Alert Server, is available on the Action tab of the Rule Properties dialog. When this option is enabled, an alert message is sent to the console and appears in the System Events window collectively with all other server alerts, and in the All Events and Real-time Monitoring Client windows as a one-line listing. By default, this option is *not enabled* when a new file management rule is added.

To establish server alerts for file management policies

- 1 Create a new file policy item or open an existing file policy item.
- 2 Add a new rule or open an existing rule, select the Alert Server option on the Action tab (apply check mark), and click OK.

Add the new file policy to the system policy.

- 3 In the individual system policy window, click Publish Policy.

A question dialog asks to save changes before publishing the policy.

- 4 Click Yes.

Server alerts appear in the Real-Time Monitoring Client window when rule evaluation results in a TRUE condition.

## Device Management Server Alerts

Device Management alerting sends an alert message to the DynaComm PointGuard server when a device policy rule evaluation results in a TRUE condition and the Alert Server option on the Action tab of the Rule Properties dialog is enabled. When a new rule is created, this option is enabled by default. The event alert is placed in the details pane of the Removable Device Monitoring Client window.

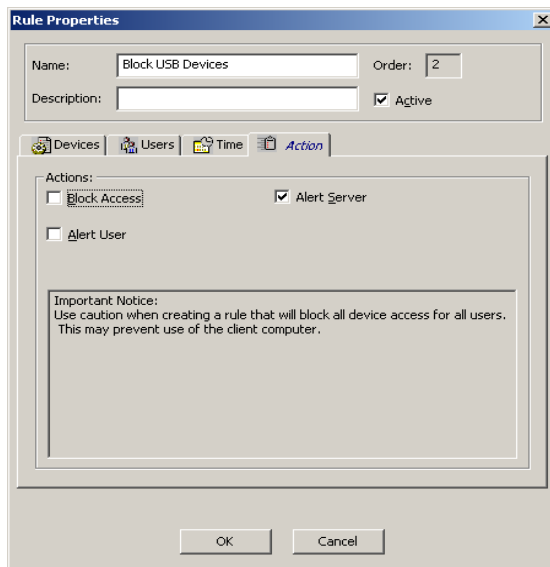


Figure 8.4  
Action tab of the Rule Properties dialog for a device management policy item

To establish server alerts for device management policies

- 1 Create a new device policy item or open an existing device policy item.
- 2 Add a new rule or open an existing rule, select the Alert Server option on the Action tab (apply check mark), and click OK.

Add the new device policy to the system policy.

- 3 In the individual system policy window, click Publish Policy.

A question dialog asks to save changes before publishing the policy.

- 4 Click Yes.

## Active Protection Server Alerts

Active Protection alerting, by default, sends an alert to the DynaComm PointGuard server when a change to a protected area is requested. The alert appears in the System Events window as a single spike. A one-line listing for each alert is shown in the Real-Time Protection Client window. This alert cannot be changed or disabled.

## Event Alert Window Management

By default, event alerts that have occurred in the last 24 hours are shown with the total number of displayed events shown to the right of the window controls. Event listings are filtered to show a date and time range for events. Events are sorted by clicking a column header. Successive clicks reverse the sort order. A small arrow in the column header indicates the sort direction (ascending/descending).

Event alert listings are removed by clicking Purge and choosing to remove all spyware alert listings or specifying an aging value of 5, 10 or 30 days. Removed event listings are deleted from the event log file and cannot be restored.

The Run Report function generates and displays the Summary of Notifications report in the Event Results viewer. This report includes a page of pie charts comparing the highest activity levels for user, level and client system. The report can be printed or exported to a file.

## Client User Alerts

User alerting for Active Protection and Device Management can include a blinking system tray icon, sound notification, or a popup dialog message. User alerting options are established:

- For both device management and active protection, one or more options in the Client User Interface Settings option group on the Policy Information tab in the details pane of the individual system policy window are enabled (Figure 8.5), **and**
- For device management rules, enable the Alert User option on the Action tab of the device management Rule Properties dialog, **or**
- For active protection, enable the Alert local user option in the Real-time Protection Settings dialog for each protected area.

Default enabled settings include:

- Enable client user interface with Flash icon only. This causes the Active Protection icon (green shield) to appear in the client's system tray and blinks when a registry change is requested.
- Enable sound notification. This option causes a two-tone bell to sound when a Registry change is requested.

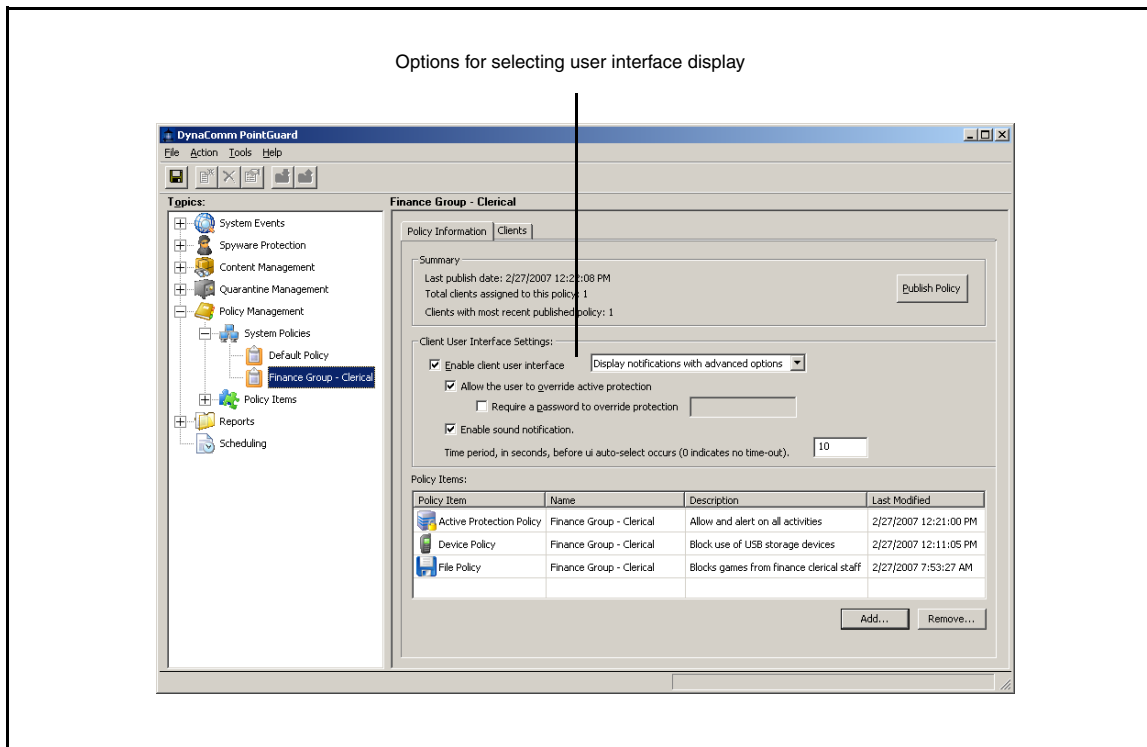


Figure 8.5  
Individual system policy window

### Active Protection Alert Dialog

The alert message dialog display is controlled with the selections on the drop-down menu of the Enable client user interface option. Three selections are available:

- Display notifications with advanced options includes Block/Allow controls in the alert message dialog and a third control, Remember Action. See Figure 8.6 for an example of the displayed alert message dialog.
- Display notifications only displays an alert message dialog but does not provide any change controls. See Figure 8.7 for an example of an alert message dialog with no controls.
- Flash client icon only displays no alert message dialog; rather, the system tray icon flashes when Registry change occurs or a monitored device activity triggers a TRUE condition by a device management rule.

The alert message remains on display until either an Allow/Block control is selected, or, after 10 seconds, the specified action is implemented. The auto-select timer function is disabled by clicking once anywhere other than on the Allow/Block controls of the alert message dialog. At this point the alert message remains on display indefinitely until an Allow/Block control is selected. This action is in effect for the current alert message only. The next message restarts the auto-select timer function. The auto-select time length can be changed by entering a new value in the Time period, in seconds, before ui auto-select occurs option on the individual system policy window.

The user can elect to automatically perform the same action (block or allow) for each subsequent matching activity by enabling the Remember Action option in the alert message dialog before selecting the Block or Allow control. This frees the user from a required response. For the next matching action, the alert message dialog is not shown and the selected action is performed automatically until

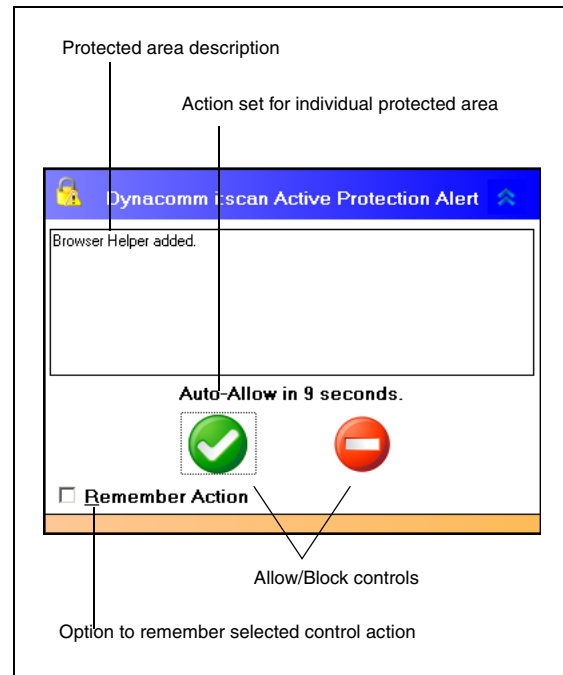


Figure 8.6  
Alert message dialog with advanced options enabled

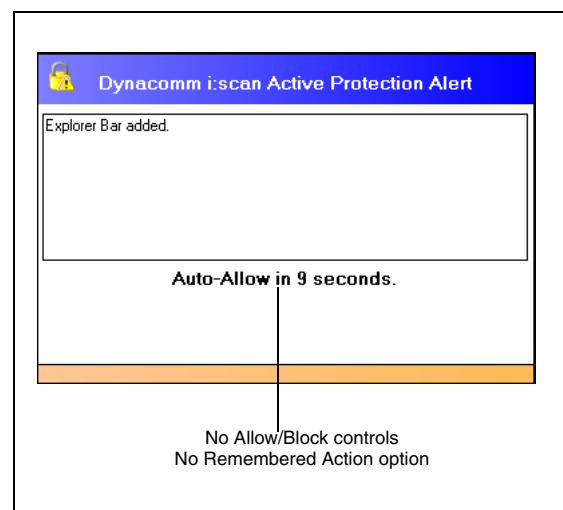


Figure 8.7  
Alert message with simplified notification enabled

“turned off” through the Remembered Actions dialog.

### Right-click Client Menu

When the Allow the user to override active protection option is enabled the expanded menu shown in Figure 8.8 is displayed on the client system when a

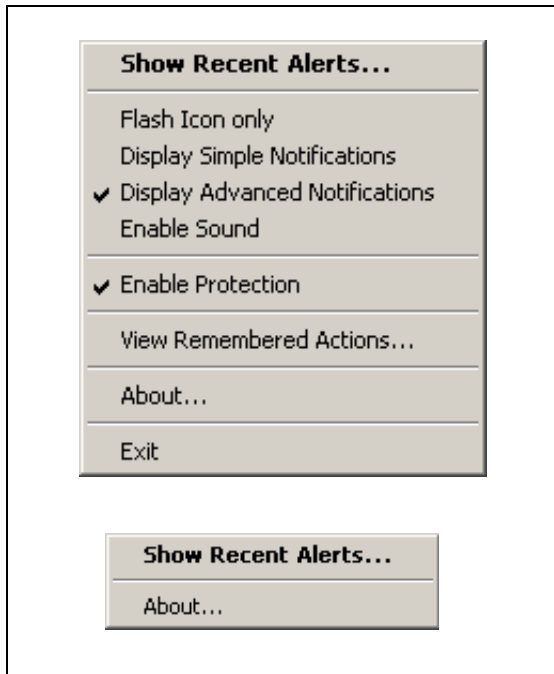


Figure 8.8  
*Expanded and limited client user menu*

right-click is performed on the active protection icon in the system tray. This menu includes selections to change the type of notification, view alert history or to disable protection completely. When

the same option is cleared or disabled, a limited menu is shown that only allows the user to view alert history.

### Remembered Actions

The Show Recent Alerts selection displays the Recent Alerts dialog with one-line listings that provides a history of all device and active protection client alerts (Figure 8.9). Remembered actions are

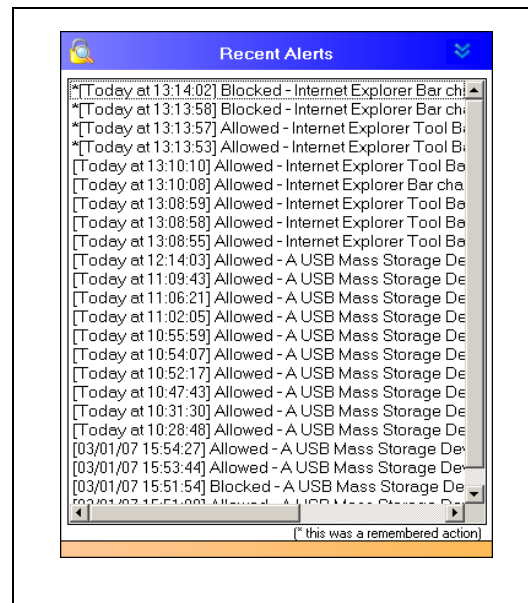


Figure 8.9  
*Limited menu shown when the user is not allowed override rights.*

flagged with an asterisk (\*). Selecting a listing displays the Alert Information dialog that provides detailed information about the action that triggered the alert notification.

The View Remembered Actions selection displays the Remembered Actions dialog that lists one-line entries for each action that was selected in the alert

message dialog after the Remember Action option was enabled. The action remains in effect until the user displays this dialog and removes the remembered action.

### Password Override

For those situations where *selected* users are to be allowed user override, the Require a password to

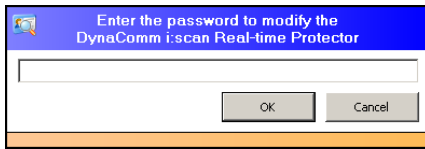


Figure 8.10  
*Password override dialog*

override protection option is enabled and a password is entered in the supplied text box. When the user attempts to change the alert notification method or to disable protection the dialog shown in Figure 8.10 appears on the client display. The user enters the password established when the option was enabled and clicks OK. The user then proceeds with his changes.

### Sound Notification

One final alerting option, Enable sound notification, sounds a two-tone bell on the client system when a change request to a protected area is made or when a device management rule evaluation results in a TRUE condition. The operating system bell volume must be active for the alert notification to sound.



---

# Chapter 9

## *Reporting & Scheduling*

---

After running scans and conducting monitoring sessions, reports provide an organized method for analyzing the data. Reports can be run on-demand or

added to a scheduled job and run during off-hours. Scheduled jobs can also include scans, database updates and database maintenance tasks.

## Reports

Data from file, registry, and spyware scans, real-time monitor sessions, and system protection sessions are retrieved from client systems and placed on the DynaComm PointGuard server system. The Reports topic offers functions to manage reports and report properties. Predefined or standard reports are placed in four report groups. Each group organizes reports by range of data or report property.

Report properties are viewed and modified with the Edit function through the Reports topic window. The Add function displays the Add New Report dialog that is used to create a new report from a report template. The Run function generates a report that is displayed with the report viewer. Schedule starts the Job Scheduler wizard to add one or more reports to a scheduled job. The Remove function removes one or more custom reports.

## Requesting Reports

Reports are generated either on-demand or through a task in a scheduled job. On-demand reports are displayed on the console monitor through the report viewer. Report details are quickly accessed by expanding top level topics in the Preview tab and selecting a detail topic. Displayed reports can be printed or exported to a file.

The Reports topic generates on-demand reports that can be saved to a file, sent as an e-mail attachment, copied to a file server or sent to an FTP site. Before running the report, a scan or session is selected to use for report data. Otherwise, the last selected log is used. If a report has never been run, the most recently created log is used.

