Symantec™ Client Security Administrator’s Guide
Technical support

As part of Symantec Security Response, the Symantec global Technical Support group maintains support centers throughout the world. The Technical Support group’s primary role is to respond to specific questions on product feature/function, installation, and configuration, as well as to author content for our Web-accessible Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering as well as Symantec Security Response to provide Alerting Services and Virus Definition Updates for virus outbreaks and security alerts.

Symantec technical support offerings include:
- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and Web support components that provide rapid response and up-to-the-minute information
- Upgrade insurance that delivers automatic software upgrade protection
- Content Updates for virus definitions and security signatures that ensure the highest level of protection
- Global support from Symantec Security Response experts, which is available 24 hours a day, 7 days a week worldwide in a variety of languages for those customers enrolled in the Platinum Support Program
- Advanced features, such as the Symantec Alerting Service and Technical Account Manager role, offer enhanced response and proactive security support

Please visit our Web site for current information on Support Programs. The specific features available may vary based on the level of support purchased and the specific product that you are using.

Licensing and registration

If the product that you are implementing requires registration and/or a license key, the fastest and easiest way to register your service is to access the Symantec licensing and registration site at www.symantec.com/certificate. Alternatively, you may go to www.symantec.com/techsupp/ent/enterprise.html, select the product that you wish to register, and from the Product Home Page, select the Licensing and Registration link.

Contacting Technical Support

Customers with a current support agreement may contact the Technical Support group via phone or online at www.symantec.com/techsupp.

Customers with Platinum support agreements may contact Platinum Technical Support via the Platinum Web site at www-secure.symantec.com/platinum/.
When contacting the Technical Support group, please have the following:

- Product release level
- Hardware information
- Available memory, disk space, NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description
  - Error messages/log files
  - Troubleshooting performed prior to contacting Symantec
  - Recent software configuration changes and/or network changes

**Customer Service**

To contact Enterprise Customer Service online, go to www.symantec.com, select the appropriate Global Site for your country, and then choose Service and Support. Customer Service is available to assist with the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information on product updates and upgrades
- Information on upgrade insurance and maintenance contracts
- Information on Symantec Value License Program
- Advice on Symantec's technical support options
- Nontechnical presales questions
- Missing or defective CD-ROMs or manuals
Technical support

Section 1  Managing Symantec Client Security

Chapter 1  Managing Symantec Client Security

About managing Symantec Client Security ..................................................... 17
Managing with the Symantec System Center ..................................................... 18
  Using console views ..................................................................................... 19
  Saving console settings .............................................................................. 21
  Understanding Symantec System Center icons ............................................. 22
  Discovering computers and refreshing the console ..................................... 24
  Auditing computers ...................................................................................... 36
About clients and servers .................................................................................. 42
  About primary servers .................................................................................. 42
  About secondary servers .............................................................................. 43
  About parent servers ..................................................................................... 43
About server and client groups .......................................................................... 43
  Deciding whether to manage with server groups and/or client groups ......... 44
  Server and client group scenario .................................................................. 46
Managing with server groups .......................................................................... 46
  Creating server groups ............................................................................... 46
  Locking and unlocking server groups ......................................................... 47
  Working with server group passwords ......................................................... 48
  Renaming server groups .............................................................................. 50
  Selecting a primary server for a server group .............................................. 50
  Changing primary and parent servers ......................................................... 51
  Moving a server to a different server group ............................................... 51
  Viewing server groups ............................................................................... 52
  Deleting server groups ............................................................................... 53
Enhancing server group security .................................................................... 53
  How the access list works ............................................................................ 53
  Implementing enhanced server group security .............................................. 54
Managing with client groups ................................................................. 58
  Creating new client groups ............................................................... 58
  Adding clients to a client group ......................................................... 58
  Configuring settings and running tasks at the client group level ....... 59
  Finding client group settings ............................................................. 59
  Moving clients in client groups ......................................................... 59
  Viewing client groups ...................................................................... 59
  Filtering the client group view ........................................................... 61
  Renaming client groups .................................................................... 62
  Deleting client groups ...................................................................... 62
  Configuring clients directly ............................................................... 63
  Changing an unmanaged client into a managed client (and the
  reverse) .............................................................................................. 63
  How settings propagate ..................................................................... 64
  New Grc.dat files overwrite old Grc.dat files .................................... 65

Chapter 2 Setting up the Alert Management System

About the Alert Management System .................................................... 67
How Alert Management System works ................................................ 68
Configuring alert actions ...................................................................... 69
  Alert configuration tasks ................................................................. 69
  Configuring alert action messages .................................................... 70
  Speeding up alert configuration ....................................................... 72
  Configuring the Message Box alert action ........................................ 74
  Configuring the Broadcast alert action ............................................. 75
  Configuring the Run Program alert action ....................................... 75
  Configuring the Load An NLM alert action ...................................... 76
  Configuring the Send Internet Mail alert action .............................. 77
  Configuring the Send Page alert action ........................................... 78
  Configuring the Send SNMP Trap alert action .................................. 80
  Configuring the Write To Event Log alert action ............................. 83
Working with configured alerts ............................................................. 83
  Testing configured alert actions ....................................................... 84
  Deleting an alert action from an alert .............................................. 84
  Exporting alert actions to other computers ..................................... 84
Using the Alert Management System Alert Log .................................. 86
  Viewing detailed alert information ................................................. 88
  Filtering the Alert Log display list ................................................. 89
  Forwarding alerts from unmanaged clients ..................................... 90
Section 2  Configuring Symantec Client Security antivirus protection

Chapter 3  Scanning for viruses and other threats

About threats ........................................................................................................ 95
About scans in Symantec Client Security ............................................................ 97
   Understanding Auto-Protect scans ............................................................... 98
   Understanding scheduled scans ................................................................ 98
   Understanding manual scans .................................................................... 98
   Selecting computers to scan ...................................................................... 99
Configuring Auto-Protect scans ........................................................................ 102
   Configuring Auto-Protect for files ..........................................................102
   Configuring Auto-Protect email scanning for groupware applications ..........111
   Configuring Auto-Protect scanning for Internet email .............................112
   How to specify exclusions ........................................................................114
   Configuring Auto-Protect settings ............................................................115
   How to lock and unlock Auto-Protect options ......................................116
Configuring manual scans ................................................................................116
   How to specify exclusions ........................................................................119
   Deleting files and folders that are left on computers by threats ......119
Configuring scheduled scans ...........................................................................119
   Scheduling scans for server groups or individual Symantec Client Security servers .................................................................120
   Scheduling scans for Symantec Client Security clients .........................122
   Setting options for missed scheduled scans ........................................125
   Editing, deleting, or disabling a scheduled scan ..................................125
   Running a scheduled scan on demand ..................................................126
   Deleting files and folders that are left on computers by threats ......127
Handling Symantec Client Security clients with intermittent connectivity ...........................................................................................................127
Contents

Configuring scan options ............................................................................................................. 129
How to assign primary actions and secondary actions for detected viruses ................................................................. 129
How to assign primary actions and secondary actions for other detected threats ......................................................... 130
Controlling the user experience .............................................................................................. 131
Scanning for in-memory threats ............................................................................................ 138
Excluding files from scanning ............................................................................................... 138
Selecting file types and extensions to scan for viruses ................................................................................. 140
Enabling expanded threat categories .................................................................................. 145
Setting options for scanning compressed files ................................................................... 147
Configuring HSM settings .................................................................................................. 147
Setting CPU utilization ....................................................................................................... 150

Chapter 4  Updating virus definitions files

About virus definitions files .................................................................................................. 151
Virus definitions files update methods ................................................................................ 152
Best practice: Using the Virus Definition Transport Method and LiveUpdate together ......................................................... 153
Best practice: Using Continuous LiveUpdate on 64-bit computers ........................................ 153
Updating virus definitions files on Symantec Client Security servers ................................ 154
Updating and configuring Symantec Client Security servers using the Virus Definition Transport Method .................................. 154
Updating servers using LiveUpdate .................................................................................... 160
Updating servers with Intelligent Updater ........................................................................ 163
Updating servers using Central Quarantine polling ......................................................... 163
Minimizing network traffic and handling missed updates .................................................... 164
Updating virus definitions files on Symantec Client Security clients ................................ 166
Updating virus definitions files on Symantec Client Security clients immediately ................................................................. 168
Configuring managed clients to use an internal LiveUpdate server ........................................ 169
Enabling and configuring Continuous LiveUpdate for managed clients ....................................... 170
Setting LiveUpdate usage policies ................................................................................... 171
Controlling virus definitions files ........................................................................................ 172
Verifying the version number of virus definitions files ..................................................... 173
Viewing the threat list ....................................................................................................... 173
Rolling back virus definitions files .................................................................................... 173
Testing virus definitions files ........................................................................................... 174
Update scenarios ........................................................................................................... 175
About scanning after updating virus definitions files ......................................................... 175
Chapter 5  Responding to virus outbreaks

About responding to virus outbreaks ............................................................. 177
Preparing for a virus outbreak ........................................................................ 178
Creating a virus outbreak plan ....................................................................... 178
Defining Symantec Client Security actions for handling
suspicious files ............................................................................................... 180
Automatically purging suspicious files from local Quarantines ................... 180
Handling a virus outbreak on your network ................................................. 181
Using virus alerts and messages ................................................................... 182
Running a virus sweep .................................................................................... 182
Tracking virus alerts using Event Logs and Histories ................................. 183
Tracking submissions to Symantec Security Response with
Central Quarantine Console ......................................................................... 183

Chapter 6  Managing roaming clients

About roaming clients ...................................................................................... 185
Roaming client components ........................................................................... 186
How roaming works ........................................................................................ 187
Implementing roaming .................................................................................... 187
Analyzing and mapping your Symantec Client Security network .... 188
Identifying servers for each hierarchical level ..................................... 189
Creating a list of 0 level Symantec Client Security servers .......... 189
Creating a hierarchical list of Symantec Client Security servers ..... 190
Configuring roaming client support options from the Symantec
System Center console .............................................................................. 190
Configuring additional roaming client support for roam servers .... 193
Configuring additional server types for roaming clients .................. 195
Command-line options .................................................................................. 195
Registry values ............................................................................................... 197

Chapter 7  Working with Histories and Event Logs

About Histories and Event Logs ..................................................................... 199
Sorting and filtering History and Event Log data ...................................... 201
Viewing Histories ........................................................................................... 203
Working with Threat Histories ................................................................. 204
Working with Scan Histories ........................................................................ 206
Understanding Event Log icons ................................................................... 208
Section 3 Configuring Symantec Client Security firewall protection

Chapter 8 Managing policies

About policies ..................................................217
Policy components .............................................218
Configuring policies and updates ..........................223
Creating and opening policies and updates .............224
Adding and editing policy descriptions ..................225
Saving policies and updates ................................226
Importing and exporting policies and updates ...........228
About importing and exporting ..........................230
About importing and exporting rules and pRules ......231
About importing and exporting Locations ...............232
About importing and exporting Location Awareness settings ....233
About importing and saving the default client policy file ..234
Merging rules and pRules in policy files ..................235
Distributing policies ........................................238
How policy distribution affects Locations, rules, and settings ....238
Using the policy file import/export utility ..............238

Chapter 9 Using Location Awareness and Zones

Using Locations .............................................241
Configuring required Location information ............242
Implementing Location Awareness .......................247
Deleting Locations .........................................253
Editing Locations and NetSpecs .........................254
Using Network Zones ......................................254
Adding computers to Zones ................................255
Copying Zones to other Locations .......................256
About locking Zones .......................................256
Deleting locked and unlocked Zones when exporting policies ..........257
Chapter 10 Creating and testing rules

About rules ........................................................................................................... 259
Rule categories ................................................................................................. 260
Rule types .......................................................................................................... 260
Rule processing order ...................................................................................... 260
Elements of a rule ............................................................................................ 261
About stateful inspection ................................................................................. 266

Working with firewall rules ............................................................................... 267
Creating rules .................................................................................................... 268
Displaying rules by Location .......................................................................... 270
Adding rules to different Locations ............................................................... 271
Deleting rules .................................................................................................... 271
Configuring rule lock settings ......................................................................... 272
About updating rulebases on Symantec Client Security firewall client .......... 272

Using port groups .............................................................................................. 273
Adding named port groups ............................................................................. 273
Deleting named port groups ........................................................................... 275

Using address groups ........................................................................................ 276
Adding named address groups ....................................................................... 277
Deleting named address groups ..................................................................... 278

Incorporating Secure Port ................................................................................. 279

Testing firewall rules ........................................................................................ 281

Chapter 11 Using pRules

About pRules ...................................................................................................... 287
pRules and user types ....................................................................................... 288
Using a digest value to identify a program ...................................................... 288
Priority of pRule evaluation .......................................................................... 289
Program rules and pRules .............................................................................. 289
Guidelines for using pRules ............................................................................ 290

Symantec-supplied pRules ............................................................................... 291
Creating and editing pRules ............................................................................ 292
Selectively disabling auto-create .................................................................... 294
Ignoring file name matching ........................................................................... 294
Specifying the program identity for a pRule .................................................. 295
Adding or editing match names for a pRule .................................................... 295
Configuring match criteria .............................................................................. 296
Adding a rule to a pRule .................................................................................. 300

Configuring pRules to support Active Directory .......................................... 301
Using Profiling to generate pRules and NetSpecs ........................................302
  Profiling overview .....................................................................................302
  Enabling Profiling in policy files .............................................................304
  About exporting the policy file to clients ..............................................304
  Viewing and saving profiled data with Symantec System Center .....305
  Retrieving profiled information ............................................................306
  Processing profiled firewall rule exceptions .........................................307
  Processing profiled connections .............................................................309
  Refreshing profiled data ...........................................................................310
  About working with .csv files ..............................................................310

Chapter 12 Customizing Intrusion Detection

About the Intrusion Detection System ...........................................................315
  Excluding attack signatures from being blocked .........................................316
  Configuring AutoBlock .....................................................................................317
  Excluding computers from AutoBlock ...................................................318
  Locking IDS exclusions and IP addresses ......................................................320

Chapter 13 Configuring Client Settings and Web Content settings

About Client Settings ........................................................................................321
  Access level settings ..................................................................................323
  Global settings ............................................................................................323
  Status settings ............................................................................................324
  Client firewall settings ..............................................................................325
  Intrusion Detection settings ....................................................................326
  Privacy Control settings ...........................................................................327
  Ad Blocking settings ..................................................................................327
  General options settings ...........................................................................328
  Tray Menu options settings .....................................................................328
  Advanced options settings .......................................................................329
  Alert Customization settings ...................................................................330

Setting user access levels .................................................................................331
  Web Content settings ..................................................................................333
  Global Settings ...........................................................................................334
  User Settings ..............................................................................................335
  Ad Blocking settings ..................................................................................335
### Chapter 14 Managing client log data

- About logging .......................................................... 339
- Saving client log data to text files .......................... 340
- Log Export utility syntax ........................................ 341
- Using wildcard characters in filters with LogExp.exe .... 342
- Log Export utility examples ......................................... 343
- Viewing Event Logs from the Symantec System Center ... 344
  - Displaying logs ..................................................... 346
  - Filtering log data .................................................... 347
  - Sorting log data .................................................... 347
  - Understanding Event Log icons .............................. 347

### Chapter 15 Creating network rulebases

- Choosing an implementation approach ..................... 349
- Considering implementation options ...................... 350
  - Using the Trusted Zone approach ......................... 350
  - Using the network-level firewall approach ............ 351
  - Using the program-level firewall approach ........... 351
- Implementing network rulebases ............................... 352
  - Implementing Trusted Zones ................................. 352
  - Implementing network-level firewalls ................. 353
  - Implementing program-level firewalls .................. 355
- Configuring an initial network rulebase .................... 358
- Fine-tuning and troubleshooting rulebases .................. 360
- Configuring a default-permit rulebase ...................... 362
- Configuring user interaction .................................... 363

### Index
Section 1

Managing Symantec Client Security

- Managing Symantec Client Security
- Setting up the Alert Management System
Managing Symantec Client Security

This chapter includes the following topics:

- About managing Symantec Client Security
- Managing with the Symantec System Center
- About clients and servers
- About server and client groups
- Managing with server groups
- Enhancing server group security
- Managing with client groups
- Configuring clients directly
- Changing an unmanaged client into a managed client (and the reverse)
- How settings propagate

About managing Symantec Client Security

Using the Symantec System Center, you can perform Symantec Client Security administrative operations such as installing antivirus protection on workstations and network servers, updating virus definitions, and managing Symantec Client Security servers and clients. In addition to the Symantec System Center, you can also use configuration files (Grc.dat) to configure Symantec Client Security clients. You can use configuration files if you want to use a third-party tool to perform remote configuration on your network.
Managing the Symantec System Center

When the Symantec System Center runs, it displays a system hierarchy of server groups, client groups, and servers displayed in an expandable/collapsible tree. The system hierarchy is the top level that contains all server groups and client groups.

**Note:** The system hierarchy is not populated until you install at least one Symantec Client Security server.

**To start the Symantec System Center**
- On the Windows taskbar, click **Start > Programs > Symantec System Center Console > Symantec System Center Console.**
Using console views

Each product management snap-in makes a new product view available within the Symantec System Center console. For example, when you install the Symantec AntiVirus management snap-in, the Symantec AntiVirus view is added, which includes fields related to Symantec Client Security, such as Last Scan and Definitions.

The columns that appear in the right pane change based on the selected view. When System Hierarchy is selected, the Console Default View includes the following data columns:

- Name
- Status
- Primary Server
- Valid State

Table 1-1 lists the data columns in the Symantec AntiVirus view.

<table>
<thead>
<tr>
<th>Object selected in left pane</th>
<th>Data columns that appear in right pane</th>
</tr>
</thead>
<tbody>
<tr>
<td>System hierarchy icon</td>
<td>Server Group</td>
</tr>
<tr>
<td></td>
<td>Status</td>
</tr>
<tr>
<td></td>
<td>Definition Sharing</td>
</tr>
<tr>
<td></td>
<td>Newest Definitions</td>
</tr>
<tr>
<td></td>
<td>Status of server updates</td>
</tr>
<tr>
<td>Server group icon</td>
<td>Server</td>
</tr>
<tr>
<td></td>
<td>Type</td>
</tr>
<tr>
<td></td>
<td>Status</td>
</tr>
<tr>
<td></td>
<td>Last Scan</td>
</tr>
<tr>
<td></td>
<td>Definitions</td>
</tr>
<tr>
<td></td>
<td>Version</td>
</tr>
<tr>
<td></td>
<td>Scan Engine</td>
</tr>
<tr>
<td></td>
<td>Address</td>
</tr>
<tr>
<td></td>
<td>Status of client updates</td>
</tr>
<tr>
<td>Groups icon (for client groups)</td>
<td>Group Name</td>
</tr>
<tr>
<td></td>
<td>Configuration Change Date</td>
</tr>
<tr>
<td></td>
<td>Number of Clients</td>
</tr>
</tbody>
</table>
Table 1-1  Data columns in the Symantec AntiVirus view

<table>
<thead>
<tr>
<th>Object selected in left pane</th>
<th>Data columns that appear in right pane</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client group icon or Server icon</td>
<td>■ Client&lt;br&gt; ■ User&lt;br&gt; ■ Status&lt;br&gt; ■ Last Scan&lt;br&gt; ■ Definitions&lt;br&gt; ■ Version&lt;br&gt; ■ Scan Engine&lt;br&gt; ■ Address&lt;br&gt; ■ Group&lt;br&gt; ■ Server</td>
</tr>
</tbody>
</table>

Table 1-2 lists the data columns in the Symantec Client Firewall view.

Table 1-2  Data columns in the Symantec Client Firewall view

<table>
<thead>
<tr>
<th>Object selected in left pane</th>
<th>Data columns that appear in right pane</th>
</tr>
</thead>
<tbody>
<tr>
<td>System hierarchy icon</td>
<td>■ Server Group&lt;br&gt; ■ Status</td>
</tr>
<tr>
<td>Server group icon</td>
<td>■ Server&lt;br&gt; ■ Type&lt;br&gt; ■ Status&lt;br&gt; ■ Version&lt;br&gt; ■ Server Policy File&lt;br&gt; ■ Server Policy Rollout Time&lt;br&gt; ■ Client Policy File&lt;br&gt; ■ Client Policy Rollout Time&lt;br&gt; ■ Address</td>
</tr>
<tr>
<td>Groups icon (for client groups)</td>
<td>■ Group&lt;br&gt; ■ Client Policy File&lt;br&gt; ■ Client Policy Rollout Time&lt;br&gt; ■ Number of clients</td>
</tr>
</tbody>
</table>
Changing console views

Unless you change the view, the Symantec System Center console displays the Console Default View. The other views available depend upon which managed Symantec Client Security products you have installed.

To change console views

1. In the Symantec System Center console, in the left pane, expand **System Hierarchy**.
2. On the View menu, in the list that appears at the bottom of the menu, select a view.

Saving console settings

When you close the console, you are prompted to save console settings for the Symantec System Center.

To save console settings

- Do one of the following:
  - Click **Yes** if you want to see the same console view the next time that you launch the Symantec System Center.
  - Click **No** if you want to see the last saved view the next time you launch the Symantec System Center.

---

**Table 1-2**

<table>
<thead>
<tr>
<th>Object selected in left pane</th>
<th>Data columns that appear in right pane</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client group icon or Server icon</td>
<td>Client</td>
</tr>
<tr>
<td></td>
<td>User</td>
</tr>
<tr>
<td></td>
<td>Status</td>
</tr>
<tr>
<td></td>
<td>Version</td>
</tr>
<tr>
<td></td>
<td>Policy File</td>
</tr>
<tr>
<td></td>
<td>Policy Rollout Time</td>
</tr>
<tr>
<td></td>
<td>Address</td>
</tr>
<tr>
<td></td>
<td>Group</td>
</tr>
<tr>
<td></td>
<td>Server</td>
</tr>
</tbody>
</table>

You can rearrange the order of the columns to better suit your needs.
Choosing No may result in lost settings. For example, if you change settings for an attached Quarantine Server, and then choose No when exiting the console, the changes are not retained for the Quarantine Server.

**Note:** If a newer version of MMC is present on the system, you may need to upgrade to the newer version to save changes upon exiting the Symantec System Center console.

### Understanding Symantec System Center icons

The Symantec System Center uses icons to represent the different states of computers that are running Symantec managed products. For example, if the server group icon in the server group view appears with a padlock icon, the server group must be unlocked with its password before you can configure or run scans for the computers in the server group.

*Table 1-3* lists the Symantec System Center icons.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Icon descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Icon]</td>
<td>Highest level object representing the system hierarchy, which contains all server groups.</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Unlocked server group or client group. Compare this icon to the locked server group icon. For security reasons, all server groups default to locked when you start the Symantec System Center.</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Locked server group. You must enter a password before you can view the computers in the server group to configure and run updates and scans.</td>
</tr>
<tr>
<td>![Icon]</td>
<td>An issue needs to be resolved in this server group. For example, there may not be a primary server assigned to the server group or a server may be infected with a threat.</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Symantec Client Security server running on a supported Windows or NetWare computer. Compare this icon to the next one, which is the primary server for the server group.</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Symantec Client Security primary server running on a supported Windows or NetWare computer.</td>
</tr>
</tbody>
</table>
### Table 1-3 Symantec System Center icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Icon descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="Icon" /></td>
<td>Unavailable Symantec Client Security server. This icon appears when communication is severed between the Symantec Client Security server and the Symantec System Center console. The communication error may result from one of several different causes. For example, the server system is not running, the Symantec software has been removed, or there could be a network failure between the console and the system.</td>
</tr>
<tr>
<td><img src="image2.png" alt="Icon" /></td>
<td>A virus was detected on the computer that is running Symantec Client Security server.</td>
</tr>
<tr>
<td><img src="image3.png" alt="Icon" /></td>
<td>A threat other than a virus, such as adware or spyware, was detected on the computer that is running Symantec Client Security server. <strong>Note:</strong> If Symantec Client Security detects a virus and a threat other than a virus on the same computer, the virus icon appears.</td>
</tr>
<tr>
<td><img src="image4.png" alt="Icon" /></td>
<td>Symantec Client Security client running on a supported Windows computer. When you select this computer, you view options only on that computer.</td>
</tr>
<tr>
<td><img src="image5.png" alt="Icon" /></td>
<td>A virus was detected on the computer that is running Symantec Client Security client.</td>
</tr>
<tr>
<td><img src="image6.png" alt="Icon" /></td>
<td>A threat other than a virus, such as adware or spyware, was detected on the computer that is running Symantec Client Security client. <strong>Note:</strong> If Symantec Client Security detects a virus and a threat other than a virus on the same computer, the virus icon appears.</td>
</tr>
<tr>
<td><img src="image7.png" alt="Icon" /></td>
<td>An issue needs to be resolved with this client. For example, virus definitions files may be out-of-date or the client group to which the client was assigned is no longer valid. The status field in the Symantec System Center console indicates the actual problem.</td>
</tr>
<tr>
<td><img src="image8.png" alt="Icon" /></td>
<td>The computer, which runs Symantec Client Security client software, is not currently connected to the network. You must enable a setting for the Symantec System Center console to show when clients are not connected to the network.</td>
</tr>
</tbody>
</table>
Showing when clients are offline
You can configure the Symantec System Center console to show when computers running Symantec Client Security client software are not currently connected to the network. The icon in the last row of Table 1-3 indicates that the client is offline.

To show when clients are offline
1. In the Symantec System Center console, on the Tools menu, click **SSC Console Options Properties**.
2. In the SSC Console Options Properties dialog box, on the Client Filter tab, under Group Options, check **Indicate when clients are offline**. This option is unchecked by default.

Showing client Auto-Protect status
You can configure the antivirus client or antivirus server icon to appear in the Windows system tray.

The icon shows a client or server’s Auto-Protect status as follows:
- When Auto-Protect is enabled, a check mark appears next to Enable Auto-Protect and the icon appears as a full shield.
- When Auto-Protect is disabled, the icon is covered by a universal no sign (a red circle with a diagonal slash).

Discovering computers and refreshing the console
At the first startup of a newly installed Symantec System Center console, the console will ping the network to find all available computers running Symantec Client Security servers. As soon as the servers respond, they are added to the console. Connected workstations running a managed Symantec client product are added when their parent server is selected in the console tree.

If you start servers that are running a manageable Symantec product while the Symantec System Center is already running, you may need to locate the server using the Find feature or Discovery Service so that it will display in the server group view.

You can also use Discovery to locate network computers on which Symantec Client Security is not installed.
Using the Discovery Service

The Symantec System Center console runs a single Windows NT service, the Symantec System Center Discovery Service (Nsctop.exe). This service is responsible for discovering the computers running Symantec Client Security server that appear in the Symantec System Center console. The Discovery service also populates the Symantec System Center console with objects.

You can choose one of the following Discovery types:

- Load from cache only
- Local Discovery
- Intense Discovery

See “Understanding Load from cache only discovery type” on page 27.

See “Understanding Local Discovery” on page 27.

See “Understanding Intense Discovery” on page 28.

How discovering computers on the network works

To discover computers on the network, a computer running Symantec Client Security server sends a ping packet to a computer running Symantec Client Security client. The ping program verifies that the remote computer exists and can accept requests. When the Ping Discovery Service (Intel PDS) hears a ping, it responds with a pong packet. Ping and pong packets are about 1 KB. A successful ping-pong discovery ensures that the computer is working.

The pong also provides valuable information, such as the following:

- Date of the computer’s virus definitions files
- When the computer was last infected
- Firewall version
- Timestamp of the firewall policy
- If the firewall is installed, enabled, and whether there was an error importing the last policy sent
- If the firewall policy on the server and client differ

Both IP and IPX pings are sent to the remote computer running Symantec Client Security server to determine what type of protocol it uses.

The data from the computer running Symantec Client Security antivirus client is stored on the computer running Symantec Client Security antivirus server that is the client’s parent server.

The Symantec System Center console reads each parent server’s registry to get the data that it displays in the console.
Following the completion of this process, Normal Discovery runs.

**Normal Discovery**

Following all types of Discovery, a Normal Discovery runs. In a Normal Discovery, the Symantec System Center console broadcasts to all servers that are in unlocked server groups. This additional Discovery queries the primary server of the server group for the list of secondary servers in its address cache.

The Symantec System Center console address cache stores information for all servers that have ever reported to it. The primary server address cache contains information for every server within the server group. The address cache includes the names of all secondary servers and their IP addresses.

The Symantec System Center console compares its own address cache with the address cache sent by the primary server. When a mismatch is identified, the console pings the associated server. When the pong data returns, it is added to all other servers in the list.

In this way, Normal Discovery can identify every server in the server group and attempt to resolve information conflicts between parent servers.

**Discovery Service WINS or Active Directory requirement**

The Discovery Service requires the use of WINS (Windows Internet Naming Service) or Active Directory name resolution. If you are attempting discovery in an environment where WINS or Active Directory is not available you will need to find at least one computer running Symantec Client Security server on your network first. To find the computer, you can use the Find Computer feature or the Importer tool.

See “Using the Find Computer feature” on page 32.


**How to find NetWare computers**

The Discovery Service may not find NetWare computers that are running IP only. To find computers not located by the Discovery Service, you can use the Find Computer feature.

See “Using the Find Computer feature” on page 32.

**Understanding the Discovery Cycle configuration**

The Discovery Cycle time-out is configurable. Depending on how you configure your Discovery Service, you can set the time-out from 1 to 1440 minutes between discovery attempts. By default, the interval is set to 480 minutes (every 8 hours).
A new discovery is skipped if the last discovery is still running. For example, if you have discovery set to run once a minute, and discovery takes 20 minutes, 19 discovery attempts will be skipped.

**Changing the Discovery Cycle interval**
While the Discovery Cycle interval can be changed, be aware that increasing the interval can result in a display of outdated information from the Symantec System Center console.

**To change the Discovery Cycle interval**
1. In the Symantec System Center console, on the Tools menu, click **Discovery Service**.
2. Change the Interval In Minutes setting as necessary.

**Understanding Load from cache only discovery type**
Load from cache only offers the most basic type of discovery. It tries to refresh all of the servers for which the Symantec System Center console contains information in its address cache. Each server is then sent a series of pings to see if the server will check back in, and to refresh information on the console.

Following the Load from cache only operation, the Normal Discovery runs.

See “**Normal Discovery**” on page 26.

Load from cache only is the default Discovery method. This reduces unwanted traffic on the network when launching the Symantec System Center. In most cases, you may find that choosing Load from cache only finds all of the servers that you need to add to the Symantec System Center console.