On-demand spyware reports are generated through the Spyware Protection topic or through the Reports topic. See Chapter 7 Protecting Client Systems for

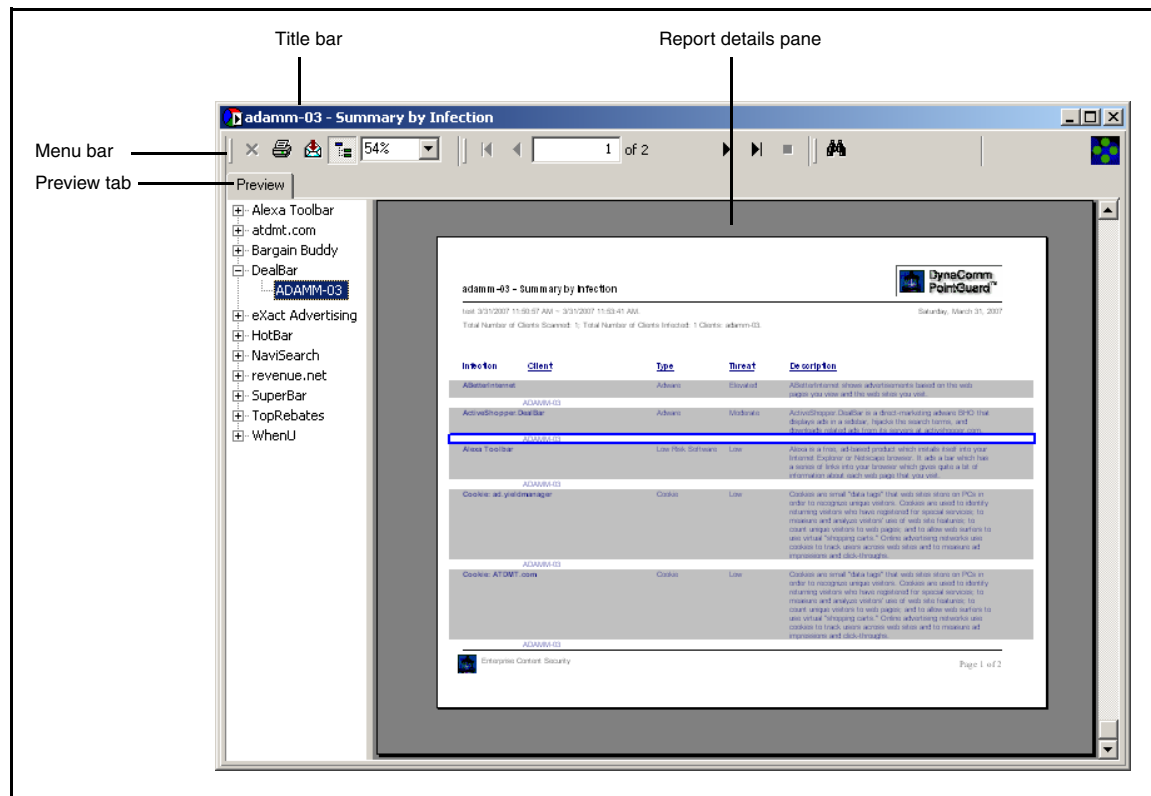


Figure 9.1  
Report Viewer window

examples of these reports. An on-demand report for alert data is generated through the individual System Events windows.

On-demand reports for file and registry scans are generated either from a right-click menu selection from the respective topic window or through the Reports topic. On-demand reports for system policy sessions are generated through the Reports topic.

On-demand reports generated through a topic window use the current report property settings. Change the settings through the Reports topic before running the report, when needed.

Scheduled reports are set up as tasks in a scheduled job through the Scheduling topic. One or more reports can be included in a single scheduled job. Scheduled report results are saved in a selected format and then placed on a file server, sent to an FTP site or sent as an e-mail attachment to one or more e-mail addresses.

Exported reports are saved with one of the following formats:

- Adobe Acrobat (PDF)
- Comma Separated values (CSV)
- Microsoft Excel (XLS)
- Microsoft Word (DOC)
- Rich Text Format (RTF)
- Tab Separated Values (CTV)
- Text (TXT)

Adobe Acrobat (PDF) is the default report format selection.

## Notes

- ❖ *PDF and RTF formats support most display features. The other formats display reports according to the installed applications that exist on the console machine.*
- ❖ *Reports that produce no data cannot be saved in either Microsoft Word (.DOC) or Rich Text Format (.RTF). Attempting to do so produces an error. A scheduled job aborts in this situation.*

## Report Types

Standard reports are predefined reports that organize information by a selected property, such as, file type, category, process, etc. Standard reports provide summary and/or detail information with charts and data tables. Standard reports cannot be removed; however, any report property, except report type, can be modified. Modified standard reports cannot be automatically restored to their original settings — properties must be restored manually. See Appendix C Predefined Reports in DynaComm PointGuard for standard report property settings.

Custom reports are created with the Add New Report dialog. In this dialog you supply a unique report name and choose a scan or session name, log file and standard report type to base the report on. Report properties are set up in the Report Properties dialog. Custom reports can be modified and removed.

## Report Properties

The Report Properties dialog is used to set up properties for a new report or change properties for an existing report. The report name appears at the top of the dialog. Remaining report properties appear on a set of dialog tabs. The available tabs (properties) depend on the reporting area. Two tabs are common to all reports:

- General tab

This tab includes the report name, the scan or session log and standard report type that the report is based on.

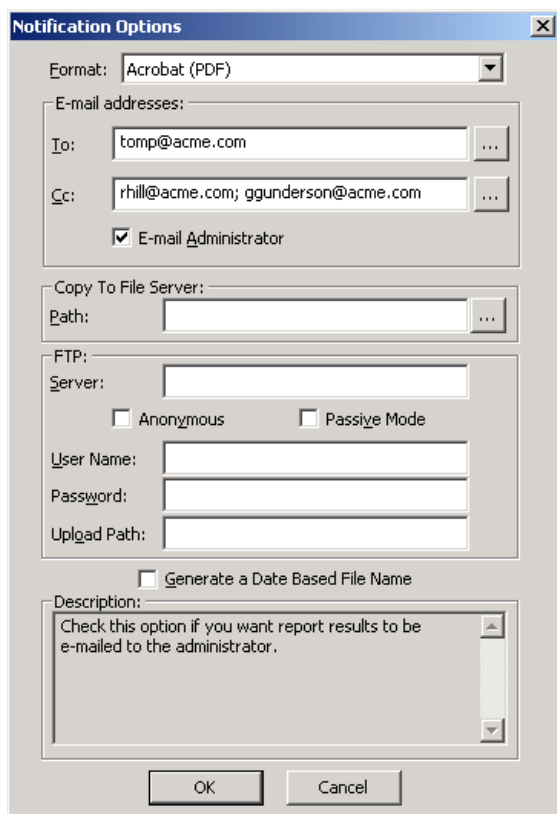


Figure 9.2  
*Notification Options dialog*

- Notify tab

This tab displays current notification settings. Notification options are set up or changed on the Notifications Options dialog accessed with the Modify function.

The Notification Options dialog includes all options to save and send report results with four option groups:

- *Format option group*

Select one format; PDF is the default format.

- *E-mail Address option group*

Set up one or more addresses for direct or copied recipients — use a semicolon to separate multiple recipients; enabling E-mail Administrator uses settings on the E-mail tab of the Options dialog to send a report to the DynaComm PointGuard administrator.

- *Copy To File Server option group*

Include a complete file path with file name; file path must be relative to the server component that produces the report.

- *FTP option group*

Include a complete file path with file name; a valid user account can be set up or the “Anonymous” user account can be used — selecting Anonymous sends no password information.

The last option, Generate a Date Based File Name, appends the report creation date to the file name so that previously saved reports are not overwritten.

The remaining tabs include settings that pertain to the reporting area, such as, process and media selections for real-time monitor sessions, registry keys and categories for registry scans, and file criteria for file scans.

## Reporting Considerations

The following points should be carefully evaluated before running reports.

- The first time a report is run, you must select a log file. Therefore, client logs must be retrieved and merged into a database log file before running a report.
  - A file or registry scan that includes two or more systems creates an individual client log file on each client system. All client log files are then merged into a single database file on the DynaComm PointGuard server component. The same is true for a real-time monitor session.
- Note**
- Adding or removing a computer to a system policy does not force the retrieval of the current log file and subsequent creation of a new log file.*
- A real-time monitor session can be run concurrently with a file or registry scan on the same system with no impact to the scan. However, this scenario does impact the real-time monitor session:
    - If the scan is distributed (runs on the client system), the real-time monitor session ignores the scan process and does not log session activity, does not send alerts or messages and does not block access or prevent update of target files, processes, etc.
    - If a file scan is running non-distributed (runs on the DynaComm PointGuard server), the real-time monitor session does log session activity and performs all selected actions.
  - By default, all reports use the most current database (logs). A new database is created on the server when:
    - An updated configuration is pushed to the client systems.
    - Database size on the server reaches 4 GB.
  - When reports are included in a scheduled job and the most recent log file is used, the report data may or may not include the information you are looking for. Check the beginning date/time and ending date/time of the report data below the report header.
  - The first time a report is used in a scheduled job, it must be associated with a log file, even if the default log file is to be used. The report displays <disabled> in the Select a Task dialog until the Report Properties dialog for the selected report is opened, closed and saved through the Reports topic. The report can be selected with a status of <disabled> but the job aborts if the Abort on Error option is enabled for the job. Any tasks listed after the aborted task are not run (General tab in Job Scheduler dialog).
  - DynaComm PointGuard cannot predict when a file or registry scan run will complete. Therefore, placing a task that runs a scan in a scheduled job and a second task that generates a report from the scan log file in the same scheduled job will most likely not produce the desired report. A second scheduled job that includes the report can be set up to run at a later time. However, the same problem remains because the run completion time is still unknown.

- Certain report fields will display “Unknown” unless options are enabled to collect and store specific data. In particular:
  - Categories are shown when Filter search by categories is enabled on the File Filter tab of the file scan properties dialog.
  - File types are shown when Filter search by file types is enabled on the File Filter tab of the *file scan properties* dialog.
  - File Owner, Permission and User/Group are shown when the Log file security settings option is enabled on the File Locations tab of the file scan properties dialog. Certain reports that produce data only on file permissions will display the message “There is no data for this report.” Other reports that use drill-down functions will display “Unknown”.
- If you plan to run the same report in a scheduled job for multiple real-time monitor logs, create custom reports (one for each monitored computers group) and select the respective real-time monitor session log before setting up the scheduled job tasks.

## Scheduling

Scheduling automates report generation, running scans and sessions, and retrieving database updates from FutureSoft. A scheduled job includes one or more tasks. The Scheduling topic offers functions to manage scheduled jobs.

New scheduled jobs are created with the Add function which starts the New Scheduled Job wizard. This wizard displays the Run As User Account dialog that collects account information (privileges) that the scheduled job will run with. The Job Scheduler dialog appears next to collect job properties.

The Edit function displays the Job Scheduler dialog to modify job properties. The Remove function removes one or more selected scheduled jobs.

## Scheduled Job Procedure

The general steps to create and implement a scheduled job include:

- 1 Plan the scheduled job.
 

Determine the purpose of the scheduled job, the tasks that need to be included in the job, and when the scheduled job should run.
- 2 Set up supporting structures.
  - Reporting tasks are disabled until data exists to run reports against.
  - Scans and system policy sessions must be created before creating a scheduled job that includes them.
  - Database updates use the connection method established on the Web Update Proxy Settings tab in the Options dialog.
  - Job notification uses settings established on the E-mail tab of the Options dialog.
- 3 Add a new scheduled job configuration.
 

A user account and associated password must be supplied for each scheduled job. The scheduled job runs with the rights and privileges of the supplied account. The user account must have access permissions to run the tasks included in the scheduled job or the job aborts.

In the Job Scheduler dialog, enter a name for the scheduled job, select job occurrence rate and times, select tasks and establish notification options, if needed.
- 4 Save the new scheduled job configuration.

## Scheduled Job Properties

A scheduled job is created and modified through the Job Scheduler dialog. Four tabs in the dialog define scheduled job properties.

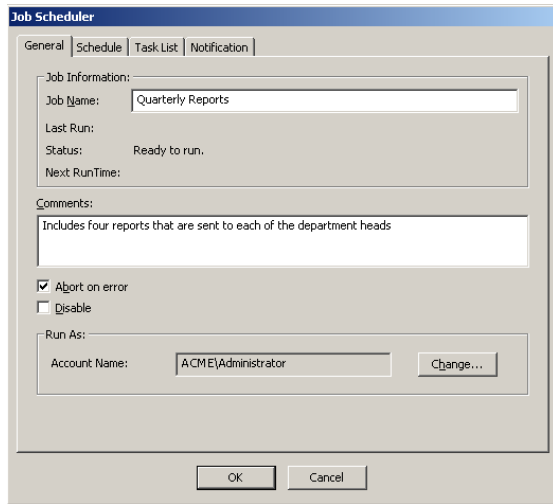


Figure 9.3  
Job Scheduler *dialog*

- General *tab*

This tab includes job information such as, job name, date and time of last run and status. An area is provided to collect comments about the job. The Disable option is used to temporarily inactivate the job. The Abort on error option provides the choice to stop or continue remaining job tasks if an error is encountered. The Change function displays the Run As User Account dialog that is used to change the associated user account and password when needed.

- Schedule *tab*

This tab provides options for when and how often the scheduled job is to run. Jobs can run just once or each day, each week or each month.

- Task List *tab*

This tab lists all tasks included in the scheduled job. Tasks can be added, removed or reordered as needed.

- Notification *tab*

This tab includes options to send a job-end status messages to one or more e-mail addresses as well as to the DynaComm PointGuard administrator. An event log entry can also be performed if the job ends successfully, aborts or in either situation.

---

# Appendix A

## *Predefined Categories*

---

Table A.1 Predefined Categories

Category Name	Description
ActiveX Compatibility in Internet Explorer	Includes Registry entries used to prevent specified ActiveX controls from installing or executing in Internet Explorer.
Adult Material/Offensive Language	Includes keywords and keyword phrases commonly regarded as adult, pornographic or offensive in nature.  Note: This category is used in the Inappropriate Content system scan.
Allow/Disallow Run for Specific Applications or Modules	Includes Registry entries used to lock/unlock specific applications or modules executed through the user interface. Removable Keys are used to unlock items. Writable Keys are used to lock items.
Application Software	Includes file signatures of common PC applications and removable Registry entries used to discover installed applications located in “Add/Remove Programs” including operating systems, service packs and security fixes.
Browser Helper Objects	Includes Registry entries used to identify browser helper objects (BHO).
Disable USB Mass Storage Devices	Includes Registry entries used to disable the operation of installed USB mass storage devices.
Enable USB Mass Storage Devices	Includes Registry entries used to enable the operation of installed USB mass storage devices.
Enable USB Mass Storage Installations	Includes a Registry entry used to allow the Device Manager to assist during installation of a new USB device.
Enable/Disable Downloads in Internet Explorer	Includes Registry entries used to enable/disable downloads that require the use of the Internet Explorer “Downloads” dialog.

Table A.1 Predefined Categories, *continued*

Category Name	Description
File Sharing Programs	Includes keywords, keyword phrases, file signatures and Registry entries of commonly used applications, programs and utilities used to download, swap or exchange files.
Games	Includes keywords, keyword phrases, and file signatures of common PC games.
Identify All Installed USB Devices	Includes a Registry entry used to identify all currently installed USB Devices; returns Device Description (DeviceDesc), Manufacturer (Mfg), and Name of Device (LocationInformation). Note: Some device vendors do not include this information.
Identify All Installed USB Mass Storage Devices	Includes a Registry entry used to Identify all currently installed USB Mass Storage Devices; returns Name of each device (FriendlyName).
Instant Messaging/Chat	Includes keywords, keyword phrases, and file signatures of common utilities used to exchange real-time messages online.
Internet Explorer Default Settings	Includes Registry entries of default settings for Internet Explorer. Writing these keys to a client system resets Internet Explorer to default settings.
Internet Explorer Settings	Includes wildcard Registry entries to identify main Internet Explorer settings.
Internet Explorer UI Options	Includes Registry entries to enable/disable Internet Explorer user interface options.
Network Utilities	Includes keywords, keyword phrases, and file signatures of network utility products; these are administrative tools that can be used inappropriately to capture restricted information.
Racially Insensitive	Includes keywords and keyword phrases used to demean or insult based on race, religion, creed or ethnicity.
Run Keys	Includes Registry entries used to identify applications and modules that are loaded on system startup.

Table A.1 Predefined Categories, *continued*

Category Name	Description
Shared Folders	Includes Registry entries used to scan for shared folders, including default and hidden folders but not “Administrative Shares.”
System Protected Game Files	Includes file signatures of game files that certain Windows OS versions (Win XP, for example) protect at the system level and cannot be permanently removed.
Uninstall Programs	Includes Registry entries used to identify uninstall programs for specific applications.

---

## Appendix B

### *Predefined File Types*

---

Table B.1 Predefined File Types

File Type	File Extensions
Application Data Files	
Adobe Illustrator	AI
Adobe Photoshop	PSD
Adobe Photoshop Script	ATN
Apple Quick Time file	QTM
Caligari Truespace 2 file	COB; SCN
Common Gateway Interface Script	CGI
Compiled HTML Help file	CHM
Computer Eyes file	CE1; CE2
Corel Photopaint file	CPT
HP Laser Jet Font file	HPF
Kodak Camera DC20/40/50 file	KDC
Kodak Photo CD file	PCD
Lotus 123 v1 Worksheet	WK1
Lotus 123 v3 FMT file	FM3
Lotus 123 v3 Worksheet	WK3
Lotus 123 v4FMT file	FMT
Lotus 123 v4 Worksheet	WK4
Lotus Ami Pro	AMI
Lotus Approach ADX file	ADX
Lotus Notes Data file	NSF; NTF
Micrografix Designer 4	DS4
Micrografix Designer Template	DST
Microsoft Excel 2.1 Worksheet	
Microsoft Excel 3.0 Worksheet	
Microsoft Excel 4.0 Workbook/Worksheet	XLW
Microsoft Excel 97-2000 & 5.0/95 Workbook	XLS
Microsoft Excel Macro	XLM
Microsoft Money file	MNY
Microsoft Works file	WKS
Multiple Image Format	MNG1
ObjectScript	OBS

Table B.1 Predefined File Types, *continued*

File Type	File Extensions
Paintshop Pro file	PSP
PGP Public Key-ring file	PKR
PGP Secret Key-ring file	SKR
Polygon Model	POL
QEMM/Sysedit Backup file	SYD
Quicken Data file	ABD; QSD
Quicken Data file QDF	QDF
QV-10 Camera file	CAM
Ricoh Camera Image file	J61
Slide Library file	SLB; SLD
Vector Map Data format	CBD
Vista Landscape Format DEM	DEM
Windows 3.1 Calendar	CAL
Windows HyperTerminal file	HI
WordPerfect v5-v6 file	WP; WPG; WPD
<b>Audio Files</b>	
AU Format Sound file	SND
Audio Interchange File Format	AIF; AIFF; AIFC
CD Audio Track	CDA
Metafile (point to Windows Media Video WMA file)	WAX
MIDI Music Sequence file	RMI
MP3 Playlist file	M3U
MPEG Audio Datafile	MD3
MPEG-1 Layer 3 (Audio)	MP3
MPEG-1 Layer 3 (Audio) Native	
Musical Instrument Digital Interface (MIDI) file	MID; MIDI
SoundMachine Audio file	AU
Wave Audio file	WAV; WAVE
Windows Media Audio	WMA

Table B.1 Predefined File Types, *continued*

File Type	File Extensions
Compression/Archive	
ARJ Archive file	ARJ
BAG Archive	BAG
Base 64 MIME-encoded file	B64
Binhex Archive file	BHX
Broderbund Mohawk Archive Format	MHK
Bzip Archive file	BZ
Compressed Archive	TAR
Compressed ASCII Archive (TAR)	TAZ
Compressed File (tar.z)	TZ
ICE Archive File	ICE
Jar Archive File	JAR; J
LH ARC Compressed Archive	LZH
LHA Compressed File	LHA
Machintosh Bin Hex	HQX
Microsoft Archive file	MARC
Microsoft Cabinet file	CAB; CDM
Microsoft Compressed File v5	
Microsoft Compressed File v6	
Quantum Archive	Q
RAR Compressed file	RAR
Redhat Linux Archive	RPM
ShrinkToFit Compressed Archive file	STF
SQZ Archive file	SQZ
Stuffit v1 Archive file	
Stuffit v5 Archive file	SIT
UFA Archive file	UFA
UNIX Gzip Comporessed Archive file	GZ
UNIX TAR file Zipped	TGZ
UU-Encoded file	UU; UUE
Winzip Compressed file	
XCR Archive file	XCR
Xx-Encoded file	XXE
Zip file	ZIP
Zoo Comporessed file	ZOO

Table B.1 Predefined File Types, *continued*

File Type	File Extensions
Database Files	
Database file	DBF
Microsoft Access MDE Database	MDE; MDB
Disk Image Files	
Norton Ghost Image file	GHO
E-mail Files	
AOL Web E-mail	DCi
Eudora Mail Message	
Generic E-mail Message	
Netscape E-mail Message	
Outlook 97 Mailbox file	PST
Outlook Express E-mail file	EML
Outlook Express Mail Storage	DBX
Executable	
Batch file	BAT
Binary Executable file	EXE; DLL; OCX; SYS; SCR; PIF
System Command file	COM
Visual Basic file	VBS
Windows NT Batch file	CMD
FAX Files	
eFax file	EFX
Fax Image file	QFX
Generic Fax file	FAX
Microsoft Office Fax Cover	CPE

Table B.1 Predefined File Types, *continued*

File Type	File Extensions
<b>Graphics Files</b>	
AMFF Image file	AMFF
AOLART1	
AOLART 2	
AutoCAD v13-v14 file	DWG
Bitmap Image file	BMP
Cineon Image file	DPX
DCX Graphic file	DCX
Enhanced Metafile Graphic file	EMF
GEM Raster file	IMG
Graphics Interchange file	GIF
Infini-D Graphics file	INFINI-D
JPEG file	MPEG; JPG; JPE
Micrographix Graphic file	DRW
PC Paintbrush file	PCX
Portable Network Graphics file	PNG
PC Paintbrush file	PCX
Portable Network Graphics file	PNG
Seamless Image Graphic file	SID
Simple Animation file	SMJPEG
Stereo CAD-3D 2 file	3D2
Storm 3D Object Definition	SOD
Tagged Image file	
Tagged Image file 2	TIF; TIFF
Windows Cursor Animation file	ANI
Windows Graphics Metafile	WMF
Windows Paint file	MSP
<b>Mixed Media</b>	
3D Media file	3DMF
Creative Sound file	VOC
Microsoft Advanced Streaming Format	ASF
Microsoft Advanced Streaming Redirector file	ASX
Microsoft Media Clip file	MMM
Real Audio file	RA; RAM
Real Media file	RM
Windows Media video.audio file	WMV; WMP; WVX; WMX

Table B.1 Predefined File Types, *continued*

File Type	File Extensions
Password Protected Files	
Password Protected Zip File 1	
Password Protected Zip File 2	
Password Protected Zip File 3	
Password Protected Zip File 4	
Password Protected Zip File 5	
Password Protected Zip File 6	
Password Protected Zip File 7	
Password Protected Zip File 8	
Programming Code Files	
Compiled Resources	RSC
Microsoft C++ Precompiled Header file	PCH
Microsoft Developer Build Log	PLG
Windows Dial-up Network Script	SCP
Text	
Adobe Acrobat file	PDF
Adobe Encapsulated PostScript file	EPS
Microsoft Word 6.0 file	
Microsoft Word 97/2000 file	
Microsoft Word file	
Microsoft Word for DOS v6 file	
Rich Text Format file	RTF
Star Writer 6.0 file	
Star Writer v3 - v5 file	SDW
Text file	TXT; TEXT
Unknown Document file	DOC
Windows Write file	WR1
Uncategorized	
<i>(empty)</i>	

Table B.1 Predefined File Types, *continued*

File Type	File Extensions
<b>Video Files</b>	
AVI file	AVI
Intel Digital Video Interface file	AVS
Interactive File Viewer	IFV
MPEG file	MPEG; MPG; MPS; MPV; MPA; MP2; M1S; M1V; M1A; M2S; M2V; M2A; MPE; MPV2; MP4
Quicktime Move file	QT
Quicktime Movie file	MOV
<b>Web Site Content</b>	
Active Server Page	ASP
Cascading Style Sheet	CSS
HTML file	HTML; HTM
Java Server Page	JSP
JavaScript Source Code	JS
PHP: Hypertext Preprocessor	PHP; PHTML; PHP3
Secure HTML Page	SHTM; SHTML
XML Data Type Definition	DTD
XML file	XML
<b>Windows System Files</b>	
Windows 3.1 Registry file	
Windows 95 Registry file	
Windows Application Log file	LGC
Windows Bitmap Font file	FON
Windows Desktop Folder Setting file	INI
Windows General Index file	GID
Windows NT Registry file	REG; SUD
Windows Password file	PWL
Windows Printer Spool file	SHD
Windows Scheduled Tasks file	JOB
Windows Shell Command file	SCF
Windows Shortcut file	LNK

---

# Appendix C

## *Predefined Reports*

---

## File Scan Reports

Table C.1 Details Reports

<p>Name: <b>File Version Information</b>            Format: Data table            Description: Presents detailed file version and other information.            Report Type: File Version Information            File Criteria: All files            Categories: Any (all)            File Types: Any (all)            Notify: (<i>none</i>); format = PDF</p>	<p>Name: <b>Scan Detail by File Type</b>            Format: Data table            Description: Presents all file names, file sizes and identified category sorted by file type.            Report Type: Scan Detail by File Type            File Criteria: All files            Categories: Any (all)            File Types: Any (all)            Notify: (<i>none</i>); format = PDF</p>
<p>Name: <b>Scan Detail by Category</b>            Format: Data table            Description: Presents all file names, file sizes and identified file type sorted by category.            Report Type: Scan Detail by Category            File Criteria: All files            Categories: Any (all)            File Types: Any (all)            Notify: (<i>none</i>); format = PDF</p>	<p>Name: <b>Scan Detail by Filename</b>            Format: Data table            Description: Presents all file names, identified category and file type for all files logged in the scan.            Report Type: Scan Detail by Filename            File Criteria: All files            Categories: Any (all)            File Types: Any (all)            Notify: (<i>none</i>); format = PDF</p>
<p>Name: <b>Scan Detail by File Size</b>            Format: Data table            Description: Presents all file names, identified category and file type sorted by file size.            Report Type: Scan Detail by File Size            File Criteria: All files            Categories: Any (all)            File Types: Any (all)            Notify: (<i>none</i>); format = PDF</p>	<p>Name: <b>Scan Detail by Terminated Process</b>            Format: Data table            Description: Presents all terminated processes with time created, time terminated, the user who ran the process and the file associated with the process.            Report Type: Scan Detail by Terminated Process            File Criteria: All files            Categories: Any (all)            File Types: Any (all)            Notify: (<i>none</i>); format = PDF</p>

## File Scan Reports

Table C.2 Drill-down Reports

<p>Name: <b>File Version Information Drill-down</b></p> <p>Format: Data table</p> <p>Description: Presents the total number of files for each machine in the domain. First-level drill-down displays all files for each machine; second-level drill-down displays version information for each file.</p> <p>Report Type: File Version Information Drill-down</p> <p>File Criteria: All files</p> <p>Categories: Any (all)</p> <p>File Types: Any (all)</p> <p>Notify: (<i>none</i>); format = PDF</p>	<p>Name: <b>Scan Drill-down by Category</b></p> <p>Format: Data table</p> <p>Description: Presents the total number of files by machine for each category. First- and second-level drill-downs display general file information and file property details that met the category definition.</p> <p>Report Type: Scan Drill-down by Category</p> <p>File Criteria: All files</p> <p>Categories: Any (all)</p> <p>File Types: Any (all)</p> <p>Notify: (<i>none</i>); format = PDF</p>
<p>Name: <b>Machine Information Drill-down</b></p> <p>Format: Data table</p> <p>Description: Presents the total number of logged files for each machine within each domain. First- and second-level drill-downs display details for each machine.</p> <p>Report Type: Machine Information Drill-down</p> <p>File Criteria: All files</p> <p>Categories: Any (all)</p> <p>File Types: Any (all)</p> <p>Notify: (<i>none</i>); format = PDF</p>	<p>Name: <b>Scan Drill-down by Domain</b></p> <p>Format: Data table</p> <p>Description: Presents the total number of files by machine for each domain. First- and second-level drill-downs display general file information and file property details.</p> <p>Report Type: Scan Drill-down by Domain</p> <p>File Criteria: All files</p> <p>Categories: Any (all)</p> <p>File Types: Any (all)</p> <p>Notify: (<i>none</i>); format = PDF</p>

## File Scan Reports

Table C.2 Drill-down Reports, *continued*

---

<p>Name: <b>Scan Drill-down by File Type</b>            Format: Data table            Description: Presents the total number of files and file size by machine in each domain sorted by file type. First- and second-level drill-downs display general file information and file properties.            Report Type: Scan Drill-down by File Type            File Criteria: All files            Categories: Any (all)            File Types: Any (all)            Notify: (<i>none</i>); format = PDF</p>	<p>Name: <b>Scan File Permission Drill-down</b>            Format: Data table            Description: Presents the domain/machine name, file name and file owner. Drill-down displays all files associated with all users and permissions.            Report Type: Scan File Permission Drill-down            File Criteria: All files            Categories: Any (all)            File Types: Any (all)            Notify: (<i>none</i>); format = PDF</p>
--	---

---

## File Scan Reports

Table C.3 Scan Errors Reports

<p>Name: <b>File Processing Errors Drill-down</b></p> <p>Format: Data table</p> <p>Description: Presents the total number of error messages by message type. Drill-down displays all files associated with the error message.</p> <p>Report Type: File Processing Errors Drill-down</p> <p>File Criteria: All files</p> <p>Categories: Any (all)</p> <p>File Types: Any (all)</p> <p>Notify: (none); format = PDF</p>	<p>Name: <b>Scan General Error Details</b></p> <p>Format: Listing</p> <p>Description: Presents general scan information that includes processed and logged file totals and general error number with corresponding error message.</p> <p><b>Note</b> <i>This report only allows for selecting a log file and setting up notification properties. No other report properties can be modified.</i></p> <p>Report Type: Scan Error Details</p> <p>Notify: (none); format = PDF</p>
<p>Name: <b>Scan Error Details by Error Type</b></p> <p>Format: Data table</p> <p>Description: Presents all error messages and all files associated with each error message.</p> <p>Report Type: Scan Error Details by Error Type</p> <p>File Criteria: All files</p> <p>Categories: Any (all)</p> <p>File Types: Any (all)</p> <p>Notify: (none); format = PDF</p>	<p>Name: <b>Scan Summary by Error Type</b></p> <p>Format: Listing</p> <p>Description: Presents total number of errors for each error message.</p> <p>Report Type: Scan Summary by Error Type</p> <p>File Criteria: All files</p> <p>Categories: Any (all)</p> <p>File Types: Any (all)</p> <p>Notify: (none); format = PDF</p>
<p>Name: <b>Scan Error Details by Filename</b></p> <p>Format: Data table</p> <p>Description: Presents all files and all error messages associated with each file.</p> <p>Report Type: Scan Error Details by Filename</p> <p>File Criteria: All files</p> <p>Categories: Any (all)</p> <p>File Types: Any (all)</p> <p>Notify: (none); format = PDF</p>	

## File Scan Reports

Table C.4 Summary Reports

<p>Name: <b>Scan Summary by Category</b>            Format: Three dimensional (3D) pie chart            Percentage legend            Data table            Description: Compares the file size and number of files identified in each category.            Report Type: Scan Summary by Category            File Criteria: All files            Categories: Any (all)            File Types: Any (all)            Notify: <i>(none)</i>; format = PDF</p>	<p>Name: <b>Scan Summary by File Type</b>            Format: Three dimensional (3D) pie chart            Percentage legend            Data table            Description: Presents the number of files and file sizes for each file type included in the scan.            Report Type: Scan Summary by File Type            File Criteria: <i>(none)</i>            Categories: Any (all)            File Types: Any (all)            Notify: <i>(none)</i>; format = PDF</p>
<p>Name: <b>Scan Summary by Domain</b>            Format: Three dimensional (3D) pie chart            Percentage legend            Data table            Description: Compares the file size and number of files for each domain included in the scan            Report Type: Scan Summary by Domain            File Criteria: All files            Categories: Any (all)            File Types: Any (all)            Notify: <i>(none)</i>; format = PDF</p>	<p>Name: <b>Scan Summary by Machine</b>            Format: Three dimensional (3D) pie chart            Percentage legend            Data table            Description: Compares the number of files found on each machine included in the scan. Optionally, detailed file and machine data can be accessed.            Report Type: Scan Summary by Machine            File Criteria: All files            Categories: Any (all)            File Types: Any (all)            Notify: <i>(none)</i>; format = PDF</p>