**Understanding Local Discovery**
When you use Local Discovery, a broadcast of a ping packet is sent over the local subnet of the computer running the Symantec System Center console. Intel PDS services running on servers on the local subnet reply with pong data.

Local Discovery generates less ping noise, but is limited to working on the local subnet. Local Discovery works very well on small subnets. In very large subnets, you may experience better results using Intense Discovery.

Following a Local Discovery, the following Discovery types run:
- Load from cache only
- Normal Discovery

See “**Normal Discovery**” on page 26.
Understanding Intense Discovery

Intense Discovery walks My Network Places on the local Windows 2000 computer or the Network Neighborhood on the local Windows NT computer, and attempts to resolve all computers that it finds into a network address. Once it has the network address, it attempts to send ping requests. You can configure whether Intense Discovery walks the NetWare or Microsoft branches of the network tree, or both.

From the Symantec System Center console, you can select any node beneath the console root, and then choose Discovery Service from the Tools menu to perform a new discovery of servers.

Following an Intense Discovery, the following Discovery types run:

- Local Discovery
- Load from cache only
- Normal Discovery

See “Normal Discovery” on page 26.

Note: The ability of Intense Discovery to locate computers is limited by several factors: the availability of a WINS server or Active Directory, network subnet and router configuration, DNS configuration, and Microsoft domain and workgroup configuration. Searching by IP address range in most cases is not affected by these factors. For this reason, you may want to use IP Discovery.

Understanding IP Discovery

IP Discovery provides discovery by either IP address range or IP subnet range. You may want to run IP Discovery only periodically. It can be used to discover computers across the network.

Once the computers are in the address cache, you can then rely on the Load from cache only method.

Running the Discovery Service

You manually run all forms of Discovery directly from the Symantec System Center console.
Note: The Discovery service uses WINS (Windows Internet Naming Service) or Active Directory when browsing for new computers that are running Symantec Client Security. If you are trying to discover new computers in an environment in which WINS or Active Directory is unavailable, you may want to run the Find Computer feature or the Importer tool first. See “Using the Find Computer feature” on page 32. See the Symantec Client Security Reference Guide for information about the Importer tool.

Run the Discovery Service
You can run the Discovery Service and find servers with or without including IP addresses and subnets.

To run IP Discovery
1. In the Symantec System Center console, in the left pane, select any node below the console root.
2. On the Tools menu, click Discovery Service.
3. In the Discovery Service Properties window, on the Advanced tab, check Enable IP Discovery.
Once Enable IP Discovery is checked, an IP Discovery session runs whenever you run an Intense Discovery. To run Intense Discovery without also running IP Discovery, uncheck Enable IP Discovery.

4 In the Scan Type list, select one of the following:
   - IP Subnet: The console broadcasts to each subnet.
   - IP Address: The console pings every computer in the range of IP addresses.

5 In the Beginning of range and End of range boxes, type the addresses.

6 If you clicked IP Subnet, type the subnet mask to refine the search.
   IP Address search results appear in the Machine list box. IP Subnet search results are displayed in the Symantec System Center console status bar.

You can also access IP Discovery functionality in the Find Computer dialog box. See “Using the Find Computer feature” on page 32.

To discover without IP

1 In the Symantec System Center console, on the Tools menu, click **Discovery Service**.
2 In the Discovery Service Properties window, on the General tab, select one of the following options:

- **Load from cache only**: This is the quickest method. The Symantec System Center reads the list of servers and clients stored in the local cache. See “Understanding Load from cache only discovery type” on page 27.

- **Local Discovery**: Broadcasts to the Symantec System Center console’s local subnet. Servers respond immediately with information about themselves and their clients. Each server’s server group will appear in the console (unless filtered using the View menu). Load from cache only will run as well. See “Understanding Local Discovery” on page 27.

- **Intense Discovery**: This is the most thorough method. If you have a large network, the discovery process may take a long time. The Symantec System Center serially pings every server in the Network Neighborhood. Server names appear in the message area of the Symantec System Center console as they are found during the discovery process. Intense Discovery also performs the same local subnet broadcast as Local Discovery. Load from cache only and Local Discovery will run as well.

  For Intense Discovery, you can limit the search to NetWare or Windows NT servers only, or search for both. See “Understanding Intense Discovery” on page 28.

3 Under Discovery Cycle, select the Interval in minutes if necessary.

4 If you want to immediately run discovery, click **Run Discovery Now**, and then click **Close**. Only one discovery can run at a time.

5 Under Intense Discovery Properties, specify the number of intense discovery threads.

  You can choose any number of threads between 2 and 50. This setting affects Intense Discovery sessions only. Each discovery thread is an independent search for servers and clients. To maintain the most up-to-date discovery information, select a lower discovery interval and a higher number of discovery threads.

6 If you want to clear all server and client information out of the active memory and address cache, and immediately run Discovery based on the current discovery settings, under Cache Information, click **Clear Cache Now**. When you clear the cache, unlocked server groups will be locked unless the password for the server group has been saved.
Note: Rebuilding a list of servers on a large network may take a long time.

Using the Find Computer feature
If you want to quickly find a server without having to expand and browse through the tree, you can use the Find Computer feature. You can search using TCP/IP or IPX addresses, or computer names.

The Find Computer feature is also useful if you install a server and then do not see it in the tree view when you expand a server group or server. This may occur for the following reasons:

- The Symantec System Center may not automatically discover servers on LAN segments separated by routers.
- Servers may not be visible in the Network Neighborhood. For example, Windows Internet Naming Service (WINS) servers or Active Directory may not be replicated across network segments.

Servers on segments using only IPX protocol can also be skipped in the discovery process. If you cannot locate some servers on your LAN, you can locate them manually with the Find Computer feature in the Symantec System Center console. Once you use the Find Computer feature to locate a server, you can manage it from the Symantec System Center console.

Note: If you don’t have IPX installed, you may not see all NetWare computers in the console. While you will be able to find the computers using the Find Computer feature, installing IPX and TCP/IP ensures that the computers will be discovered.

Finding computers by searching the local cache
Rather than search the entire network for computers, you can restrict the search to those known to be stored in the local cache.
To find computers by searching the local cache

1 In the Symantec System Center console, on the Tools menu, click **Find Computer**.

2 In the Find Computer window, on the Local Search tab, type the network name of the server that you want to find.

3 Under Match Type, select one of the following:
   - **Exact**: Searches for a server name that is an exact match.
   - **Partial**: Searches for a server name that is a partial match.

   If you leave the Search For text box empty and use Partial as the Match Type, all computers in the local cache will appear when you run the search.

**Finding computers using a network search**

You can use a network search to find individual computers running the Symantec Client Security server product.

**Find computers**

You can find computers using a network search or by specifying an IP address or subnet range.

**To find computers using a network search**

1 In the Symantec System Center console, on the Tools menu, click **Find Computer**.

2 In the Find Computer window, on the Network Discovery tab, specify whether you want to use a TCP/IP address, IPX address, or a computer name as the search criteria.
3 Type the server address or computer name.
4 Click **Find Now**.

**To use IP addresses to find a range of computers running Symantec Client Security for servers**

1 In the Symantec System Center console, on the Tools menu, click **Find Computer**.
2 In the Find Computer window, on the Scan Network tab, select one of the following:
   ■ IP Subnet: Sends out a broadcast to each subnet.
   ■ IP Address: Pings every computer in the range of IP addresses.
3 Type the addresses for **Beginning of range** and **End of range**.
4 If you clicked IP Subnet in step 2, type the subnet mask to refine the search.
5 Click **Find Now**.
   IP Address search results will appear in the Machine list box. IP Subnet search results will be displayed in the Symantec System Center console status bar.

**Locating found items in the Symantec System Center console**

You can match an item in a Find Computer list to the same item as it appears in the Symantec System Center console tree. To do so, the server group to which the item belongs must be unlocked.
To locate found items in the Symantec System Center console

1. In the Find Computer window, select the desired system.

2. Click Sync Item to locate the selected item.

Using the Refresh feature

From the Symantec System Center console, you can refresh at the system hierarchy, server group, or individual server level to validate active communication with the list of currently displayed servers. However, the Refresh feature does not find servers or server groups that may have been added since the current session of the Symantec System Center started. If the refresh determines that a server that previously appeared in the server group view is no longer communicating, the unavailable server icon appears.

To use the Refresh feature
- In the Symantec System Center console, in the left pane, right-click the system hierarchy, unlocked server group, server, or client group, and then click Refresh.
Auditing computers

Computers on your network that do not have Symantec Client Security running leave holes open in your network security. You can run a network audit of remote computers to determine the following:

- Whether a Symantec Client Security component is installed and running.
- The type of protection, such as antivirus server, client, or unmanaged client, that is installed.
- Whether antivirus software from other vendors or from Symantec (such as a Symantec AntiVirus consumer version), including the type and version of that software, is installed on the computer.

You must be able to log in as Administrator to the remote computers that you are auditing.

**Note:** If a firewall is running on the remote computer, the network audit may not be able to gather information.

**Run a network audit and sync items**

You can run a network audit to determine the antivirus protection status of the computers that you manage. Once the status for the computers in the range within which you searched is identified, you can locate selected computers by syncing to them.
To run a network audit

1. In the Symantec System Center console, on the Tools menu, click **Find Computer**.

2. In the Find Computer dialog box, on the Audit Network tab, type the beginning and end of the IP address range.

3. To change the default options, click **Options**. See “Setting network audit options” on page 39.
4 Click **Find Now** to run the audit.

You can see the audit progress at the bottom of the Find Computer dialog box.

When the audit completes, the following types of information appear:

- **Machine**  The name of the remote computer.
- **Server Group**  The name of the server group to which the remote computer belongs.
- **Server**  The name of the server that controls the remote computer.
- **Type**  The server or client type. Login errors are also reported in this column.
- **Version**  The version of the antivirus product running on the computer.
- **Address**  The IP address of the computer.
- **User**  The user name associated with the computer.

**To sync items**

1. In the Find Computer dialog box, click **Sync Item** to locate a selected computer running Symantec Client Security antivirus client.
2. Type the password for the server group to which the item belongs.
Labeling items and rerunning audits

You can label items such as the following:

- Computers that cannot be located or to which a connection cannot be made
- Routers and network drives
- Computers that do not have Symantec Client Security software installed

To label an item and rerun the audit

1. In the Find Computer dialog box, in the Machine column, right-click an item, and then click **Label**.
2. In the Edit description for dialog box, type a new label for the computer.
3. Click **OK**.
4. Right-click the item again, and then click **Audit again**.

Setting network audit options

You can set custom network audit options. For example, if you want to find remote computers running an unmanaged antivirus client, you can enable the related option.
To set network audit options

1. In the Find Computer dialog box, on the Audit Network tab, click **Options**.

2. In the Audit Network Options dialog box, specify the number of network audit threads to use. A higher number yields faster results but requires more network utilization.

3. Under Ping Options, specify the timeout period in milliseconds for a Windows ICMP ping or Symantec PDS ping.

4. Check **Continue auditing even if ICMP ping fails** if you want auditing to continue if the ICMP ping fails.

5. Under Display Options, check **Show previously labeled machines** if you labeled computers during a previous audit and want the computers to appear in the results as they were previously labeled.

6. Check **Show parent servers discovered through clients even if they fall out of the specified IP range** if you want the parent servers of the computers running Symantec Client Security antivirus client or antivirus server out of the specified range to appear in the results.
7 Under Symantec AntiVirus UDP Ports, enter up to four port numbers that you want to ping. 
   Port 1 defaults to 2967, which is the default port number for RTVScan, the main Symantec Client Security service.

8 Under Search Options, check the appropriate boxes to find computers running unmanaged Symantec Client Security, offline servers and clients, or computers running antivirus software from other vendors. 
   You must provide valid Admin account information. 
   See “Setting Admin account options” on page 41.

Setting Admin account options

If you choose to find computers running unmanaged Symantec Client Security, offline servers and clients, or computers running antivirus software from other vendors, the Remote Administrator Account dialog box appears.

See Figure 1-1.

Figure 1-1  Remote Administrator Account dialog box

To set Admin account options

1 In the Remote Administrator Account dialog box, do one of the following:
   ■ Type the name of the domain that contains the computers that you want to find, followed by valid domain administrator account information.
   ■ Check Use local accounts to access a specific computer, and then type the Admin user name and password.

2 Click OK.
About clients and servers

The Symantec Client Security client program provides antivirus protection for networked and non-networked computers. The Symantec Client Security client program protects 32-bit and supported 64-bit computers running supported Windows versions.

The Symantec Client Security server program manages other computers running Symantec Client Security and supported legacy versions of Norton AntiVirus Corporate Edition, and can push configuration and virus definitions files updates to these clients. In addition, the Symantec Client Security software provides antivirus protection for the computers on which it runs. Symantec Client Security clients are always managed by a server.

Note: The Symantec Client Security server program is not supported on 64-bit computers.

When you manage with the Symantec System Center, computers running Symantec Client Security server can assume the following roles:

- Primary server
- Secondary server
- Parent server

About primary servers

Each server group has an administrator-designated primary server. The primary server is responsible for configuration functions in the server group. It can also be responsible for new virus definitions files updates.

From the Symantec System Center console, when you launch a task at the server group level, the task runs on the server group’s primary server. The primary server also forwards the task on to all other servers in the server group.

If you are using Alert Management System², the primary server also processes all notifications.

Computers running any of the supported operating systems for servers can be made primary servers.

How the registry is affected

When you modify server options, you directly modify the registries of the selected servers. The modification is made through the transport manager, which handles communications.
The primary server acts as the repository of all server options on a group level. If you modify on a group level, the changes are recorded first in the registry of the primary server for that group in the HKLM\Software\Intel\LANDesk\VirusProtect6\CurrentVersion\DomainData key.

Then they are recorded in each of the other servers.

About secondary servers

Servers that are not assigned primary server status are called secondary servers. Secondary servers are children of primary servers. They retrieve information from the primary server and share it with clients.

All servers in a server group are secondary servers until you assign one as the primary server. You must designate the primary server before you can perform most tasks at the server group level.

Note: Symantec product configuration changes cannot be managed at a level higher than the server group.

About parent servers

A parent server is a computer running Symantec Client Security server with which a connected computer running Symantec Client Security client communicates to obtain configuration updates and to send alerts. Some servers may act as parent servers; others may act as primary servers. These two functions are not mutually exclusive. A primary server may also act as a parent server.

About server and client groups

Server group members can share a single Symantec Client Security configuration, and you can also run a Symantec Client Security operation on all members of a server group. From the Symantec System Center console, you can create new server groups and manage their membership. Server groups are independent of Windows domains and other products. You can combine NetWare and Windows computers into the same server groups, which allows simultaneous remote configuration of these systems.

Client groups are logical groupings of computers running Symantec Client Security client software. Although client groups are always attached to a server group, each client group can be managed individually. By setting up client
About server and client groups

You can set up and manage different policies under a single parent server.

- **Assigned clients** are Symantec clients that have been assigned to a client group. They receive virus definitions files from the server to which they are physically attached, but receive configuration settings and updates based upon the client group to which the Symantec Client Security policies are applied.

- **Unassigned clients** are Symantec clients that have not been assigned to a client group. They receive configuration settings and updates from their parent server.

### Deciding whether to manage with server groups and/or client groups

Each Symantec Client Security server group supports a single configuration for all of the clients it manages. Each additional configuration requires adding an additional server to the server group. Server groups may provide you with all the configuration flexibility you need if all of your clients require the same configuration options. If you need more configuration flexibility, you may benefit from using client groups. When you manage using client groups, clients on the same physical server do not need to share the same configuration as other clients in the same server group. In addition, client groups can also decrease the number of servers required to manage Symantec Client Security. While each server group requires at least one server per unique configuration, a server group can contain any number of client groups, each with its own configuration.

**Note:** If you want to use client groups, Symantec recommends managing all clients with groups. While it is possible to manage in a mixed environment with some clients assigned to a group and some not assigned to a group, this adds complexity and may produce unexpected results.

### Client groups and configuration priority

When you manage using client groups, clients assigned to a group receive their configuration from their group, rather than their parent server. Configuration changes made at the server level are ignored, and will only apply to unassigned clients. Configuration changes made at the server group level or system hierarchy level have priority over client group settings, and override any settings made at the client group level.
Table 1-4 lists each context you can select in the Symantec System Center, and what it configures, when selected.

**Table 1-4**  
**Configuration priority**

<table>
<thead>
<tr>
<th>Context</th>
<th>What it configures</th>
</tr>
</thead>
<tbody>
<tr>
<td>System hierarchy</td>
<td>All unlocked server groups and the clients they manage (regardless of their client group membership)</td>
</tr>
<tr>
<td>Server group</td>
<td>All servers and clients in the server group (regardless of their client group membership)</td>
</tr>
</tbody>
</table>
| Server           | The server and its clients (regardless of their client group membership):  
|                  | ▪ Virus Sweep  
|                  | ▪ Update virus definitions now  
|                  | ▪ History configuration  
|                  | The server and/or its unassigned clients:  
|                  | ▪ Scheduled and manual scans  
|                  | ▪ Virus definitions updating  
|                  | ▪ Quarantine options  
|                  | ▪ Client and server Auto-Protect options  
|                  | ▪ Client administrator only options  
|                  | ▪ Client roaming options  
|                  | ▪ LiveUpdate  
|                  | ▪ Update client policy now  
|                  | ▪ Auto-Protect status  
|                  | ▪ View virus list  
|                  | ▪ Clear virus status |
| Client group     | Clients assigned to the client group:  
|                  | ▪ Scheduled scans  
|                  | ▪ Virus definitions updating  
|                  | ▪ Quarantine options  
|                  | ▪ History configuration  
|                  | ▪ Client Auto-Protect options  
|                  | ▪ Client roaming options  
|                  | ▪ Client administrator only options  
|                  | ▪ Update client policy now  
|                  | ▪ LiveUpdate |
| Client           | Read only                                                                                                                                            |
Server and client group scenario

A company has Telemarketing and Accounting departments. These departments have staff in the company's Boston, New York, and Newark offices. All computers in both departments have been assigned to the same server group so that they receive virus definitions updates from the same source. However, IT reports indicate that the Telemarketing department is more vulnerable to threats than the Accounting department. As a result, the system administrator creates Telemarketing and Accounting client groups. Telemarketing clients share configuration options that strictly limit how users can interact with their threat protection.

Managing with server groups

You can create as many server groups as you need to manage your servers and clients efficiently.

Creating server groups

The installation program groups all of the servers that you select into one server group. This might be adequate if you want all of your managed computers running Symantec Client Security to use the same settings. However, if you want to make global configuration changes for groups of servers, you can create new server groups and easily use a drag-and-drop operation (or cut-and-paste) to move servers from one server group to another. When you move a server, all of its connected client computers move with it.

For example, if you have servers that require higher levels of protection, you can place all of them in the same server group and set special options to protect the server group. Note that you could also set up a new client group to achieve this same purpose.

See “About server and client groups” on page 43.
To create a server group

1. In the Symantec System Center console, in the left pane, right-click System Hierarchy, and then click New > Server Group.

2. In the New Server Group dialog box, type the name for the server group. The name cannot have more than 47 characters.

3. In the Password text box, type a password for the server group.

4. In the Confirm Password text box, retype the password.

5. Click OK.

Each server group requires a primary server.

See “Selecting a primary server for a server group” on page 50.

Locking and unlocking server groups

You can lock a server group with a password to prevent unauthorized administrators from making configuration changes. You can add or change passwords at any time. The default password for the server group was created during installation.

Passwords are case sensitive.

Lock and unlock server groups

You can lock and unlock server groups as necessary. To unlock a server group, you must type its password correctly. Passwords are case sensitive. You can also prevent server groups from locking when you exit the console.

To lock a server group

◆ In the Symantec System Center console, in the left pane, right-click the server group that you want to lock, and then click Lock Server Group.
To unlock a server group

1. In the Symantec System Center console, in the left pane, right-click the server group, and then click **Unlock Server Group**.

2. Type the password to unlock the server group.

3. Check **Save This Password** if you do not want to retype the password in future sessions or for other server groups that have the same password. If the password is correct, it will be saved.

To prevent unlocked server groups from locking when you exit the console

1. In the Symantec System Center console, in the left pane, right-click **System Hierarchy**, and then click **Properties**.

2. Uncheck **Lock All Server Groups When Exiting Console**.

Working with server group passwords

You can save, unsave, and change the server group password as necessary. To do so, the server group must have a primary server assigned to it. Empty passwords are allowed.

Saving server group passwords

You can save passwords if you do not want to reenter them in future sessions. Once the password is saved, you will not need to enter it when opening any server group that uses the same password. Saved passwords are DES encrypted and are stored in the registry of the local computer. When you attempt to unlock a server group, the Symantec System Center tries all of the saved passwords. You will be prompted for a password only if none of the saved passwords works.

Save or unsave server group passwords

The Save this password check box saves a password so that you do not have to enter it the next time the server group is opened.

When the password is saved, any previously accessed server group is either already unlocked or it does not prompt you for a password when you attempt to unlock it.

If you unchecked Lock All Server Groups When Exiting Console on the System Hierarchy properties page, the server group remains unlocked when the Symantec System Center console is reopened.

If you do not save passwords, all server groups are automatically locked by default each time that the Symantec System Center runs, even if you unlocked them the last time that you ran the program.
To save a server group password
1. In the Symantec System Center console, in the left pane, right-click a locked server group, and then click **Unlock Server Group**.
2. Type the password for the server group.
   - If the server already has a password and you checked the Save This Password checkbox, the password dialog box does not appear. Create a new password in order to use this feature.
3. Check **Save This Password**.
4. Click **OK**.

See “Changing server group passwords” on page 49.

To no longer save the server group password
1. In the Symantec System Center console, in the left pane, right-click an unlocked server group, and then click **Lock Server Group**.
2. Type the old password.
3. Press Tab, and then type the new password.
4. Press Tab, and then retype the password.
5. Click **OK**.
6. Close the Symantec System Center console.
7. When prompted to save, click **No**.

**Changing server group passwords**
You can change server group passwords. For example, you may want to change passwords regularly for security purposes.

To change a server group password
1. In the Symantec System Center console, in the left pane, right-click the server group, and then click **Configure Server Group Password**.
2. Type the old password.
3. Press Tab, and then type the new password.
4. Press Tab, and then retype the password.
5. Click **OK**.
Renaming server groups

You can rename server groups as necessary.

To rename a server group
1. In the Symantec System Center console, in the left pane, unlock the server group that you want to rename, if necessary.
2. Right-click the server group, and then click Rename.
3. Type the new server group name.

Selecting a primary server for a server group

When you select a server group object in the Symantec System Center console and set options, the settings are saved to the primary server in the server group. Other servers in the server group will also use the new configuration.

You must specify which server in the server group is the primary server. No server is specified as the primary server by default. Until you designate a primary server, you cannot perform some Symantec product management operations.

Computers that are running any of the following operating systems can be primary servers:

- Windows 2000 Server/Advanced Server/Professional
- Windows XP Professional
- Windows NT 4.0 Server/Workstation
- NetWare Server

The primary server plays an important role, so select a stable server that is always running.

To select the primary server for a server group
- In the Symantec System Center console, in the left pane, right-click the server that you want to be the primary server, and then click Make Server A Primary Server.

Note: When changing primary servers, you may lose the AMS² alerts that you have set up. You can reconfigure the alerts on the new primary server, or export the alerts to the new server before you change primary servers.
Changing primary and parent servers

You can change primary servers and parent servers easily.

**Change primary and parent servers**

You can demote primary servers and promote secondary servers as necessary.

To change a parent server, you must copy a configurations file (Grc.dat) from the new parent to the client, and then restart the client.

The configurations file is a text format file that acts as a repository of changes being made to a group of clients. Configurations files are the heart of the communication between computers running Symantec Client Security server and computers running Symantec Client Security client. They store important information such as parent server identity and Symantec Client Security product configuration settings.

To change a primary server

1. In the Symantec System Center console, in the left pane, double-click the server group icon.

2. Right-click the secondary server that you are designating as a primary server, and then click **Make Server A Primary Server**.

To change a parent server of a client

1. On the intended parent server, copy the configurations file (Grc.dat) from `\Program Files\SAV\`

2. On the client, paste the configurations file into one of the following folders:
   - For Windows 98\Me: `C:\Program Files\Symantec AntiVirus`
   - For Windows NT: `C:\Winnt\Profiles\All Users\Application Data\Symantec\Symantec AntiVirus Corporate Edition\7.5`
   - For Windows 2000\XP\2003: `C:\Documents and Settings\All Users\Application Data\Symantec\Symantec AntiVirus Corporate Edition\7.5`

3. Restart the client.

Moving a server to a different server group

You can move a server between groups using a drag-and-drop operation.

When you move a server, a server configurations file (Grcsrv.dat) is created on the server automatically. This file synchronizes the new server group settings to the server. The new server group must have a primary server.
Managing with server groups

The server configurations file is located in the same directory to which Symantec Client Security was installed on the server. It has the same format as a client configurations file (Grc.dat). It is created only when synchronizing a server to a new server group’s settings.

The server configurations file works only for servers that are running Norton AntiVirus Corporate Edition version 7.5 or later, and Symantec Client Security server. For older servers, the Symantec System Center topology service copies registry settings from the primary server to the server that is being moved.

Viewing server groups

When you run the Symantec System Center console, you see servers that are running managed Symantec Client Security products in a tree format. Servers are grouped under server groups.

Viewing a single server group

You can view a single server group and its contents.

To view a single server group

◆ In the Symantec System Center console, right-click the server group, and then click New Window From Here.

Filtering the server group view

You can filter which server groups display in the Symantec System Center server group list. You can monitor and administer only the server groups that display in the list. By default, the Symantec System Center console displays all server groups. To remove server groups from your console, filter the view.

You receive notifications for displayed server groups only. If you filter a server group, you will not receive notifications from that server group.

To filter the server group view

1 In the Symantec System Center console, in the left pane, right-click System Hierarchy, and then click View > Filter Server Group View.

2 Uncheck the server groups that you want to filter from the server group list. All server groups display by default.

3 Click OK.
Deleting server groups

Before you can delete a server group, you must move its members to a new or existing server group.

To delete a server group
1. In the Symantec System Center console, in the left pane, right-click the server group that you want to delete, and then click Unlock Server Group if necessary.
2. In the server group that you want to delete, move any existing servers using a drag-and-drop operation into another server group. You can only delete a server group if it is empty.
3. Right-click the empty server group, and then click Delete.
4. Right-click System Hierarchy, and then click Refresh.

Enhancing server group security

You can enhance the security that is provided by server group passwords by creating an access list that restricts inbound communication to only the IP and IPX addresses that are specified in the access list. For example, you can prevent an attacker who has access to the Symantec System Center console and a valid server group password from making unauthorized changes to the following:

- Server and client antivirus protection settings
- Auto-Protect settings
- Client group member assignments
- Primary server assignments
- Grc.dat file distribution
- Virus definitions file rollbacks

How the access list works

The access list is stored in the Windows registry on every computer that you want to protect. The address for each Symantec System Center console that communicates with the computer is validated against the access list. Symantec System Center consoles with IP or IPX addresses that are not included in the access list are limited to read-only access for antivirus protection and other settings (see Figure 1-2).
Implementing enhanced server group security

You can perform the following tasks to implement protection and monitor unauthorized configuration changes:

- Choose which computers to protect.
- Create the access list.
- Roll out the access list.
- Log unauthorized configuration change attempts.
Choosing which computers to protect

The IP address of the computer running the Symantec System Center console should be included in the access list of every server in a server group. If you are only changing client group settings, you only need to include the address for the primary server.

You do not need to include the access list on every client. You can effectively lock down a server group and prevent IP spoofing by creating the access list on each server and leaving it empty. Add IP and IPX addresses to the access list only when you need to allow the Symantec System Center to access the server. Delete the value for an address when you no longer require access.

Creating the access list

To create an access list, you create a registry subkey and specify the authorized IP and IPX addresses.

To create the access list

1. Start a registry editor, such as Regedt32.
2. Open the HKEY_LOCAL_MACHINE\SOFTWARE\INTEL\LANDesk\VirusProtect6\CurrentVersion key.
3. Type AccessList as a new subkey.
4. In the AccessList subkey, add string values for IP and IPX addresses and subnet addresses of the computers that you want included in the access list. Use the following formats:

   **IP**  
   Type (IP)-<0.0.0.0> where <0.0.0.0> is the numeric address for the computer.

   **IP subnet**  
   Type (IP)-<0.0.0.0>/<n> where <0.0.0.0> is the numeric address for the computer and <n> is the subnet notation (for example, 16 or 24).

   **IPX**  
   Type (IPX)-<00000000:0000000000000000> where <00000000:0000000000000000> is the numeric address for the computer.

   **IPX subnet**  
   Type (IPX)-<00000000::FFFFFFFFFFFF> where <00000000> is the numeric address for the computer and <FFFFFFFFFFFF> is the subnet notation.

5. Close the registry editor.
Forcing the access list to reload

By default, the access list is refreshed every five minutes. If you want a change that you make to the list to take place immediately, you can force the reload.

To force the access list to reload

1. Start a registry editor, such as Regedt32.
2. Open the HKEY_LOCAL_MACHINE\SOFTWARE \INTEL\LANDesk\VirusProtect6\CurrentVersion\ProductControl key.
3. Type **ReadAccessList** as a new DWord.
4. Type 1 as the binary data associated with the ReadAccessList DWord value.
5. Close the registry editor.

Rolling out the access list

You can roll out the access list by performing the following tasks:

- Create a registry script with the information that you want to add to the access list, such as new values to authorize additional computers.
- Roll out the access list via your preferred distribution tool.
- Force the Symantec Client Security antivirus component to import the access list immediately.
  
  See “Forcing the access list to reload” on page 56.

Logging unauthorized configuration change attempts

When the Symantec Client Security antivirus component receives communication from an address that is not included in the access list, an event can be written to the Symantec AntiVirus Event Log. When the event occurs on a computer running Symantec Client Security, the log event is forwarded to the parent server.

**Note:** Unauthorized configuration change information is not written to logs by default.

Log changes and set logging frequency

You can edit the registry to log unauthorized changes. You can specify the frequency with which these items are logged.
To log unauthorized configuration changes

1. Start a registry editor, such as Regedt32.
2. Open the HKEY_LOCAL_MACHINE\SOFTWARE\INTEL\LANDesk\VirusProtect6\CurrentVersion\AccessList key.
3. Type `LogAccessDenied` as a new DWord.
4. Type `1` as the binary data associated with the LogAccessDenied DWord value to enable logging.
5. Close the registry editor.