## Real-time Monitor Session Reports

Table C.5 Files Reports

<p>Name: <b>Activity Summary by Filename</b>  Format: Data table  Description: Presents a summary of activities performed on each monitored file.  Report Type: Summary by Filename  Files: All files  Users: Any (all)  Users: All users  Owners: All owners  Dates: All dates  Applications: Any (all) applications  File Operations: <i>(none)</i>  Notify: <i>(none)</i>; format = PDF</p>	<p>Name: <b>Blocked Access by File Name</b>  Format: Data table  Description: Presents blocked process activity data listed by file name.  Report Type: Blocked Process Access by File-name  Files: All files  Users: All users  Owners: All owners  Computers: All computers  Dates: All dates  Applications: Any (all) applications  File Operations: <i>(none)</i>  Notify: <i>(none)</i>; format = PDF</p>
<p>Name: <b>Blocked File Access by File-name</b>  Format: Data table  Description: Presents file information for all files blocked from access. Drill-down displays properties of the rule that triggered the blocking action.  Report Type: Blocked File Access by Filename  Files: All files  Users: All users  Owners: All owners  Computers: All computers  Dates: All dates  Applications: Any (all) applications  File Operations: <i>(none)</i>  Notify: <i>(none)</i>; format = PDF</p>	<p>Name: <b>File Access Summary</b>  Format: Data table  Description: Presents user and process information with time specifics and statistics for all monitored files.  Report Type: File Access Summary  Files: All files  Users: All users  Owners: All owners  Computers: All computers  Dates: All dates  Applications: Any (all) applications  File Operations: <i>(none)</i>  Notify: <i>(none)</i>; format = PDF</p>

## Real-time Monitor Session Reports

Table C.5 Files Reports, *continued*

<p>Name: <b>File Detail by Time</b>            Format: Data table            Description: Presents file access details as file name, user, process and event sorted by time.            Report Type: File Detail by Time                Files: All files                Users: All users                Owners: All owners                Computers: All computers                Dates: All dates                Applications: Any (all) applications            File Operations: <i>(none)</i>            Notify: <i>(none)</i>; format = PDF</p>	<p>Name: <b>File Renaming by Renamed Filename</b>            Format: Data table            Description: Presents all renamed files and associated information sorted by renamed file name.            Report Type: File Renaming by Renamed Filename                Files: All files                Users: All users                Owners: All owners                Computers: All computers                Dates: All dates                Applications: Any (all) applications            File Operations: <i>(none)</i>            Notify: <i>(none)</i>; format = PDF</p>
<p>Name: <b>File Renaming by Original Filename</b>            Format: Data table            Description: Presents all renamed files with associated information sorted by original file name.            Report Type: File Renaming by Original Filename                Files: All files                Users: All users                Owners: All owners                Computers: All computers                Dates: All dates                Applications: Any (all) applications            File Operations: <i>(none)</i>            Notify: <i>(none)</i>; format = PDF</p>	<p>Name: <b>Top 25 Accessed Files</b>            Format: Data table            Description: Presents number of file access attempts on each monitored machine for the top 25 files. First-level drill-down displays detailed access information; second-level drill-down displays detailed rule information for the access attempt.            Report Type: Top 25 Accessed Files                Files: All files                Users: All users                Owners: All owners                Computers: All computers                Dates: All dates                Applications: Any (all) applications            File Operations: <i>(none)</i>            Notify: <i>(none)</i>; format = PDF</p>

## Real-time Monitor Session Reports

Table C.5 Files Reports, *continued*

<p>Name: <b>Top 25 Allowed Files</b>  Format: Data table  Description: Presents number of file access attempts allowed by active rules on each monitored machine for the 25 files with the highest allow rate. First-level drill-down displays detailed access information; second-level drill-down displays detailed rule information for the access attempt.  Report Type: Top 25 Allowed Files  Files: All files  Users: All users  Owners: All owners  Computers: All computers  Dates: All dates  Applications: Any (all) applications  File Operations: <i>(none)</i>  Notify: <i>(none)</i>; format = PDF</p>	<p>Name: <b>Top 25 Continuously Used Files</b>  Format: Data table  Description: Presents time information and statistics for the 25 files with the highest amount of open time.  Report Type: Top 25 Continuously Used Files  Files: All files  Users: All users  Owners: All owners  Computers: All computers  Dates: All dates  Applications: Any (all) applications  File Operations: <i>(none)</i>  Notify: <i>(none)</i>; format = PDF</p>
<p>Name: <b>Top 25 Blocked Files</b>  Format: Data table  Description: Presents number of file access attempts blocked by active rules on each monitored machine for the 25 files with the highest block rates. First-level drill-down displays detailed access information.; second-level drill-down displays detailed rule information for the access attempt.  Report Type: Top 25 Blocked Files  Files: All files  Users: All users  Owners: All owners  Computers: All computers  Dates: All dates  Applications: Any (all) applications  File Operations: <i>(none)</i>  Notify: <i>(none)</i>; format = PDF</p>	<p>Name: <b>Top 25 Most Recently Accessed Files</b>  Format: Data table  Description: Presents the 25 files with the most recent access attempts, sorted by access date.  Report Type: Top 25 Most Recently Accessed Files  Files: All files  Users: All users  Owners: All owners  Computers: All computers  Dates: All dates  Applications: Any (all) applications  File Operations: <i>(none)</i>  Notify: <i>(none)</i>; format = PDF</p>

## Real-time Monitor Session Reports

Table C.5 Files Reports, *continued*

<p>Name: <b>Top 25 Most Recently Allowed Files</b></p> <p>Format: Data table</p> <p>Description: Presents the 25 files with the most recent successful access attempts, sorted by access date. First-level drill-down displays the user name and associated rule id.; second-level drill-down displays detailed rule information.</p> <p>Report Type: Top 25 Most Recently Allowed Files</p> <p>Files: All files</p> <p>Users: All users</p> <p>Owners: All owners</p> <p>Computers: All computers</p> <p>Dates: All dates</p> <p>Applications: Any (all) applications</p> <p>File Operations: <i>(none)</i></p> <p>Notify: <i>(none)</i>; format = PDF</p>	<p>Name: <b>Top 25 Most Recently Renamed Files</b></p> <p>Format: Data table</p> <p>Description: Presents the 25 files on which the rename operation was performed most recently. First-level drill-down displays user name and associated rule id; second-level drill-down displays detailed rule information.</p> <p>Report Type: Top 25 Most Recently Renamed Files</p> <p>Files: All files</p> <p>Users: All users</p> <p>Owners: All owners</p> <p>Computers: All computers</p> <p>Dates: All dates</p> <p>Applications: Any (all) applications</p> <p>File Operations: <i>(none)</i></p> <p>Notify: <i>(none)</i>; format = PDF</p>
<p>Name: <b>Top 25 Most Recently Blocked Files</b></p> <p>Format: Data table</p> <p>Description: Presents the 25 files with the most recently blocked access attempts, sorted by access date.</p> <p>Report Type: Top 25 Most Recently Blocked Files</p> <p>Files: All files</p> <p>Users: All users</p> <p>Owners: All owners</p> <p>Computers: All computers</p> <p>Dates: All dates</p> <p>Applications: Any (all) applications</p> <p>File Operations: <i>(none)</i></p> <p>Notify: <i>(none)</i>; format = PDF</p>	<p>Name: <b>Top 25 Most Used Files</b></p> <p>Format: Data table</p> <p>Description: Presents the 25 files with the highest amount of open time.</p> <p>Report Type: Top 25 Most Used Files</p> <p>Files: All files</p> <p>Users: All users</p> <p>Owners: All owners</p> <p>Computers: All computers</p> <p>Dates: All dates</p> <p>Applications: Any (all) applications</p> <p>File Operations: <i>(none)</i></p> <p>Notify: <i>(none)</i>; format = PDF</p>

## Real-time Monitor Session Reports

Table C.5 Files Reports, *continued*

---

Name:	<b>User Access by Filename</b>
Format:	Data table
Description:	Presents all files accessed and includes user and other access details.
Report Type:	User Access by Filename
Files:	All files
Users:	All users
Owners:	All owners
Computers:	All computers
Dates:	All dates
Applications:	Any (all) applications
File Operations:	<i>(none)</i>
Notify:	<i>(none)</i> ; format = PDF

---

## Real-time Monitor Session Reports

Table C.6 Machines Reports

---

Name: **Activity Summary by Machine**  
 Format: Data table  
 Description: Presents monitored activity and statistical data listed by machine name.  
 Report Type: Activity Summary by Machine  
     Files: All files  
     Users: All users  
     Owners: All owners  
     Computers: All computers  
     Dates: All dates  
 Applications: Any (all) applications  
 File Operations: *(none)*  
 Notify: *(none)*; format = PDF

---

Name: **File Access Summary by Machine**  
 Format: Data table  
 Description: Presents summary of file access information sorted by machine.  
 Report Type: File Access Summary by Machine  
     Files: All files  
     Users: All users  
     Owners: All owners  
     Computers: All computers  
     Dates: All dates  
 Applications: Any (all) applications  
 File Operations: *(none)*  
 Notify: *(none)*; format = PDF

---

Name: **Blocked File Access by Machine**  
 Format: Data table  
 Description: Presents all blocked file activities sorted by machine. Drill-down displays detailed rule information associated with the blocking function.  
 Report Type: Blocked File Access by Machine  
     Files: All files  
     Users: All users  
     Owners: All owners  
     Computers: All computers  
     Dates: All dates  
 Applications: Any (all) applications  
 File Operations: *(none)*  
 Notify: *(none)*; format = PDF

---

Name: **Top 25 Machines by Blocked File Access**  
 Format: Data table  
 Description: Presents the 25 machines with the highest blocked file access rate. First-level drill-down displays blocked file details; second-level drill-down displays detailed rule information associated with the blocking function.  
 Report Type: Top 25 Machines by Blocked File Access  
     Files: All files  
     Users: All users  
     Owners: All owners  
     Computers: All computers  
     Dates: All dates  
 Applications: Any (all) applications  
 File Operations: *(none)*  
 Notify: *(none)*; format = PDF

---

## Real-time Monitor Session Reports

Table C.6 Machines Reports, *continued*

---

Name:	<b>Top 25 Machines by File Access</b>
Format:	Data table
Description:	Presents the 25 machines with the highest file access attempts. First-level drill-down displays file details; second-level drill-down displays detailed associated rule information.
Report Type:	Top 25 Machines by File Access
Files:	All files
Users:	All users
Owners:	All owners
Computers:	All computers
Dates:	All dates
Applications:	Any (all) applications
File Operations:	<i>(none)</i>
Notify:	<i>(none)</i> ; format = PDF

---

## Real-time Monitor Session Reports

Table C.7 Processes Reports

---

Name:	<b>Activity Summary by Process</b>	Name:	<b>Process Access by Filename</b>
Format:	Data table	Format:	Data table
Description:	Presents activity statistics listed by process.	Description:	Presents process activity data listed by file name.
Report Type:	Summary by Process	Report Type:	Process Access by Filename
Files:	All files	Files:	All files
Users:	All users	Users:	All users
Owners:	All owners	Owners:	All owners
Computers:	All computers	Computers:	All computers
Dates:	All dates	Dates:	All dates
Applications:	Any (all) applications	Applications:	Any (all) applications
File Operations:	<i>(none)</i>	File Operations:	<i>(none)</i>
Notify:	<i>(none)</i> ; format = PDF	Notify:	<i>(none)</i> ; format = PDF

---

## Real-time Monitor Session Reports

Table C.8 Users Reports

Name:	<b>Activity Summary by User</b>	Name:	<b>File Access by User</b>
Format:	Data table	Format:	Data table
Description:	Presents user activity and statistical data listed by user name.	Description:	Presents allowed and blocked file activity data by user.
Report Type:	Summary by User	Report Type:	File Access by User
Files:	All files	Files:	All files
Users:	All users	Users:	All users
Owners:	All owners	Owners:	All owners
Computers:	All computers	Computers:	All computers
Dates:	All dates	Dates:	All dates
Applications:	Any (all) applications	Applications:	Any (all) applications
File Operations:	<i>(none)</i>	File Operations:	<i>(none)</i>
Notify:	<i>(none)</i> ; format = PDF	Notify:	<i>(none)</i> ; format = PDF
<hr/>		<hr/>	
Name:	<b>Blocked File Access by User</b>	Name:	<b>File Access Summary by User</b>
Format:	Data table	Format:	Data table
Description:	Presents blocked file activity data by user. Drill down displays detailed rule information associated with the blocking function.	Description:	Presents summary of file access information sorted by user.
Report Type:	Blocked File Access by User	Report Type:	File Access Summary by User
Files:	All files	Files:	All files
Users:	All users	Users:	All users
Owners:	All owners	Owners:	All owners
Computers:	All computers	Computers:	All computers
Dates:	All dates	Dates:	All dates
Applications:	Any (all) applications	Applications:	Any (all) applications
File Operations:	<i>(none)</i>	File Operations:	<i>(none)</i>
Notify:	<i>(none)</i> ; format = PDF	Notify:	<i>(none)</i> ; format = PDF
<hr/>		<hr/>	

## Real-time Monitor Session Reports

Table C.8 Users Reports, *continued*

<p>Name: <b>File Renaming by User</b>            Format: Data table            Description: Presents renamed file information by user.            Report Type: File Renaming by User            Files: All files            Users: All users            Owners: All owners            Computers: All computers            Dates: All dates            Applications: Any (all) applications            File Operations: <i>(none)</i>            Notify: <i>(none)</i>; format = PDF</p>	<p>Name: <b>Top 25 Most Recently Blocked Users</b>            Format: Data table            Description: Presents the 25 users that were most recently blocked.            Report Type: Top 25 Most Recently Blocked Users            Files: All files            Users: All users            Owners: All owners            Computers: All computers            Dates: All dates            Applications: Any (all) applications            File Operations: <i>(none)</i>            Notify: <i>(none)</i>; format = PDF</p>
<p>Name: <b>Top 25 Blocked Users</b>            Format: Data table            Description: Presents detailed information for the 25 users with the highest blocked file access rate. First-level drill-down displays blocked file details; second-level drill-down displays detailed rule information associated with the blocking function.            Report Type: Process by Filename            Files: All files            Users: All users            Owners: All owners            Computers: All computers            Dates: All dates            Applications: Any (all) applications            File Operations: <i>(none)</i>            Notify: <i>(none)</i>; format = PDF</p>	<p>Name: <b>Top 25 Users by File Use</b>            Format: Data table            Description: Presents the 25 users with the highest amount of file open time.            Report Type: Top 25 Users by File Use            Files: All files            Users: All users            Owners: All owners            Computers: All computers            Dates: All dates            Applications: Any (all) applications            File Operations: <i>(none)</i>            Notify: <i>(none)</i>; format = PDF</p>

---

## Registry Scan Reports

Table C.9 Details Reports

<p>Name: <b>Details by Category and Machine</b></p> <p>Format: Data table</p> <p>Description: Presents detail of registry scan with category names, machine names and registry keys logged.</p> <p>Report Type: Details by Category and Machine</p> <p>Key: Any (all) keys</p> <p>Computers: All computers</p> <p>Categories: Any (all) categories</p> <p>Notify: <i>(none)</i>; format = PDF</p>	<p>Name: <b>Details by Machine and Category</b></p> <p>Format: Data table</p> <p>Description: Presents detail of registry scan with category names, machine names and registry keys logged.</p> <p>Report Type: Details by Machine and Category</p> <p>Key: Any (all) keys</p> <p>Computers: All computers</p> <p>Categories: Any (all) categories</p> <p>Notify: <i>(none)</i>; format = PDF</p>
<p>Name: <b>Details by Category and Registry Key Name</b></p> <p>Format: Data table</p> <p>Description: Presents detail of registry scan with category names, registry keys logged and machine names.</p> <p>Report Type: Details by Category and Registry Key Name</p> <p>Key: Any (all) keys</p> <p>Computers: All computers</p> <p>Categories: Any (all) categories</p> <p>Notify: <i>(none)</i>; format = PDF</p>	<p>Name: <b>Details by Machine and Registry Key Name</b></p> <p>Format: Data table</p> <p>Description: Presents detail of registry scan errors with machine names, registry keys logged and category names.</p> <p>Report Type: Details by Machine and Registry Key Name</p> <p>Key: Any (all) keys</p> <p>Computers: All computers</p> <p>Categories: Any (all) categories</p> <p>Notify: <i>(none)</i>; format = PDF</p>
<p>Name: <b>Details by Error</b></p> <p>Format: Data table</p> <p>Description: Presents detail of registry scan errors for each machine.</p> <p>Report Type: Details by Error</p> <p>Key: Any (all) keys</p> <p>Computers: All computers</p> <p>Categories: Any (all) categories</p> <p>Notify: <i>(none)</i>; format = PDF</p>	<p>Name: <b>Details by Registry Key Name</b></p> <p>Format: Data table</p> <p>Description: Presents detail of registry scan errors for each machine.</p> <p>Report Type: Details by Registry Key Name</p> <p>Key: Any (all) keys</p> <p>Computers: All computers</p> <p>Categories: Any (all) categories</p> <p>Notify: <i>(none)</i>; format = PDF</p>

## Registry Scan Reports

Table C.10 Drill-down Reports

<p>Name: <b>Drill-down by Category</b>            Format: Data table            Description: Presents total number of registry keys and total number of machines for each category. Three levels of drill-down functions display registry key information on the machines with key, name, type and data.            Report Type: Drill-down by Category                Key: Any (all) keys            Computers: All computers            Categories: Any (all) categories            Notify: (<i>none</i>); format = PDF</p>	<p>Name: <b>Drill-down by Machine and Registry Key Name</b>            Format: Data table            Description: Presents total number of machines for each logged registry key. First- and second-level drill-down functions display general key information that includes key, name, type and data.            Report Type: Drill-down by Category                Key: Any (all) keys            Computers: All computers            Categories: Any (all) categories            Notify: (<i>none</i>); format = PDF</p>
<p>Name: <b>Drill-down by Machine</b>            Format: Data table            Description: Presents total number of registry keys for each machine. First- and second-level drill-down functions display general key information that includes key, name, type and data.            Report Type: Drill-down by Machine                Key: Any (all) keys            Computers: All computers            Categories: Any (all) categories            Notify: (<i>none</i>); format = PDF</p>	<p>Name: <b>Drill-down by Registry Key Name</b>            Format: Data table            Description: Presents registry keys and the machine on which they were found. First- and second-level drill-down functions display general key information that includes key, name, type and data.            Report Type: Drill-down by Registry Key Name                Key: Any (all) keys            Computers: All computers            Categories: Any (all) categories            Notify: (<i>none</i>); format = PDF</p>

## Registry Scan Reports

Table C.11 Summary Reports

<p>Name: <b>Summary by Category</b>  Format: Data table  Description: Presents category names, total number of machines and total number of registry keys that match the category.  Report Type: Summary by Category  Key: Any (all) keys  Computers: All computers  Categories: Any (all) categories  Notify: (<i>none</i>); format = PDF</p>	<p>Name: <b>Summary of Action by Machine</b>  Format: Data table  Description: Presents summary of scan actions sorted by machine name.  Report Type: Summary of Action by Machine  Key: Any (all) keys  Computers: All computers  Categories: Any (all) categories  Notify: (<i>none</i>); format = PDF</p>
<p>Name: <b>Summary by Machine</b>  Format: Data table  Description: Presents all machines and total number of keys logged on the machine.  Report Type: Drill-down by Category  Key: Any (all) keys  Computers: All computers  Categories: Any (all) categories  Notify: (<i>none</i>); format = PDF</p>	<p>Name: <b>Summary of Machine by Registry Key</b>  Format: Data table  Description: Presents listing of all logged registry keys and the machine names on which the keys were found.  Report Type: Summary of Machines by Registry Key  Key: Any (all) keys  Computers: All computers  Categories: Any (all) categories  Notify: (<i>none</i>); format = PDF</p>
<p>Name: <b>Summary by Registry Key Name</b>  Format: Data table  Description: Presents all logged keys and total number of machines on which the keys were found.  Report Type: Summary by Registry Key Name  Key: Any (all) keys  Computers: All computers  Categories: Any (all) categories  Notify: (<i>none</i>); format = PDF</p>	

## Spyware Scan Reports

Table C.12 Summary Reports, *continued*

<p>Name: <b>Summary by Infection</b>            Format: Data table            Description: Presents each infection with infection details and all clients on which the infection was found.            Report Type: Summary by Infection            Computers: All computers            Notify: (<i>none</i>); format = PDF</p>	<p>Name: <b>Summary by Client</b>            Format: Data table            Description: Presents all detected infections and infection details for each scanned client.            Report Type: Summary by Client            Computers: All computers            Notify: (<i>none</i>); format = PDF</p>
<hr/>	
<p>Name: <b>Summary by Threat Type and Level</b>            Format: Three dimensional (3D) pie chart            Percentage legend            Data table            Description: Presents summary graphics for the ratio of the 5 most-frequently detected infections and all other infections grouped into "Others." A second pie chart displays the ratio of detected infections by threat level. A data table provides infection details with the number of clients on which the infection was found.            Report Type: Summary by Threat Type and Level            Computers: All computers            Notify: (<i>none</i>); format = PDF</p>	

---

---

## Appendix D

### *Predefined Rules & Policy Items*

---

## Preconfigured Rule Sets

Table D.1 Block Malware Installations Via Browsers Rule Set

---

Includes one rule that is active by default.

Name:	Block and log malware installations via browsers
Description:	Block and log Internet browsers from accessing and installing executable files; log access attempts
Files:	*.dll, *.exe, *.ocx, *.scr, *.sys, *.vbs Except: ddhelp.exe
Processes:	iexplore.exe netscape.exe thunderbird.exe
Users:	All users
File Owners:	Administrators
Media:	All media types
Times:	All Times
Action:	Block Access Log

Table D.2 Sample Rules Rule Set

---

Includes nineteen rules that are *not* active by default.

## Rule 1

Name: Block and log malware installations via browsers

Description: Block and log Internet browsers from accessing and installing executable files; log access attempts

Files: \*.dll, \*.exe, \*.ocx, \*.scr, \*.sys, \*.vbs  
Except ddhelp.exe

Processes: iexplore.exe  
netscape.exe

Users: All users

File Owners: All file owners except Administrators

Media: All media types

Times: All times

Action: Block access  
Log

## Rule 2

Name: Block and log access to removable media

Description: Block and log any access to USB drives, burners, CD-ROM, floppy drives, etc.

Files: All files

Processes: All processes

Users: All users

File Owners: All file owners

Media: Removable drive

Times: All times

Action: Block access  
Log

Table D.2 Sample Rules Rule Set, *continued*

---

Rule 3

Name: Block and log any access to MP3 and audio files  
Description: Block and log any access to MP3 and other audio files  
Files: \*.aac, \*.aid, \*.aifc, \*.aiff, \*.au, \*.cdr, \*.m3d, \*.m3u, \*.mid, \*.midi, \*.mp3, \*.mpeg, \*.ra, \*.rmi, \*.snd, \*.wav, \*.wave, \*.wax, \*.wma  
Processes: All processes  
Users: All users  
File Owners: All file owners  
Media: All media types  
Times: All times  
Action: Block access  
Log

Rule 4

Name: Block and log access to compressed files  
Description: Block and log access to any compressed/archive files  
Files: \*.arj, \*.B64, \*.bag, \*.BHX, \*.bz, \*.cab, \*.cdm, \*.GZ, \*.hqx, \*.ICE, \*.jar, \*.j, \*.lha, \*.LZH, \*.MARC, \*.MHK, \*.Q, \*.RAR, \*.RPM, \*.SIT, \*.SQZ, \*.STF, \*.TAR, \*.TAZ, \*.TGZ, \*.TZ, \*.UFA, \*.UU, \*.UUE, \*.XCR, \*.XXE, \*.zip, \*.ZOO  
Processes: All processes  
Users: All users  
File Owners: All file owners  
Media: All media types  
Times: All times  
Action: Block access  
Log

Table D.2 Sample Rules Rule Set, *continued*

## Rule 5

Name: Block and log access to graphics files

Description: Block and log access to graphics file types

Files: \*.3d2, \*.amff, \*.ani, \*.art, \*.bmp, \*.dcx, \*.dpx, \*.drw, \*.dwg, \*.emf, \*.fig, \*.img, \*.infini-d, \*.jpe, \*.jpeg, \*.jpg, \*.msp, \*.pcx, \*.png, \*.sid, \*.smjpeg, \*.sod, \*.tif, \*.tiff, \*.wmf

Processes: All processes

Users: All users

File Owners: All file owners

Media: All media types

Times: All times

Action: Block access  
Log

## Rule 6

Name: Block and log access to mixed media files

Description: Block and log access to mixed media file types

Files: \*.3dmf, \*.asf, \*.asx, \*.mmm, \*.ra, \*.ram, \*.rm, \*.voc, \*.wmp, \*.wmv, \*.wmx, \*.wvx

Processes: All processes

Users: All users

File Owners: All file owners

Media: All media types

Times: All times

Action: Block access  
Log

Table D.2 Sample Rules Rule Set, *continued*

---

Rule 7

Name: Block and log access to programming code files  
Description: Block and log access to programming code file types  
Files: \*.pch, \*.plg, \*.rsc, \*.scp  
Processes: All processes  
Users: All users  
File Owners: All file owners  
Media: All media types  
Times: All times  
Action: Block access  
Log

Rule 8

Name: Block and log access to video files  
Description: Block and log access to video file types  
Files: \*.avi, \*.avs, \*.ifv, \*.mla, \*.mls, \*.mlv, \*.m2a, \*.m2s, \*.m2v, \*.mov, \*.mp2, \*.mp4, \*.mpa, \*.mpe, \*.mpeg, \*.mpg, \*.mps, \*.mpv, \*.mpv2, \*.qt  
Processes: All processes  
Users: All users  
File Owners: All file owners  
Media: All media types  
Times: All times  
Action: Block access  
Log

Table D.2 Sample Rules Rule Set, *continued*

## Rule 9

Name: Block and log access to web site content files  
Description: Block and log access to web site content file types  
Files: \*.asp, \*.css, \*.dtd, \*.htm, \*.html, \*.js, \*.jsp, \*.php, \*.php3, \*.phtml, \*.shtm,  
\*.shtml, \*.xml  
Processes: All processes  
Users: All users  
File Owners: All file owners  
Media: All media types  
Times: All times  
Action: Block access  
Log

## Rule 10

Name: Log malware installations via browsers  
Description: Log Internet browser access of executable files  
Files: \*.exe, \*.dll, \*.ocx, \*.scr, \*.scr, \*.sys, \*.vbs  
Except: ddhelp.exe  
Processes: iexplore.exe, netscape.exe  
Users: All users  
File Owners: All file owners except Administrators  
Media: All media types  
Times: All times  
Action: Log

Table D.2 Sample Rules Rule Set, *continued*

---

Rule 11

Name: Log access to removable media  
Description: Log any access to USB drives, burners, CD-ROM, floppy drives, etc.  
Files: All files  
Processes: All processes  
Users: All users  
File Owners: All file owners  
Media: Removable drive  
Times: All times  
Action: Log

Rule 12

Name: Log access to MP3 and audio files  
Description: Log any access to MP3 and other audio files  
Files: \*.aac, \*.aif, \*.aifc, \*.aiff, \*.au, \*.cdr, \*.m3d, \*.m3u, \*.mid, \*.midi, \*.mp3, \*.mpeg, \*.ra, \*.rmi, \*.snd, \*.wav, \*.wave, \*.wax, \*.wma  
Processes: All processes  
Users: All users  
File Owners: All file owners  
Media: All media types  
Times: All times  
Action: Log

Table D.2 Sample Rules Rule Set, *continued*

## Rule 13

Name: Log access to compressed files

Description: Log-only access to compressed archive files

Files: \*.arj, \*.B64, \*.bag, \*.BHX, \*.bz, \*.cab, \*.cdm, \*.GZ, \*.hqx, \*.ICE, \*.jar, \*.j, \*.lha, \*.LZH, \*.MARC, \*.MHK, \*.Q, \*.RAR, \*.RPM, \*.SIT, \*.SQZ, \*.STF, \*.TAR, \*.TAZ, \*.TGZ, \*.TZ, \*.UFA, \*.UU, \*.UUE, \*.XCR, \*.XXE, \*.zip, \*.ZOO

Processes: All processes

Users: All users

File Owners: All file owners

Media: All media types

Times: All times

Action: Log

## Rule 14

Name: Log access to graphics files

Description: Log access to graphics files

Files: \*.3d2, \*.amff, \*.ani, \*.art, \*.bmp, \*.dcx, \*.dpx, \*.drw, \*.dwg, \*.emf, \*.fig, \*.img, \*.infini-d, \*.jpe, \*.jpeg, \*.jpg, \*.msp, \*.pcx, \*.png, \*.sid, \*.smjpeg, \*.sod, \*.tif, \*.tiff, \*.wmf

Processes: All processes

Users: All users

File Owners: All file owners

Media: All media types

Times: All times

Action: Log

Table D.2 Sample Rules Rule Set, *continued*

---

Rule15

Name: Log access to mixed media files  
Description: Log access to mixed media file types  
Files: \*.3dmf, \*.asf, \*.asx, \*.mmm, \*.ra, \*.ram, \*.rm, \*.voc, \*.wmp, \*.wmv, \*.wmx, \*.wvx  
Processes: All processes  
Users: All users  
File Owners: All file owners  
Media: All media types  
Times: All times  
Action: Log

Rule 16

Name: Log access to programming code files  
Description: Log access to programming code file types  
Files: \*.pch, \*.plg, \*.rsc, \*.scp  
Processes: All processes  
Users: All users  
File Owners: All file owners  
Media: All media types  
Times: All times  
Action: Log

Table D.2 Sample Rules Rule Set, *continued*

## Rule 17

Name: Log access to pvideo files  
Description: Log any access to video file types  
Files: \*.avi, \*.avs, \*.ifv, \*.mla, \*.mls, \*.mlv, \*.m2a, \*.m2s, \*.m2v, \*.mov, \*.mp2, \*.mp4, \*.mpa, \*.mpe, \*.mpeg, \*.mpg, \*.mps, \*.mpv, \*.mpv2, \*.qt  
Processes: All processes  
Users: All users  
File Owners: All file owners  
Media: All media types  
Times: All times  
Action: Log

## Rule 18

Name: Log access to web site content files  
Description: Log access to web site content file types  
Files: \*.asp, \*.css, \*.dtd, \*.htm, \*.html, \*.js, \*.jsp, \*.php, \*.php3, \*.phtml, \*.shtm, \*.shtml, \*.xml  
Processes: All processes  
Users: All users  
File Owners: All file owners  
Media: All media types  
Times: All times  
Action: Log

Table D.2 Sample Rules Rule Set, *continued*

---

Rule 19

Name: Disable installation of USB mass storage devices  
Description: Disables new installations of USB mass storage devices  
Files: usbstor.ing, usbstor.pnf  
Processes: All processes  
Users: All users  
File Owners: All file owners  
Media: All media types  
Times: All times  
Action: Block access  
Log

---

## Appendix E

### *Predefined System Scans*

---

## Application Inventory System Scan

The Application Inventory system scan looks for application files. The Application Inventory system scan creates one registry scan to list all registry entries that match those included in the Application Software category.

## Application Lockdown System Scan

The Application Lockdown system works with Registry entries to disable applications, or to find and allow previously disabled applications. Three options are available:

### [1] Find Previously Disabled Applications

Creates one registry scan to list all registry entries under the keys:

```
HKEY_EACHUSER\ SOFTWARE\Microsoft
\Windows\CurrentVersion\Policies\Explorer with
Name=DisallowRun
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft
\Windows\CurrentVersion\Policies\Explorer with
Name=DisallowRun
```

Note: Uses the Allow/Disallow Run for Specific Applications or Modules category.

### [2] Disable Specific Applications or Modules

Creates one registry scan to write the registry entries:

```
HKEY_EACHUSER\ SOFTWARE\Microsoft
\Windows\CurrentVersion\Policies\Explorer with
Name=DisallowRun
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft
\Windows\CurrentVersion\Policies\Explorer with
Name=DisallowRun
```

Note: Uses the Allow/Disallow Run for Specific Applications or Modules category.

### [3] Allow Previously Disabled Applications

Creates one registry scan to remove the registry entries:

```
HKEY_EACHUSER\ SOFTWARE\Microsoft
\Windows\CurrentVersion\Policies\Explorer with
Name=DisallowRun
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft
\Windows\CurrentVersion\Policies\Explorer with
Name=DisallowRun
```

Note: Uses the Allow/Disallow Run for Specific Applications or Modules category.

See the next page for instructions on how to use this scan.

### Application Lockdown Instructions

To use the Application Lockdown system scan to *prevent applications from running*, you must set up a registry entry for each application that is to be blocked. Follow these steps to create those registry entries.

- 1 In the topics pane, expand Categories under the Content Management topic and expand a category.
- 2 In the topics pane, select Writable Registry Entries under the selected category.
- 3 In the details pane, click Add.
- 4 In the Registry Entry dialog
  - a In Key, enter: HKEY\_EACHUSER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\DisallowRun
  - b In Name, enter: 1
  - c In Data, enter the complete application executable name. For example, for the Windows Solitaire game, you would enter “sol.exe”.
  - d In Type, enter: String
  - e In Description, enter: This entry will prevent *applicationname* from running.
- 5 Click OK.
- 6 For each application that you want to stop from running, repeat steps 3 through 5 and increment the number entered in Name by 1.

You are now ready to run a new system scan to prevent applications from running.

To use the Application Lockdown system scan to *allow previously blocked applications*, you must set up a registry entry for each application that is to be re-allowed to run. Follow these steps to create those registry entries.