To set the frequency for logging unauthorized configuration change attempts

1. Start a registry editor, such as Regedt32.
2. Open the HKEY_LOCAL_MACHINE\SOFTWARE\INTEL\LANDesk\VirusProtect6\CurrentVersion\AccessList key.
3. Type `LogAccessDeniedWindowMinutes` as a new DWord.
4. Do one of the following:
   - To record every incident, type `0` as the binary data associated with the LogAccessDeniedWindowMinutes DWord value.
     The following message will appear when an unauthorized event occurs: Access denied to network communication from unauthorized address: `<IP or IPX address>` `<port>` where `<IP or IPX address>` is the IP or IPX address of the computer that was denied access and `<port>` is the port number that the computer attempted to use.
   - To record incidents based on a frequency in minutes, type a number (in minutes) as the binary data associated with the LogAccessDeniedWindowMinutes DWord value.
     The following message will appear when an unauthorized event occurs: Access denied to network communication from unauthorized addresses `<N>` time(s) in the last `<N>` minute(s). Most recent address: `<IP or IPX address>` `<port>` where `<N>` is the frequency and the number of minutes, `<IP or IPX address>` is the IP or IPX address of the computer that was denied access, and `<port>` is the port number that the computer attempted to use.
5. Close the registry editor.
Managing with client groups

You can create as many client groups as you need to manage your clients efficiently.

Creating new client groups

All server groups contain a single Groups folder that contains all of the groups for that server group. When you create a new client group, the client group appears inside the Groups folder.

To create a new client group

1. In the Symantec System Center console, in the left pane, right-click the server group to which you want to add the client group, and then click Unlock Server Group.
2. Right-click the Groups folder, and then click New Group.
3. In the New Client Group dialog box, in the Enter name of the new client group text box, type the name for the new client group.
   The name cannot have more than 15 characters.
4. To apply the settings from an existing client group to the new client group, select the name of the existing client group from the drop-down list.
5. Click Create.

Adding clients to a client group

Computers running Symantec Desktop Firewall, Norton Internet Security, or Norton Personal Firewall must be migrated to Symantec Client Security firewall client before they can be managed.

A client can belong to only one client group.

To add a client to a client group

1. In the Symantec System Center console, in the left pane, click the server that contains the client.
2. In the right pane, move the client to the client group using a drag-and-drop operation.
Configuring settings and running tasks at the client group level

You can set configuration options and run tasks at the client group level. The settings will be applied to, or the task run on, all clients in the client group.

To configure settings and run tasks at the client group level
1. In the Symantec System Center console, in the left pane, right-click the client group.
2. Click All Tasks.
3. Click the product for which you want to set options.
4. Click the type of settings that you want to configure or the task that you want to run.

Finding client group settings

Client group settings are stored in the primary server’s registry. They are rolled out to each server in a client group configurations file (Grcgrp.dat). The primary server packages all client group settings into the client group configurations file, and then copies it to each secondary server in the server group. The secondary server rolls out the settings to the clients that it manages.

See the Symantec Client Security Reference Guide for information about configurations files.

Moving clients in client groups

You can move clients from one client group to another using a drag-and-drop operation. Once you move the client, it receives the new client group’s configuration settings.

Viewing client groups

When you view client groups, you can do the following:

- View a single client group.
- View information about client groups.
- Filter the client group view to show only the information that interests you.

Viewing a single client group

You can view the contents of client groups one group at a time.
To view a single client group

1. In the Symantec System Center console, in the left pane, right-click the server group that contains the client group, and then click Unlock Server Group.
2. Double-click the server group.
3. Double-click the Groups folder.

The client groups appear nested beneath the Groups folder.

Viewing information about client groups

When the Groups folder is selected in the left pane and Default Console View or a Symantec product view is selected from the View menu, the client groups appear in the right pane along with information specific to the view. For example, when the Default Console View is active, the number of clients in each client group appears.

Client group filtering must be enabled for the clients to be enumerated. When you select the Groups folder, the number of clients reported for each client group may not be accurate until a client group is selected.

See “Filtering the client group view” on page 61.
Filtering the client group view

When you select a client group in the left pane, all of the clients assigned to it can appear in the right pane.

Filtering improves client viewing performance in the Symantec System Center console. However, if there are many clients and servers in the server group, filtering may have a performance impact. The clients must be enumerated to display the client groups accurately. Filtering is disabled by default.

To filter the client group view

1. In the Symantec System Center console, on the Tools menu, click SSC Console Options.

2. In the SSC Console Options Properties dialog box, on the Client Filter tab, under Group Options, click **Show client machines when viewing Groups**.

3. Under Server Options, click the following options as desired:
   - **Build client lists when the Server Group is unlocked**: Enumerates all clients in the server group when it is unlocked. When this option is unchecked, clients are not added to their client groups until the server is selected. The number of clients in a client group is not accurate until all the servers in the server group have been selected.
   - **Cache all client info (including clients in locked Server Groups)**: Enumerates clients in both unlocked and locked server groups that are discovered by the Topology Service. These options may impact performance if there are many clients and servers in the server group.

4. Under Client Options, check **Indicate when clients are offline** to display a unique icon in the Symantec System Center console when a client is not connected to the network.

5. Click **OK**.

6. On the Action menu, click **Refresh**.
Renaming client groups

The Symantec System Center does not support renaming client groups directly. If you need to change the client group name, you must complete the following tasks:

- Create a new client group, importing settings from another client group if desired.
  See “Creating new client groups” on page 58.
- Move clients from the old client group to the new client group using a drag-and-drop operation.
- Delete the old client group.
  See “Deleting client groups” on page 62.

Deleting client groups

Before you delete a client group, you may want to reassign the clients to another client group.

When a client group is deleted, the clients that are assigned to it retain the settings of the deleted client group. The clients are not assigned new settings until one of the following actions occurs:

- The client checks in with its parent server. The client is then assigned the server’s default settings for unassigned clients.
- The client is assigned to another client group. The client is then assigned the settings of the new client group.

If you delete a client group, and then recreate it before the clients check in with their parent servers or are reassigned, the clients resume membership in the group automatically. They continue to assume the settings of that group.

To delete a client group

1. In the Symantec System Center console, in the left pane, unlock the server group from which you want to delete the client group.
2. Double-click the server group.
3. Double-click the Groups folder.
4. Right-click the target group, and then click Delete Group.
5. Click Yes.
6. Click Delete.
Configuring clients directly

You can allow for the direct configuration of Symantec Client Security clients. The options that you set directly remain in force until a new configurations file (Grc.dat) is copied to the client.

To allow direct client configuring

- In the SSC Console Options Properties dialog box, on the Client Filter tab, under Group Options, click **Allow direct configuration of individual clients**.
  This option is unchecked by default.

Changing an unmanaged client into a managed client (and the reverse)

You can change an unmanaged client into a managed client, and a managed client into an unmanaged client.

**Change a client’s management mode**

When you change an unmanaged client into a managed client, it will appear in and be configurable by the Symantec System Center. Similarly, changing a managed client into an unmanaged client will cause the client to disappear from the Symantec System Center.

To change an unmanaged client into a managed client

1. Decide which server is going to be the client’s parent server.
2. Open Network Neighborhood or My Network Places.
3. Locate and double-click the computer that you want to act as the parent server.
   The Symantec Client Security server must be installed on the computer that you select.
4. Open the `VPHOME\Clt-inst\Win32` folder.
5. Copy Grc.dat to the desired location.
6. Paste the Grc.dat file to one of the following folders on the unmanaged client:
   - Windows 98/Me: `C:\Program Files\Symantec AntiVirus`
   - Windows NT 4.0: `C:\Winnt\Profiles\All Users\Application Data\Symantec\Symantec AntiVirus Corporate Edition\7.5`
Windows 2000/XP/2003: C:\Documents and Settings\All Users\Application Data\Symantec\Symantec AntiVirus Corporate Edition\7.5

7 Restart the client.

To change a managed client into an unmanaged client
1 Uninstall Symantec Client Security from the client workstation.
2 Using the registry editor, delete the following subkey:
   HKEY_LOCAL_MACHINE\Software\Intel\LANDesk\VirusProtect6
3 Reinstall Symantec Client Security.
4 When prompted to make the client either managed or unmanaged, choose unmanaged.

How settings propagate

The method that Symantec Client Security uses to propagate settings depends upon the item that you choose in the Symantec System Center console.

Table 1-5 describes how settings propagate when you choose server groups, servers, and clients.

Table 1-5 How settings propagate from the Symantec System Center console

<table>
<thead>
<tr>
<th>Object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server groups</td>
<td>When you set options at the server group level, and then click OK, the Symantec System Center topology service communicates directly with the primary server and only overwrites the settings that you change. If you click Cancel, no options change. The primary server updates other servers in the server group through a temporary Grgrp.dat file, and only overwrites the settings that you change. Parent servers update their clients by rolling out a new Grc.dat file. This file replaces the existing Grc.dat file. Custom settings in the old Grc.dat file are not retained. Whenever you click Reset All, Symantec Client Security overwrites all settings in the dialog box.</td>
</tr>
</tbody>
</table>
Managing Symantec Client Security

How settings propagate

Note: Auto-Protect scanning settings must be locked before they are propagated to clients. See “Scanning for viruses and other threats” on page 95.

<table>
<thead>
<tr>
<th>Object</th>
<th>Description</th>
</tr>
</thead>
</table>
| Servers      | When you set options at the server level, and then click OK, the Symantec System Center topology service communicates directly with the selected server. Only the selected server is affected.  
If you click Cancel, no options change.  
If you click OK without changing options, Symantec Client Security does not overwrite the server’s current options. |
| Client groups| When you set options at the client group level, and then click OK, the primary server creates a Grcgrp.dat file and sends it to secondary servers.  
The secondary servers update their clients by rolling out a new Grc.dat file. This file replaces the existing Grc.dat file. Custom settings in the old Grc.dat file are not retained.  
If you click Cancel, no options change. |
| Clients      | When you set options at the client level, and then click OK, the System Center Topology service communicates with the client directly and makes the single change in the registry.  
If you click Cancel, no options change. |

**New Grc.dat files overwrite old Grc.dat files**

New Grc.dat files are propagated and overwrite old Grc.dat files any time that they are sent to the client. This behavior occurs even when you open a Symantec Client Security window or dialog box that contains options from the Symantec System Center console, and then click OK without changing options. If the earlier Grc.dat version contained custom settings that are not in the new Grc.dat, the settings are overwritten.

See the Symantec Client Security Reference Guide for additional information on using Grc.dat files.
How settings propagate
Chapter 2

Setting up the Alert Management System

This chapter includes the following topics:

- About the Alert Management System
- How Alert Management System works
- Configuring alert actions
- Working with configured alerts
- Using the Alert Management System Alert Log
- Forwarding alerts from unmanaged clients

About the Alert Management System

Alert Management System² (AMS²) provides emergency management capabilities. AMS² supports alerts on supported NetWare servers, Windows NT/2000 servers and workstations, Windows XP Home Edition/Professional, and Windows 98/Me workstations.

AMS² can generate alerts through the following means:

- Message box
- Broadcast
- Internet mail
- Page
- Run a program
- Write to the Windows NT Event Log
Setting up the Alert Management System

How Alert Management System works

- Send an SNMP trap
- Load an NLM

**Note:** Alerts generated through SNMP traps can be sent to any third-party SNMP management console. To receive SNMP traps from Symantec Client Security, you must have the Symantec System Center and AMS² installed. (Only a primary server will run AMS². You must use the Symantec System Center to designate the primary server.)

See “Configuring the Send SNMP Trap alert action” on page 80.

How Alert Management System works

AMS² alerts are transferred from Symantec Client Security into AMS² through the Symantec Client Security service. On a computer running the Symantec Client Security client, the Symantec Client Security service waits for an event thread that requires an alert.

These threads can be generated by the following events:

- Configuration change
- Default Alert
- Symantec Client Security startup/shutdown
- Scan Start/Stop
- Virus Definitions File Update
- Threat Found

If you have configured an alert for any of these events, when the event occurs it will generate a thread. The thread prompts the Symantec Client Security service to create a threat information block, which it forwards to the client’s parent server. When the parent server receives the threat information block, it enters it into its AMS² log. The threat information is then forwarded to the primary server, which makes a call to AMS². AMS² enters the information into the AMS² database and acts on it. The action taken depends upon how you have the alert configured.

Communication in AMS² is carried out through CBA, which is part of the Intel Communication Method.
Configuring alert actions

AMS² lets you configure many different methods of notification—such as pager, SNMP, and email—for detected threats and configuration changes.

Alert configuration tasks

AMS² alert configuration requires the following related tasks:

- Select an alert in the Alert Actions dialog box.
- Select the alert action that you want to configure for that alert. The alert action is the response AMS² sends you when an alert parameter is detected.
- Configure the alert action that you selected.

For example, you could configure the Send Page alert action to notify you if a threat was detected on a protected server. The pager message could also include information such as threat name and type, and actions taken on the infected file.

There are no default alert actions for any of the alerts. Until you configure AMS², no alerts are generated, though threat events are logged in the AMS² log file.

You can set up more than one action for each alert. Once you have configured alert actions for an alert, a plus (+) or minus (-) sign appears next to each configured alert, depending on whether the entry is collapsed or expanded.

Each AMS² alert action has its own configuration wizard. Once you have configured an alert action, the action appears in the Alert Actions dialog box under the alert for which you configured the action.

All alert actions execute on the computer that you select when you configure the action. Actions will not execute if you configure them on a computer that doesn’t support that particular action. For example, any computer that you configure the Send Page action on must have a modem.
To configure an alert

1. In the Symantec System Center console, right-click the server group, and then click **All Tasks > AMS > Configure**.

2. Select an alert, and then click **Configure** to define an alert action.

**Configuring alert action messages**

For alert actions that generate messages (for example, Message Box, Broadcast, Send Page, and Send Internet Mail), you can include additional information from the alert that generated the message. The additional types of information appear in **Table 2-1**.

<table>
<thead>
<tr>
<th>Alert parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;Alert name&gt;</td>
<td>The name of the alert; for example, Symantec Client Security Startup/Shutdown</td>
</tr>
<tr>
<td>&lt;Computer&gt;</td>
<td>The name of the computer where the alert originated</td>
</tr>
<tr>
<td>&lt;Host Name&gt;</td>
<td>Alert server name</td>
</tr>
<tr>
<td>&lt;Date&gt;</td>
<td>The date when the notification was generated</td>
</tr>
<tr>
<td>&lt;Time&gt;</td>
<td>The time when the notification was generated</td>
</tr>
<tr>
<td>&lt;Severity&gt;</td>
<td>The level of severity assigned to the alert; for example, Critical or Non-Critical</td>
</tr>
</tbody>
</table>
Table 2-1  Alert parameters

<table>
<thead>
<tr>
<th>Alert parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;Source&gt;</td>
<td>The product source of the notification; for example, Symantec Client Security</td>
</tr>
<tr>
<td>&lt;Description&gt;</td>
<td>More information about the nature of the notification; for example, “Symantec Client Security services shutdown was successful”</td>
</tr>
</tbody>
</table>

The Message dialog box includes a text box in which you can enter as many as 256 characters to be used as the text of the message that you want to send. You can use the variables in Alert parameters to insert information generated by the alert. Parameters are delimited by < and > characters. Each parameter placeholder that you add to the Message text box is substituted with corresponding alert information when an alert occurs.

See Figure 2-1.

Figure 2-1  Alerting System Notification

See “Testing configured alert actions” on page 84.

If the AMS² alerting system detects a message larger than 1 KB, the message will not be delivered. If you have configured a default alert message, it will be delivered instead. You can configure this default alert to notify you when a message exceeds 1 KB.

To configure a default alert message

1. In the Symantec System Center console, right-click the server group, and then click All Tasks > AMS > Configure.
2. Click Default Alert, and then click Configure.
3. Click Message Box, and then click Next.
4. Select a computer on which to execute the action, and then click Next.
5 Select whether you want an error beep and whether you want the dialog box to always appear on top until it is cleared.

6 Click Next.

7 Type the action name that describes the message that you are configuring. The action name and the action computer name appear in the Alert Actions dialog box beside this action.

8 In the Message box, do one of the following:
   ■ Type custom message text that you want to display and move available parameters that you want from Alert Parameters to the Message box.
   ■ Click Default to use the default message information for this alert action, and then type custom message text that you want to display.
     Note that the default message includes the following information:
     Computer: <Host Name>
     <Host Name> is the name of the alert server. To include the name of the computer where the notification originated, you must add the <Computer> parameter to the message.

9 Click Finish.

Speeding up alert configuration

If you have a large network, you may be able to speed up and simplify your configuration of AMS^2 by only searching a certain segment of your network for AMS^2 computers.

This is especially useful if you manage a large network with many different servers, and you want to confine your search to one section of the network, or one specific subnet mask. The process is faster when you limit your search, and alerts are contained in the defined network segment.

You can get a faster response across a large network if you limit the network segments. You can use this option with either IPX or TCP/IP network protocols. You can specify whether you want AMS^2 to discover clients only within a certain octet or subnet mask.
To speed up alert configuration

1. In the Symantec System Center console, right-click the server group, and then click **All Tasks > AMS > Configure**.

2. Click **Options**.

3. In the Options dialog box, do one of the following:
   - If you use an IPX network, in the Add IPX address box, type the IPX network broadcast address where you want to search for AMS² computers.
   - If you use a TCP/IP network, in the Add IP address box, type the TCP/IP network broadcast address where you want to search for AMS² computers.
     
     This is the first three segments of the computer’s IP address followed by an all-inclusive segment. For example, if you enter a search broadcast address of 192.168.0.255, any of the 256 computers with AMS² in the subnet will receive the broadcast. So if you are searching for an AMS² computer that has an IP address of 192.168.0.50, you will find it.

4. Click **Add** to add this net address to the Current discovery broadcast addresses list.

Only broadcast networks listed here are searched to discover new AMS² computers. If you have not specified any broadcast networks, the entire network is searched each time that you start a discovery.
To remove a net address that is no longer needed from the Current discovery broadcast addresses list, select the address, and then click **Remove**. When you remove a net address from this list, it doesn’t disable that section of the network. Removing a net address only prevents AMS² from searching that section of the network for AMS² computers.

Click **OK** to save the list and return to the Alert Actions dialog box.

### Configuring the Message Box alert action

The Message Box alert action displays a message box on the computer from which you configure the action. You can select whether the message box sounds a beep when it appears and whether the message box always appears on the screen until cleared.

**To configure the Message Box alert action**

1. In the Symantec System Center console, right-click the server group, and then click **All Tasks > AMS > Configure**.
2. Select the alert for which you want to configure alert actions.
3. Click **Configure**.
4. Click **Message Box**, and then click **Next**.
5. Select a computer to execute the action, and then click **Next**.
6. Select whether you want an error beep and whether you want the dialog box to always appear on top until it is cleared.
7. Click **Next**.
8. Type an action name. The action name and the action computer name appear in the Alert Actions dialog box beside this action.
9. In the Message box, type any message text that you want to display and move available parameters that you want from Alert Parameters to the Message box.
10. Click **Finish**.
Configuring the Broadcast alert action

The Broadcast alert action sends a message to all computers logged on to the server that generates the alert.

**To configure the Broadcast alert action**

1. In the Symantec System Center console, right-click the server group, and then click **All Tasks > AMS > Configure**.
2. Select the alert for which you want to configure alert actions.
3. Click **Configure**.
4. Click **Broadcast**, and then click **Next**.
5. Select a computer to execute the action, and then click **Next**.
6. In the Message box, type any message text that you want to display and move available parameters you want from Alert Parameters to the Message box.
7. Type an action name.
   The action name and the action computer name will appear in the Alert Actions dialog box beside this action.
8. Click **Finish**.

Configuring the Run Program alert action

The Run Program alert action runs a program on the computer for which you configure the alert action. You must complete two fields in the Run Program dialog box.

The Program box should contain the full path to the program that you want to run. The Command Line box should contain any command-line options for that program. The program that you select should be on the computer’s local drive to ensure that AMS can find it.

If you are running the program on a remote computer, you must enter the path to the program from that computer.

If you are running a Windows program, you can select whether that program runs in a normal, minimized, or maximized state. This option has no effect on DOS programs.
To configure the Run Program alert action
1. In the Symantec System Center console, right-click the server group, and then click All Tasks > AMS > Configure.
2. Select the alert for which you want to configure alert actions.
3. Click Configure.
4. Click Run Program, and then click Next.
5. Select a computer to execute the action, and then click Next.
6. Type the full path name to the program that you want to run, including the program name.
7. Type any command-line options that you want the program to use.
8. Select an execution state of normal, minimized, or maximized.
9. Click Finish.

Configuring the Load An NLM alert action
The Load An NLM alert action loads a NetWare Loadable Module (NLM) on a selected NetWare server when the AMS² alert occurs. You must configure this alert to determine which NLM is loaded, and the server onto which it loads. This alert action is similar to the Run Program alert action for a Windows NT computer.

For example, if you were running the Symantec Client Security management snap-in, you could configure the Load An NLM alert action to load an NLM that you or a third party created on a selected NetWare server when Symantec Client Security detects a threat. This NLM could monitor who accesses the server and who is using the infected file. It could also back up files should the server crash because of the infection.

To configure the Load An NLM alert action
1. In the Symantec System Center console, right-click the server group, and then click All Tasks > AMS > Configure.
2. Select the alert for which you want to configure alert actions.
3. Click Configure.
4. Click Load An NLM, and then click Next.
   The first time that you configure this action, AMS² needs to search the network for NetWare computers that can perform this action.
   When completed, the NetWare computers appear in tree format.
5 If the computer that you are looking for does not appear in the list, click **Discover** to search for all computers again and find that computer.
6 Select the computer where the NLM will load, and then click **Next**.
7 Type or select the NLM to load.
   NLMs are usually stored in the SYS:SYSTEM directory on NetWare servers.
8 Type any command-line options you want the program to use.
9 Click **Finish**.

**Configuring the Send Internet Mail alert action**

The Send Internet Mail alert action sends an Internet mail message to the user that you specify. When using the Send Internet Mail alert action, you need to also specify the SMTP Internet mail server through which the alert action will send the message. If you specify the mail server by name, you need to have a DNS server configured so that the Send Internet Mail alert action can resolve the server’s IP address. If you do not have a DNS server, you can enter the mail server’s IP address directly.

If you do not have access to an SMTP Internet mail server at your site, this alert action won’t work.

**To configure the Send Internet Mail alert action**

1 In the Symantec System Center console, right-click the server group, and then click **All Tasks > AMS > Configure**.
2 Select the alert for which you want to configure alert actions.
3 Click **Configure**.
4 Click **Send Internet Mail**, and then click **Next**.
5 Select the computer to execute the action, and then click **Next**.
6 In the Internet Address, Sender Name, Subject, and Mail Server boxes, type or select information as appropriate.
   It is preferable to provide the mail server’s IP address rather than its name. The Sender Name box must contain a valid Internet email address. Most email servers will not send a message if the server can’t validate the sender’s email address.
7 Click **Next**.
8 In the Message box, type any message text you need and move available parameters you want from Alert Parameters to the Message box.
9 Type an action name.
The action name and the action computer name appear in the Alert Actions dialog box beside this action.

10 Click Finish.

Configuring the Send Page alert action

The Send Page alert action sends a pager message to the number that you specify. Any computer that you configure a Send Page action on needs to have a modem.

See “Testing configured alert actions” on page 84.

Send Page alert action configuration is divided into the following parts:

- Configuring a modem for AMS2 to use
- Configuring for a paging service
- Entering a pager message

To configure the Send Page alert action

1 In the Symantec System Center console, right-click the server group, and then click All Tasks > AMS > Configure.

2 Select the alert for which you want to configure alert actions.

3 Click Configure.

4 Click Send Page, and then click Next.

5 Select a computer to execute the action, and then click Next.

6 Type the access telephone number that you are calling to reach the paging service.
   Be sure to include any numbers necessary to access an outside line from your site.

7 Type the pager ID number and password that you use to access the paging service network.
   If your paging service doesn’t use a password, leave the Password box blank.

8 Select your service type.
   If your paging service is not listed, try one of the generic types.
   See “Configuring for a paging service” on page 79.
9 Click **Next**.

If you're creating a message for an alphanumeric pager, in the Message box type any message text you want to display and move available parameters from Alert Parameters to the Message box.

If you're creating a message for a numeric pager, you can only type numbers in the Message box.

10 Type an action name.

The action name and the action computer name appear in the Alert Actions dialog box beside this action.

11 Click **Finish**.

### Configuring for a paging service

You can access a paging service either directly or indirectly. Direct paging refers to dialing the service provider network access phone number and accessing the service provider's computer network directly to enter the pager identification number. The paging service network then sends the message to the pager.

AMS² alerting does not work with indirect paging. Indirect paging involves calling a paging service, speaking with an operator, and giving the operator the pager's identification number. The paging service operator enters the information into the paging network, and then sends the message to the pager. The indirect paging method that is often used when contacting the network directly may be a toll call, and the pager service offers toll-free service through the operator.

You need to configure the Pager alert action for your paging service. At a minimum, this information includes the paging service phone number and the name of the paging service that you are using.

Always put the paging service's phone number in the Send Page dialog box's Service Provider box. If your paging service is not in the Send Page dialog box's Service drop-down list, you can try using the Generic Beeper or the Generic Alphanumeric service (select the one that matches the type of pager that you are using). Type the password that you use to access the paging service network in the Password box.

If the generic service that you select doesn't work with your pager, you must configure the communication parameters that the Send Page alert action needs to use. This information includes the baud rate, data and stop bits, parity, and the paging protocol used by your paging service. If your paging service is in the Service drop-down list, these parameters are configured automatically when you select the service.
To configure the Send Page alert action for an unlisted paging service

1. In the Symantec System Center console, right-click the server group, and then click All Tasks > AMS > Configure.
2. Select the alert for which you want to configure alert actions.
3. Click Configure.
4. Click Send Page, and then click Next.
5. Select a computer to execute the action, and then click Next.
6. Click Settings.
7. Type the protocol, maximum message length, baud rate, data bits, stop bits, and parity that your paging service requires. You can get this information from your paging service.
8. Click OK, and then continue configuring the pager action starting with step 6 in “To configure the Send Page alert action” on page 78.

Entering a pager message

The Send Page alert action supports both alphanumeric and numeric-only pagers (numeric-only pagers are sometimes called beepers).

If you're paging an alphanumeric pager, the message can include any text that you type in and information from the alert that generated the message. This message should not exceed the maximum number of characters that your paging service supports; otherwise, you could get a truncated message.

If you’re paging a numeric-only pager, you may want to create a system of server numbers and numeric error codes that correspond to alerts that you configure. For instance, you could create a system where “1” refers to your main production server and number “101” means some specific event has occurred. If you received the message “1 101,” then you would know that the event had occurred on your main production server.

Configuring the Send SNMP Trap alert action

Simple Network Management Protocol (SNMP) is a message-based protocol based on a manager/agent model consisting of Get, GetNext, and Set messages and responses. SNMP uses traps to report exception conditions such as component failures and threshold violations.

AMS² can generate an SNMP trap when an alert occurs. You can configure systems generating alerts to send these traps to a management console, such as HP OpenView, Tivoli Enterprise Console, or Computer Associates Unicenter.
You must specify the address (either IP or IPX) of the computers to which you want SNMP traps sent.

**To configure the Send SNMP Trap alert action**

1. In the Symantec System Center console, right-click the server group, and then click **All Tasks > AMS > Configure**.
2. Select the alert for which you want to configure alert actions.
3. Click **Configure**.
4. Click **Send SNMP Trap**, and then click **Next**.
5. Select a computer to execute the action, and then click **Next**.
6. In the SNMP trap, type any message text that you want to display and move the parameters that you want from Alert Parameters to the Message box.
7. Type an action name.
   The action name and the action computer name appear in the Alert Actions dialog box beside this action.
8. Click **Finish**.

**Configuring trap destinations for Windows NT 4.0**

You can configure SNMP traps for Windows NT 4.0.

**To configure trap destinations for Windows NT 4.0**

1. In the Windows NT Control Panel, double-click **Network**.
2. Click **Services**.
3. Click **SNMP Service**, and then click **Properties**.
4. Click **Traps**.
5. In the Community Name box, click **Public**.
6. If there is no public entry in the list, type it in, and then click **Add**.
7. Under Trap Destinations, click **Add**.
8. Type the addresses of the computers to which you want traps sent, and then click **Add**.
9. Click **OK**, and then click **Close**.
Configuring trap destinations for Windows 2000 Server
You can configure SNMP traps for Windows 2000 Server.

To configure trap destinations for Windows 2000 Server
1. On the Windows taskbar, click Start > Settings > Control Panel.
2. Double-click Administrative Tools.
4. Click Services and Applications.
5. Click Services.
6. In the right pane, click SNMP Service.
7. On the Action menu, click Properties.
8. On the Traps tab, under Community name, type the case-sensitive community name to which this computer will send trap messages, and then click Add to List.
10. In Host name, IP or IPX address, type information for the host, and click Add.
11. Repeat steps 8 through 10 until you have added all the communities and trap destinations you want.

Configuring trap destinations for NetWare
You can configure SNMP traps for NetWare 5.x and 6.x servers.

To configure trap destinations for NetWare
1. In the NetWare server console, type:
   \load inetcfg
2. Select Protocols and press Enter.
4. Select SNMP Manager Table, and then press Enter to display the SNMP Manager Table.
5 Do one of the following:

- To modify an existing address, select it, and then press **Enter**.
- To add a new address, press **Insert**, type an IP address, and then press **Enter**.
- To delete an address, select it, press **Delete**, and then press **Enter** to confirm the deletion.

6 Press the **Esc** key to close the dialog box.

7 Press **Enter** to confirm the change to the database.

### Configuring the Write To Event Log alert action

The Write To Event Log alert action creates an entry in the Windows NT/2000/XP Event Log’s Application Log. This entry is logged on the server from which the alert came. This alert action is available only on Windows NT/2000/XP computers.

**To configure the Write To Event Log alert action**

1 In the Symantec System Center console, right-click the server group, and then click **All Tasks > AMS > Configure**.
2 Select the alert for which you want to configure alert actions.
3 Click **Configure**.
4 Click **Write To Event Log**, and then click **Next**.
5 Select a computer to execute the action, and then click **Next**.
6 In the Message box, type any message text that you want to display and move parameters that you want from Alert Parameters to the Message box.
7 Type an action name.
   The action name and the action computer name appear in the Alert Actions dialog box beside this action.
8 Click **Finish**.