- 1 In the topics pane, expand Categories under the Content Management topic and expand a category.

- 2 In the topics pane, select Removable Registry Entries under the selected category.
- 3 In the details pane, click Add.
- 4 In the Registry Entry dialog
  - a In Key, enter: HKEY\_EACHUSER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\DisallowRun
  - b In Name, enter: 1
  - c In Data, enter the complete application executable name. For example, for the Windows Solitaire game, you would enter “sol.exe”.
  - d In Type, enter: String
  - e In Description, enter: This entry will allow *applicationname* to run again.
- 5 Click OK.
- 6 In the details pane, click Add.
- 7 In the Registry Entry dialog
  - a In Key, enter: HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\DisallowRun
  - b In Name, enter: 1
  - c In Data, enter the complete application executable name that you entered in step 4c.
  - d In Type, enter: String
  - e In Description, enter: This entry will allow *applicationname* to run again.
- 8 Click OK.
- 9 For each application that you want to stop from running, repeat steps 3 through 8 and increment the number entered in Name by 1.

You are now ready to run a new system scan to re-allow blocked applications to run.

## Inappropriate Content System Scan

The Inappropriate Content system scan looks for files that include adult, offensive or racially insensitive language in either file names or file contents. Two options are available:

### [1] Find Inappropriate Content

Creates one file scan to:

- Find files that include any keyword or keyword phrase from the Adult Material/Offensive Language category, or the Racially Insensitive category in the file path or file contents, *and*
- Calculate file signatures for all files and compare with the file signatures in the Adult Material/Offensive Language and Racially Insensitive categories, *and*
- Scan files of file types of Application Data, Audio, Database, E-mail, Fax, Graphics, Mixed Media, Text, Video and Web Site Content files.

Creates one registry scan to find Registry entries that match the entries in the Adult Material/Offensive Language category, and the Racially Insensitive category.

When a file makes a match with the first item, include the file and file type in the log.

### [2] Find & Quarantine Inappropriate Content

Creates one file scan to:

- Find files that include any keyword or keyword phrase from the Adult Material/Offensive Language category, or the Racially Insensitive category in the file path or file contents, *and*
- Calculate file signatures for all files and compare with the file signatures in the Adult Material/Offensive Language and Racially Insensitive categories, *and*
- Scan files of file types of Application Data, Audio, Database, E-mail, Fax, Graphics, Mixed Media, Text, Video and Web Site Content files, *and*
- Move all matching files to the specified quarantine folder.

Creates one registry scan to delete Registry entries that match the Removable Registry entries in the Adult Material/Offensive Language category, and the Racially Insensitive category.

When a file makes a match with the first item, include the file and file type in the log.

## Instant Messaging System Scan

The Instant Messaging system scan looks for files associated with instant messaging programs. Instant messaging (IM) is the ability to talk online in real-time through software that allows immediate communication between two or more people through a network. Three options are available:

### [1] Find Instant Messaging Software

Creates one file scan to:

- Find files under 10000 KB in size, *and*
- Find files that include any keyword or keyword phrase from the Instant Messaging/Chat category in any file path, *and*
- Calculate file signatures for all files and compare with the file signatures in the Instant Messaging/Chat category, *and*
- Scan files to determine file type.

Creates one registry scan to list Registry entries that match the entries included in the Instant Messaging/Chat category.

### [2] Find & Quarantine Instant Messaging Software

Creates one file scan to:

- Find files under 10000 KB in size, *and*
- Find files that include any keyword or keyword phrase from the Instant Messaging/Chat category in any file path, *and*
- Calculate file signatures for all files and compare with the file signatures in the Instant Messaging/Chat category, *and*
- Scan files to determine file type.
- Move all matching files to the specified quarantine folder.

Creates one registry scan to delete Registry entries that match the Removable Registry entries included in the Instant Messaging/Chat category.

### [3] Find, Stop & Quarantine Instant Messaging Software

Creates one file scan to:

- Find files under 10000 KB in size, *and*
- Find files that include any keyword or keyword phrase from the Instant Messaging/Chat category in any file path, *and*
- Calculate file signatures for all files and compare with the file signatures in the Instant Messaging/Chat category, *and*
- Scan files to determine file type.
- Move all matching files to the specified quarantine folder.
- Terminate processes that use any of the logged executable files.

Creates one registry scan to delete Registry entries that match the Removable Registry entries included in the Instant Messaging/Chat category.

When a file makes a match with the first item, include the file and file type in the log.

## Internet Access Management System Scan

The Internet Access Management system scan looks for files and registry settings associated with the Windows Internet Explorer web browser. Four groups of options are available. All option groups can be used or options can be randomly selected as needed.

[1] Internet Explorer Default Settings

Creates a registry scan that will either:

- Find and display current default settings, *or*
- Reset settings to installation defaults.

Note: This scan uses the Internet Explorer Settings category.

[2] Internet Explorer Browser Maintenance

Creates one or two file scans to either:

- Delete temporary Internet files, *or*
- Delete browsing history, *or*
- Delete browsing history and temporary Internet files.

[3] Internet Explorer Downloads

Creates one registry scan to either:

- Disable downloads, *or*
- Enable downloads.

[4] Internet Explorer User Interface

Creates one registry scan to either:

- Disable use of user interface options, *or*
- Enable use of user interface options.

[5] ActiveX Compatibility in Internet Explorer

Creates one registry scan to either:

- Enable use of ActiveX controls in IE, *or*
- Disable use of ActiveX controls in IE.

[6] Hosts File

Creates one file scan to either:

- Set the Hosts file to read-only rights, *or*
- Set the Hosts file to read and write rights.

## Network Shared Folders

The Network Shared Folders system scan lists all available shared files or folders. This scan creates one registry scan that lists Registry entries that match entries included in the Shared Folders category.

## P2P File Sharing System Scan

The P2P File Sharing system scan looks for files associated with peer-to-peer networking. A peer-to-peer network is one in which each workstation has the same capabilities and responsibilities. This type of network is most often associated with movie, music, games and software file sharing activities. Three options are available:

### [1] Find P2P File Sharing Software

Creates one file scan to:

- Find files that include any keyword from the File Sharing Programs category in the file path or file contents, *and*
- Calculate file signatures for all files and compare with the file signatures in the File Sharing Programs category, *and*
- Determine file type.

When a file makes a match with the first item, include the file and file type in the log.

Creates one registry scan to list Registry entries that match the entries included in the File Sharing Programs category.

[2] Find & Quarantine P2P File Sharing Software

Creates one file scan to:

- Find files that include any keyword from the File Sharing Programs category in the file path or file contents, *and*
- Calculate file signatures for all files and compare with the file signatures in the File Sharing Programs category, *and*
- Determine file type.
- Move all matching files to the specified quarantine folder.

When a file makes a match with the first item, include the file and file type in the log.

Creates one registry scan to list Registry entries that match the entries included in the File Sharing Programs category.

[3] Find, Stop & Quarantine P2P File Sharing Software

Creates one file scan to:

- Find files that include any keyword from the File Sharing Programs category in the file path or file contents, *and*
- Calculate file signatures for all files and compare with the file signatures in the File Sharing Programs category, *and*
- Determine file type.
- Move all matching files to the specified quarantine folder.
- Stop all processes associated with the matching quarantined files.

When a file makes a match with the first item, include the file and file type in the log.

Creates one registry scan to list Registry entries that match the entries included in the File Sharing Programs category.

## Suspected Pornographic Images System Scan

The Suspected Pornographic Images system scan looks for selected characteristics associated with pornographic material. Two options are available:

### [1] Find suspected pornographic images

Creates one file scan to:

- Scan all files of any file type to find files that include keywords from the Adult Material/Offensive Language categories or pornographic image characteristics in the file content, *or*
- Calculate file signatures to locate known pornographic files whose names have been changed.
- Determine file type.

### [2] Find and quarantine suspected pornographic images.

Creates one file scan to:

- Scan all files of any file type to find files that include keywords from the Adult Material/Offensive Language categories or pornographic image characteristics in the file content, *or*
- Calculate file signatures to locate known pornographic files whose names have been changed.
- Determine file type.
- Move all matching files to the specified quarantine folder.

#### Note

*Use of the pornographic image scanner requires a separate valid license. See your FutureSoft Account Manager for more information.*

## System Information System Scan

The System Information system scan retrieves one or four selected Windows Registry settings. Five options are available:

### [1] Display ActiveX Cache Folder

Creates a file scan that:

- Scans the \*downloaded program files folder for all files except .INI files.
- Scans file contents to determine file type.
- Calculates file signatures for all files.

### [2] Display Run Key Entries

Creates one registry scan to list all registry entries under the keys:

```
HKEY_EACHUSER\SOFTWARE\Microsoft
\Windows\CurrentVersion\run*
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft
\Windows\CurrentVersion\run*
```

Note: Uses the Run Keys category.

### [3] Display Browser Helper Objects

Creates one registry scan to list all registry entries under the keys:

```
HKEY_EACHUSER\SOFTWARE\Microsoft\
Windows\CurrentVersion\Explorer\Browser Helper
Objects
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft
\Windows\CurrentVersion\Explorer\Browser Helper
Objects
```

Note: Uses the Browser Helper Objects category.

### [4] Display Browser Default Settings

Creates one registry scan to list all registry entries under the keys:

```
*software\microsoft\internet explorer\main
*software\microsoft\internet explorer\search
```

Note: Uses the Internet Explorer Settings category.

### [5] Display all of the above information

Creates one file scan and three registry scans to include all of the above.

## USB Devices System Scan

Universal Serial Bus (USB) is a standard for connecting devices without adding separate expansion cards and allows for improved plug-n-play capabilities by allowing devices to be added to a computer without rebooting.

The USB Devices system scan identifies installed USB devices and USB mass storage devices. New installations or use of existing USB devices can be blocked. Four options are available and can be randomly selected as needed:

[1] Find All Installed USB Devices

Creates a registry scan that lists all entries under the Windows Registry key:

```
HKEY_LOCAL_MACHINE\SYSTEM  
\CurrentControlSet\Enum\USB\Vid*
```

Note: Uses the Identify All Installed USB Devices category.

[2] Find All Installed USB Mass Storage Devices

Creates a registry scan that lists all entries under the key:

```
HKEY_LOCAL_MACHINE\SYSTEM  
\CurrentControlSet\Enum\USBSTOR\Disk*
```

Note: Uses the Identify All Installed USB Mass Storage Devices category.

[3] New USB Mass Storage Device Installations

Creates a file scan that searches for the “usbstor.pnf” and “usbstor.inf” files and sets the file permissions for both files to “DENY” for all file actions for all users, or sets the SYSTEM and Administrators accounts to FULL CONTROL and the Users and Power Users accounts to SPECIAL permissions.

Creates a registry scan that lists all installed USB devices.

Note: Uses the Identify All Installed USB Devices category.

[4] Installed USB Mass Storage Devices

Creates a registry scan that writes the keys (to disable):

```
HKEY_EACHUSER\SYSTEM  
\CurrentControlSet\Services\USBSTOR  
Name=Start; Data=4
```

```
HKEY_LOCAL_MACHINE\SYSTEM  
\CurrentControlSet\Services\USBSTOR  
Name=Start; Data=3
```

Note: Uses the Disable USB Mass Storage Devices category

Creates a registry scan that writes the keys (to enable):

```
HKEY_EACHUSER\SYSTEM  
\CurrentControlSet\Services\USBSTOR  
HKEY_LOCAL_MACHINE\SYSTEM  
\CurrentControlSet\Services\USBSTOR
```

Note: Uses the Enable USB Mass Storage Devices category.

---

## Appendix F

### *Predefined Time Intervals*

---

Table F.1 Predefined Time Intervals

Time Interval Name	Description
All Times	Active: 24 hours, seven days a week
Business Hours	Active: Monday through Friday 8:00 am to 12:00 pm 1:00 pm to 5:00 pm  Inactive: All other times
Off Hours	Active: Monday through Friday 5:00 pm to 8:00 am 12:00 pm to 1:00 pm All hours on Saturday and Sunday  Inactive: All other times

---

## Appendix G

### *Sunbelt Threat Database Descriptions*

---

Table G.1 Sunbelt Threat Database Threat Level Descriptions

Threat Level	Description
Low	Low risk threats should not harm your machine or compromise your privacy and security unless they have been installed without your knowledge and consent. A low risk threat may be a program, network tool, or system utility that you knowingly and deliberately installed and that you wish to keep. Although some low risk programs may track online habits -- as provided for in a privacy policy or End User License Agreement (EULA) -- or display advertising within the applications themselves, these programs have only vague, minimal or negligible effects on your privacy. Low risk threats may also be cookies, which can be used to track your online activities, though without identifying you personally.
Moderate	Moderate risk threats are often bundled with functionally unrelated software or installed without adequate notice and consent, and may display unwanted advertising on the user's desktop. Such threats may track users' online browsing habits and transmit non-personally identifying data back to a server in order to target advertising. These threats may be configured to start automatically with the operating system, use an auto-updater that the user cannot control, or install other functionally separate programs without adequate notice and consent.
Elevated	Elevated threats are typically installed without adequate notice and consent, and may make unwanted changes to your system, such as reconfiguring your browser's home page and search settings. These threats may install advertising-related add-ons, including toolbars and search bars, or insert advertising-related components into the Winsock Layered Service Provider chain. These new add-ons and components may block or redirect your preferred network connections, and can negatively impact your computer's performance and stability. Elevated threats may also collect, transmit, and share potentially sensitive data without adequate notice and consent.
High	High risk threats are typically installed without user interaction through security exploits, and can severely compromise system security. Such threats may open illicit network connections polymorphic tactics to self-mutate, disable security software, modify system files, and install additional malware. These threats may also collect and transmit personally identifiable information (PII) without your consent and severely degrade the performance and stability of your computer.
Severe	Severe risk threats are typically installed without user interaction through security exploits, and may allow an attacker to remotely control the infected machine. Such threats may allow the attacker to install additional malware and use the compromised machine to participate in denial of service attacks, spamming, and bot nets, or to transmit sensitive data to a remote server. The malware may be cloaked and not visible to the user. These threats severely compromise the system by lowering security settings, installing "backdoors," infecting system files, or spreading to other networked machines.

Table G.2 Sunbelt Threat Database Infection Type Descriptions

Infection Type	Description
Adware	Adware, also known as advertising software, displays third-party advertising on the computer. The ads can take several forms, including pop-ups, pop-unders, banners, or links embedded within web pages or parts of the Windows interface. Some adware advertising might consist of text ads shown within the application itself or within side bars, search bars, and search results. Adware is often contextually or behaviorally based and tracks browsing habits in order to display ads that are meant to be relevant to the user.
Cookie	Cookies are small “data tags” that web sites and services store on users’ PCs in order to distinguish and recognize unique visitors. Cookies are used by web sites to identify returning visitors who have registered for special services; to monitor, measure, and analyze visitors to web pages and web sites; and to allow web surfers to use virtual “shopping carts” at e-commerce sites. Online advertising networks use Cookies to track users across web sites and to measure ad impressions and click-through. Although Cookies do not identify you personally and generally do not represent an immediate threat to your privacy and security.
Dialer	A Dialer is a program that uses the computer’s modem to dial telephone numbers, often without the user’s knowledge and consent. A Dialer can connect to a toll number that adds long distance charges to the telephone bill without the user’s knowledge or permission. Dialers may be downloaded through exploits and installed without notice and consent. A Dialer may be legitimate if downloaded and installed with full, meaningful, and informed user consent.
Low Risk Software	Low Risk Software should not harm your machine or compromise your privacy and security unless it has been installed without your knowledge and consent. A Low Risk software application may be a program that you knowingly and deliberately installed and that you wish to keep. Although some Low Risk Software programs may track online habits — as provided for in a privacy policy or End User License Agreement (EULA) — or display advertising within the applications themselves, these programs have only vague, minimal or negligible effects on your privacy.
Malware	Malware (“malicious software”) consists of software with clearly malicious, hostile, or harmful functionality or behavior and that is used to compromise and endanger individual PCs as well as entire networks.
Misc	Miscellaneous threats include applications that do not fit into other categories or that fall into multiple categories. Miscellaneous threats typically include some form of potentially objectionable functionality that may pose privacy or security risks to users and their PCs.
Potential I.T. Risk	Potential I.T. Risk include applications that may not be harmful to a single computer but could pose a risk to the network in an enterprise environment.
Remote Control Tool	Remote Control Tool is a network application that allows users to manage and control PCs or networks from a remote location.
Surveillance Tool	Surveillance Tools are software applications that monitor and capture data from computers including screenshots, keystrokes, web cam and microphone data, instant messaging chat sessions, e-mail, visited websites, programs run and files accessed and files shared on a P2P (peer to peer) network. Many Surveillance Tools can run in stealth mode, hidden from the user, and have the ability to store captured data for later retrieval by or transmission to another computer. A key logger is one simple, standard type of Surveillance Tool.