### Working with configured alerts

Once you have configured alert actions, you can do the following:

- Test them to make sure they work as expected.
- Delete them.
- Export them to other computers.
Testing configured alert actions

After you configure alert actions, you can test them in the Alert Actions dialog box. When you select an alert and then click Test Action, all alert actions configured for that alert execute. When you select a specific alert action and click Test Action, only that alert action executes.

To test an alert
◆ In the Alert Actions dialog box, select an alert, and then click Test Action.

Deleting an alert action from an alert

You can delete actions associated with an alert as necessary.

To delete an alert action from an alert
1 In the Symantec System Center console, right-click the server group, and then click All Tasks > AMS > Configure.
2 Select the alert action you want to delete, and then click Delete.

Exporting alert actions to other computers

Each computer that generates AMS2 alerts stores its alert information in a local AMS2 database. Typically, the alerts and actions stored in one database are not visible to AMS2 databases on other computers.

There may be times when you want to duplicate configurations of AMS2 alert actions on a computer across multiple computers so you do not have to repeat your work. The AMS2 export option lets you export alert actions to other computers that generate AMS2 alerts.

Alert actions, such as a Send Page alert action configuration or a Message Box alert action configuration, only export if the alert for which you configured the action exists on both computers. In most cases, you can ensure this is the case by installing the same application on both computers. This way, both applications will register their alerts with their respective AMS2 databases.

When you export alert actions from one computer to another, you have the choice of exporting a single alert action or all alert actions. Once AMS2 exports alert actions to a computer, AMS2 displays the Export Status dialog box to let you know the results of the export.

If the export option cannot export an alert action because the alert for which the action was configured doesn’t exist on the target computer (or for any other reason), the Export Status dialog box indicates that the alert action couldn’t be
exported. Alert actions also may fail to export if the target computer’s AMS² installation is not working correctly.

**To export alert actions to other computers**

1. In the Symantec System Center console, right-click the server group, and then click **All Tasks > AMS > Configure**.
2. Do one of the following:
   - Click the **Symantec AntiVirus** folder if you want to export all alerts associated with Symantec Client Security.
   - Select either an alert (if you want to export all of that alert’s actions) or a specific alert action (if you want to export only the selected alert action).
3. Click **Export**.
4. In the Available Computers list, double-click the computers that you want to receive the alert actions you selected.
   - The computers will be added to the Selected Computers list.
   - If the computer you want has AMS² active on it and it is not in the Available Computers list, click **Discover** to rediscover computers with AMS².
5. Click **Export**.
6. Click **Yes** in reply to the confirmation message.
7. In the Export Status dialog box, verify that the alert actions exported successfully.

**Viewing export status**

After AMS² exports alert actions to the computers that you selected in the Select Computers dialog box, AMS² displays the export results in the Export Status dialog box.

The Export Status dialog box displays alert actions that do not export successfully. If alerts do not export successfully, it may be for the following reasons:

- AMS² is not up or working correctly on the target computer. Verify AMS² by testing a configured alert action on that computer from the Alert Actions dialog box.
- The alert for which the action was configured doesn't exist on the target computer. Make sure that the application that registered the alert with AMS² on the source computer is installed on the target computer.
Using the Alert Management System Alert Log

You can use the Alert Log to view a list of all alerts generated by network computers running Symantec Client Security.

You can configure the Alert Log to do one of the following:

- Display only the alerts that match the conditions that you specify.
- Display a specified number of entries.

The Alert Log displays a list of alerts with the following information about each alert:

- Alert Name
- Source
- Computer
- Date
- Time
- Severity

In addition to the basic information the Alert Log dialog box displays, you can access more detailed information about each alert in the Alert Information dialog box.

Each server stores its own copy of the Alert Log locally. When you select a server and view its alert log, you’re actually retrieving a copy of that server’s Alert Log to your local console. Therefore, if that server is not powered on or available, you won’t be able to retrieve its Alert Log for viewing.

View and interact with the Alert Log

You can view the Alert Log and interact with it in the following ways:

- Change the number of entries displayed in the log
- Delete entries
- Copy the contents to the clipboard
To view the Alert Log

- Right-click the server group, and then click All Tasks > AMS > View Log.

To change the number of entries displayed in the Alert Log

1. In the Alert Log window, right-click, and then click Options.
2. Specify the number of log entries that you want the log to hold.

**Note:** You can independently configure the number of entries that an Alert Log holds on each server.

To delete a single entry

- Right-click the log entry, and then click Delete > Selected Entries.

To delete multiple log entries

1. Press Ctrl and select the multiple log entries.
2. In the Alert Log window, right-click, and then click Delete > Selected Entries.
   To select a range, click the first entry, and then press Shift and click the last entry.
To delete all visible log entries

◆ In the Alert Log window, right-click, and then click **Delete > Filtered Entries**.

**To copy Alert Log contents to the Clipboard**

1. Press and hold the **Ctrl** key, and then select the multiple log entries.
2. In the Alert Log window, right-click, and then click **Copy**.

Only the alerts visible in the log are copied. If you want to limit the number of entries that the Alert Log copies to the Clipboard, apply filters to limit the number of visible log entries.

**Viewing detailed alert information**

You can view detailed information about each alert that the Alert Log displays. The Alert Information dialog box displays the detailed information and includes alerts, their values, and the action status of each alert.

The Alert Information dialog box displays a list of parameters such as Alert name, Source, Date, Severity, and Description, as well as values for the selected alert action.

The Alert Information dialog box also displays the types of status that appear in **Table 2-2**.

**Table 2-2**  
Action Status types

<table>
<thead>
<tr>
<th>Action Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action Type</td>
<td>The type of action generated by the alert, such as Message Box, Pager, Internet Mail, Execute Program, or Broadcast.</td>
</tr>
<tr>
<td>Action Name</td>
<td>A name given to the specific action.</td>
</tr>
<tr>
<td>Computer</td>
<td>The name of the computer generating the alert.</td>
</tr>
<tr>
<td>Status</td>
<td>The status of the alert. The status type can include Pending, Processing Action, Error, Completed Successfully, and Failed To Complete.</td>
</tr>
</tbody>
</table>
To view the alert information and Action Status

1. In the Alert Log window, double-click the alert for which you want to display detailed information.

2. When you finish viewing the alert information, click Close.

The computer listed in the Alert Log is the primary server that recorded the action because it records all events for the Symantec server group. To see which computer actually generated the alert, double-click the Alert Log entry about which you want more information. The Alert Information dialog box provides additional alert details, including the name of the computer that generated the alert.

Filtering the Alert Log display list

You can configure the Alert Log to display only those alerts that match specified criteria. You can filter which alerts display according to the parameters that appear in Table 2-3.

<table>
<thead>
<tr>
<th>Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer</td>
<td>Displays alerts from a specific computer.</td>
</tr>
<tr>
<td>Source</td>
<td>Displays alerts from the same type of alert source on one or more computers.</td>
</tr>
<tr>
<td>Alert</td>
<td>Displays all alerts with a specific alert name.</td>
</tr>
<tr>
<td>Severity</td>
<td>Displays only alerts matching the severity levels that you select. You can specify the following severity levels: Monitor, Information, OK, Non-critical, Critical, and Non-recoverable.</td>
</tr>
</tbody>
</table>
To specify which alerts display in the Alert Log

1. In the Symantec System Center console, right-click the server group, and then click **All Tasks > AMS > View Log.**

2. In the Alert Log window, right-click, and then click **Options.**

3. Select the filters you want to apply to the Alert Log list.

4. Click **OK.**

Forwarding alerts from unmanaged clients

The AMS² client software is not installed as part of the client installation. If you want to use the alerting features that AMS² provides for unmanaged clients, you can install the AMS² client program that is included on the Symantec Client Security CD.

Unmanaged Symantec Client Security clients can be configured to forward their alerts to an AMS² server.

For the alert to be sent, the client computer must be connected to the network and must be able to connect to the AMS server.
To forward alerts to an AMS server

1. Use a text editor such as Notepad to create a new text file.

2. Add the following lines:

```
[KEYS]
!KEY!=$REGROOT$\Common
AMSServer=S<AMSServerName>
AMS=D1
!KEY!=$REGROOT$\ProductControl
LoadAMS=D1
```

3. In the `<AMSServerName>` line, do one of the following:
   - Type the IP or IPX address for the intended AMS² server.
   - Type the name of the intended AMS² server (make sure that the client can resolve the server name).
   Be sure to include the S preceding `<SERVERNAME>`. Do not include the brackets.

4. Save the file as Grc.dat to one of the following folders on the client:
   - For Windows 98\Me: C:\Program Files\Symantec AntiVirus
   - For Windows NT: C:\Winnt\Profiles\All Users\Application Data\Symantec\Symantec AntiVirus Corporate Edition\7.5
   - For Windows 2000\XP\2003: C:\Documents and Settings\All Users\Application Data\Symantec\Symantec AntiVirus

Once you have created the configurations file (Grc.dat), you can copy it to other unmanaged clients. These unmanaged clients will then forward alerts to the same AMS² server.
Setting up the Alert Management System

Forwarding alerts from unmanaged clients
Configuring Symantec Client Security antivirus protection

- Scanning for viruses and other threats
- Updating virus definitions files
- Responding to virus outbreaks
- Managing roaming clients
- Working with Histories and Event Logs
Scanning for viruses and other threats

This chapter includes the following topics:

- About threats
- About scans in Symantec Client Security
- Configuring Auto-Protect scans
- Configuring manual scans
- Configuring scheduled scans
- Handling Symantec Client Security clients with intermittent connectivity
- Configuring scan options

About threats

Symantec Client Security can scan for viruses and known and emerging threats, such as spyware, adware, and other files that could put your computer at risk. Symantec Client Security can scan for the following threat types:

- **Viruses**: Programs or code that attach a copy of themselves to another computer program or document when it runs. Whenever the infected program runs or a user opens a document containing a macro virus, the attached virus program activates and attaches itself to other programs and documents. Viruses generally deliver a payload, such as displaying a message on a particular date. Some viruses specifically damage data by corrupting programs, deleting files, or reformatting disks.
Worms: Programs that replicate without infecting other programs. Some worms spread by copying themselves from disk to disk, while others replicate only in memory to slow a computer down.

Trojan horses: Programs that contain code that is disguised as or hiding in something benign, such as a game or utility.

Blended threats: Threats that blend the characteristics of viruses, worms, Trojan horses, and code with server and Internet vulnerabilities.

Spyware: Stand-alone programs that can secretly monitor system activity and detect passwords and other confidential information and relay it back to another computer.

Adware: Stand-alone or appended programs that secretly gather personal information through the Internet and relay it back to another computer. Adware may track browsing habits for advertising purposes. Adware can also deliver advertising content.

Spyware and adware can be unknowingly downloaded from Web sites (typically in shareware or freeware), email messages, and instant messenger programs. Often a user unknowingly downloads adware by accepting an End User License Agreement from a software program.

Dialers: Programs that use a computer, without the user’s permission or knowledge, to dial out through the Internet to a 900 number or FTP site, typically to accrue charges.

Joke programs: Programs that alter or interrupt the operation of a computer in a way that is intended to be humorous or frightening. For example, a program can be downloaded from a Web site, email message, or instant messenger program. It can then move the Recycle Bin away from the mouse when the user attempts to delete it or cause the mouse to click in reverse.

Remote access programs: Programs that allow access over the Internet from another computer so that they can gain information or attack or alter a user’s computer. For example, a program may be installed by the user, or installed as part of some other process without the user’s knowledge. The program can be used for malicious purposes with or without modification of the original remote access program.

Hack tools: Programs used by a hacker to gain unauthorized access to a user’s computer. For example, one hack tool is a keystroke logger, which tracks and records individual keystrokes and sends this information back to the hacker. The hacker can then perform port scans or vulnerability scans. Hack tools may also be used to create viruses.
Trackware: Stand-alone or appended applications that trace a user's path on the Internet and send information to the target system. For example, the application can be downloaded from a Web site, email message, or instant messenger program. It can then obtain confidential information regarding user behavior.

Security risks: Threats that do not conform to the strict definitions of viruses, Trojan horses, worms, or other expanded threat categories, but which may present a threat to a user's computer and its data.

Viruses, Trojan horses, and worms are scanned for by default. You must enable expanded threat scanning for Symantec Client Security to detect other types of threats.

Some threats, such as Back Orifice, were detected as viruses in earlier versions of Symantec Client Security. They remain detected as viruses so that Symantec Client Security can continue to provide protection for legacy systems.

About scans in Symantec Client Security

You can configure the following types of scans from the Symantec System Center console:

- File System Auto-Protect scans
- Scheduled scans
- Manual scans
- Auto-Protect email attachment scanning for Lotus Notes, and Microsoft Exchange and Outlook (MAPI)
- Auto-Protect scanning for Internet email messages and attachments that use the POP3 or SMTP communications protocols; Auto-Protect scanning for Internet email also includes outbound email heuristics scanning

File System Auto-Protect and Auto-Protect email scans detect viruses. Manual and scheduled scans detect viruses and other threats, such as adware and spyware.

You can perform scans on:

- Individual and multiple Symantec Client Security servers and clients
- Groups of Symantec Client Security servers and clients, using server groups
Understanding Auto-Protect scans

Auto-Protect scans continuously inspect files and email data for viruses as they are read from or written to a computer. Auto-Protect does not scan for other threats, such as spyware and adware. Auto-Protect is enabled by default. You can configure Auto-Protect settings for servers at the server group or server level, and clients at the server group, server, or client group level. When you configure Auto-Protect, the configuration pages look slightly different depending on whether you are setting options for servers or clients. You can lock Auto-Protect settings on clients if you want to enforce a threat policy. Users cannot change options that you lock.

Auto-Protect includes the SmartScan feature, which, when enabled, can determine a file’s type even when a virus changes the file’s extension.

Symantec Client Security scans email data on Symantec Client Security clients only.

Understanding scheduled scans

From the Symantec System Center console, you can schedule scans for Symantec Client Security servers or clients. Users can also schedule scans for their computers from Symantec Client Security clients, but they cannot change or disable scans that you schedule for their computers. Symantec Client Security runs one scheduled scan at a time. If more than one scan is scheduled at the same time, they will run sequentially.

When you create and save a scheduled scan, Symantec Client Security remembers the server group, server, or computer on which to run the scan and the settings that you chose for that scan.

If a computer is turned off during a scheduled scan, the scan will not run unless the computer has been configured to run missed scan events.

Scheduled scans can inspect files for viruses and other threats, such as spyware and adware.

See “Setting options for missed scheduled scans” on page 125.

Understanding manual scans

Manual or on-demand scans inspect selected files and folders on selected computers. Manual scans provide immediate results from a scan on a small area of the network or a local hard drive.

Manual scans can inspect files for viruses and other threats, such as spyware and adware.
You can set scan options in the Scan Options dialog box shown in Figure 3-1.

**Figure 3-1**  Scan Options dialog box

Selecting computers to scan

In the Symantec System Center console, you select the computers that you want to scan, determine the types of scans that are available, where scans are performed, and the scan options.
Table 3-1 lists what you can scan, by object type.

<table>
<thead>
<tr>
<th>Object selected</th>
<th>Scans available</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Hierarchy</td>
<td>Virus sweep scanning of all Symantec Client Security servers and clients in the network</td>
</tr>
<tr>
<td>Multiple server groups</td>
<td>- Virus sweep scanning of all Symantec Client Security servers and their clients in the selected server groups</td>
</tr>
<tr>
<td></td>
<td>- Scheduled scanning for the selected Symantec Client Security servers</td>
</tr>
<tr>
<td>Server group</td>
<td>- Virus sweep scanning of all Symantec Client Security servers and their clients in the selected server group</td>
</tr>
<tr>
<td></td>
<td>- Scheduled scanning for the Symantec Client Security servers in the selected server group</td>
</tr>
<tr>
<td>Selected servers in a server group</td>
<td>- Virus sweep scanning of the selected Symantec Client Security servers</td>
</tr>
<tr>
<td></td>
<td>- Manual scanning of the selected Symantec Client Security servers</td>
</tr>
<tr>
<td>Single server</td>
<td>- Virus sweep scanning of the Symantec Client Security server and all of its Symantec Client Security clients</td>
</tr>
<tr>
<td></td>
<td>- Manual scanning of the Symantec Client Security server</td>
</tr>
<tr>
<td></td>
<td>- Scheduled scanning of the Symantec Client Security server or its Symantec Client Security clients</td>
</tr>
<tr>
<td>Selected Symantec Client Security clients for a single Symantec Client Security server</td>
<td>Manual scanning of the selected Symantec Client Security clients that are managed by the Symantec Client Security server</td>
</tr>
<tr>
<td></td>
<td>- Scheduled scanning of the selected Symantec Client Security client</td>
</tr>
</tbody>
</table>

**Note:** Clients' settings must be locked before Auto-Protect options that are configured in the Symantec System Center console can be propagated to them. If you make a change but do not lock the setting, the change is not propagated to clients.

See “Configuring Auto-Protect scans” on page 102.
Determining scan options for multiple computers

When you view Auto-Protect, virus sweep, or manual scan options for multiple selected computers, the configuration check boxes and options have a tri-state feature that is apparent only when the computers have different options configured. Click the same option multiple times to see the different states:

- A solid black check mark in a check box or a solid black bullet in an option means that the option is selected for all of the computers in that group. Setting an option to a state other than the dimmed state resets that option for selected computers.

- A blank check box means that the option is not selected for any computer in that group. Setting an option to a state other than the dimmed state resets that option for selected computers.

- A dimmed check mark in a dimmed box, a blank series of options, or a blank box means that some of the computers in the group have that option selected and some do not. Setting an option to a state other than the dimmed state resets that option for selected computers.

Some options, such as excluding files and folders, are not available when you select multiple computers because the option applies only to a specific computer.

Scan option precedence

Scan configuration changes made at the server group level override any changes made at the client group or server level.

Note: Auto-Protect options work differently from the other scan options. Auto-Protect options must be locked at the server group or server level before they can be propagated to clients. If you make a change but do not lock the setting, the change is not propagated to clients.

See “Understanding Auto-Protect scans” on page 98.
Configuring Auto-Protect scans

Configuring Auto-Protect scans consists of the following tasks:

- Configuring Auto-Protect for files
- Configuring Auto-Protect email scanning
- Specifying exclusions
- Configuring Auto-Protect settings
- Locking and unlocking Auto-Protect options

Configuring Auto-Protect for files

When you configure Auto-Protect for files, you select a server group or server, configure scan settings, and configure other settings that define how Auto-Protect and its associated features behave.

When you configure Auto-Protect options for files, specify which of the following drive types that you want Symantec Client Security to scan:

- Floppy drive: Symantec Client Security can scan files as they are read from or written to floppy disks. Floppy disks are common sources of virus infections because users may bring infected disks from home.

- Network drive: If you enable Auto-Protect on network drives, Symantec Client Security can scan files as they’re written from a client computer to a server (or from a server to another server). This option is not necessary if you enable Auto-Protect on your servers. For example, if you enable scanning of network drives on client A and also have Auto-Protect enabled on server B, when client A writes a file to a network drive on server B, Symantec Client Security scans the file on client A and scans the file again on server B. This could reduce network performance on the client computer.

To configure Auto-Protect for files

1. In the Symantec System Center console, do one of the following:

   - Right-click the server group or Symantec Client Security servers that you want to configure, and then click All Tasks > Symantec AntiVirus > Server Auto-Protect Options.
     
     If you select a server group, the Symantec System Center will configure all of the servers that are in the server group.

   - Right-click an individual server or multiple selected servers, and then click All Tasks > Symantec AntiVirus > Client Auto-Protect Options.
Right-click the server group or servers with Symantec Client Security clients that you want to configure, and then click **All Tasks > Symantec AntiVirus > Client Auto-Protect Options**.
The Symantec System Center will configure all of the clients that are associated with the server or server group.

Right-click an individual client or multiple selected clients for a server, and then click **All Tasks > Symantec AntiVirus > Client Auto-Protect Options**.

2 In the Auto-Protect Options dialog box, ensure that Enable Auto-Protect is checked.

3 Under File types, do one of the following:
   - Select file types and extensions to scan.
   - Click **Selected**, and then check **SmartScan**.
   See “About Scan all file types and SmartScan” on page 104.

4 On the Macro Virus and Non-Macro Virus tabs, assign primary actions and secondary actions for detected viruses.

5 Under Options, ensure that Display message on infected computer is checked.
6 Configure the warning message to display on infected computers. See “Displaying and customizing a warning message on an infected computer” on page 134.

7 Exclude files or folders from Auto-Protect scans, if necessary. See “Selecting file types and extensions to scan for viruses” on page 140.

8 Under Drive types, select drive types to scan. See “Configuring Auto-Protect for files” on page 102.

9 Set advanced file options. See “Configuring Advanced Auto-Protect options” on page 104.

10 Lock any client Auto-Protect options that you want to propagate to clients. See “How to lock and unlock Auto-Protect options” on page 116.

11 If you are configuring Auto-Protect options for a server group, click Reset All to ensure that all of the computers are using the Auto-Protect scanning configuration that you set at this level. See “Configuring Auto-Protect settings” on page 115.

12 Click OK.

About Scan all file types and SmartScan
You can configure Symantec Client Security to scan all file types or to use SmartScan. SmartScan scans a specific, configurable group of file extensions that contain executable code and all .exe and .doc files. SmartScan reads each file’s header to determine its file type. It scans .exe and .doc files even if the file extensions for the .exe and .doc files are changed by a virus to extensions that are different from the file extensions that SmartScan has been configured to scan. SmartScan is enabled by default.

Configuring Advanced Auto-Protect options
When you configure Advanced Auto-Protect options, you can define the following:

- When to start Auto-Protect
- When to reload Auto-Protect when a reload is necessary
- When to scan files with Auto-Protect
- How many entries to cache in an index of clean files
- How long to wait before enabling Auto-Protect when it is disabled
- Whether Auto-Protect backs up files before it attempts to repair them
Scanning for viruses and other threats

Configuring Auto-Protect scans

- When the Leave alone (log only) option is enabled, whether to delete infected files delete when they are created
- Whether file times are preserved so that unchanged files are not backed up unnecessarily

To configure Advanced Auto-Protect options

1. In the Auto-Protect Options dialog box, on the File System tab, click Advanced.

2. In the Auto-Protect Advanced Options dialog box, under Startup options, select one of the following:

   **System start**
   Load Auto-Protect when the computer’s operating system starts and unload it when the computer shuts down. This option can help protect against some viruses, such as Fun Love. If Auto-Protect detects a virus during shutdown, it places the infected file in a temporary Quarantine directory. Auto-Protect then detects the virus on startup and creates an alert notification.

   **Symantec AntiVirus start**
   Load Auto-Protect when Symantec Client Security starts.
3 Under Changes requiring Auto-Protect reload, select one of the following:

- Wait until system restart
- Stop and reload Auto-Protect when the computer restarts.
- Stop and reload Auto-Protect immediately.

4 Under Scan files when, set Auto-Protect file monitoring options.
   See “Auto-Protect file system protection options” on page 109.
   See “How to bypass Auto-Protect for files that are being backed up” on page 109.

5 Under Scan files when, do the following:

   - For Leave Alone (Log only), delete infected files on creation: Enable this option if you want the Scan on Modify and Scan on Access and Modify file monitoring options to delete a newly created infected file when you configure Leave alone (log only) as the action. For an existing infected file, Scan on Access and Modify detects the infected file and the Leave alone action applies.
     - The file is denied access and logged, but it is not deleted.
     - When you disable this option, Symantec Client Security permits the infected file to be created.

   - Preserve file times: Enable this option if you do not want the file system to change the last access time.
     - Preserving the last access time prevents backup software from backing up unchanged files.

6 Under File cache, select one of the following:

   - Disable file cache: Disable the file cache; for example, you may use this option during troubleshooting.

   - Use default file cache size: Use the default file cache size setting for desktop computers and use as close to the maximum setting as possible for servers.
     - The default file cache size is based on the computer's operating system and the amount of available disk space.
     - File caching decreases Auto-Protect's memory usage and can help you to track problems. Symantec Client Security adds a 16-byte entry to the cache index, which remains until Symantec Client Security detects a change to the file.
Custom file cache entries. Select the number of custom file cache entries to include. This option is useful for file servers or Web servers where you want to be able to cache a large number of files.

See “File cache options” on page 110.

7 Under Threat Tracer, to set options for tracing threats from computers running under Windows NT/2000/XP/2003 operating systems, do the following:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Threat Tracer</td>
<td>Ensure that this option is checked to use Threat Tracer.</td>
</tr>
<tr>
<td>Resolve source computer IP address</td>
<td>If Resolve source computer IP address is unchecked, Symantec Client Security looks up and records the computer’s NetBIOS name only.</td>
</tr>
<tr>
<td>Poll for network sessions every ___ milliseconds</td>
<td>Symantec Client Security polls once every second (1000 milliseconds) by default. Lower values use greater amounts of CPU and memory. Higher values decrease Threat Tracer’s ability to detect infections.</td>
</tr>
<tr>
<td>Client firewall auto blocks IP address of the source computer</td>
<td>Enable this option if you are using Symantec Client Security firewall client and want the firewall to automatically block the IP addresses of computers that transmit infected files. The firewall automatically blocks all IP traffic to the IP address for 30 minutes by default.</td>
</tr>
</tbody>
</table>

See “How to trace threats” on page 110.

8 Under Automatic enabler, ensure that When Auto-Protect is disabled, enable after is checked, and then specify a length of time after which Auto-Protect is enabled on the computers for which you are configuring options. For example, if an end user disables Auto-Protect on the desktop, you can set this option to enable it automatically after thirty minutes.

9 Under Backup options, ensure that Back up file before attempting repair is checked as a data safety precaution. The files are encrypted and backed up to the Quarantine directory. Once a file is backed up, it must be restored before it can be accessed again.

10 Under Additional advanced options, if you want to change the level of protection that is provided by Bloodhound Heuristic Scanning, click Heuristics.
In the Heuristic Scanning dialog box, select the setting that you want, and then click **OK**.

In the Auto-Protect Advanced Options dialog box, under Additional advanced options, if you want to change the current settings for floppy disk scans, click **Floppies**.

In the Check Floppies dialog box, select one of the following:

- **Check floppies for boot viruses upon access**
  - Symantec Client Security scans the floppy disk in the floppy drive for boot viruses when the drive is first accessed. When Symantec Client Security finds a boot virus, select whether to clean a virus from the boot record or leave it alone.
  - If you click Leave alone (log only), an alert is sent when a virus is detected but no action is taken. Use this option if you want to take direct control over the virus cleaning and handling process. For example, after you receive the alert, you can decide what course of action to take.

- **Do not check floppies upon system shutdown**
  - Symantec Client Security skips the scan of any floppy disk in the floppy drive when the computer is shut down normally.

Click **OK**.

In Windows 98 only, in the Auto-Protect Advanced Options dialog box, under Additional advanced options, if you want to disable protection monitors for virus-like activities, click **Monitor**.

Virus-like activities are activities that viruses perform when they attempt to infect your files. Any of these activities might be legitimate depending on your work context.

In the Monitor dialog box, to exclude activities from monitoring, select one or more of the following:

- **Low-Level Format Of Hard Disk**
  - All information on the drive is erased and cannot be recovered. This type of formatting is generally performed at the factory only. If this activity is detected, it usually indicates an unknown virus at work. This is not an option for NEC PC98xx computers.

- **Write To Hard Disk Boot Records**
  - Very few programs write to hard disk boot records. If this activity is detected, it could indicate an unknown virus at work.

- **Write To Floppy Disk Boot Records**
  - Only a few programs (such as the operating system Format command) write to floppy disk boot records. If this activity is detected, it could indicate an unknown virus at work.
17 Click **OK**.

18 In the Auto-Protect Advanced Options dialog box, click **OK**.

**Auto-Protect file system protection options**

There are several file system protection options that determine the file operations that Auto-Protect monitors. **Table 3-2** lists and describes these options.

**Table 3-2**  Auto-Protect file system protection options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>When to use it</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modified (scan on create)</td>
<td>Scans files when they are written, modified, or copied.</td>
<td>Use this option for slightly faster performance because Auto-Protect only scans files when they are written, modified, or copied.</td>
</tr>
<tr>
<td>Accessed or modified (scan on create, open, move, copy, or run)</td>
<td>Scans files when they are written, opened, moved, copied, or run.</td>
<td>Use this option for more complete file system protection. This option may have a performance impact, because Auto-Protect scans files during all types of file operations.</td>
</tr>
<tr>
<td>Opened for backup</td>
<td>Scans files when they are accessed during a backup operation. Only available for computers that are running Windows NT/2000/XP/2003.</td>
<td>Use this option if you haven’t run a virus check on files that you want to back up. Using this option can significantly slow backup operations, because Auto-Protect scans each file that is included in the backup. Do not enable this option if you want to bypass Auto-Protect for files that are being backed up. See “How to bypass Auto-Protect for files that are being backed up” on page 109.</td>
</tr>
</tbody>
</table>

**How to bypass Auto-Protect for files that are being backed up**

You can have Symantec Client Security bypass Auto-Protect during a backup. This allows backup software to operate without the overhead of an additional Auto-Protect scan. The setting applies only to files that are being backed up.
Files that are being restored from a backup are scanned regardless of this setting.

**Note**: This option is available for Windows NT/2000/XP/2003 only.

**File cache options**

File caching decreases Auto-Protect’s memory usage and can help you to track problems. The file cache includes an index of files that were scanned and determined to be clean. Symantec Client Security adds a 16-byte ID to the cache index, which remains until Symantec Client Security detects a change to the file.

**How to trace threats**

You can use Threat Tracer to identify the source of network share-based virus infections on computers that are running Windows NT/2000/XP/2003 operating systems.

When Auto-Protect detects an infection, it sends information to RtvScan, the main Symantec Client Security service. RtvScan determines if the infection originated locally or remotely. If the infection came from a remote computer, RtvScan can look up and record the computer’s NetBIOS computer name and its IP address, and then display this information in the Threat Properties dialog box.

RtvScan polls every second by default for network sessions, and then caches this information as a remote computer secondary source list. This information maximizes the frequency with which Threat Tracer can successfully identify the infected remote computer. For example, a threat may close the network share before RtvScan can record the network session. Threat Tracer then uses the secondary source list to try to identify the remote computer.

When Threat Tracer cannot identify the remote computer, the source is listed as Unknown in the Threat Properties dialog box.

When Threat Tracer determines that the infection came from local host activity, it lists the local host.

The source is also listed as Unknown in the Threat Properties dialog box when the authenticated user for a file share refers to multiple computers. This can occur when a user ID is associated with multiple network sessions.

**Heuristic scanning**

Bloodhound can detect a high percentage of unknown viruses by isolating and locating the logical regions of a file. Bloodhound then analyzes the program logic for virus-like behavior.
Configuring Auto-Protect email scanning for groupware applications

Auto-Protect scans can scan email attachments for the following applications:

- Lotus Notes 4.5x, 4.6, and 5.0
- Microsoft Exchange 5.0 and 5.5
- Microsoft Outlook 97/98/2000/2002 (MAPI only, not Internet)

When Auto-Protect is enabled for email, attachments are immediately downloaded to the computer that is running the email client and scanned when the user opens the message. If you are downloading a large attachment over a slow connection, mail performance is affected. You may want to disable this feature for users who regularly receive large attachments.

Symantec Client Security supports email scanning for Symantec Client Security clients only.

To configure email scanning

1. In the Symantec System Center console, right-click the server group or servers to configure, and then click All Tasks > Symantec AntiVirus > Client Auto-Protect Options.

2. In the Client Auto-Protect Options dialog box, on the Lotus Notes or Microsoft Exchange tab, check Enable Auto-Protect.
   You can use the Microsoft Exchange tab to configure both Microsoft Exchange and Microsoft Outlook.

3. To set Auto-Protect options, do any of the following:
   - Select file types or extensions to scan.
   - Assign primary actions and secondary actions for detected viruses.
   - Display a warning message on infected computers.
   - Insert a warning into an email message.
   - Send email to the sender of an infected attachment.
   - Send email to selected recipients when a virus is detected.

4. Click Advanced to configure scanning of compressed files.

5. Set the options, and then click OK.

6. Lock or unlock options as desired.

7. Click Reset All to ensure that all of the computers are using the Auto-Protect scanning configuration that you have specified.

See “Configuring Auto-Protect scans” on page 102.
If your email program is not supported

If your email system is not one of the supported data formats, you can still protect your network by enabling Auto-Protect on your file system. For example, if you are running a Novell GroupWise email system and one of your users receives a message with an infected attachment, Symantec Client Security can detect the virus as soon as the user tries to open the attachment. This is because most email programs (such as GroupWise) save attachments to a temporary directory when users launch attachments from the email program. If you enable Auto-Protect on your file system, Symantec Client Security detects the virus as it is written to the temporary directory. Symantec Client Security also detects the virus if the user tries to save the infected attachment to a local drive or network drive.

Configuring Auto-Protect scanning for Internet email

Auto-Protect scanning for Internet email protects both incoming and outgoing email messages that use the POP3 or SMTP communications protocol. When Auto-Protect scanning for Internet email is enabled, Symantec Client Security scans both the body text of the email and any attachments that are included.

Symantec Client Security also provides outbound email heuristics scanning that uses Bloodhound Virus Detection to identify threats that may be contained in outgoing messages. Scanning outgoing email messages helps to prevent the spread of threats such as worms that can use email clients to replicate and distribute themselves across a network.

When Auto-Protect scanning for Internet email is enabled, attachments are immediately downloaded to the computer that is running the email client and scanned when the user opens the message. If you are downloading a large attachment over a slow connection, mail performance is affected. You may want to disable this feature for users who regularly receive large attachments.

Email scanning does not support the following email clients:

- IMAP clients
- AOL clients
- POP3 that uses SSL (Secure Sockets Layer)
- HTTP-based email such as Hotmail and Yahoo!
To configure Auto-Protect scanning for Internet email

1. In the Symantec System Center console, right-click the server group or servers to configure, and then click All Tasks > Symantec AntiVirus > Client Auto-Protect Options.

2. In the Client Auto-Protect Options dialog box, on the Internet E-mail tab, check Enable Internet E-mail Auto-Protect. The settings that you choose apply to both the POP3 and SMTP protocols.

3. To set Auto-Protect options, do any of the following:
   - Select file types or extensions to scan.
   - Assign primary actions and secondary actions for detected viruses.
   - Display a warning message on infected computers.
   - Insert a warning into an email message.
   - Send an email message to the sender of an infected attachment.
   - Send an email message to selected recipients when a virus is detected.

4. Click Advanced to configure scanning of compressed files.

5. In the Internet E-mail Advanced Options dialog box, set the scanning options that you want, and then click OK.

6. On the Internet E-mail tab, lock or unlock options as desired.

7. Click Reset All to ensure that all of the computers are using the Auto-Protect scanning configuration that you have specified.

See “Configuring Auto-Protect scans” on page 102.

Changing the POP3 and SMTP ports that are scanned

Auto-Protect scanning for Internet email uses the standard POP3 and SMTP email ports by default. However, if you have configured your network to use a different port for either protocol, you must change the port setting in Symantec Client Security to match the port that you have selected.

To change the POP3 and SMTP ports that are scanned

1. In the Symantec System Center console, right-click the server group or servers to configure, and then click All Tasks > Symantec AntiVirus > Client Auto-Protect Options.

2. In the Client Auto-Protect Options dialog box, on the Internet E-mail tab, check Enable Internet E-mail Auto-Protect.

3. Click Advanced.
4 In the Internet E-mail Advanced Options dialog box, under Server Port Numbers, change the port number to match the port that you are using for each protocol.
   If you want to reset the port numbers to the default setting, click Use Defaults.
5 Click OK.
6 Click Reset All to ensure that all of the computers are using the Auto-Protect scanning configuration that you have specified.
   See “Configuring Auto-Protect scans” on page 102.

Enabling outbound email heuristics scanning

Auto-Protect scanning for Internet email provides outbound email protection against threats such as worms that can distribute themselves using email applications. Symantec Client Security utilizes Bloodhound Virus Detection technology to successfully identify threats in outbound email messages.

To enable outbound email heuristics scanning
1 In the Symantec System Center console, right-click the server group or servers to configure, and then click All Tasks > Symantec AntiVirus > Client Auto-Protect Options.
2 In the Client Auto-Protect Options dialog box, on the Internet E-mail tab, check Enable Internet E-mail Auto-Protect.
3 Click Advanced.
4 In the Internet E-mail Advanced Options dialog box, check Outbound Worm Heuristics.
5 Click OK.
6 Click Reset All to ensure that all of the computers are using the Auto-Protect scanning configuration that you have specified.
   See “Configuring Auto-Protect scans” on page 102.

How to specify exclusions

Exclusions help you balance the amount of protection that your network requires with the amount of time and resources that are required to provide that protection. For example, when you scan all file types, you may want to exclude certain folders that contain only data files that are not subject to viruses. This decreases the overhead that is associated with scanning files.
Configuring Auto-Protect settings

You can configure Auto-Protect settings at the server group, server, and client group level. When you configure Auto-Protect settings, follow these rules:

- Changing server Auto-Protect settings for an individual server allows you to push a specific configuration to that server, which overrides settings that are made at the server group level. Resetting server Auto-Protect settings at the server group level allows you to reset previous settings made at the individual server level.

- Changing client Auto-Protect settings at the parent server or client group level allows you to push a specific configuration to the clients of that parent server or client group.
  - Resetting client Auto-Protect settings at the server group level resets previous settings made at the parent server or client group level, for all clients.
  - Changing client Auto-Protect settings at the parent server level changes the settings for clients not assigned to client groups; clients assigned to a client group retain their settings.

- Clicking OK in the Auto-Protect Options dialog box propagates the settings that you change. Clicking Cancel propagates the settings you visit in the Auto-Protect Options dialog box. (In this instance, visiting means changing a setting, and then changing it back to the way it was set when you opened the dialog box.) Settings that are unchanged or unvisited are not propagated.
  
  For example, when you change the Auto-Protect settings (but do not visit or change the settings on any other configuration tab in any other dialog box), and click OK, only the Auto-Protect options are propagated.

- Clicking Reset All propagates all settings in the dialog box, regardless of whether you change or visit them.

For more information about settings propagation, see “How settings propagate” on page 64.

To configure Auto-Protect settings

1. In the Symantec System Center console, do one of the following:
   - To change server Auto-Protect settings, right-click a server group or server, and then click All Tasks > Symantec AntiVirus > Server Auto-Protect Options.
   - To change client Auto-Protect settings, right-click a server-group, server, or client group, and then click All Tasks > Symantec AntiVirus > Client Auto-Protect Options.
2  In the Auto-Protect Options dialog box, change one or more settings.
3  Click OK until the main Symantec System Center console window appears.

How to lock and unlock Auto-Protect options

The lock icons in the Auto-Protect Options dialog box allow you to control user experience at the Symantec Client Security client. Table 3-3 lists and describes the lock icons.

**Table 3-3**  Auto-Protect lock icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
<th>What it does</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1" alt="Icon" /></td>
<td>This is an unlocked setting.</td>
<td>Users can change an unlocked setting from Symantec Client Security client.</td>
</tr>
<tr>
<td><img src="image2" alt="Icon" /></td>
<td>This is a locked setting.</td>
<td>This setting is not available to users from Symantec Client Security client.</td>
</tr>
</tbody>
</table>

Configuring manual scans

Configuring a manual scan consists of the following tasks:

- Select a Symantec Client Security server or client.
- Select folders to scan.
- Specify scanning options.
- Specify advanced options.

If you want to scan all servers and clients in a server group, run a virus sweep or create a scheduled scan.

Symantec Client Security backs up viruses but does not back up other threats, such as adware or spyware, when it deletes them. Once you delete the file, Symantec Client Security cannot restore it.
To configure a manual scan

1. In the Symantec System Center console, do one of the following:
   - Right-click a server or client computer.
   - Select one or more servers that are in the same server group, and then right-click the servers.
   - Select one or more clients that are managed by the same server, and then right-click the clients.

2. Click **All Tasks > Symantec AntiVirus > Start Manual Scan**.

3. In the Select Items dialog box, select the folders to scan.
   If you are scanning multiple computers, this option is not available. Go to step 5.

4. Click **Save Settings** if you want Symantec Client Security to remember your selections for future manual scans on this computer.
   Symantec Client Security also remembers these settings for future scans when multiple computers are selected.

5. Click **Options**.
   See Figure 3-1, “Scan Options dialog box,” on page 99.

6. In the Scan Options dialog box, you can:
   - Select file types or extensions to scan.
   - Assign primary and secondary actions for detected viruses, blended threats, and some other threats. If deleting a threat in an expanded threat category can cause a system failure, the only available action is to log it.
   - Enable scanning for threats that are in memory. See “Scanning for in-memory threats” on page 138.
   - Enable expanded threat scanning and exclude threat categories from the scan if necessary.
     When you exclude a folder, Symantec Client Security cannot protect the affected computer from infected files in the folder.
     When you exclude a threat category, Symantec Client Security cannot protect the affected computer from threats that are included in the category. See “Enabling expanded threat categories” on page 145.
   - Display a warning message on infected computers.
   - Exclude files and folders from the scan. (Not available for multiple clients or servers.)
   - Set throttling options. See “Setting CPU utilization” on page 150.

7. Click **Advanced**.
8 In the Scan Advanced Options dialog box, you can:

- Set options for scanning compressed files.
- Back up files infected by viruses or blended threats before attempting to repair them as a data safety precaution. The files are encrypted before Symantec Client Security backs them up. The files get backed up to the Quarantine directory. Once the file is backed up, it must be restored before it can be accessed again.

Symantec Client Security does not back up threats other than viruses and blended threats; for example, Symantec Client Security does not back up spyware or adware files.
- Determine whether a progress dialog box appears on the computer while the scan runs. You can configure the progress dialog box to close automatically when the scan has completed. You can also display or hide a Stop button on the remote computer. When this option is disabled, the scan cannot be stopped from the remote computer.
- Set storage migration options. See “Configuring HSM settings” on page 147.
- Enable scans of compressed files on NetWare servers.

9 Click OK to save advanced options.

10 In the Scan Options dialog box, click Save Settings if you want Symantec Client Security to remember these options for future manual scans on this computer.

Symantec Client Security will also remember these settings for future scans when multiple computers are selected.

11 Click OK to continue with these options.

12 Click Start.

See “Setting CPU utilization” on page 150.
How to specify exclusions

You can exclude files, folders, and expanded threat categories from scans.

**Excluding files and folders**

You may want to exclude folders that contain only data files that are not subject to viruses. You can also exclude folders that contain other allowable threats. For example, your company’s security policy may allow users to run an adware program.

*Note:* Because excluded files and folders are not scanned, they are not protected from viruses and other threats.

**Excluding expanded threat categories**

You can exclude expanded threat categories for which you do not want Symantec Client Security to scan. For example, if you monitor user Internet behavior with a company approved trackware application that is installed on every network node, you can exclude the trackware category.

See “Enabling expanded threat categories” on page 145.

Deleting files and folders that are left on computers by threats

When Symantec Client Security deletes a file that is part of a threat category, such as adware or spyware, other files related to the threat may remain on the computer. The remaining files are not likely to cause a problem but you may want to delete them manually to free up disk space on the computer.

Configuring scheduled scans

Configuring scheduled scans consists of:

- Scheduling scans for Symantec Client Security servers and clients
- Setting options for missed scans
- Optionally editing, deleting, or disabling a scan, or running a scheduled scan on demand

Scheduled scans have settings that are similar to Auto-Protect scan settings, but each type of scan is configured separately. For example, exclusions settings that are set for Auto-Protect scanning only affect Auto-Protect scanning, and do not affect scheduled scanning.
Scheduling scans for server groups or individual Symantec Client Security servers

You can schedule scans for one or more server groups as well as for individual Symantec Client Security servers.

**To schedule a scan for a server group**

1. In the Symantec System Center console, do one of the following:
   - In the console tree, click **System Hierarchy**. In the right pane, Shift+click or Ctrl+click to select multiple server groups, and then right-click the selection.
   - Right-click a server group.
   - Right-click a server.
2. Click **All Tasks > Symantec AntiVirus > Scheduled Scans**.

![Scheduled Scans Interface](image)
In the Scheduled Scans dialog box, on the Server Group Scans tab, click **New**.

In the Scheduled Scan dialog box, under Name, type a name for the scan.

Ensure that Enable scan is checked.

Set a frequency for the scan.

Set a time for the scan.

You can type any time in increments of 1 minute or use the drop-down list to select a time in 15-minute increments.

Click **Advanced**.

In the Advanced Schedule Options dialog box, check **Handle Missed Events Within**, and then set the time limit within which you want the scan to run. For example, you may want a weekly scan to run only if it is within three days after the scheduled time for the missed event.

Click **OK**.

In the Scheduled Scan dialog box, click **Scan Settings**.

In the Select Items dialog box, click **Options**.

In the Scheduled Scans Options dialog box, you can:

- Select file types or extensions to scan.
- Assign primary and secondary actions for detected viruses, blended threats, and some other threats. If deleting a threat in an expanded threat category can cause a system failure, the only available action is to log it.
- Enable scanning for threats that are in memory. See “Scanning for in-memory threats” on page 138.
Scanning for viruses and other threats

Configuring scheduled scans

- Enable expanded threat scanning and exclude threat categories from the scan if necessary.
  When you exclude a folder, Symantec Client Security cannot protect the affected computer from infected files in the folder.
  When you exclude a threat category, Symantec Client Security cannot protect the affected computer from threats that are included in the category. See “Enabling expanded threat categories” on page 145.
- Display a warning message on infected computers.
- Exclude files and folders from the scan. (Not available for multiple clients or servers.)
- Set throttling options. See “Setting CPU utilization” on page 150.

14 Click **Advanced**.

15 In the Scan Advanced Options dialog box, you can:
- Display a scan progress window on a computer that is being scanned.
- Close a scan progress window on a computer when the scan completes.
- Back up infected files before you attempt to repair them as a data safety precaution. The files are encrypted and backed up to the Quarantine directory. Once the file is backed up, it must be restored before it can be accessed again.
  Symantec Client Security does not back up threats other than viruses, such as adware or spyware, when you delete them. Once you delete the file, Symantec Client Security cannot restore it.
- Set options for scanning compressed files.

16 Click **OK** until you return to the main screen in the Symantec System Center console.

See “Configuring scan options” on page 129.

Scheduling scans for Symantec Client Security clients

You can schedule Symantec Client Security client scans at the Symantec Client Security server or client level.

**To schedule scans for Symantec Client Security clients**

1 In the Symantec System Center console, right-click a server or individual client, and then click **All Tasks > Symantec AntiVirus > Scheduled Scans**.
2 In the Scheduled Scans dialog box, on the Client Scans tab, click **New**.

3 In the Scheduled Scan dialog box, under Name, type a name for the scan.

4 Set a frequency for the scan.

5 Set a time for the scan.
   You can type any time in increments of 1 minute or use the drop-down list to select a time in 15-minute increments.

6 Click **Advanced**.

7 In the Advanced Schedule Options dialog box, check **Handle missed events within**, and then set the time limit within which you want the scan to run. For example, you may want a weekly scan to run only if it is within three days after the scheduled time for the missed event.

8 Click **OK**.

9 In the Scheduled Scan dialog box, click **Scan Settings**.

10 Select the folders to scan.
   This option is not available if you are scanning multiple computers because folders are specific to each computer.

11 Click **Options**.
12 In the Scheduled Scan Options dialog box, you can:

- Select file types and extensions to scan.
- Assign primary and secondary actions for detected viruses. If deleting a threat can cause a system failure, the only available action is to log the threat.
- Select file types or extensions to scan.
- Enable scanning for threats that are in memory. See “Scanning for in-memory threats” on page 138.
- Enable expanded threat scanning and exclude threat categories from the scan if necessary.
  When you exclude a folder, Symantec Client Security cannot protect the affected computer from infected files in the folder.
  When you exclude a threat category, Symantec Client Security cannot protect the affected computer from threats that are included in the category. See “Enabling expanded threat categories” on page 145.
- Display a warning message on infected computers.
- Exclude files and folders from the scan. (Not available for multiple clients or servers.)
- Set throttling options. See “Setting CPU utilization” on page 150.

13 Click **Advanced**.

14 In the Scan Advanced Options dialog box, you can:

- Set options for scanning compressed files.
- Back up files infected by viruses or blended threats before attempting to repair them as a data safety precaution. The files are encrypted before Symantec Client Security backs them up. The files get backed up to the Quarantine directory. Once the file is backed up, it must be restored before it can be accessed again.

  Symantec Client Security does not back up threats other than viruses and blended threats; for example, Symantec Client Security does not back up spyware or adware files.

- Determine whether a progress dialog box appears on the computer while the scan runs. You can configure the progress dialog box to close automatically when the scan has completed. You can also display or hide a Stop button on the remote computer. When this option is disabled, the scan cannot be stopped from the remote computer.
- Set storage migration options. See “Configuring HSM settings” on page 147.
- Enable scans of compressed files on NetWare servers.
15 Click OK until you return to the main screen in the Symantec System Center console.

See “Configuring scan options” on page 129.

Setting options for missed scheduled scans

If a computer misses a scheduled scan (for example, if it is turned off), Symantec Client Security will attempt the scan for a specific time interval. If Symantec Client Security cannot start the scan within the time interval, it will not run the scan. The default time intervals are as follows:

- Daily scans: 8 hours
- Weekly scans: 3 days
- Monthly scans: 11 days

You can specify a time interval in which to attempt a scheduled scan.

To set options for missed scheduled scans

1 In the Symantec System Center console, right click a Symantec Client Security server, server group, client group, or individual client, and then click All Tasks > Symantec AntiVirus > Scheduled Scans.
2 In the Scheduled Scans dialog box, select a scan in the list of scans.
3 Click Edit.
4 In the Scheduled Scan dialog box, click Advanced.
5 In the Advanced Schedule Options dialog box, click Handle Missed Events Within.
6 Specify the time interval for reattempting the scheduled scan.
7 Click OK until the main Symantec System Center console window appears.

Editing, deleting, or disabling a scheduled scan

If you want to modify the properties of an existing scheduled scan, you can edit it. If you want to stop a scheduled scan from occurring, you can delete or disable it.

Edit, delete, or disable a scheduled scan

You can edit, delete, or disable a scheduled scan.
To edit or delete a scheduled scan

1. In the Symantec System Center console, right-click one or more server groups, a server, or a client for which you want to edit or delete the scheduled scan, and then click All Tasks > Symantec AntiVirus > Scheduled Scans.

2. In the Scheduled Scans dialog box, select one of the following:
   - Server Scans: Edit or delete scans for servers. This option is not available if you selected a client computer in step 1.
   - Client Scans: Edit or delete scans for clients. This option is not available if you selected a server group in step 1.

3. Do one of the following:
   - Select an existing scan, and then click Edit. Change any properties that you want, and then click OK until you return to the Symantec System Center main window.
   - Select an existing scan, and then click Delete. Click OK until you return to the Symantec System Center main window.

To disable a scheduled scan

1. In the Symantec System Center console, right-click one or more server groups, a server, or a client for which you want to disable the scheduled scan, and then click All Tasks > Symantec AntiVirus > Scheduled Scans.

   The scans that you can disable depend on the object that you select.

2. In the Scheduled Scans dialog box, select one of the following:
   - Server Scans: Disable scans for servers. This option is not available if you selected a client computer in step 1.
   - Client Scans: Disable scans for clients. This option is not available if you selected a server group in step 1.

3. Uncheck the previously scheduled scan.

4. Click OK.

Running a scheduled scan on demand

When you create and save a scheduled scan, Symantec Client Security remembers the server group, server, or computer on which to run the scan and also remembers all of the settings that you chose for that specific scan.

After you configure a scheduled scan (and all of its scan properties), you might want to run it on demand at some time other than when you originally scheduled it. This can save you the effort of configuring and running a manual scan with similar properties.
Scanning for viruses and other threats

Handling Symantec Client Security clients with intermittent connectivity

To run a scheduled scan on demand
1 In the Symantec System Center console, right-click a server group or a server, and then click All Tasks > Symantec AntiVirus > Scheduled Scans.
2 In the Scheduled Scans dialog box, select one of the following:
   ■ Server Scans: Run a server scan on demand. This option is not available if you selected a server group in step 1.
   ■ Client Scans: Run a client scan on demand. This option is not available if you selected a server group in step 1.
3 Select an existing scheduled scan.
4 Click Start Scan.

Deleting files and folders that are left on computers by threats
When Symantec Client Security deletes a file that is part of a threat category, such as adware or spyware, other files related to the threat may remain on the computer. The remaining files are not likely to cause a problem but you may want to delete them manually to free up disk space on the computer.

Handling Symantec Client Security clients with intermittent connectivity
Each Symantec Client Security server stores a list of Symantec Client Security clients that it manages, and provides this data to the Symantec System Center. By default, clients check in with their parent servers once an hour, and parent servers review their lists of clients once an hour. Parent servers track client check-in times; if a client fails to check in with its parent server for more than thirty days, the parent server removes that client from its list of clients and logs that client as deleted. The next time that the Symantec System Center queries the parent server for a list of its clients, that client will not appear.

You can control this behavior by configuring the following settings:
■ The client expiration interval
■ The client check-in interval

Handle Symantec Client Security clients with intermittent connectivity
By default, the client check-in interval is set to 60 minutes. The interval may be changed with the CheckConfigMinutes registry value.

The client expiration interval must be greater than the client check-in interval or the parent server will delete and add clients continually.
If the new client configuration is not immediately received by the parent server or by the client, the information is updated during the client check-in.

To modify the client expiration interval
1 On the parent server, locate the following registry key:
   HKEY_LOCAL_MACHINE\Software\Intel\LANDesk\VirusProtect6\CurrentVersion directory
2 On the Edit menu, click New > DWORD Value.
3 Name the value as follows:
   ClientExpirationTimeout
4 Right-click the new key, and then click Modify.
5 In the Value Data box, replace the 0 with a number greater than 0. Without the use of the ClientExpirationTimeout value, the default time is 720 hours. Use a smaller value to decrease the number of minutes that it takes for the client to be removed from the console, or use a larger value to increase the time. For example, if a large number of your client computers are being removed from the Symantec System Center because people are away from the office and their computers are turned off, you can specify a larger number.
6 Click OK.
7 Exit Regedit.

To modify the client check-in interval
1 In the Symantec System Center console, right-click a server, server group, or client group, and then click All Tasks > Symantec AntiVirus > Virus Definition Manager.
2 In the Virus Definition Manager dialog box, check Update Virus Definitions From Parent Server.
3 Click Settings.
4 In the Update Settings dialog box, in the Check for updates every box, type the interval in minutes.
5 Click OK until the main Symantec System Center console window appears.
Configuring scan options

Many of the same scan options are available in different types of scans. For example, you can assign primary actions and secondary actions when configuring manual, scheduled, or Auto-Protect scans.

How to assign primary actions and secondary actions for detected viruses

You can assign a primary action and, in case the primary action is not possible, a secondary action for Symantec Client Security to take when it discovers a virus. You can assign separate actions for macro viruses and non-macro viruses.

You can assign the following actions for detected viruses:

- **Clean virus from file**: Attempts to clean an infected file upon detection.
- **Quarantine infected file**: Attempts to move the infected file to the Quarantine on the infected computer as soon as it is detected. After an infected file is moved to the Quarantine, no user can execute it until you take an action (for example, clean or delete) and move the file back to its original location.
- **Delete infected file**: Attempts to delete the file. Use this option only if you can replace the infected file with a virus-free backup copy because the file is permanently deleted and cannot be recovered from the Recycle Bin.
  
  If Symantec Client Security cannot delete the file, detailed information about the action that Symantec Client Security took appears in the Notification dialog box and Symantec Client Security Event Log.
- **Leave alone (log only)**: Denies access to the file, displays a threat notification, and logs the event. Use this option to control how Symantec Client Security handles a virus. When you are notified of a virus, open the Threat History for the computer, right-click the name of the infected file, and select one of the following actions: Clean, Delete Permanently, or Move To Quarantine.

By default, Symantec Client Security first attempts to clean the file. If Symantec Client Security cannot clean the file, it moves the file to the Quarantine on the infected computer, denies access to the file, and logs the event.
How to assign primary actions and secondary actions for other detected threats

You can assign a primary action and, in case the primary action is not possible, a secondary action for Symantec Client Security to take when it discovers a threat other than a virus, such as adware or spyware.

**Figure 3-2** Scheduled Scan Options dialog box with Exp. Threats tab

In the Scheduled Scan Options dialog box, shown in *Figure 3-2*, you can assign the following actions for other detected threats:

- **Delete infected file**: Attempts to delete the file. This action is available when deleting the file will not cause a system failure.

- **Leave alone (log only)**: Denies access to the file, displays a virus notification, and logs the event. Use this option to control how Symantec Client Security handles a threat. An alert is sent when the threat is detected but no action is taken. You must then take action. For example, you may need to notify the user, and then instruct the user to uninstall the software that poses a threat.
Controlling the user experience

Symantec Client Security allows you to control several aspects of the Symantec Client Security client user experience. You can do any of the following:

- Deny or permit users the ability to unload Symantec Client Security.
- Require a password before permitting an uninstallation.
- Allow users to pause or stop a scheduled scan.
- Display a scan progress window.
- Display and customize a warning message on an infected computer. For example, if users have a spyware program installed on their computers, you can notify them that they have violated your corporate policy and must uninstall the application immediately.
- Add an infection warning to an infected email message.
- Notify the sender of an infected email message.
- Notify others about the receipt of an infected email message.

Denying or permitting users the ability to unload Symantec Client Security

You can deny or permit users the ability to unload Symantec Client Security.

To deny or permit users the ability to unload Symantec Client Security

1 In the Symantec System Center console, right-click a server, server group, or client group, and then click All Tasks > Symantec AntiVirus > Client Administrator Only Options.
2 Click the Security tab.
3 Change the setting for Lock the ability of users to unload Symantec AntiVirus Services.
4 Click OK.

Requiring a password before uninstalling

You can require Symantec Client Security to prompt for a password before permitting an uninstallation.
To require a password before uninstalling

1. In the Symantec System Center console, right-click a server, server group, or client group, and then click All Tasks > Symantec AntiVirus > Client Administrator Only Options.

2. Click the Security tab.

3. Check Ask for password to allow uninstall of Symantec AntiVirus Client.

4. Click Change.

5. In the Configure Password dialog box, type a new password, and then confirm by typing the password again.

6. Click OK until the main Symantec System Center console window appears.

Allowing users to pause, snooze, or stop a scheduled scan

You can allow users to temporarily pause or snooze a scheduled scan, as well as stop the scan entirely. The results are as follows:

- Paused scan: When a user pauses a scan, the Scan Results dialog box remains open, waiting for the user to either continue or abort the scan. If the computer is shut off, the paused scan will not continue.

- Snoozed scan: When a user snoozes a scheduled scan, the user has the option of snoozing the scan for one hour, or (depending on the configuration) for three hours. In addition, the number of snoozes is configurable. When a scan is snoozing, the Scan Results dialog box closes, and reappears when the snooze period ends and the scan resumes.

Allow users to pause, snooze, or stop a scan

A paused scan automatically restarts after a specified time interval elapses. A stopped scan will not restart.

To allow users to pause or snooze a scan

1. In the Symantec System Center console, right-click a server group, server, or client group, and then click All Tasks > Symantec AntiVirus > Scheduled Scan.

2. In the Scheduled Scans dialog box, do one of the following:
   - Select a scheduled scan, and then click Edit.
   - Click New to create a new scan.

3. In the Scheduled Scan dialog box, click Scan Settings.

4. In the Select Items dialog box, click Options.

5. In the Scheduled Scan Options dialog box, click Advanced.
6 In the Scan Advanced Options dialog box, click **Show scan progress on computer being scanned**.

7 Uncheck **Allow user to stop scan**.

8 Check **Allow user to pause/snooze scan**.

9 Click **Pause Options**.

10 In the Pause Options dialog box, do one of the following:
   - Limit the number of minutes that a user may pause a scan: Check **Limit the time this scan may be paused** and type a number of minutes.
   - Limit the number of times a user may pause a scan: In the Number of times it can snooze box, type a number.
   - Display a three-hour snooze button: Check **Enable the 3 hour snooze**.

By default, a user can pause a scan for one hour. You must enable this option to allow a user to pause a scan for three hours.

11 Click **OK** until the main Symantec System Center console window appears.

**To allow users to stop a scan**

1 In the Symantec System Center console, right-click a server group, server, or client group, and then click **All Tasks > Symantec AntiVirus > Scheduled Scan**.

2 In the Scheduled Scans dialog box, do one of the following:
   - Select a scheduled scan, and then click **Edit**.
   - Click **New** to create a new scan.