Table G.2 Infection Type Descriptions, *continued*

---

Infection Type	Description
Virus	<p>A Virus is a piece of malicious code that has the ability to replicate itself and invade other programs or files in order to spread within the infected machine. Viruses typically spread when users execute infected files or load infected media, especially removable media such as floppy disks or CD-ROMs. Viruses can also spread via e-mail through infected attachments and files. Most Viruses include a “payload” of some sort. Some payloads are merely annoying and disruptive; other payloads may damage software and data on a computer or even the computer hardware itself.</p>
Worm	<p>A Worm is a malicious program that spreads itself without any user intervention. Worms are similar to viruses in that they self-replicate. Unlike a Virus, however, Worms spread without attaching to or infecting other programs and files. A Worm can spread across computer networks via security holes on vulnerable machines connected to the network. Worms can also spread through e-mail by sending copies of itself to everyone in the user’s address book. A Worm may consume a large amount of system resources and cause the machine to become noticeably sluggish and unreliable. Some Worms may be used to compromise infected machines and download additional malicious software.</p>

---

---

## Appendix H

### *Active Directory Deployment of the DynaComm PointGuard Client*

---

## Deploying the DynaComm PointGuard Client via Active Directory

Use these steps to deploy the DynaComm PointGuard client with Active Directory:

- 1 Set up .MSI package.
  - a Install the DynaComm PointGuard server component and configure.
  - b Copy the “ClientInstall.MSI” package to the Active Directory server.
- 2 Set up Active Directory structures.
  - a In the Active Directory Users and Computers window, do the following:
    - (1) In the right pane, right-click the Domain name and select Properties.
    - (2) In the *DomainName* Properties dialog, select the Group Policy tab.
  - b On the Group Policy tab, do the following:
    - (1) In the Group Policy Object Links list, highlight the domain policy.
    - (2) Click Edit.
  - c In the Group Policy Object window, do the following:
    - (1) In the left pane, expand Software Settings and select Software Installation.
    - (2) In the right pane, right-click and highlight New.
    - (3) Select Package.
    - (4) In the Open dialog, navigate to and select the “clientinstall.msi” package.
    - (5) Click OK.

- 3 Deploy the client package.

Use one of the following techniques:

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

# Index

## A

About dialog 74  
 access rights 16, 25, 39, 69  
 Account Manager, FutureSoft 23  
 account rights, required 25, 26, 30  
 actions performed by  
   active protection policy 65  
   file scan 47, 49  
   registry scan 6  
   rules 65, 67  
   system policies 62  
 Active Directory 39, 51, 56, 162  
 active protection 6, 64–65  
   auto-select function 90  
   client alerts 88–91  
   disabling 91  
   server alerts 87  
 Active Protection Alert dialog 89  
   Allow/Block controls 89  
   Remember Action option 91  
 Active Protection Policies window 68  
 ActiveX controls 150  
 Add New Report dialog 94, 95  
 administrator  
   DynaComm PointGuard 96, 100  
   e-mail address 36  
   Guide 3, 24  
   notification 17  
   privileges and rights 16, 30  
   system 20, 27, 30  
 Administrators user group 65  
 adware, described 159  
 Alert dialog 17  
 Alert Information dialog 90  
 alert message  
   database 17  
   file system policy session 17  
   Remember Action dialog 89  
   required settings 17  
 alerts  
   active protection 6, 11, 65  
   considerations 69  
   device management 87  
   file management 67, 86  
 algorithm, encryption 14, 75  
 All Events window 85, 86

All Times time interval 156  
 Allow/Block controls 89  
 application, DynaComm PointGuard  
   installing 20  
   modifying 27  
   removing 28  
   repairing 28  
   security 16  
 archive files 136, 141  
 audio files 136, 140  
 Authorized Access dialog 25  
 auto-select function, active protection 89

## B

blinking icon alerts 88  
 blocking access to  
   files 6, 67  
   Registry changes 6, 65  
   USB devices 67  
 blocking web browsers 134, 135  
 browser helper objects (BHO) 153  
 Business Hours time interval 156

## C

categories 34  
   custom 45  
   predefined 45  
   registry scans 52  
   Removable Registry Entries 44, 52, 53  
   special operators 44  
   Writable Registry Entries 44, 52, 53  
 categories, predefined  
   ActiveX Compatibility in Internet Explorer 102  
   Adult Material/Offensive Language 49, 102, 148, 153  
   Allow/Disallow Run for Specific Applications or  
     Modules 102, 146  
   Application Software 102, 146  
   Browser Helper Objects 102, 153  
   Disable USB Mass Storage Devices 102, 154  
   Enable USB Mass Storage Devices 102, 154  
   Enable USB Mass Storage Installations 102  
   Enable/Disable Downloads in Internet Explorer 102  
   File Sharing Programs 103, 151, 152  
   Games 103  
   Identify All Installed USB Devices 103, 154  
   Identify All Installed USB Mass Storage Devices 103,  
     154

- Instant Messaging/Chat 103, 149
  - Internet Explorer Default Settings 103
  - Internet Explorer Settings 103, 150, 153
  - Internet Explorer UI Options 103
  - Network Utilities 103
  - Racially Insensitive 103, 148
  - Run Keys 103, 153
  - Shared Folders 151
  - System Protected Game Files 104
  - Uninstall Programs 104
  - CD Autorun 21
  - changes
    - pushing 42
    - saving 42, 62
  - Choose Destination Location dialog 24
  - Choose Folder (Windows) dialog 24
  - client
    - area, server 13
    - communications 33, 35
    - component 8
    - log files 13, 15, 62
  - Client Details dialog 63
  - Client Management dialog 7, 16, 28, 35, 40, 41, 75, 76
    - details pane 40, 41
    - right-click menu selections
      - Add New Client 40
      - Remove Client 40
      - Show Client Processes 41
      - Uninstall Client Software 40
  - Client Processes dialog 41
    - right-click menu selections
      - System Info 41
  - client service 7, 9, 15, 16, 28, 30, 39, 41, 62
    - removing 30
    - version 40
  - client systems 30, 39
    - console 53
    - deploying 162
    - log file creation 70
    - remote 53
    - retrieving logs 63
  - communications
    - client 33, 35, 40
    - proxy server 37
  - components
    - client 7, 8, 11, 15, 18
    - installing 29
    - modifying 29
    - server 7, 14, 15, 18
  - Computer and File Selector dialog 55
  - Computer Selector dialog 76
  - configuration properties 7, 15
  - configurations
    - file scan 11, 13, 14, 46
    - real-time monitor 7, 11, 14
    - registry scan 11, 54
    - running 7
    - updating 14, 15, 40, 97
  - connection method 37
  - console component 16, 39
    - installing 25
    - interface 7
  - console interface 7, 13, 34, 42
  - console messages 42
  - console window 34
    - details pane 34
  - Content Management window 56
  - content scanning 15
  - Control Panel selections 21
  - cookies, described 159
  - CPU utilization 55
- ## D
- database
    - alerts 17
    - considerations 14
    - creating 97
    - maintenance 37, 38
    - size 14, 51, 55, 97
    - updates 6, 37
  - database files 70
  - databases 7, 28
    - Admin 42
    - Categories & File Types 38
    - File Scans logs 13
    - PointGuardAdmin 13
    - Quarantine 14, 59
    - Real-time Threat Protection 14
    - Scans 14
    - Spyware Scans logs 14
    - System Scans logs 14
    - Threat, Sunbelt Software 38, 74, 76
  - default settings
    - aborting scans 47
    - active protection 65
    - database update connection 37
    - file filtering options 51
    - new client 35
    - program group 24
    - quarantine lifetime 60
    - report format 17
    - reports 95
  - deploying client systems 162
  - deployment, controlled 39
  - Destination folder 24
  - detailed information
    - active protection alerts 90
    - server alerts 85
  - Details window 14, 60
    - Client Items list 60
    - Filter option group 60
    - Quarantine Items list 60
  - device management policies 65–68, 71
    - notification 67
  - Device Policies window 68
  - dialer, described 159
  - dialog message alerting 88

- disabling active protection 91
  - distributed file scans 8, 13, 15, 69
  - distributed processes 8
  - documentation 2
    - Administrator Guide 3, 24
    - e-mail contact 3
    - folder 3, 24
    - Online Reference (Help) 2
    - readme file (Release Notes) 2, 24
  - driver, real-time monitor 40
- E**
- elevated threats, described 158
  - e-mail address 17
    - Administrator, DynaComm PointGuard 17
    - product information 23
    - sending report results 96
  - e-mail settings 36
  - encryption, log data 14, 75
  - End User License Agreement (EULA) 158, 159
  - endpoints, server 33
  - Enter User Information dialog 23
  - enterprise environment risks 159
  - error conditions 17
  - evaluating client system activities 66
  - evaluation version 23
  - Event Results viewer 87
  - events
    - active protection 87
    - all 85
    - device management policy 67
    - Event Results viewer 87
    - File Management policy 67
  - examples, rule processing 67
  - executable files 134, 135, 139
  - Exit Setup dialog 21, 22, 23, 24, 25, 29
- F**
- file attributes 6, 49, 150
  - file content 6
  - file items, quarantined 7
  - file management 6
  - file management policies 65–68
  - file policies 71
    - notification 67
  - File Policies window 68
  - file processes, terminating 6, 152
  - file scan 7, 8, 10
    - categories 44, 45
    - configuration 13
    - copying files with 11
    - distributed 10, 69
    - moving files with 11
    - non-distributed 12, 69
    - processes 8, 16
    - quarantining files with 6
    - reports 10
    - results 50, 51, 59
    - running 7, 56
    - scheduling 15
    - security 16
  - file scan properties dialog 15, 47, 48
    - Actions tab 49
      - Terminate processes that use any of the logged executable files option 38, 52
    - File Filter tab 15, 46, 49
      - Calculate file signatures option 49
      - Filter search by categories option 49, 98
      - Filter search by file types option 98
    - File Locations tab
      - Log file security settings option 98
    - File Scan tab 48
      - CPU Usage option 48, 51
      - Distribute Processing option 8, 15, 48, 52
      - File system exception option 48
      - Scan content for keywords and file signatures option group 49
      - Search NTFS Streams option 48
      - Search of compressed files option 49
      - Search of sub folders option 48
  - File Scans logs database 10
  - File Scans results database 13
  - File Scans window 47, 50
    - right-click menu selections
      - Run 47
  - file sharing 151
    - programs (P2P) 44
  - file signatures 44, 49
    - calculating 148, 149, 151, 152, 153
  - file systems
    - FAT 8
    - NTFS 8, 49, 52
  - file type 6, 46
    - database update 37, 47
    - determining 151, 152
  - file types, predefined
    - application data files 106
    - audio files 107
    - compression/archive 108
    - database files 109
    - disk image files 109
    - e-mail files 109
    - executable 109
    - FAX files 109
    - graphics files 110, 137
    - mixed media 110, 137, 142
    - password protected files 111
    - programming code files 111, 138, 142
    - text 111
    - video files 112, 138, 143
    - web site content 112, 139, 143
    - Windows system files 112
  - file writing and sharing 8
  - file, quarantine 7, 59
  - filters, category 44
  - folder
    - ActiveX Cache 153
    - Destination 24
    - program group 24
  - FTP site 16, 94, 95

### functions

- accessing 34
- auto-select timer (active protection) 89
- client management 30, 41
- dialog
  - Add 76
  - Auto-set 37
  - Change 100
  - Client Details 41
  - Modify 17, 96
  - Repair 29
  - Update 42
- toolbar
  - Save 62

### window

- Add 50, 63, 68, 75, 94, 99
- Delete 50, 55
- Details 63, 84
- Down 68
- Edit 50, 54, 68, 94, 99
- Properties 50, 55
- Publish 63
- Purge 60, 87
- Remove 50, 54, 63, 68, 94, 99
- Restore 60
- Results 59
- Retrieve 60
- Retrieve Logs 63, 70
- Run 47, 50, 52, 54, 94
- Run Report 87
- Schedule 94
- Stop 50, 51, 54, 55, 59
- Up 68
- View Files 50
- View Results 55

### G

- graphics file types 137
- graphics files 141
- group, system policy client
  - changes, saving 42
- Guest account (XP) 16

### H

- Health Check routine 40
- help 2, 3
- high risk threats, described 158
- Hosts file 150

### I

- infection types, described 159
- installation program 21
- InstallShield Wizard Complete dialog 21, 27, 30
- InstallShield Wizard dialog 21
- instant messaging 149
- interface, console 7
- Internet Explorer (IE) 22, 37
- IP addresses 33

### J

- Job Scheduler dialog 36, 99
  - General tab 97, 100
    - Abort on error option 97, 100
  - Notification tab 17, 100
    - Send an e-mail to the Administrator option 17
  - Schedule tab 100
  - Task List tab 100

### K

- keywords, category
  - threshold 44
  - updating 37
  - weight 44

### L

- language, racially insensitive 148
- license, pornographic image scanner 153
- listening service 7, 11, 13, 14
- Listening Service Account dialog 26
- Local System account 16
- log data 9, 55
  - encryption 14, 75
  - file scans 6
  - policy management sessions (real-time) 6
  - registry scans 6
  - unmerged 51
- log files
  - considerations 15
  - creation 70
  - policy management session (real-time) 11
  - reporting 97
  - retrieving 9, 15, 40, 63
  - size 15
  - system scan 47
  - using in reporting 53
- logging 8, 11
  - policy management session activity 15
  - real-time monitor session activity 15
- low risk software, described 159
- low risk threats, described 158

### M

- malware
  - described 159
  - installations, blocking 134, 135
  - use of 158
- managed computers 17
- menu, Windows Start
  - menu selections 21, 24
- menus, menubar
  - File menu selections
    - Save 42, 52, 62, 75
  - Tools menu selections
    - Client Management 39
    - Options 32, 33
    - Update 37, 46, 47, 74
- menus, right-click 34, 41, 59, 95
  - Active Protection icon
    - Show Recent Alerts 90
    - View Remembered Actions 90

- Add New System Policy selection 63
  - policy item window
    - Copy 68
    - New Policy 68
    - Paste 68
    - Paste Policy 68
  - Quarantine Management window
    - Purge All 60
    - Restore 60
    - Restore All 60
  - System Policies window
    - Copy 68
    - Paste 68
    - Retrieve Logs 70
  - system policy window, individual
    - Retrieve all logs 63
    - Retrieve Logs 63
  - System Scans window
    - Delete 59
    - Edit 58
    - Reports 59
    - Results 59
    - Run 58
    - Stop All 59
  - message attachments 17
  - messages
    - alert 17
    - Confirm Uninstall 30
    - confirmation 42
    - server endpoints 32
  - Microsoft Networking 39, 51, 56
  - miscellaneous threats, described 159
  - mixed media file types 137, 142
  - mobile computers 33
  - moderate risk threats, described 158
  - monitoring
    - file activities 6, 65, 84
    - Registry changes 6, 64, 84
    - spyware infections 85
    - USB device activities 6, 65, 84
  - MP3 files 136, 140
  - MSTASK.EXE 22
- N**
- network traffic 8
    - considerations 15
  - New System Scan wizard 6, 57
  - New Time Interval dialog 71
  - non-distributed file scans 69
  - non-distributed processing
    - example 12–13
  - notification 16–17
    - active protection 91
    - configuring 36
    - considerations 17
    - policy item 67
    - real-time monitor alerts 17
    - report 17, 96
    - required settings 17
    - scheduled job 17, 100
  - Notification Options dialog
    - Anonymous option 96
    - Copy To File Server option group 96
    - E-mail Address option group 96
    - E-mail Administrator option 17
    - Format option group 96
    - FTP option group 96
    - Generate a Date Based File Name option 96
- O**
- Off Hours time interval 156
  - on-demand
    - file scan 47
    - registry scan 52, 56
    - report 47, 53, 75, 95
    - spyware scan 75
  - online advertising 159
  - Online Reference (Help) 2, 16, 24, 28, 30
  - operating system 40
    - XP 16
  - operators, special 44
  - Options dialog
    - Active Protection Settings tab
      - User Interface Settings option group 88
    - E-mail tab 17, 36, 96, 99
    - Process White List tab 38
    - Server tab 32
      - External path to this server option 33
      - Internal path to this server option 33
      - Server Endpoints option group 33
    - Settings tab 47
      - Automatically add new clients to the 'Default' system policy 35
      - Automatically push new installations to clients option 35
      - Default client quarantine lifetime option 60
      - General Settings option group 38
      - New Client Settings option group 35, 60
      - Perform daily database update check at option 37, 46, 47
      - Web Update Proxy Settings tab 99
        - Proxy Settings option group 37
        - Use the following manual proxy settings for web updates option 37
  - overriding
    - active protection 91
    - default processing 15
    - system protection 6
- P**
- parasites. *See* spyware infections
  - password override, active protection 91
  - Password Request dialog 91
  - peer-to-peer network 151, 159
  - personally identifying information (PI) 158
  - policy item window, individual 66