3 In the Scheduled Scan dialog box, click **Scan Settings**.

4 In the Select Items dialog box, click **Options**.

5 In the Scheduled Scan Options dialog box, click **Advanced**.

6 In the Scan Advanced Options dialog box, click **Show scan progress on computer being scanned**.

7 Check **Allow user to stop scan**.

8 Uncheck **Allow user to pause/snooze scan**.

9 If you want to automatically close the scan progress indicator after the scan completes, check **Close scan progress when done**.

10 Click **OK** until the main Symantec System Center console window appears.
Displaying and customizing a warning message on an infected computer

When you run a remote scan on a user’s computer, you can immediately notify the user of a problem by displaying a warning message on the infected computer’s screen. You can customize the warning message by including information such as the name of the threat, the name of the infected file, the status of the infection, and so on.

The default warning message contains message variables and text. The message variable is in brackets. Everything outside the brackets is text. You can change the text and message variables that are in the warning message to suit your needs. Table 3-4 describes the message variables.

Table 3-4 Warning message variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>[LoggedBy]</td>
<td>Type of scan that logged the event: Auto-Protect, scheduled, or manual scan.</td>
</tr>
<tr>
<td>[Event]</td>
<td>Type of event, such as Threat Found.</td>
</tr>
<tr>
<td>[VirusName]</td>
<td>Name of detected threat.</td>
</tr>
<tr>
<td>[PathAndFilename]</td>
<td>Full path and file name.</td>
</tr>
<tr>
<td>[Location]</td>
<td>Drive location on the infected computer.</td>
</tr>
<tr>
<td>[Computer]</td>
<td>Name of the computer.</td>
</tr>
<tr>
<td>[User]</td>
<td>Network logon name of the user.</td>
</tr>
<tr>
<td>[ActionTaken]</td>
<td>Action that was taken on the infected file (such as cleaned, moved to the Quarantine, deleted, or left alone).</td>
</tr>
<tr>
<td>[DateFound]</td>
<td>Date and time that the threat was found.</td>
</tr>
<tr>
<td>[Status]</td>
<td>State of the file: Infected, Not Infected, or Deleted. This message variable is not used by default. If you want to display this information, you must manually add the variable to the warning message.</td>
</tr>
</tbody>
</table>

For example, a warning message might look as follows:

Scan type: Scheduled Scan
Event: Threat Found
VirusName: Stoned-C
File: C:\Autoexec.bat
Location: C:
To display and customize a warning message on an infected computer

1. In the Symantec System Center console, right-click a server group, Symantec Client Security server, or client group, and then click **All Tasks > Symantec AntiVirus > Client Auto-Protect Options**.

2. In the Client Auto-Protect Options dialog box, click **Display Message on infected Computer**.

3. Do one of the following:
   - Click **OK** to accept the default message.
   - Click **Message** and customize the text, and then click **OK**.

4. Click **OK** until the Client Auto-Protect Options dialog box disappears.

Adding an infection warning to an infected email message

For supported email software, you can configure Auto-Protect to automatically insert a warning into the body of an infected email message. This type of warning can be important if Symantec Client Security is unable to clean the virus from the message, and if an infected attachment file is moved, left alone, deleted, or renamed. The warning message tells you which virus was found and explains the action that was taken.

Symantec Client Security appends this text to the top of the email message that is associated with the infected attachment:

Symantec Client Security found a virus in an attachment from [EmailSender].

For each infected file, the following information is also added to the email message:

- Name of the file attachment
- Name of the virus
- Action taken (such as cleaned, moved to the Quarantine, deleted, or left alone)
- File status (infected or not infected)

You can customize the subject and body of the message.

The email message contains a field called [EmailSender]. All fields in brackets contain variable information. You can customize the default message by right-clicking the body of the message and selecting a field to insert into the message.
The message would look as follows to the recipient:

Symantec Client Security found a virus in an attachment from John.Smith@mycompany.com.

**To add an infection warning to an infected email message**

1. In the Symantec System Center console, right-click a server group, Symantec Client Security server, or client group, and then click **All Tasks > Symantec AntiVirus > Client Auto-Protect Options**.
2. In the Client Auto-Protect Options dialog box, on either the Lotus Notes or Microsoft Exchange tab, click **Insert warning into email message**.
3. Do one of the following:
   - Click **OK** to accept the default message.
   - Click **Warning** and customize the text, and then click **OK**.
4. Click **OK** until the Client Auto-Protect Options dialog box disappears.

**Notifying the sender of an infected email message**

For supported email software, you can configure Auto-Protect to respond automatically to the sender of an email message that contains an infected attachment.

Symantec Client Security sends a reply email message with the following subject:

Virus Found in message “[EmailSubject]”

The body of the message informs the sender of the infected attachment:

Symantec Client Security found a virus in an attachment you ([EmailSender]) sent to [EmailRecipientList].

For each infected file, the following information is also added to the email message:

- Name of the file attachment
- Name of the virus
- Action taken (such as cleaned, moved to the Quarantine, deleted, or left alone)
- File status (infected or not infected)
To notify a sender of an infected email message

1. In the Symantec System Center console, right-click a server group, Symantec Client Security server, or client group, and then click **All Tasks > Symantec AntiVirus > Client Auto-Protect Options.**

2. In the Client Auto-Protect Options dialog box, on either the Lotus Notes or Microsoft Exchange tab, click **Enable Lotus Notes (Microsoft Exchange) Auto-Protect.**

3. Click **Send e-mail to sender.**

4. Click **Message.**

5. Do one of the following:
   - Click **OK** to accept the default message.
   - Click **Message** and customize the text, and then click **OK.**

6. Click **OK** until the Client Auto-Protect Options dialog box disappears.

Notifying others of an infected email message

For supported email software, you can configure Auto-Protect to notify others whenever an email message that contains an infected attachment is opened.

Symantec Client Security sends an email message to the selected recipients with the following subject:

```
Virus Found in message “[EmailSubject]”
```

The body of the message includes information on the sender of the infected attachment:

```
Symantec Client Security found a virus in an attachment from [EmailSender].
```

For each infected file, the following information is also added to the email message:

- Name of the file attachment
- Name of the virus
- Action taken (such as cleaned, moved to the Quarantine, deleted, or left alone)
- File status (infected or not infected)
To notify others of an infected email message

1 In the Symantec System Center console, right-click a server group, Symantec Client Security server, or client group, and then click All Tasks > Symantec AntiVirus > Client Auto-Protect Options.

2 In the Client Auto-Protect Options dialog box, on either the Lotus Notes or Microsoft Exchange tab, click Enable Lotus Notes (Microsoft Exchange) Auto-Protect.

3 Click Send e-mail to selected.

4 Click Addresses.

5 In the Email Address dialog box, provide one or more email addresses to which notification will be sent.

6 Click OK.

7 Click Message.

8 Do one of the following:

   ■ Click OK to accept the default message.

   ■ Click Compose and customize the message, and then click OK.

9 Click OK until the Client Auto-Protect Options dialog box disappears.

Scanning for in-memory threats

You can configure manual and scheduled scans to scan running processes to identify and handle threats that are loaded into memory. Symantec Client Security can terminate the process and handle the threat-infected file based on your specified primary and secondary actions.

If the infected file is associated with an important process, you may need to shut down the computer, and then restart it.

In-memory scanning does not scan specifically for memory-resident threats, such as the SQL Slammer worm. It scans for all threats that may be in memory.

Excluding files from scanning

Exclusions help you balance the amount of protection your network requires with the amount of time and resources that are required to provide that protection. For example, when you scan all file types, you may want to exclude certain folders that contain only data files that are not subject to viruses. This decreases the overhead that is associated with needlessly scanning files.
Using the Symantec System Center, you can set exclusions for specific file extensions and folders. In addition, certain Symantec Client Security scans allow exclusion by named folder (for example, you can exclude scans of the path C:\Temp\Install). To maintain security, you cannot view or exclude specific files from the Symantec System Center. You can, however, exclude specific files using the Symantec Client Security client or server user interface. You may want to exclude files that trigger false positive alerts. For example, if you used another virus scanning program to clean infected files and the program did not completely remove the virus code, the file may be harmless but the disabled virus code might cause Symantec Client Security to register a false positive. Check with Symantec Technical Support if you are not sure if a file is infected.

Table 3-5 describes exclusions.

**Table 3-5** Exclusions by object type

<table>
<thead>
<tr>
<th>Object type</th>
<th>Exclusions available</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server group</td>
<td>Server scans: File extensions and named folders</td>
</tr>
</tbody>
</table>
| Server         | ■ Server scans: File extensions, drivers, files, and folders  
|                | ■ Client scans: File extensions, drivers, and named folders |
| Client group   | Client scans: File extensions, drivers, and named folders  |
| NetWare servers| Files by drivers and named folders; you cannot exclude files by file extension |

### Setting exclusions

Symantec Client Security exclusions behavior is as follows:

- When Symantec Client Security applies exclusions, the excluded items are not scanned. If the file is not excluded, it is scanned.
- For virus sweep, manual, Auto-Protect, and scheduled scans, Symantec Client Security takes no action on excluded files.

Enabling and disabling exclusions can improve performance depending on the situation. For example:

- If you copied a large folder that was in the exclusions list and the exclusions setting was enabled, the copying process would not take as long since the folder’s contents would be excluded.
- If you copied a large folder that was not in the exclusions list, disabling exclusions would improve performance.
To set exclusions

1. In the Scan Options dialog box for the type of scan that you want to configure, click **Exclude files and folders**.
2. Click **Exclusions**.
3. In the Exclusions dialog box, check **Check file for exclusion before scanning** to enable prescan exclusions.
4. Depending on the types and numbers of computers that you are configuring, you can do the following:
   - Select file extensions to exclude by extension or wildcard.
   - Select files to exclude within specific folders by extension, wildcard, or file type.
   - Select folders to exclude from the scan.
5. Click **OK** until the Symantec System Center console appears.

Selecting file types and extensions to scan for viruses

By default, Symantec Client Security scans all files during a virus scan. For scans other than Auto-Protect scanning, you can select to scan only files of a specific file type or with specific extensions. Scans by file type and extension are available when you select the following objects and scan types:

- **Client object**: Manual scan, scheduled scan, and client Auto-Protect
- **Server object**: Virus sweep, manual scan, scheduled server scan, and server Auto-Protect (Windows only)

When you scan by file type, Symantec Client Security reads each file’s header to determine the file type. For example, if you enable document scanning, Symantec Client Security scans all documents even if you name them with nonstandard extensions, such as Document3.mlt instead of Document3.doc.

**Note:** This option doesn’t apply to NetWare servers; it applies only to Windows-based computers.
When you scan by file extension, Symantec Client Security does not read the file header to determine the file type and scans only files with the extensions that you specify. Table 3-6 describes the recommended extensions.

Table 3-6  Recommended file extensions for scanning

<table>
<thead>
<tr>
<th>File extension</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>386 Driver</td>
<td></td>
</tr>
<tr>
<td>ACM</td>
<td>Driver; audio compression manager</td>
</tr>
<tr>
<td>ACV</td>
<td>Driver; audio compression/decompression manager</td>
</tr>
<tr>
<td>ADT</td>
<td>ADT file; fax</td>
</tr>
<tr>
<td>AX</td>
<td>AX file</td>
</tr>
<tr>
<td>BAT</td>
<td>Batch</td>
</tr>
<tr>
<td>BTM</td>
<td>Batch</td>
</tr>
<tr>
<td>BIN</td>
<td>Binary</td>
</tr>
<tr>
<td>CLA</td>
<td>Java Class</td>
</tr>
<tr>
<td>COM</td>
<td>Executable</td>
</tr>
<tr>
<td>CPL</td>
<td>Applet Control Panel for Microsoft Windows</td>
</tr>
<tr>
<td>CSC</td>
<td>Corel Script</td>
</tr>
<tr>
<td>DLL</td>
<td>Dynamic Link Library</td>
</tr>
<tr>
<td>DOC</td>
<td>Microsoft Word</td>
</tr>
<tr>
<td>DOT</td>
<td>Microsoft Word</td>
</tr>
<tr>
<td>DRV</td>
<td>Driver</td>
</tr>
<tr>
<td>EXE</td>
<td>Executable</td>
</tr>
<tr>
<td>HLP</td>
<td>Help file</td>
</tr>
<tr>
<td>HTA</td>
<td>HTML application</td>
</tr>
<tr>
<td>HTM</td>
<td>HTML</td>
</tr>
<tr>
<td>HTML</td>
<td>HTML</td>
</tr>
<tr>
<td>HTT</td>
<td>HTML</td>
</tr>
<tr>
<td>INF</td>
<td>Installation script</td>
</tr>
<tr>
<td>INI</td>
<td>Initialization file</td>
</tr>
</tbody>
</table>
### Table 3-6  Recommended file extensions for scanning

<table>
<thead>
<tr>
<th>File extension</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>JS</td>
<td>JavaScript</td>
</tr>
<tr>
<td>JSE</td>
<td>JavaScript Encoded</td>
</tr>
<tr>
<td>JTD</td>
<td>Ichitaro</td>
</tr>
<tr>
<td>MDB</td>
<td>Microsoft Access</td>
</tr>
<tr>
<td>MP?</td>
<td>Microsoft Project</td>
</tr>
<tr>
<td>MSO</td>
<td>Microsoft Office 2000</td>
</tr>
<tr>
<td>OBD</td>
<td>Microsoft Office binder</td>
</tr>
<tr>
<td>OBT</td>
<td>Microsoft Office binder</td>
</tr>
<tr>
<td>OCX</td>
<td>Microsoft object linking and embedding custom control</td>
</tr>
<tr>
<td>OV?</td>
<td>Overlay</td>
</tr>
<tr>
<td>PIF</td>
<td>Program information file</td>
</tr>
<tr>
<td>PL</td>
<td>PERL program source code (UNIX)</td>
</tr>
<tr>
<td>PM</td>
<td>Presentation Manager Bitmaps Graphics</td>
</tr>
<tr>
<td>POT</td>
<td>Microsoft PowerPoint</td>
</tr>
<tr>
<td>PPT</td>
<td>Microsoft PowerPoint</td>
</tr>
<tr>
<td>PPS</td>
<td>Microsoft PowerPoint</td>
</tr>
<tr>
<td>PPS</td>
<td>Microsoft PowerPoint</td>
</tr>
<tr>
<td>RTF</td>
<td>Rich Text Format document</td>
</tr>
<tr>
<td>SCR</td>
<td>Fax/screensaver/snapshot, script for Faxview/Microsoft Windows</td>
</tr>
<tr>
<td>SH</td>
<td>Shell Script (UNIX)</td>
</tr>
<tr>
<td>SHB</td>
<td>Corel Show Background file</td>
</tr>
<tr>
<td>SHS</td>
<td>Shell scrap file</td>
</tr>
<tr>
<td>SMM</td>
<td>AmiPro</td>
</tr>
<tr>
<td>SYS</td>
<td>Device driver</td>
</tr>
<tr>
<td>VBE</td>
<td>VESA BIOS (Core Functions)</td>
</tr>
<tr>
<td>VBS</td>
<td>VBScript</td>
</tr>
<tr>
<td>VSD</td>
<td>Visio</td>
</tr>
<tr>
<td>VSS</td>
<td>Visio</td>
</tr>
</tbody>
</table>
Configuring scan options

Select file types and extensions to scan for viruses

For all scan types, you can select files to scan by program type and extension. For scheduled and manual scans, you can also select files to scan by extension and program type at the folder level.

To select files to scan by extension

1. In the Scan Options dialog box for the scan that you want to configure, click the appropriate Selected button.
2. Click Extensions.
3. In the Selected Extensions dialog box, you can select one of the following:
   - Add: Add your own extension by typing the extension and clicking Add.
   - Documents: Add all document extensions.
   - Programs: Add all program extensions.
   - Use Defaults: Add all extensions and program types.
4. Click OK until the Symantec System Center console appears.

To select files to scan by program type

1. In the Scan Options dialog box for the scan that you want to configure, click the appropriate Selected button.
2. Click Types.
3. In the Selected Types dialog box, select one of the following:
   - Document files: Scan document files regardless of their extensions.
   - Program files: Scan MS-DOS and Windows program files.
4. Click OK until the Symantec System Center console appears.

---

### Table 3-6: Recommended file extensions for scanning

<table>
<thead>
<tr>
<th>File extension</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VST</td>
<td>Visio</td>
</tr>
<tr>
<td>VXD</td>
<td>Virtual device driver</td>
</tr>
<tr>
<td>WSF</td>
<td>Windows Script File</td>
</tr>
<tr>
<td>WSH</td>
<td>Windows Script Host Settings File</td>
</tr>
<tr>
<td>XL?</td>
<td>Microsoft Excel</td>
</tr>
</tbody>
</table>

---

Select file types and extensions to scan for viruses

For all scan types, you can select files to scan by program type and extension. For scheduled and manual scans, you can also select files to scan by extension and program type at the folder level.

To select files to scan by extension

1. In the Scan Options dialog box for the scan that you want to configure, click the appropriate Selected button.
2. Click Extensions.
3. In the Selected Extensions dialog box, you can select one of the following:
   - Add: Add your own extension by typing the extension and clicking Add.
   - Documents: Add all document extensions.
   - Programs: Add all program extensions.
   - Use Defaults: Add all extensions and program types.
4. Click OK until the Symantec System Center console appears.

To select files to scan by program type

1. In the Scan Options dialog box for the scan that you want to configure, click the appropriate Selected button.
2. Click Types.
3. In the Selected Types dialog box, select one of the following:
   - Document files: Scan document files regardless of their extensions.
   - Program files: Scan MS-DOS and Windows program files.
4. Click OK until the Symantec System Center console appears.
To select files to scan by folder for manual scans
1. In the Symantec System Center console, right-click the object that you want to scan, and then click **All Tasks > Symantec AntiVirus > Start Manual Scan**.

2. In the Select Items dialog box, select the folders to scan.

3. Click **Options** and select the extensions and types to scan for the selected folders.

4. Click **OK** until the Symantec System Center console appears.

To select files to scan by folder for scheduled scans
1. In the Symantec System Center console, right-click the object that you want to scan, and then click **All Tasks > Symantec AntiVirus > Scheduled Scans**.

2. On the Server Scans tab, in the Server scans list, select a scan.

3. Click **Edit**.

4. In the Scheduled Scan dialog box, click **Scan Settings**.

5. In the Select Items dialog box, select the folders to scan.

6. Click **Options** and select the extensions and types to scan for the selected folders.

7. Click **OK** until the Symantec System Center console appears.

When you make selections in the tree, the icons change as listed in **Table 3-7**.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Icon]</td>
<td>Symantec Client Security will scan all of the files in this folder and also all of the files in subfolders.</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Symantec Client Security will scan one or more items that you’ve selected in the folder or one of the subfolders.</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Symantec Client Security will scan the selected file. This is available only from the client or server interface.</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Symantec Client Security does not scan the folder or subitems.</td>
</tr>
</tbody>
</table>
Enabling expanded threat categories

You can scan client or server objects for the following threat categories during manual scan and scheduled scans:

- Spyware
- Adware
- Dialers
- Joke programs
- Remote access programs
- Hack tools
- Trackware

See “About threats” on page 95.

Enable expanded threat scanning and exclude threat categories if necessary

By default, Symantec Client Security does not scan for threats other than viruses and blended threats. You must enable expanded threat scanning.

You can also exclude an expanded threat category for which you don’t want Symantec Client Security to scan.

To enable expanded threat scanning

1. In the Symantec System Center console, do one of the following:
   - Right-click a server or client computer.
   - Select one or more servers that are in the same server group, and then right-click the servers.
   - Select one or more clients that are managed by the same server, and then right-click the clients.

2. Click All Tasks > Symantec AntiVirus > Start Manual Scan.

3. In the Select Items dialog box, click Options.

4. In the Scan Options dialog box, click Scan for expanded threats.

5. Click Save Settings if you want Symantec Client Security to remember these options for future manual scans on this computer. Symantec Client Security also remembers these settings for future scans when you select multiple computers.
Scanning for viruses and other threats
Configuring scan options

To exclude an expanded threat category from scanning

1  In the Symantec System Center console, do one of the following:
   ■  Right-click a server or client computer.
   ■  Select one or more servers that are in the same server group, and then right-click the servers.
   ■  Select one or more clients that are managed by the same server, and then right-click the clients.

2  Click All Tasks > Symantec AntiVirus > Start Manual Scan.

3  In the Select Items dialog box, click Options.

4  In the Scan Options dialog box, ensure that Scan for expanded threats is enabled.

5  Click Exclusions.

6  In the Select Items dialog box, uncheck each threat category that you want to exclude.

7  Click OK until you return to the Scheduled Scans dialog box.
Setting options for scanning compressed files

Table 3-8 lists and describes the scanning options that are available for compressed files.

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Scanning option</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>Symantec Client Security scans compressed files during manual, email, and scheduled scans. Because of the significant processing overhead, Auto-Protect does not scan files that are within compressed files on Windows computers; however, the files are scanned as they are extracted from compressed files.</td>
</tr>
<tr>
<td>NetWare</td>
<td>Symantec Client Security scans compressed files during Auto-Protect and scheduled scans. In order to scan the contents of a compressed file, Symantec Client Security extracts each file, one file at a time, from the container and copies it to the SYS volume where it is scanned. The SYS volume must have enough space available on the volume to accommodate the largest file in the container.</td>
</tr>
</tbody>
</table>

In the Scan Advanced Options dialog box, you can set options for scanning compressed files that are nested within compressed files. If you check Scan Inside Compressed Files, Symantec Client Security scans the container (such as Files.zip) and the contents of the container, which are the individual, compressed files. Symantec Client Security supports a maximum depth of ten levels of nested compressed files; NetWare servers are limited to eight levels.

Note: You cannot stop a scan that is in progress on a compressed file. If you click Stop Scan, Symantec Client Security stops the scan only after it has finished scanning the compressed file.

Configuring HSM settings

Symantec Client Security includes settings that allow you to fine tune scans of files that are maintained by Hierarchical Storage Management (HSM) and offline backup systems. An HSM system migrates files to secondary storage such as CD-ROM, tape jukebox, SAN storage, and so on, but it may leave parts of the original file on the disk. Performance and disk space issues arise during scans if Symantec Client Security opens all of the stubs and the HSM system places the files back on the original disk. Consult your HSM or backup vendor to select the appropriate settings. The settings are dependent on how your HSM application operates.
Table 3-9 lists HSM scanning options for Windows 2000 and later.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Skip offline files</td>
<td>If the offline bit is set, the file is skipped. A small clock over a file’s icon in Windows Explorer indicates that the offline bit is set. Any application may set the offline bit without actually placing the file offline.</td>
</tr>
<tr>
<td>Skip offline and sparse files</td>
<td>Some applications set the file sparse bit to indicate that part of the file is not present on the disk. Because some HSM products set this bit and others don't, consult your HSM vendor to verify whether the sparse bit is set. With a sparse file, a stub of the file remains on the disk with the majority of the file moved to offline storage.</td>
</tr>
<tr>
<td>Skip offline and sparse files with a reparse point</td>
<td>Some vendors use reparse points. An application that uses reparse points will also use an appropriate device driver to manage reparse points in the files. This is the default Symantec Client Security setting because it is the most reliable for vendors that use reparse points. Consult your HSM vendor to determine if this setting is appropriate. With a reparse point, a portion of the file remains on disk with the remainder transparently accessed through an application filter (the device driver).</td>
</tr>
<tr>
<td>Scan resident portions of offline and sparse files</td>
<td>Symantec Client Security identifies resident portions of a file. If the file is sparse, only the resident portion is scanned; the nonresident portion remains in secondary storage. Because some vendors support this capability and others do not, consult your HSM vendor to determine if this setting is appropriate.</td>
</tr>
<tr>
<td>Scan all files, forcing demigration (fills drive)</td>
<td>The entire file is scanned, which forces demigration from secondary storage if necessary. Because the size of the secondary storage is usually greater than the size of the local volume, this setting may fill the local volume and cause further files that are opened for scanning to fail.</td>
</tr>
</tbody>
</table>
To configure HSM settings

◆ In the Scan Advanced Options dialog box, for the type of scan that you want to configure, select the appropriate options.

---

**Table 3-9** Storage migration options (Windows 2000 and later)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Scan all files without forcing demigration (slow) | Symantec Client Security copies a file from secondary storage to the local hard drive as a temp file for scanning, but the HSM application leaves the original file on the secondary storage.  
   This method is slow and not supported by all HSM vendors. Because a file is copied from secondary storage to a disk for scanning, resource demand is high. Processor and network performance may further degrade as infected content is detected when a repair or deletion is returned to secondary storage. |
| Scan all files recently touched without forcing demigration | To reduce some of the resource demand issues with the Scan all files without forcing demigration option, this option lets you specify that only files that have been migrated recently and may still reside on faster secondary storage are scanned. It may be appropriate to scan files if they still reside on the faster secondary disk, and skip demigration and scanning if the files reside on the slow, long-term storage.  
   For example, files may first be migrated to a remote disk after 30 days of no access. After 60 days of no access, the file is migrated to CD-ROM or remote SAN storage. In many cases, this method may still be slow because accessing files without forcing demigration is a relatively slow operation. |
| Open files using backup semantics           | You can allow scanning of files that, for security reasons, are normally not readable except by a specific user.                                |

---

**Table 3-10** lists the HSM scanning option for NetWare.

**Table 3-10** Storage migration option (NetWare)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan NetWare compressed or migrated files</td>
<td>NetWare compressed or migrated files are scanned.</td>
</tr>
</tbody>
</table>
Setting CPU utilization

For scheduled and manual scans, Symantec Client Security allows you to control the scan’s CPU priority. Giving a scan a lower priority means that the scan will take longer to complete, but also frees the CPU to work on other tasks. You may want to set a lower priority in some situations. For example, if you have scans running at lunch time during the work week, you might want to lower the scan priority to minimize the impact on user productivity.

You set scan priority using sliders in the Scan Options dialog box. You can specify scan priority for:

- **Windows computers**: Priority differs depending on whether the computer is idle or not idle. The idle setting specifies the priority that is assigned to scans when the computer is idle. The not idle setting specifies the priority that is assigned to scans when the computer is actively working.

- **NetWare computers**: Symantec Client Security can throttle its load on NetWare servers. A lower load setting means the server scan will take longer to complete.
Updating virus definitions files

This chapter includes the following topics:

- About virus definitions files
- Virus definitions files update methods
- Updating virus definitions files on Symantec Client Security servers
- Updating virus definitions files on Symantec Client Security clients
- Controlling virus definitions files
- Testing virus definitions files
- Update scenarios
- About scanning after updating virus definitions files

About virus definitions files

Virus definitions files contain sample code for thousands of threats. When Symantec Client Security scans for threats, it attempts to find matches between your files and sample code that is inside of the virus definitions files. If Symantec Client Security finds a match, the file may be infected.

Every server and client that runs Symantec Client Security has a copy of the virus definitions files. These files can become outdated as new viruses and other threats are discovered. Symantec updates virus definitions files about once a week, or more frequently if needed. It’s important to keep virus definitions files current to maintain the highest level of protection for your network.
Virus definitions files update methods

There are several methods that are available for downloading virus definitions and setting up servers and clients to retrieve them.

Table 4-1 describes the virus definitions files update methods.

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
<th>When to use it</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virus Definition Transport Method</td>
<td>A push operation starts when new virus definitions are received via the Symantec FTP site or LiveUpdate server by a primary server on your network. The primary server passes a virus definitions package to all of the secondary servers in the server group. Secondary servers extract the definitions and place them in the appropriate directory. Clients receive the package from their parent servers. Clients extract the definitions and place them in the appropriate directory.</td>
<td>Use the Virus Definition Transport Method when you want to control virus definitions files updates from the Symantec System Center. In addition, use this method during a virus outbreak to push the latest virus definitions files to the computers on your network immediately.</td>
</tr>
<tr>
<td>LiveUpdate</td>
<td>A scheduled pull operation starts when a client or server on which LiveUpdate is being used requests new definitions. LiveUpdate may be configured on each computer to request the update from a designated internal LiveUpdate server or directly from the Symantec LiveUpdate server.</td>
<td>Use LiveUpdate when you want protected computers to pull virus definitions files updates from an internal LiveUpdate server, or directly from Symantec.</td>
</tr>
<tr>
<td>Central Quarantine polling</td>
<td>The Central Quarantine Server periodically polls the Symantec Digital Immune System gateway for new virus definitions files. When new definitions are available, the Central Quarantine Server can push the new definitions to the computers that need it automatically.</td>
<td>Use Central Quarantine when you want to automate the distribution of virus definitions files updates across your network.</td>
</tr>
</tbody>
</table>
Updating virus definitions files

Virus definitions files update methods

Note: 64-bit computers receive virus definitions files using LiveUpdate. All other methods of updating these files are not supported.

Best practice: Using the Virus Definition Transport Method and LiveUpdate together

You can use the Virus Definition Transport Method and LiveUpdate together. Using LiveUpdate allows for updates to the software components of Symantec Client Security. Using the Virus Definition Transport Method allows you to schedule and push virus definitions files updates from the Symantec System Center. In addition, you can use the Virus Definition Transport Method as an emergency system for distributing new virus definitions files quickly when the network is threatened by a new virus.

Although the Virus Definition Transport Method is used more often, some large networks depend on LiveUpdate. These installations do not permit direct access to the Symantec site by a large number of servers and clients. One or more servers act as an internal LiveUpdate server to all of the other servers on the network, and in some installations, to all clients.

Best practice: Using Continuous LiveUpdate on 64-bit computers

To ensure that each managed 64-bit computer maintains the latest virus definitions, you can use Continuous LiveUpdate to require each computer to check for updates after a specified interval has expired. If you have more than one 64-bit computer on your network and you are using the Symantec System Center console, you can group these computers into a client or server group and manage the virus definitions from the console. If you are not using the console, you can enable this feature and set the interval on the client computer.

See “Enabling and configuring Continuous LiveUpdate for managed clients” on page 170.

Table 4-1 Virus definitions files update methods

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
<th>When to use it</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intelligent Updater</td>
<td>Intelligent Updater is a self-extracting executable file that contains virus definitions files.</td>
<td>Use Intelligent Updater when you need to distribute virus definitions files updates to users who do not have active network connections.</td>
</tr>
</tbody>
</table>

Note: 64-bit computers receive virus definitions files using LiveUpdate. All other methods of updating these files are not supported.
Updating virus definitions files on Symantec Client Security servers

There are several methods for updating virus definitions files on servers:

- Virus Definition Transport Method
- LiveUpdate
- Intelligent Updater
- Central Quarantine polling

See “Virus definitions files update methods” on page 152.

Updating and configuring Symantec Client Security servers using the Virus Definition Transport Method

Update Symantec Client Security servers manually when you need to force an immediate update. Schedule automatic updates to handle routine virus definitions files updating without requiring further interaction.

Update servers manually or automatically using the Virus Definition Transport Method

You can update servers manually or automatically. Updates occur only when the virus definitions files on a server are older than the definitions that are available on the LiveUpdate server.

To update all unlocked servers in the system

1. In the Symantec System Center console, right-click System Hierarchy, and then click Symantec AntiVirus > Update Virus Defs Now.
2. Click Yes in the confirmation dialog box.
3. Click OK in the status dialog box.

To update servers manually

1. In the Symantec System Center console, right-click a server or server group, and then click All Tasks > Symantec AntiVirus > Virus Definition Manager.
2. Select one of the following:
   - Update The Primary Server Of This Server Group Only: To update all servers in the group from the primary server
   - Update Each Server In This Server Group Individually: To update servers individually
The option that you select affects all of the servers in the server group, whether you right-click a server group or an individual server.

3  Click \textit{Configure}.

4  Click \textit{Update Now}.
   A message appears with information about how you can view the date of the new virus definitions file.

5  Read the information that appears, and then click \textit{OK} until the Symantec System Center console reappears.

\textbf{To update servers automatically}

1  In the Symantec System Center console, right-click a server or server group, and then click \textit{All Tasks} > \textit{Symantec AntiVirus} > \textit{Virus Definition Manager}.

2  Select one of the following:
   \begin{itemize}
   \item Update The Primary Server Of This Server Group Only: To update all servers in the group automatically from the primary server
   \item Update Each Server In This Server Group Individually: To update servers individually
   \end{itemize}
   The option that you select affects all servers in the server group, whether you right-click a server group or an individual server.

3  Click \textit{Configure}.

4  Ensure that Schedule For Automatic Updates is checked, and then click \textit{Schedule}.

5  Select options to determine when the virus definitions file will update (for example, every Tuesday at 10:00 P.M.).

6  Click \textit{OK} until you return to the Symantec System Center main window.

\textbf{Updating a master primary server}

Configure a master primary server to limit your network’s exposure to the Internet.

\textbf{To configure a master primary server}

1  In the Symantec System Center console, right-click a server, and then click \textit{All Tasks} > \textit{Symantec AntiVirus} > \textit{Virus Definition Manager}.

2  In the Virus Definition Manager dialog box, click \textit{Update the Primary Server of this Server Group only}.

3  Click \textit{Configure}.
4 In the Configure Primary Server Updates dialog box, click Source.

5 In the Setup Connection dialog box, in the Update definition file via list, click Another Protected Server, and then click Configure, if necessary.

6 In the Configure Update From Server dialog box, select the master primary server from the list of servers that appears.

7 Click OK.

8 Click OK.

9 In the Configure Primary Server Updates dialog box, do one of the following:
   - Click Update Now to retrieve the virus definitions files from the master primary server immediately.
   - Click Schedule For Automatic Updates, and then click Schedule and set a frequency and time when the server will check for updates on the master primary server to schedule automatic updates.

10 Click OK until you return to the Symantec System Center main window.

Updating NetWare servers using the Virus Definition Transport Method

Updating a NetWare server is similar to updating other types of servers with the following differences:

- You can designate a NetWare server as the primary server for your network, or designate a Windows NT/2000 computer as the primary server. If your NetWare servers are running on faster computers or have a higher bandwidth connection than your Windows NT/2000 servers, you can designate a NetWare server as a primary server for increased performance.

- NetWare primary servers must have TCP/IP and FTP running (FTP is not enabled by default on NetWare servers), and must be able to connect to the Internet. In addition, NetWare environments require a Windows NT/2000 computer to run the Symantec System Center console.

- NetWare servers do not store the addresses of Windows NT/2000 servers in their address caches. As a result, if your NetWare server is not running TCP/IP and is not using a domain naming system (DNS) server, you might have difficulty updating a NetWare server from a Windows NT/2000 server that resides in a different server group.
To update NetWare servers without TCP/IP

- Temporarily move the NetWare server into a server group that has a Windows NT server that is running the IPX protocol. After one day, you can move the NetWare server back to its original server group. This adds the Windows NT/2000 server address to the NetWare server’s address cache, which lets the NetWare server locate the Windows NT/2000 server to obtain the updated virus definitions file.

Figure 4-1 shows you one way you could configure virus definitions files updates for your computer if you have a small network of six file servers divided into two server groups.
Configure a primary server to retrieve the latest virus definitions files updates; you can download through FTP or another computer. Enable virus definitions file sharing so that Symantec Client Security servers in server group A automatically retrieve the latest updates from primary server 1. Clients automatically receive the updates from their parent servers. Configure primary server 2 to retrieve the latest update from primary server 1. This makes primary server 1 a master primary server. Symantec Client Security servers in server group B receive updates from their primary server. Clients automatically receive updates from their Symantec Client Security servers.
Figure 4-2 illustrates how you might configure virus definitions files updates if your organization has multiple sites that are linked over a wide area network (WAN).

**Figure 4-2**  
Virus definitions file updating for multiple sites over a WAN

Server group primary servers on separate WANs retrieve the update from the Symantec FTP site or LiveUpdate server. Primary servers distribute the update to primary servers in other server groups in their local networks. The primary servers distribute the update to other protected servers and clients in their server group.
Updating servers using LiveUpdate

Depending on the size of your network, you can use LiveUpdate to update virus definitions files in the following ways:

- For smaller networks (less than 1000 nodes), configure managed servers to directly retrieve updates from the Symantec FTP site, Symantec LiveUpdate server, or an internal LiveUpdate server.
- For larger networks (greater than 1000 nodes), set up an internal LiveUpdate server, download updates to that server, and have your managed servers retrieve updates from the internal LiveUpdate server.

Updating Symantec Client Security servers from the Symantec FTP site or LiveUpdate server

You need to configure updating for the primary server in each server group to ensure that its virus definitions files are current. You can also configure individual servers to update directly from Symantec.

Update Symantec Client Security servers directly from the Symantec FTP site or LiveUpdate server

You can update all of the Symantec Client Security servers in a server group from a primary server, or update each server in the group individually.

To update primary servers

1. In the Symantec System Center console, right-click a server group, and then click **All Tasks > Symantec AntiVirus > Virus Definition Manager**.
2. In the Virus Definition Manager dialog box, click **Update The Primary Server Of This Server Group Only**.
3. Click **Configure**.
4. In the Configure Primary Server Updates dialog box, do one of the following:
   - Click **Update Now** to launch a LiveUpdate session immediately.
   - Click **Schedule For Automatic Updates**, and then click **Schedule** to set a frequency and time when the server will run a LiveUpdate session.
5. Click **OK**.
6. In the Configure Primary Server Updates dialog box, click **Source**.
7. In the Update definition file via list, click **LiveUpdate**.
8. Click **OK** until you return to the Symantec System Center main window.
To update individual servers from the Symantec FTP site or LiveUpdate server

1. In the Symantec System Center console, right-click a server group, and then click **All Tasks > Symantec AntiVirus > Virus Definition Manager.**
2. In the Virus Definition Manager dialog box, click **Update Each Server In This Server Group Individually.**
3. Click **Configure.**
4. In the Configure Primary Server Updates dialog box, click **Source.**
5. Click **LiveUpdate (Win32)/FTP (NetWare).**
6. Click **OK.**
   If you are configuring a NetWare server, make sure that the server is running FTP.
7. Do one of the following:
   - Click **Update Now** to launch a LiveUpdate session immediately.
   - Click **Schedule For Automatic Updates**, and then click **Schedule** to set a frequency and time when the server will run a LiveUpdate session.
8. Click **OK** until you return to the Symantec System Center main window.

**Updating servers from an internal LiveUpdate server**

You can set up an internal LiveUpdate server on any computer. If you use a Symantec Client Security server as an internal LiveUpdate server, you can use the standard update methods that are available in the Virus Definition Manager dialog box to manually and automatically update the virus definitions files on that server. If you use a computer that does not run Symantec Client Security as an internal LiveUpdate server, use the LiveUpdate Administration Utility to update the virus definitions on that server.

See “Updating servers using LiveUpdate” on page 160.

For more information, see the *LiveUpdate Administrator’s Guide.*

**To update servers from an internal LiveUpdate server**

1. In the Symantec System Center console, right-click a server group, and then click **All Tasks > LiveUpdate > Configure.**
2. In the Configure LiveUpdate dialog box, click **Internal LiveUpdate Server.**
3 Set the following internal LiveUpdate server options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the server. This name will appear when you run LiveUpdate.</td>
</tr>
<tr>
<td>Location</td>
<td>This box is optional. You can type descriptive information that is related to the server (for example, the name of the site).</td>
</tr>
<tr>
<td>Login Name</td>
<td>The logon name that is associated with the server. Leave this box blank so that users can log on and retrieve the files without typing information.</td>
</tr>
<tr>
<td>Login Password</td>
<td>The logon password that is associated with the server. Leave this box blank so that users can log on and retrieve the files without typing information.</td>
</tr>
</tbody>
</table>
| URL or IP Address | If you are using the FTP method (recommended), under Type, you can click FTP, and then type the FTP address for the server. For example: ftp.myliveupdateserver.com  
If you are using the HTTP method, under Type, you can click HTTP, and then type the URL for the server. For example: http:\\myliveupdateserver.com or 155.66.133.11\Export\Home\Ludepot  
If you are using the LAN method, under Type, you can click LAN, and then type the server UNC path name. For example: \\Myserver\LUDepot  
In the Login box, type the name and password to access the server. |

If you leave the Login Name and Login Password boxes empty, an anonymous logon will be used. This requires that anonymous logons be enabled on the FTP server. If your policy prohibits anonymous logons on FTP servers, type the logon name and password for the FTP server and directory that will be accessed.

4 Click OK until you return to the Symantec System Center main window.

**Specifying multiple internal LiveUpdate servers for failover support**

To compensate for unavailable internal LiveUpdate servers, Symantec Client Security supports multiple internal LiveUpdate servers.
Updating servers with Intelligent Updater

To distribute updated virus definitions, download a new Intelligent Updater, and then use your preferred distribution method to deliver the updates to your managed servers and clients. Intelligent Updater is available as a single file or as a split package, which is distributed across several smaller files. The single file is for computers with network connections. The split package can be copied to floppy disks and used to update computers that do not have network connections or Internet access.

Update servers with Intelligent Updater files

Download Intelligent Updater from the Symantec Web site, and then install Intelligent Updater to servers with the latest virus definitions files.

Note: Make sure to use Intelligent Updater files for Symantec Client Security rather than the consumer version of the product.

To download Intelligent Updater

1. Using your Web browser, go to: http://securityresponse.symantec.com
2. Click Download Virus Definitions.
3. Click Download Updates (Intelligent Updater Only).
4. Select the appropriate language and product.
5. Click Download Updates.
6. Click the file with the .exe extension.
7. When you are prompted for a location in which to save the files, select a folder on your hard drive.

To install the virus definitions files

1. Locate the Intelligent Updater file that you downloaded from Symantec.
2. Double-click the file and follow the on-screen instructions.

Updating servers using Central Quarantine polling

If you use Symantec Central Quarantine, you can configure the Central Quarantine Server to periodically poll the Digital Immune System gateway for new virus definitions files. When new definitions are available, the Central Quarantine Server can automatically push the new definitions to the computers that need it, using the Virus Definition Update Method.
For more information, see the *Symantec Central Quarantine Administrator’s Guide*.

**Minimizing network traffic and handling missed updates**

LiveUpdate provides advanced scheduling options for minimizing network traffic and handling missed updates. Table 4-2 describes LiveUpdate scheduling options.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>When to use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Randomization options</td>
<td>Randomizes updates:</td>
<td>When you want to stagger updates for multiple computers to minimize the impact on network traffic. By default, Symantec Client Security randomizes LiveUpdate sessions to minimize bandwidth spikes.</td>
</tr>
<tr>
<td></td>
<td>■ Plus or minus a specified number of minutes of the scheduled time</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Any day of the week within a specified time interval</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Any day of the month plus or minus a specified number of days of the scheduled date</td>
<td></td>
</tr>
<tr>
<td>Missed Event options</td>
<td>Determines how missed LiveUpdate events will be handled. An event might be missed if a computer is turned off when the LiveUpdate session is scheduled to run. You can set options so that scheduled LiveUpdate events that were missed run at a later time.</td>
<td>To ensure that computers that are unavailable for a regularly scheduled LiveUpdate event will attempt to pull definitions at a later time.</td>
</tr>
</tbody>
</table>

**Minimize network traffic and handle missed updates**

You can set separate randomization schedules for Symantec Client Security servers and clients on your network to minimize the impact on network traffic.

You can specify separate policies for handling missed LiveUpdate events for Symantec Client Security servers and clients.
To randomize the LiveUpdate schedule for servers

1. In the Symantec System Center console, right-click a server or server group, and then click **All Tasks > Symantec AntiVirus > Virus Definition Manager.**
2. In the Virus Definition Manager dialog box, click **Configure.**
3. In the Configure Primary Server Updates dialog box, check **Schedule For Automatic Updates.**
4. Click **Schedule.**
5. Set the frequency and time when the server will check for updates.
6. In the Virus Definition Update Schedule dialog box, click **Advanced.**
7. In the Advanced Scheduled Options dialog box, under Randomization Options, check **Options,** and then set the minutes, day of the week, or day of the month options.
8. Click **OK** until you return to the Symantec System Center main window.

To randomize the LiveUpdate schedule for clients

1. In the Symantec System Center console, right-click a server or server group, and then click **All Tasks > Symantec AntiVirus > Virus Definition Manager.**
2. In the Virus Definition Manager dialog box, check **Schedule Client For Automatic Virus Definition Updates Using LiveUpdate.**
3. In the Virus Definition Update Schedule dialog box, click **Schedule.**
4. Set the frequency and time when the clients will check for updates.
5. Click **Advanced.**
6. In the Advanced Schedule Options dialog box, under Randomization Options, check **Options,** and then set the minutes, day of the week, or day of the month options.
7. Click **OK** until you return to the Symantec System Center main window.

To handle missed LiveUpdate events for servers

1. In the Symantec System Center console, right-click a server or server group, and then click **All Tasks > Symantec AntiVirus > Virus Definition Manager.**
2. In the Virus Definition Manager dialog box, click **Configure.**
3. Click **Schedule for Automatic Updates.**
4. In the Configure Primary Server Updates dialog box, click **Schedule.**
In the Virus Definition Update Schedule dialog box, click **Advanced**.

In the Advanced Schedule Options dialog box, check **Handle Missed Events Within**.

Set the time limit within which you want the scan to run.
For example, you might want a weekly LiveUpdate event to run only if it is within three days after the scheduled time for the missed event.

Click **OK** until you return to the Symantec System Center main window.

**To handle missed LiveUpdate events for clients**

1. In the Symantec System Center console, right-click a server or server group, and then click **All Tasks > Symantec AntiVirus > Virus Definition Manager**.

2. In the Virus Definition Manager dialog box, click **Schedule Client For Automatic Virus Definition Updates Using LiveUpdate**.

3. Click **Schedule**.

4. In the Virus Definition Update Schedule dialog box, click **Advanced**.

5. Check **Handle Missed Events Within**.

6. Set the time limit within which you want the scan to run.
For example, you may want a weekly LiveUpdate event to run only if it is within three days after the scheduled time for the missed event.

7. Click **OK** until you return to the Symantec System Center main window.

**Updating virus definitions files on Symantec Client Security clients**

You can update the virus definitions files on Symantec Client Security clients using any of the following:

- Virus Definition Transport Method
- LiveUpdate
- Intelligent Updater
  - See “Specifying multiple internal LiveUpdate servers for failover support” on page 162.
- Central Quarantine polling
  - See “Updating servers using Central Quarantine polling” on page 163.

See “Virus definitions files update methods” on page 152.
**Update virus definitions files on Symantec Client Security clients**

You can update Symantec Client Security clients using the Virus Definition Transport Method, LiveUpdate, or both.

**Note:** LiveUpdate is the only method for updating virus definitions files that is supported on 64-bit computers.

**To update clients using the Virus Definition Transport Method**

1. In the Symantec System Center console, right-click a server group, and then click **All Tasks > Symantec AntiVirus > Virus Definition Manager**.
2. In the Virus Definition Manager dialog box, check **Update Virus Definitions From Parent Server**.
3. Click **Settings**.
4. In the Update Settings dialog box, set the frequency with which the parent server will push updates.
5. Click **OK**.
6. In the Virus Definition Manager dialog box, uncheck **Schedule Client for Automatic Updates using LiveUpdate**.
7. Click **OK** until you return to the Symantec System Center main window.

**To update clients using LiveUpdate**

1. In the Symantec System Center console, right-click a server group, and then click **All Tasks > Symantec AntiVirus > Virus Definition Manager**.
2. In the Virus Definition Manager dialog box, check **Schedule Client For Automatic Updates Using LiveUpdate**.
3. Click **Schedule**.
4. In the Virus Definition Update Schedule dialog box, select the frequency, day, and time that you want the update to occur.
5. Click **OK** until you return to the Symantec System Center main window.

**To update clients using both the Virus Definition Transport Method and LiveUpdate**

1. In the Symantec System Center console, right-click a server group, and then click **All Tasks > Symantec AntiVirus > Virus Definition Manager**.
2. In the Virus Definition Manager dialog box, check **Update Virus Definitions from Parent Server**.
3 Check **Schedule Client For Automatic Updates Using LiveUpdate**.

4 Click **Schedule**.

5 In the Virus Definition Update Schedule dialog box, select the frequency, day, and time that you want the update to occur.

6 Click **OK**.

7 Click **Settings**.

8 In the Update Settings dialog box, set the frequency with which the parent server will push updates.

9 Click **OK** until you return to the Symantec System Center main window.

### Updating virus definitions files on Symantec Client Security clients immediately

You can force clients to update virus definitions files immediately using LiveUpdate. This feature is available for clients that normally receive updates using LiveUpdate or the Virus Definition Transport Method.

This feature provides a good way to update virus definitions files when one or more clients on which LiveUpdate is installed are using outdated files for some reason (for example, when an update operation that was performed at the server group level succeeded on all but several clients).

---

**Warning**: Updating a large number of clients immediately can result in slow performance. Once you start this operation, you cannot cancel it. Do not use this feature to update virus definitions files during a virus outbreak. See “Handling a virus outbreak on your network” on page 181.

---

**Update virus definitions files on Symantec Client Security clients immediately**

Before you can update virus definitions files, you must specify the number of clients to update. When the number of selected clients exceeds this number, a confirmation dialog box appears to verify that you want to exceed the administrator-specified number.
To specify the number of clients to update immediately

1. In the Symantec System Center console, on the Tools menu, click **SSC Options**.

2. In the SSC Properties window, on the Client Filter tab, select the number of multi-selected clients to update before a confirmation dialog box appears.

3. Click **OK**.

To update one or more clients immediately with LiveUpdate

1. In the Symantec System Center console, right-click one or more clients in the right pane, and then click **All Tasks > Symantec AntiVirus > Update Virus Defs Now**.

2. If you selected more than the administrator-specified number of clients, in the confirmation dialog box, select one of the following:
   - **Yes**
   - **Cancel**

   If a client is configured to update using the Virus Definition Transport Method, Symantec Client Security prompts you to allow LiveUpdate to run.

3. Click **OK** in the status dialog box.

Configuring managed clients to use an internal LiveUpdate server

You can configure LiveUpdate settings for managed computers running Symantec Client Security client from the Symantec System Center. For unmanaged Symantec Client Security clients, use the LiveUpdate Administration Utility to create a custom .hst file.

For information on configuring LiveUpdate for unmanaged Symantec Client Security clients, see the **LiveUpdate Administrator’s Guide**.

To configure a managed Symantec Client Security client to use an internal LiveUpdate server

1. Right-click a parent server, and then click **All Tasks > LiveUpdate > Configure**.

2. In the Configure LiveUpdate dialog box, click **Internal LiveUpdate Server**.

3. If you are using an FTP or HTTP server, type the appropriate data in the Login Name and Password boxes.

4. In the Connection box, type one of the following:
   - The UNC path to your shared folder
   - The URL or IP address for your FTP or HTTP server
5 In the Type list, select one of the following:
- LAN
- FTP
- HTTP

6 Click OK until you return to the Symantec System Center main window. If you are using multiple parent servers, repeat steps 1–6 for each parent server so that all Symantec Client Security clients and servers receive the changes. You can also configure LiveUpdate for an entire group by right-clicking the server group.

Enabling and configuring Continuous LiveUpdate for managed clients

If a managed Symantec Client Security client infrequently connects to its parent server (for example, a notebook computer that is used offsite), it may not receive the most current virus definitions files updates. For these computers, Continuous LiveUpdate offers a backup option for receiving updates directly from Symantec whenever the computer connects to the Internet.

With Continuous LiveUpdate, you can specify a maximum number of days that the virus definitions files on a Symantec Client Security computer can be out-of-date before an update is forced. When the Symantec Client Security client determines that its virus definitions files exceed their maximum age, it initiates a silent (no user interaction required) LiveUpdate session when it connects to the Internet.

Enable and configure Continuous LiveUpdate

You can enable Continuous LiveUpdate using the Symantec System Center, or by changing registry values on Symantec Client Security clients. You can then configure Continuous LiveUpdate options by adding values to the client’s registry.

To enable Continuous LiveUpdate using the Symantec System Center

1 In the Symantec System Center console, right click a server group, a Symantec Client Security server, a client group, or an individual Symantec Client Security client, and then click All Tasks > Symantec AntiVirus > Virus Definition Manager.

2 In the Virus Definition Manager dialog box, check Enable Continuous LiveUpdate.

3 Click OK until you return to the Symantec System Center main window.
To enable Continuous LiveUpdate by changing registry values

1. Using Regedit, navigate to:
   \HKEY_LOCAL_MACHINE\SOFTWARE\INTEL\LANDesk\VirusProtect6\CurrentVersion\PatternManager

2. Add EnableAdminForcedLU as a new DWORD.

3. Set the value of the DWORD to one of the following values:
   - 1: Enable
   - 0: Disable

To configure Continuous LiveUpdate

Configure Continuous LiveUpdate using the following registry values:

- EnableAdminForcedLU
  - Set to 0 to disable Continuous LiveUpdate or set to 1 to enable it.

- MaxDefsDaysOldAllowed
  - Specify the age (in days) that the definition can be before Symantec Client Security executes a silent LiveUpdate.

- AdminForcedLUCheckInterval
  - Specify the interval (in minutes) to check for old definitions.

- AFLUDelay
  - Set the startup delay time (between 10 and 180 minutes) of the Continuous LiveUpdate feature. This delay time is only valid if the feature is enabled. The actual delay time is a random number between 8 and N+8 where N is the value in the registry key. The default value is 30 minutes.

Note: You should set the MaxDefsDaysOldAllowed value to 8 days or higher. Lower settings may cause problems if you need to perform a virus definitions files rollback, since the age of the definitions files that you want to roll back to may exceed the maximum number of days that Continuous LiveUpdate will allow before forcing an update.

Setting LiveUpdate usage policies

You can set LiveUpdate usage policies for managed clients. When these policies are enabled, they are dimmed on the client. The policies determine whether the following activities can be performed at the client level:
Updating virus definitions files

Controlling virus definitions files

- Change the LiveUpdate schedule.
- Manually launch LiveUpdate.

To set LiveUpdate usage policies

1. In the Symantec System Center console, right-click a server or server group, and then click All Tasks > Symantec AntiVirus > Virus Definition Manager.

2. In the Virus Definition Manager dialog box, do one of the following:
   - Check Do Not Allow Client To Modify LiveUpdate Schedule to prevent the LiveUpdate schedule from being modified on the client. (Schedule Client For Automatic Updates Using LiveUpdate must be checked or this box is dimmed.)
   - Uncheck Download Product Updates Using LiveUpdate to prevent application updates.
   - Uncheck Do Not Allow Client To Manually Launch LiveUpdate to prevent LiveUpdate from being manually launched on the client.

Note: When Do Not Allow Client To Modify LiveUpdate Schedule or Do Not Allow Client To Manually Launch LiveUpdate is unchecked, LiveUpdate can run on the client at any time.

Controlling virus definitions files

The Symantec System Center console provides a set of tools for controlling the deployment of virus definitions files on your network. Use these tools to do the following:

- Verify the dates of virus definitions files on servers.
- View the virus lists on servers and clients.
- Roll back to a previous virus definitions file (network-wide).

If new virus definitions files are causing false positives or other problems for a server, you can verify the version number of the virus definitions files on that computer and then deploy an earlier definitions set from the Symantec System Center console. All servers and clients in that server group will roll back to the specified virus definitions files. You can also control the version of the virus definitions files used on all servers and clients in a server group. Users who download a virus definitions file that was not approved for company use can be forced to use the virus definitions file that you specify. Because you can easily
undo a virus definitions file rollout, you can release new virus definitions files in less time.

The Symantec System Center displays a warning icon if a virus definitions file is out-of-date on one or more computers that are managed by a parent server, server group, or client group.

To find a computer with outdated definitions
- Expand the server, server group, or client group and look for more warning icons.

Verifying the version number of virus definitions files

Using the Symantec System Center console, you can view the version number of the virus definitions files at the Symantec Client Security server, server group, client group, and individual Symantec Client Security client level.

To verify the version number of the virus definitions files
- In the Symantec System Center console, right-click a server group, client group, Symantec Client Security server, or client, and then click Properties. On the Symantec AntiVirus tab, in the Virus Definitions box, the file version is listed as a numerical date, followed by a version number.
- Once virus definitions files are updated on a computer, it may take several minutes before the information is available from the console.

Viewing the threat list

You can view a list of viruses and other threats, such as adware and spyware, that are detectable on a selected server or client. The threat list ensures that the selected computer is protected from a specific virus.

To view the threat list
1. In the Symantec System Center console, right-click a server or client, and then click All Tasks > Symantec AntiVirus > View Threat List.
2. Click Close.

Rolling back virus definitions files

You can roll back a virus definitions file for a server group. For example, if the most recent file generated false positive virus detections you might want to roll back to a previous file.
To roll back virus definitions files

1. In the Symantec System Center console, right-click a server or server group, and then click All Tasks > Symantec AntiVirus > Virus Definition Manager.

2. In the Virus Definition Manager dialog box, ensure that Update The Primary Server Of This Server Group Only is selected, and then click Configure.

3. In the Configure Primary Server Updates dialog box, click Definition File.

4. In the Select Virus Definition File dialog box, select the virus definitions file that you want to roll back to, and then click Apply.

5. Click Yes to change the current file.

6. Click OK until you return to the Symantec System Center main window.

Testing virus definitions files

Many administrators prefer to test virus definitions files on a test network before making them available on a production server. To test virus definitions files, complete the following tasks:

- Install Symantec Client Security server to a primary server on the test network.
- From the primary server on your test network, run LiveUpdate to download the virus definitions file.
- Go to www.eicar.org and download the antivirus test file to test the operation of the virus definitions file.
- Once testing is complete, copy the virus definitions file from the \Program files\Sav folder on the test server to a folder with the same name on the primary servers on your production network.
- Once the virus definitions files are on the primary servers, they will flow to other servers in the server group.

Note: Clients are configured to automatically retrieve virus definitions from their parent servers if Update Virus Definitions From Parent Server in the Virus Definition Manager dialog box is checked.
Update scenarios

The following scenarios show how administrators at two different companies perform updates:

- At Company A, the administrator downloads the new virus definitions file from the Symantec FTP site or Symantec LiveUpdate server to a primary server on the test network. He tests the virus definitions file. When testing is completed, he copies the virus definitions file to the master primary server on his production network. He has configured other primary servers so that they retrieve the update from the master primary server. All of the other connected computers use the Virus Definition Transport Method. Secondary servers retrieve the update from their primary server. Clients retrieve the update from their parent server.

- At Company B, the administrator downloads the new virus definitions file from the Symantec FTP site or Symantec LiveUpdate server to a test network. She tests the virus definitions file. When testing is completed, she downloads the new virus definitions file from the Symantec FTP site or Symantec LiveUpdate server to the internal LiveUpdate server on her production network. Some low risk users are allowed to go outside of the firewall. When LiveUpdate runs on their computers, virus definitions files are downloaded directly from the Symantec FTP site or Symantec LiveUpdate server.

About scanning after updating virus definitions files

If Auto-Protect is enabled, Symantec Client Security begins scanning with the updated virus definitions files immediately.

Once virus definitions files are updated, Symantec Client Security offers to attempt to repair files that are stored in Quarantine.

You can run a manual scan or schedule a scan to check for expanded threats, such as adware and spyware.

See “Scanning for viruses and other threats” on page 95.
Updating virus definitions files

About scanning after updating virus definitions files
Responding to virus outbreaks

This chapter includes the following topics:

- About responding to virus outbreaks
- Preparing for a virus outbreak
- Handling a virus outbreak on your network

About responding to virus outbreaks

Responding to virus outbreaks requires preparing before an outbreak occurs, and having a strategy in place for handling an outbreak should one occur.

In addition to installing Symantec Client Security on the servers and workstations in your network, preparing for a virus outbreak consists of the following tasks:

- Creating and reviewing a virus outbreak plan.
- Defining Symantec Client Security actions for handling viruses.
- Protecting your network from blended threats. A blended threat such as Code Red uses multiple exploits to attack computers. If you are using Symantec Client Security firewall client, install it on the workstations in your network. A strategy for handling virus outbreaks includes the following:
  - Enable virus alerts and messages.
  - Run a virus sweep of your network.
Responding to virus outbreaks

Preparing for a virus outbreak

To prepare for a virus outbreak, you should create a virus outbreak plan and define actions for handling suspicious files.

Creating a virus outbreak plan

An effective response to a virus outbreak on your network requires a plan that allows you to respond quickly and efficiently.

Table 5-1 outlines the tasks for creating a virus outbreak plan.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure that virus definitions files are current.</td>
<td>Verify that infected computers have the latest virus definitions files, and use the Virus Definition Transport Method to push new definitions if needed. See “About virus definitions files” on page 151.</td>
</tr>
</tbody>
</table>
| Map your network topology.          | Prepare a network topology map so that you can systematically isolate and clean computers by segment before you reconnect them to your local network. Your map should contain the following information:  
  ■ Server names and addresses  
  ■ Client names and addresses  
  ■ Network protocols  
  ■ Shared resources |
| Isolate the affected computer.      | Blended threats such as worms can travel via shared resources without user interaction. When you respond to an infection by a computer worm, it can be critical to isolate the infected computers by disconnecting them from the network. |

Track viruses using logs.