- policy items (rule sets) 14, 62
  - active protection 64
  - copying 68
  - creating 62
  - default 62
  - predefined 67
  - properties
    - device management 65
    - file management 65
- Policy Items window 62
- policy management data 11
- policy refresh, Active Directory 162
- pornographic image scanner 49, 153
- pornographic material 153
- potential I.T. risk, described 159
- precedence, special operators 44
- predefined categories 45, 102–104
- predefined file types 46, 106–112
- predefined policy items (rule sets)
  - Block Malware Installation Via Browsers 67
  - Sample Rules 67
- predefined registry keys 8, 53
- predefined reports 6
  - file scan
    - File Processing Errors Drill-down 117
    - File Version Information 114
    - File Version Information Drill-down 115
    - Machine Information Drill-down 115
    - Scan Detail by Category 114
    - Scan Detail by File Size 114
    - Scan Detail by File Type 114
    - Scan Detail by Filename 114
    - Scan Detail by Terminated Process 114
    - Scan Drill-down by Category 115
    - Scan Drill-down by Domain 115
    - Scan Drill-down by File Type 116
    - Scan Error Details by Error Type 117
    - Scan Error Details by Filename 117
    - Scan File Permission Drill-down 116
    - Scan General Error Details 117
    - Scan Summary by Category 118
    - Scan Summary by Domain 118
    - Scan Summary by Error Type 117
    - Scan Summary by File Type 118
    - Scan Summary by Machine 118
- real-time session
  - Activity Summary by Filename 119
  - Activity Summary by Machine 124
  - Activity Summary by Process 126
  - Activity Summary by User 127
  - Blocked Access by File Name 119
  - Blocked File Access by Filename 119
  - Blocked File Access by Machine 124
  - Blocked File Access by User 127
  - File Access by User 127
  - File Access Summary 119
  - File Access Summary by Machine 124
  - File Access Summary by User 127
  - File Detail by Time 120
  - File Renaming by Original Filename 120
  - File Renaming by Renamed Filename 120
  - File Renaming by User 128
  - Process Access by Filename 126
  - Top 25 Accessed Files 120
  - Top 25 Allowed Files 121
  - Top 25 Blocked Files 121
  - Top 25 Blocked Users 128
  - Top 25 Continuously Used Files 121
  - Top 25 Machines by Blocked File Access 124
  - Top 25 Machines by File Access 125
  - Top 25 Most Recently Accessed Files 121
  - Top 25 Most Recently Allowed Files 122
  - Top 25 Most Recently Blocked Files 122
  - Top 25 Most Recently Blocked Users 128
  - Top 25 Most Recently Renamed Files 122
  - Top 25 Most Used Files 122
  - Top 25 Users by File Use 128
  - User Access by Filename 123
- registry scan
  - Details by Category and Machine 129
  - Details by Category and Registry Key Name 129
  - Details by Error 129
  - Details by Machine and Category 129
  - Details by Machine and Registry Key Name 129
  - Details by Registry Key Name 129
  - Drill-down by Category 130
  - Drill-down by Machine 130
  - Drill-down by Machine and Registry Key Name 130
  - Drill-down by Registry Key Name 130
  - Summary by Category 131
  - Summary by Machine 131
  - Summary by Registry Key Name 131
  - Summary of Action by Machine 131
  - Summary of Machine by Registry Key 131
- spyware scan
  - Summary by Client 132
  - Summary by Infection 132
  - Summary by Threat Type and Level 132
- predefined system scans
  - Application Inventory 146
  - Application Lockdown 146
  - Inappropriate Content 148
  - Instant Messaging 149
  - Internet Access Management 150
  - Network Shared Folders 151
  - P2P File Sharing 151
  - Suspected Pornographic Images 153
  - System Information 153
  - USB Devices 154
- predefined time intervals 156
- procedures
  - configuration
    - file scan 47
    - registry scan 52
    - scheduled job 99
    - spyware scan 75
    - system policy 62

- establish device management alert 87
  - establish file management alert 86
  - installation 20
  - maintenance 27
  - processes 8
    - distributed 8, 10, 97
    - infected 76
    - log data merging 55
    - non-distributed 12
    - running 7, 76
    - system policy monitoring (real-time) 9, 17
    - white listed 38
  - programming code file types 138, 142
  - properties
    - configuration 15
      - global 7
    - registry scan 54
    - spyware scan 76
    - system policy session 9
    - time interval 71
    - Windows Services 16
  - Properties dialog 68
  - protected area 38, 65
  - protection, system policy 9, 10
- Q**
- quarantine
    - file items 7, 14
    - files 7, 14
  - Quarantine database 14, 59
  - quarantine files 59
  - quarantine folder 148, 149, 152, 153
  - quarantine items 59
    - filtering display of 60
    - lifetime 60
  - quarantine location 11, 13
  - Quarantine Management window 14, 59
  - quarantining files 6, 148, 149
- R**
- racially insensitive language 148
  - readme file 2, 3
  - Real-time Monitor log database 14
  - Real-Time Monitoring Client window 86
  - Real-Time Protection Client window 14, 87
  - Real-time Protection Settings dialog 68, 88
    - Alert local user option 65, 88
    - Block changes to selected items option 65
  - real-time threat protection. *See* system policy protection
  - rebooting 20, 27, 76, 162
  - Recent Alerts dialog 90
  - Registry entry changes 89
  - registry key
    - HKEY\_EACHUSER 146, 153, 154
    - HKEY\_LOCAL\_MACHINE 146, 153, 154
  - registry keys 44, 52
    - predefined 8
    - removing existing 6
    - special operators 44
    - writing new 6
  - Registry Scan Properties dialog 52, 53, 55
    - Add writable keys option 44, 54
    - Delete removable keys option 44, 53
    - Lock Keys option 54
    - Shutdown Client option 54
    - Unlock Keys option 54
  - registry scan results 59
  - registry scans 6, 7, 8
    - as scheduled job tasks 56
    - processes 8
    - running 56
      - using categories with 44, 45
  - Registry Scans window 52
  - Registry, Windows 6, 44, 52, 65
  - Release Notes. *See* readme file.
  - Remembered Actions dialog 90
  - remote control tool, described 159
  - Removable Device Monitoring Client window 87
  - removable media 135, 140
  - report 7
    - categories 44
    - custom 6, 95
    - displaying 6
    - displaying "Unknown" 98
    - exporting 95
    - file scan 10
    - format 95
    - generating 6
    - on-demand 47, 53, 56, 62, 94, 95
    - predefined 6, 95
    - printing 6
    - properties 94, 95
    - requesting 94
    - saving 6, 94, 95, 96
    - scheduled 47, 53, 56, 62, 94
    - sending 17, 48, 94, 95, 96
    - spyware 80, 94
    - system policy session 95
    - template 94
    - type 95
      - using predefined categories in 45
  - Report Properties dialog 17, 36, 46, 95, 96, 97
    - File Types tab 46
    - General tab 96
    - Notify tab 17, 96
  - report results 17
  - reporting 6
  - reporting considerations 97
  - reports
    - as scheduled job tasks 57
    - saving 62
    - scheduled 53
  - reports, predefined 94
    - details 114, 129
    - drill-down 115–116, 130
    - files 119–123
    - machines 124–125
    - processes 126
    - scan errors 117
    - summary 118, 131–132
    - users 127–128
  - reports, sample (spyware) 80–82

- requirements, system 18
- resources 52
  - processing 51
  - required 51
- retry attempts, installation 35
- rights, access 25, 26, 39
- RTM. *See* file and device management policy items
- RTP. *See* active protection
- Rule Properties dialog 17, 36, 65, 66, 68
  - Action tab 17, 67
  - Alert option 69
  - Alert Server option 86, 87
  - Alert User option 88
  - Active option 65
  - Alert option 17
- rules
  - active status 65
  - functions 68
  - rule conditions 66
  - rule order 66
  - rule priority 66
  - setting priority 62
  - using time intervals 71
- Run (Windows) dialog 21
- Run As User Account dialog 99, 100
- S**
- saving changes 32
- scan 33, 41
  - aborting 47
  - distributed 8, 97
  - file 6, 7, 8
  - non-distributed 97
  - registry 6, 7, 8, 14
  - running with RTM session 97
  - spyware 9, 10, 75
  - starting 6
- Scan Actions dialog 58
- scan data 11
- scan run results
  - file scan 50, 51
  - registry scan 54, 55
  - spyware scan 76
- Scan Summary dialog 56
- scanning
  - compressed files 49
  - file contents 49, 51
  - for pornographic images 49
- Scans database 14
- scheduled
  - database update 46, 47
  - file scan 47
  - registry scan 53
  - report 47, 53, 75, 97
  - spyware scan 75
- scheduled job 7, 97
  - properties 100
  - security 99, 100
  - tasks 6, 97, 98
- scheduling 6
- security
  - considerations 16
  - ForceGuest 16
  - scheduled reports 16
  - XP systems 16
- security holes, use of 160
- security risks 159
- Select a Task dialog 97
- Select Components dialog 29
- Select Program Folder dialog 24
- Selection dialog (Autorun program) 21
- serial number 23, 37, 74
- server alerts
  - active protection 87
  - device management 87
  - file management 86
  - spyware 85
- server component 7, 10
  - client area 13
  - removing 30
- server endpoints 33
- server port 36
- server, DynaComm PointGuard 33, 51, 94, 97
- service
  - client 7, 9, 16, 28, 30, 41
  - listening 7, 11, 13, 14
  - subscription 46, 47
- Service Run As Account Information dialog 16, 69
- session, policy management (real-time) 10, 33, 41, 52, 56
  - logs 11
  - properties 9
  - running with scans 97
- settings
  - changing 35
  - default
    - aborting scans 47
    - database 38
    - Internet Explorer 150
    - new client 35
    - new client 35
    - notification 36
    - server endpoints 33
    - SMTP server 17
    - system protection 35
- settings, default
  - browser 153
- Setup Complete dialog 29
- Setup Maintenance program 27–30
- Setup Maintenance Welcome dialog 27, 29, 30
- Setup program 21–27
- Setup Status dialog 25, 29, 30
- severe risk threats, described 158
- sizing, database 55
- SMTP server settings 17
- Software License Agreement dialog 23
- sorting event listings 87
- sound notification alerting 88
- spyware definitions 74

- spyware infection
    - cleaning 6
    - definitions 74, 75
    - protection from 6
    - types 76
  - Spyware Scan Properties dialog 75, 76
    - Cleaning Options option group 76
    - Spyware Scan clients option group 76
    - Spyware scan options option group 76
  - Spyware Scan Results viewer 78
  - spyware scan window, individual
    - details pane
      - Clients tab 75, 77
      - Summary tab 77
    - right-click menu
      - Run 75
  - spyware scans 6, 9
    - procedure 75
    - results 75
    - type 76
  - Spyware Scans window 75, 80
    - Clients tab 80
    - Currently Defined Spyware Scans list 76
    - right-click menu 80
  - spyware threat levels 76
  - Summary by Client report 75
  - Summary by Infection report 75
  - Summary by Threat Type and Level report 75
  - summary information
    - active protection alerts 90
    - spyware scan results 78
    - spyware scan run 76
    - spyware scan runs 76
    - system policy 63
    - system scan 59
  - Summary of Notifications report 87
  - Sunbelt Software 37
  - Sunbelt Threat database 158
  - support, technical 3
  - surveillance tools, described 159
  - system administrator 20, 30
  - System Events window 84, 95
  - system information, viewing 41
  - system policies
    - properties 62
    - security 69
  - System Policies window 62, 63
    - Retrieve Logs function 14
  - System Policy dialog 63
  - system policy protection 10, 35, 97
    - blocking 6
    - configuration 16
    - sessions 9, 10, 56
  - system policy window, individual 14, 42, 62
    - Clients tab 63
    - Policy Information tab 63, 88
      - Allow the user to override active protection option 90
    - Client User Interface Settings option group
      - Display notifications with advanced options option 88
      - Require a password to override protection option 91
    - Display notifications only selection 89
    - Display notifications with advanced options selection 89
    - Enable client user interface option 89
    - Enable sound notification option 88, 91
    - Flash client icon only selection 89
    - Policy Items list 63
    - Time period, in seconds, before ui auto-select occurs option 89
    - Retrieve function 14
    - Retrieve Logs function 14
  - System Scan Clients dialog 57
  - System Scan Name dialog 57
  - System Scan Summary dialog 58
  - system scans 9
    - predefined 146–154
  - System Scans database 14
  - System Scans window 56
    - Summary pane 59
  - system tray (Windows) 64, 88
- T**
- Taskbar (Windows) 21, 64
  - tasks, scheduled job 46, 47
    - Update spyware definitions, keywords and file types 37, 74
  - technical support 3, 8
  - threat levels, descriptions 158
  - Time Interval dialog 71
  - time intervals 62
    - custom 71
    - predefined
      - All Times 71
      - Business Hours 71
  - topic, configuration 34, 50
    - Active Protection policy item 68
    - Categories 43, 44–46, 47, 52
    - Definitions 74
    - Details 60
    - Device Management policy item 68
    - File Management policy item 68
    - File Scans 11, 13, 43, 47–52
    - File Types 43, 46–47
    - Monitored Computers 35
    - Policy Items 64–68
    - Quarantine Management 14, 59–60
    - Registry Scans 11, 43, 52–56
    - Reports 47, 53, 57, 62, 94–98
    - Scheduling 47, 53, 57, 62, 95, 99–100

- Spyware Protection 74–82, 94
- Spyware Scans 11
- System Events 84–91
- System Policies 40, 62–70
- System Scans 11, 56–59
- Time Intervals 70, 71
- tracking browsing behavior 158, 159

### U

- update, database 6, 38, 46, 47
- URL (uniform resource locator) 33
- USB devices 62, 154
- USB mass storage devices 144, 154
- user account 16
  - access rights 69
  - Anonymous 96
  - Local System 16
  - Log On As 13
  - scheduled job 99, 100
- user group
  - Administrators 65
  - DynaComm PointGuard Users 16, 25
  - DynaComm Web Services 26
- user interface (IE) options 150
- user interface, active protection 6
- User Manager (Windows) 25

### V

- version, evaluation 23
- video file types 138, 143
- viewer
  - Event Results 87
  - File Scan Properties 50
  - File Scan Results 56
  - Registry Scan Properties 55
  - Registry Scan Results 56
  - Spyware Scan Results 78
  - System Scan Properties 56
- virus payload 160
- virus, described 160

### W

- warnings 17
  - Internet Explorer 22
  - listening service 26
  - uninstall 30
- web browser 150
- web site
  - FutureSoft 3, 37, 46, 47, 74
  - Sunbelt Software Research Center 76
- web site content file types 139, 143
- Welcome dialog 21, 22, 23, 28
- white-listing 38
- wild card characters 60

- windows
  - Active Protection 68
  - All Events 85
  - Content Management 56
  - Details 14
  - device management policy, individual 68
  - Device Policies 68
  - file management policy, individual 68
  - File Policies 68
  - File Scan Results viewer 56
  - File Scans 47, 50
  - Policy Items 62
  - Quarantine Management 14, 59
  - Real-Time Protection Client 87
  - Registry Scan Results viewer 56
  - Registry Scans 52
  - Removable Device Monitoring Client 87
  - Spyware Scan Results viewer 78
  - spyware scan, individual 75
  - Spyware Scans 75, 80
  - System Events 87
  - system events, individual 95
  - System Policies 62, 63, 70
  - system policy, individual 14, 42, 62, 63
  - System Scans 58
  - Windows 2000 7, 8, 10, 15
  - Windows 2003 9, 18
  - Windows 2003 Server 26
  - Windows 9.x 7, 8, 16
  - Windows 95 12
  - Windows 98 12
  - Windows Control Panel 16
  - Windows desktop 22, 29
  - Windows Internet Explorer (IE) 22, 150
  - Windows ME 12
  - Windows NT 7, 8, 12, 53
  - Windows Registry 6, 44, 52, 62, 64, 65, 153, 154
  - Windows Services 16
  - Windows Taskbar 21
  - Windows XP 9, 10, 11, 16
  - Windows, Microsoft
    - System Tray 64
- wizards
  - New File Scan 48
  - New Scheduled Job 94, 99
  - New System Scan 6, 56, 57
  - Setup 22–26
  - Setup Maintenance 28–30
- worm, described 160

### X

- XML log file 11, 13, 14, 51, 56