Use the Central Quarantine Console to track infected computers on your network, and submit suspicious file samples to Symantec Security Response for analysis and cure.
### Table 5-1 A model virus outbreak plan

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify the virus.</td>
<td>Symantec Client Security logs are a good source of information about viruses on your network. If you can identify a virus from the logs, you can use the Symantec Security Response Virus Encyclopedia to learn how to remove the virus.</td>
</tr>
<tr>
<td>Respond to unknown viruses.</td>
<td>If you cannot identify a suspicious file as a virus by examining the logs, and the latest virus definitions files do not clean the file, go to <a href="http://securityresponse.symantec.com">http://securityresponse.symantec.com</a> and look at the Latest Virus Threats and Security Advisories areas for news.</td>
</tr>
</tbody>
</table>
| Understand security solutions.| In addition to understanding your network topology, you need to understand your implementation of Symantec Client Security as well as the implementation of any other security products that are used on your network. Consider the following questions:  
  ▪ What security programs are protecting network servers and workstations?  
  ▪ What is the schedule for updating virus definitions?  
  ▪ What alternative methods of obtaining updates are available if the normal channels are under attack?  
  ▪ What log files are available for tracking viruses on your network? |
| Have a backup plan.           | In the event of a catastrophic virus infection, you may need to restore servers and clients to be sure that your network has not been compromised. Having a backup plan in place to restore critical computers is essential. |
Defining Symantec Client Security actions for handling suspicious files

By default, Symantec Client Security performs the following actions when it identifies a suspicious file:

- Symantec Client Security attempts to repair the file.
- If the file cannot be repaired with the current set of virus definitions files, the infected file is moved to the Quarantine on the local computer. In addition, the Symantec Client Security client makes a log entry of the threat event in its log. The Symantec Client Security client data is forwarded to a primary server. You can view log data from the Symantec System Center console.

You can perform the following additional actions to complete your virus handling strategy:

- Define different repair actions based on virus type. For example, you can have Symantec Client Security automatically fix macro viruses, but ask what action to take when a program file virus is detected.
- Assign a backup action for files that Symantec Client Security cannot repair, such as deleting the infected file.
- Receive virus alerts, such as a page or email message, if you are using AMS2.
- Configure the local Quarantine to forward infected files to the Central Quarantine. You can configure the Central Quarantine to attempt a repair based on its set of virus definitions files (which may be more up-to-date than the definitions on the local computer), or automatically forward samples of infected files to Symantec Security Response for analysis.

See “About the Alert Management System” on page 67.

For more information, see the Symantec Central Quarantine Administrator's Guide.

Automatically purging suspicious files from local Quarantines

When Symantec Client Security scans a suspicious file, it places the file in the local Quarantine folder on the affected computer. The Quarantine purge feature automatically deletes files in the Quarantine that exceed a specified age.

Registry settings for Quarantine purge are located in this registry key:

```
\HKEY_LOCAL_MACHINE\SOFTWARE\INTEL\LANDesk\VirusProtect6\CurrentVersion\Quarantine
```
Table 5-2 lists the possible Quarantine purge settings.

### Table 5-2 Quarantine purge settings

<table>
<thead>
<tr>
<th>Value</th>
<th>Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>QuarantinePurgeEnabled</td>
<td>0/1</td>
<td>Disables/enables purge</td>
</tr>
<tr>
<td>QuarantinePurgeAgeLimit</td>
<td>X</td>
<td>Specifies the maximum number of days to keep a file in the Quarantine directory</td>
</tr>
<tr>
<td>QuarantinePurgeFrequency</td>
<td>X</td>
<td>Sets the frequency value for purging: 0=Days, 1=Months, 2=Years</td>
</tr>
<tr>
<td>BackupItemPurgeEnabled</td>
<td>0/1</td>
<td>Disables/enables purging backup files</td>
</tr>
<tr>
<td>BackupItemPurgeAgeLimit</td>
<td>X</td>
<td>Specifies the maximum number of days to keep a backup file in Quarantine</td>
</tr>
<tr>
<td>BackupItemPurgeFrequency</td>
<td>X</td>
<td>Sets the frequency value for purging backup files: 0=Days, 1=Months, 2=Years</td>
</tr>
<tr>
<td>RepairedItemPurgeEnabled</td>
<td>0/1</td>
<td>Disables/enables purging repaired files</td>
</tr>
<tr>
<td>RepairedItemPurgeFrequency</td>
<td>X</td>
<td>Sets the frequency value for purging repaired files: 0=Days, 1=Months, 2=Years</td>
</tr>
</tbody>
</table>

**Handling a virus outbreak on your network**

Symantec Client Security provides the following tools for handling a virus outbreak on your network:

- Alerts: Sends AMS\(^2\) and built-in alerts
- Virus sweep: Forces a virus scan at the system hierarchy, server group, or individual server level
- Event Logs and Histories: Track viruses and Central Quarantine submissions at the server group, individual server, or client level
- Central Quarantine Console: Tracks submissions to Symantec Security Response
- Emergency Disk: Cleans boot sector viruses
Using virus alerts and messages

You can use alerts and messages to learn about suspicious files that Symantec Client Security discovers on your network. Symantec Client Security offers the following notification mechanisms:

- AMS2: If configured, Symantec Client Security clients can send threat events to an AMS2 server. You can configure AMS2 servers to send alerts to a pager, email address, and other notification mechanisms. See “About the Alert Management System” on page 67.

- Custom messages: From the Symantec System Center console, you can have a custom message appear on Symantec Client Security clients when they encounter a suspicious file. See “Displaying and customizing a warning message on an infected computer” on page 134.

Running a virus sweep

If you discover several suspicious files, you might not know if the problem is on the computer or server on which the suspicious files were detected, or if the problem has spread to other areas of the network. You might want to begin a virus sweep using the Symantec System Center. The number of computers that you scan depends on how you start the sweep.

If a Symantec Client Security client is not accessible during a virus sweep, Symantec Client Security will do one of the following:

- On 32-bit operating systems: Scan the computer as soon as it is turned on. The computer does not have to log on to the network.

- On 16-bit operating systems: Scan the computer as soon as it is turned on and logged on to the network.

Depending on the object that you select in the Symantec System Center console, you can run a virus sweep on your entire network, a server group, or an individual server.

**Warning:** A virus sweep can create considerable network traffic, the amount and duration of which depend on the size of your network. Once you start a virus sweep it must complete; you cannot stop it.
To run a virus sweep

1. In the Symantec System Center console, right-click the network, a server group, or a server, and then click **All Tasks > Symantec AntiVirus > Start Virus Sweep**.

2. In the Name box, type a name for the sweep.

3. Click **Start**.

   See “Configuring scan options” on page 129.

Tracking virus alerts using Event Logs and Histories

You can track Threat Found alerts from the Symantec System Center console. By default, Threat Found alerts appear for three days. You can change the number of days for which Threat Found alerts appear.

See “About Histories and Event Logs” on page 193.

Tracking submissions to Symantec Security Response with Central Quarantine Console

The Symantec System Center logs an event when a Symantec Client Security client submits a suspicious file to Symantec Security Response. In addition to the logged event, you can track the Auto-Protect status of submissions to Symantec Security Response from the Central Quarantine Console.

For information on using the Central Quarantine Console, see the *Symantec Central Quarantine Administrator’s Guide*. 
Responding to virus outbreaks
Handling a virus outbreak on your network
Managing roaming clients

This chapter includes the following topics:

■ About roaming clients
■ Roaming client components
■ How roaming works
■ Implementing roaming
■ Command-line options
■ Registry values

About roaming clients

A roaming client can do the following:

■ Automatically identify its best parent server, based on speed and proximity, and become a managed client of that parent server. For example, when a mobile user who is based in New York travels to California, the roaming client detects the new network address and reassigns the user’s laptop to the best parent server.

■ Connect to the nearest appropriate parent server whenever its network address changes.

■ Connect to a different parent server if the current parent server becomes unavailable.

■ Periodically recheck for the nearest parent server to adjust for changes in servers and server load.
■ Attempt to balance the load among a pool of equivalent servers when selecting a parent server.

■ Automatically identify the best parent server when the client connects to the network (for unmanaged clients that are converted to managed clients). For example, a corporation may have a distribution center for new computers. Administrators enable roaming on the computers before they are sent to branch offices. This entails specifying all of the possible roam servers for the new computers. When end users connect the new computers to the network, Symantec Client Security automatically assigns the best parent server.

Roaming client components

Table 6-1 lists roaming client components.

Table 6-1 Roaming client components

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
</table>
| List of 0 level servers | Lists the 0 level of servers that are available as possible roam servers for a specific roaming client. Roaming clients store this data in their registries.  
See “Analyzing and mapping your Symantec Client Security network” on page 188.  
See “Creating a list of 0 level Symantec Client Security servers” on page 189. |
| Hierarchical list of servers | Lists all roam servers, grouped by hierarchical level. Roaming servers store this data in their registries.  
See “Analyzing and mapping your Symantec Client Security network” on page 188.  
See “Creating a hierarchical list of Symantec Client Security servers” on page 190. |
| Roamadmin.exe           | Sets up Symantec Client Security servers for roaming access.  
See “Configuring additional roaming client support for roam servers” on page 193. |
| SavRoam.exe             | Provides roam server data to roaming clients.  
See “Configuring roaming client support options from the Symantec System Center console” on page 190. |
How roaming works

Roaming client support employs the following types of lists:

- One or more lists of 0 level servers
- A hierarchical list of the servers that you want to support roaming clients

Roaming clients store the 0 level list in their registries, and use it to identify the servers to which they should attempt to connect. To implement roaming on your network, start by preparing one or more lists of 0 level servers, and the hierarchical list of servers.

After you roll out this data, roaming clients work in the following manner:

- SavRoam.exe launches on the Symantec Client Security client during startup, and selects the best Symantec Client Security server, based on registry values and server feedback.

- The selected server provides the client with a list of servers at the next level in the network hierarchy. SavRoam loops through the network hierarchy until no lower level exists. The final server becomes the client’s new parent server, and immediately pushes a full configuration to the roaming client.

- SavRoam runs the following checks at regular intervals:
  - Checks for the availability and response time of its parent server. If its parent server is unavailable or another parent server can provide better performance, SavRoam connects the client with a new best parent server on the network.
  - Checks for the computer’s network address. If the address has changed, it connects to the new best parent server.
  - If the client was previously assigned to a different parent server, SavRoam attempts to delete itself from the old parent after it checks in with the new parent.

Implementing roaming

To implement roaming, you must complete the following tasks:

- Analyze and map your Symantec Client Security network.
- Identify servers in each region that point roaming clients to the next level of roam servers.
- Create a list of 0 level servers for roaming clients.
- Create a hierarchical list of all roam servers, layered hierarchically and identified by type (such as Quarantine Server or Alert server), if necessary.
- Configure roaming client support for roaming clients and servers from the Symantec System Center console.
- Configure additional roaming client options for roaming clients in the registry. This task is optional.
- Configure additional roaming client options for roam servers in the registry. This task is optional.
- Configure additional server types for roaming clients in the registry. This task is optional.

Analyzing and mapping your Symantec Client Security network

While you may have many servers in your network, you may want to identify only some of them as roam servers. Creating a hierarchical map of your network lets you quickly identify roam servers for your network.

Figure 6-1 illustrates a map of an enterprise network that spans three continents. While this organization has more Symantec Client Security servers than appear in the map, only the mapped servers are identified as regional pointer servers.

Figure 6-1 Sample enterprise map
Identifying servers for each hierarchical level

To identify servers for each hierarchical level, you must analyze the needs of your roaming users. For example, you may need to identify mobile users based on whether they travel internationally, throughout the country, or within a smaller geographic area. If users travel internationally, their server lists will contain the names of the country servers from level 0. If they travel within one country only, their server lists will contain servers from level 1.

Depending on network speeds, the server list could contain only the top level servers (level 0 in Figure 6-1). This simplifies building the clients’ server list. The only limit to the number of levels that you can define is the text file size limit of 512 characters.

Creating a list of 0 level Symantec Client Security servers

You can create the clients’ server list text file using a text editor such as Notepad. The server list text file must contain lines in the following format:

```
<local><type of server><level><server list>
```

where:

- `<local>` indicates to the client that this is the 0 level of servers that the client should attempt to contact when searching for a roam server.
- `<type of server>` is the server type, such as parent server, Quarantine Server, Grc.dat server, or Alert server.
- `<level>` is 0.
- `<server list>` is the list of servers, which are separated by commas. (Spaces between the commas are optional.)

For example, the clients’ server list text file that corresponds to Figure 6-1 is as follows:

```
<local> Parent 0 USASvr,EuropeSvr,AsiaSvr
```

This is the only line in the server list for the roaming clients in this example. The list tells the clients to contact and compare response time from these three servers only. Depending on which server is best, the client continues its search down the list into one of the three continents.
Creating a hierarchical list of Symantec Client Security servers

You can create the hierarchical list using a text editor such as Notepad. It must contain lines in the following format:

\(<computer> <type of server> <level> <server list>\)

where:

- \(<computer>\) is the host name of the server.
- \(<type of server>\) is the server type such as parent server, Quarantine Server, Grc.dat server, or Alert server.
- \(<level>\) is the level that is specified in the server list text file.
- \(<server list>\) is the list of servers, which are separated by commas. (Spaces between the commas are optional.)

For example, in the enterprise map in Figure 6-1, the USA branch would have the following server list:

USASvr Parent 1 USAWestSvr,USAEastSvr

Configuring roaming client support options from the Symantec System Center console

You can configure roaming client support options from the Symantec System Center console. You can configure options at the following levels:

- Server group
- Client group
- Server
- Client

Once you set the options, Symantec Client Security pushes them to the Symantec Client Security servers and Symantec Client Security clients based on the selected level.

To configure roaming client support options from the Symantec System Center console

1. In the Symantec System Center console, right-click the server group, Symantec Client Security servers, client group, or Symantec Client Security clients that you want to configure, and then click All Tasks > Symantec AntiVirus > Client Roaming Options.

If you select a server group, the Symantec System Center will configure all of the servers that are in the server group. If you select a client group, the
Symantec System Center will configure all of the clients that are in the client group.

2 In the Client Roaming Options dialog box, do the following:
   - Enable roaming on clients on which the Symantec Client Security roam service is installed.
   - Set the number of minutes that a client waits before it validates that its parent server is available. The default setting is 120 minutes.
   - Set the number of minutes that a client waits before it checks for a closer parent server. The default setting is 60 minutes.
   - Set the number of times that a client checks each server to determine the average number of seconds required to contact it. The client then uses this sampling to determine how close a server is to the client. The default setting is 7 times.
   - Set the number of seconds that a client that cannot find a new parent server waits before retrying to connect to a new parent server. The default setting is 30 seconds.

3 Under Use These Servers, select one of the following:
   - Roaming: You can set up 0 level parent servers.
   - Failover: You can set up a fault tolerance system by specifying backup servers to handle clients when roam servers are unavailable. A roaming client checks the response time for the first server in the list that answers. If the first backup server fails, the roaming clients that it manages migrate to the next available backup server in the list when they check their parent server availability. Backup servers do not load balance.
Loadbalance If you have multiple servers and want to distribute roaming clients among them, you can load balance by treating roam servers as equals regardless of how long it takes clients to contact them. A roaming client will contact each server in the list. Roaming servers keep a count of the Symantec Client Security clients that they manage, and return this value to the roaming client. The roaming client selects the server with the fewest clients. This server becomes the roaming client’s new parent server. Load balancing has a higher priority than finding the closest parent.

4 To specify load balancing among servers, use an equal sign (=) between the servers. For example:
   MiamiSvr=AtlantaSvr=RichmondSvr

5 To specify failover servers, use a greater than symbol (>) in the hierarchical list of servers. For example:
   MiamiSvr>AtlantaSvr>RichmondSvr

6 Click OK.

**Configuring additional roaming client support for roaming clients**

Configuring additional roaming client support for roaming clients consists of the following tasks:

- Configuring roaming on each roaming client
- Adding 0 level server data to the registry of each roaming client

**Configuring additional roaming on each roaming client**

You can configure additional roaming on Symantec Client Security clients by setting the required values in a configurations file (Grc.dat), or by directly editing each roaming client’s registry using Regedit. Type the registry values under the following key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\INTEL\LANDesk\VirusProtect6\CurrentVersion\ProductControl
```
Table 6-2 lists and describes each registry value.

Table 6-2  Roaming client registry values

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
</table>
| ProductControl\RoamQuarantine | 1: Enable Central Quarantine roaming.  
0: Disable Central Quarantine roaming (default). |
| ProductControl\RoamAlerts   | 1: Enable Alert server roaming.  
0: Disable Alert server roaming (default). |
| ProductControl\RoamManagingParentLevel0 | List of parent servers to check for proximity. |
| ProductControl\RoamManagingGRCLevel0   | List of GRC servers to check for proximity. |
| ProductControl\RoamManagingQuarantineLevel0 | List of Quarantine Servers to check for proximity. |
| ProductControl\RoamManagingAlertLevel0 | List of Alert servers to check for proximity. |

For information on using the configurations file, see the Symantec Client Security Reference Guide.

Configuring additional roaming client support for roam servers

To configure a Symantec Client Security server for additional roaming options, you must complete the following tasks:

- Enable roaming and roll out the hierarchical list of servers to each roam server using RoamAdmin.exe, which is located on Disk 1 in the AdmTools folder.

- Optionally configure additional load balancing, failover, and alternate Symantec Client Security servers.
  See “Configuring roaming client support options from the Symantec System Center console” on page 190.
Enable roaming and roll out the hierarchal list of servers

Enabling roaming requires adding a value to the registry of each roam server, and rolling out server list data. When you run RoamAdmn, it communicates with each server named at the beginning of each line in the hierarchical list of servers. On each server, RoamAdmn adds a registry value containing the servers at the next level down in the hierarchy. If the server cannot be reached, that server is bypassed.

To enable roaming
◆ Add the DWORDs to the following registry key:
  HKEY_LOCAL_MACHINE\SOFTWARE\INTEL\LANDesk\VirusProtect6\CurrentVersion\ProductControl\RoamServer

To roll out the hierarchical list of servers
1 Copy RoamAdmn to the computer from which you want to work while rolling out the hierarchical list of servers to the roaming servers.
2 At the command prompt, type the following:
  RoamAdmn /import <serverlist.txt>
  where <serverlist.txt> is the name of the hierarchical server list that you created.

Roaming server example

A corporation has a computer from which all roam servers are visible. The Serverlist.txt file includes the following lines:
USASvr Parent 1 USAWestSvr,USAEastSvr
EuropeSvr Parent 1 EUROEastSvr,EUROWestSvr
AsiaSvr Parent 1 JapanSvr,KoreaSvr

Table 6-3 describes the ServerList.txt data as it appears in each roam server’s registry.

<table>
<thead>
<tr>
<th>Server name</th>
<th>Registry value</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>USASvr</td>
<td>RoamManagingParentLevel1</td>
<td>USAWestSvr,USAEastSvr</td>
</tr>
<tr>
<td>EuropeSvr</td>
<td>RoamManagingParentLevel1</td>
<td>EUROEastSvr,EUROWestSvr</td>
</tr>
<tr>
<td>AsiaSvr</td>
<td>RoamManagingParentLevel1</td>
<td>JapanSvr,KoreaSvr</td>
</tr>
</tbody>
</table>
Configuring additional server types for roaming clients

In addition to parent, load balancing, and failover servers that you can configure from the Symantec System Center console, you can specify the following server types in the registry:

- Central Quarantine Server (this must also have Symantec Client Security server installed).
- Alert (Alert Management System²) server.
- Grc.dat server, which provides the roaming client with Grc.dat settings. Using nearest_GRC lets the roaming client get policy settings from the specified server and process them immediately.

Note: A client cannot connect with multiple parents of the same type.

To configure additional server types for roaming clients

1. Set the roaming client’s registry values that correspond to the server type to 1.
   See “Registry values” on page 197.
2. At the command prompt, type any of the following:
   - `SavRoam /nearest_parent`
   - `SavRoam /nearest_quarantine`
   - `SavRoam /nearest_GRC`
   - `SavRoam /nearest_alerts`

   The main difference between /nearest_parent and /nearest_GRC occurs when the configurations file (Grc.dat) is processed. Typing /nearest_parent lets the roaming client find the nearest parent. Policy settings are not processed until the client checks in with the parent. Typing /nearest_GRC lets the roaming client get the policy settings from the parent immediately, and the settings are processed immediately.

Command-line options

Table 6-4 describes the command-line options that can be used with SavRoam.exe and RoamAdmin.exe.
You must have local Administrator rights to use command-line options.

**Table 6-4  Command-line options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/h</td>
<td>Displays a list of the options with descriptions of their usages.</td>
</tr>
</tbody>
</table>
| /import <server list>      | Sets up client or server registry keys. When you use RoamAdmin.exe, you can import the server list to remote servers. When you use SavRoam.exe, you can import the server list to the registry of the local computer.  
  <server list> is the text file that contains the list of potential parent servers.                                                                                                                                  |
| /export > <file>            | Reports all of the roam servers that the client can find at all levels and for all parent types (including parent, Quarantine, Alert, and Grc.dat servers).  
  <file> is the name of the file to which the information is written.  
  You can use the file that is created with the export command as the server list for import.                                                                                                             |
| /install <path> <new service name> <new exe name> | Registers and starts the roaming client service. The service runs until the computer is turned off.  
  <path> is the path to the folder in which you want to copy SavRoam.exe.  
  <new service name> is SavRoam.exe.  
  <new exe name> is SavRoam.exe.                                                                                                                             |
| /remove <new service name> | Stops and removes SavRoam.exe.                                                                                                                                                                                                                                               |
| /nearest                   | Finds and sets the nearest appropriate parent for the parent, Quarantine, Alert, or Grc.dat server.  
  Requires that the parent GRC path be set manually in the registry.                                                                                                                                                                                                         |
| /nearest_parent            | Finds and sets the nearest parent server.                                                                                                                                                                                                                                                                                                 |
| /nearest_quarantine        | Finds and sets the nearest Quarantine parent server.                                                                                                                                                                                                                                                                                      |
| /nearest_GRC               | Finds and applies the configurations file (Grc.dat) from the nearest Grc.dat server.  
  Requires that the parent GRC path be set manually in the registry.                                                                                                                                                                                                        |
You can edit the roaming registry values using a registry editor such as Regedit or Regedt32.

The agent behavior is controlled by the registry keys under the following path:

HKEY_LOCAL_MACHINE\SOFTWARE\INTEL\LANDesk\VirusProtect6\CurrentVersion\ProductControl

Table 6-5 describes the registry values for roaming clients.

Table 6-5 Registry values for roaming clients

<table>
<thead>
<tr>
<th>Registry value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CheckForNewParentIntervalInSeconds</td>
<td>Checks periodically to see if the network is up if a computer cannot find the nearest parent when it first starts. The interval is set by this registry key. The default value is 30 seconds.</td>
</tr>
<tr>
<td>CheckParentIntervalInMinutes</td>
<td>Determines how often a computer checks to see if its parent is available. If the parent is not available, it tries to find a new parent. The default value is 120 minutes.</td>
</tr>
</tbody>
</table>
### Registry values for roaming clients

<table>
<thead>
<tr>
<th>Registry value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RoamClient</td>
<td>Instructs the agent to make this computer a child of the nearest parent. The default value is 1. Set this value to 0 if you do not want the computer to become a child of the nearest parent.</td>
</tr>
<tr>
<td>RoamQuarantine</td>
<td>If the value is set to 1, sets Quarantine forwarding to the nearest server that is found from the Quarantine search keys. The default value is 0.</td>
</tr>
<tr>
<td>RoamAlerts</td>
<td>If the value is set to 1, sets Alert Management System alert forwarding to the nearest server that is found from the Alerts search keys. The default value is 0.</td>
</tr>
<tr>
<td>RoamGRC</td>
<td>If the value is set to 1, lets the client roam to the server from which it should receive configurations file (Grc.dat) updates. The default value is 0.</td>
</tr>
<tr>
<td>RoamServer</td>
<td>If the value is set to 1, lets the client roam to the best parent server. The default value is 0.</td>
</tr>
<tr>
<td>ParentGRCPath</td>
<td>Sets the ParentGRCPath value to the configurations file (Grc.dat). The agent copies the configurations file to the local computer and applies it. For more information, see the RoamGRC description. If the RoamClient and RoamGRC keys are set to 1, SavRoam.exe copies the configurations file from the parent, and then copies the configurations file from the GRC parent and overwrites the parent copy.</td>
</tr>
</tbody>
</table>
| ParentLiveUpdateHstPath | Defines the directory beneath the SAV home directory. For example: \MyLiveUpdateHost\Liveupdt.hst. 

The .hst file must be placed under OSDRIVE/ProgramFiles/Symantec/LiveUpdate. The agent copies the LiveUpdate host file to this location. |
Working with Histories and Event Logs

This chapter includes the following topics:

- About Histories and Event Logs
- Sorting and filtering History and Event Log data
- Viewing Histories
- Forwarding client logs to parent servers
- Deleting Histories and Event Logs

About Histories and Event Logs

Histories and Event Logs offer a central view of virus and other threat activity and scanning on your network. Using the Symantec System Center, you can do the following:

- View data at the server group, server, or individual managed workstation level. In addition, each Symantec Client Security client stores its own Event Log data locally. The data is viewable from the Symantec Client Security client user interface.
- Sort and filter History and Event Log data.
- Perform actions based on History and Event Log data. For example, if a Threat History displays a virus found, you can perform actions such as repairing the virus or moving the infected file to the Central Quarantine.
- Export data to Microsoft Access (as an .mdb file) or in comma-separated value (CSV) format.
- Remove History and Event Log data.
Symantec Client Security provides several types of Histories and Event Logs as described in Table 7-1.

### Table 7-1  History and Event Log types

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Available for</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event Log</td>
<td>Provides information about Symantec Client Security startups and shutdowns, scans that were started, stopped, or aborted, configuration changes, virus definitions files updates, virus infections, items that were forwarded to the Central Quarantine, and items that were forwarded to Symantec Security Response.</td>
<td>■ Server groups</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Individual servers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Individual clients</td>
</tr>
<tr>
<td>Scan History</td>
<td>Provides information about scans that have run or are running on Symantec Client Security clients at the server group, server, or individual workstation level. Specify a time range to filter the view. For example, you might want to view only those scans that ran within the last seven days.</td>
<td>■ Server groups</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Individual servers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Individual clients</td>
</tr>
<tr>
<td>Threat History</td>
<td>Lists all viruses and threats that were detected for selected computers or server groups. You can select a virus item in the list and perform additional actions, such as Delete or Move To Quarantine. (Expanded threats cannot be placed in Quarantine.) Threat History shows many details about each virus infection, such as the name and location of the infected file, the name of the infected computer, the primary and secondary actions that were configured for the detected virus, and the action that was taken on the virus. You can click on the link to the right of the expanded threat item to access detailed information about it at the Symantec Security Response Web site.</td>
<td>■ Server groups</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Individual servers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Individual clients</td>
</tr>
<tr>
<td>Virus Sweep History</td>
<td>Includes information about previous virus sweeps for servers or server groups.</td>
<td>■ Server groups</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Individual servers</td>
</tr>
</tbody>
</table>
Sorting and filtering History and Event Log data

When you view the Threat History, Virus Sweep History, Scan History, or Event Log, you can filter items in the following ways:

- Today
- Past 7 days
- This month
- All items
- A selected range of days

You can also filter event types by selecting just the events that you want to view.

Sort and filter History and Event Log data

When you view Histories and Event logs, you can sort the data in any column.

You can filter History and Event Log data by date. You can also filter by event type for the Event Log.

To sort the data

◆ Click the column header.

The ascending sort icon appears within a column header the first time that you click it. The descending sort icon appears the next time that you click the column header.

To filter History and Event Log data by date

1 In the Symantec System Center console, right-click a server or server group, and then click All Tasks > Symantec AntiVirus > Logs, and then select one of the following:
   - Event Log
   - Scan History
   - Threat History
   - Virus Sweep History

2 In the list, select one of the following:
   - Today
   - Past 7 Days
   - This Month
   - All Items
   - Selected Range
If you select Selected Range, select start and end dates, and then click OK.

**To filter Event Log data by event type**

1. In the Symantec System Center console, right-click a server or server group, and then click **All Tasks > Symantec AntiVirus > Logs > Event Log**.

2. In the Event Log dialog box, click the filter icon.

3. In the Filter Event Log dialog box, select the events you want to display:
   - Configuration change
   - Symantec AntiVirus startup and shutdown
   - Virus definition file
   - Scan omissions
   - Forwarded to the Quarantine Server
   - Delivered to Symantec Security Response
   - Realtime protection load/unload
   - Client management and roaming
   - Unauthorized communication (access denied) warnings

4. Click **OK**.
Viewing Histories

Table 7-2 describes the Histories that you can view in the Symantec System Center console.

<table>
<thead>
<tr>
<th>History</th>
<th>Description</th>
</tr>
</thead>
</table>
| Threat Histories      | ■ At the server group level, displays all of the viruses and other threats that were found in that server group  
                        | ■ At the server level, displays all of the viruses and other threats that were found for clients that are managed by that server  
                        | ■ At the client level, displays all of the viruses and other threats that were found for the client |
| Virus Sweep Histories | ■ At the server group and server level, displays all of the virus sweeps for all servers in a server group or a server |
| Scan Histories (current and scheduled) | ■ At the server group level, displays all of the virus scans for that server group  
                        | ■ At the server level, displays all of the virus sweeps for clients that are managed by that server  
                        | ■ At the client level, displays all of the virus sweeps for that client |

View Histories

You can view Threat Histories, Virus Sweep Histories, and Virus Scan Histories.

See “Working with Threat Histories” on page 198.

To view a Threat History

◆ In the Symantec System Center console, right-click a server, server group, or client, and then click All Tasks > Symantec AntiVirus > Logs > Threat History.

See “Understanding Event Log icons” on page 202.

To view a Virus Sweep History

1 In the Symantec System Center console, right-click a server or server group, and then click All Tasks > Symantec AntiVirus > Logs > Virus Sweep History.

2 In the Virus Sweep History dialog box, click View Results to examine the results of previous sweeps.
To view the Scan History

- In the Symantec System Center console, right-click a server group, server, or client, and then click All Tasks > Symantec AntiVirus > Logs > Scan History.

Working with Threat Histories

In the Threat History window, icons display information about the viruses that were found. You can also perform actions such as saving the data as a CSV file.

**Note:** You cannot perform additional actions on email data. You can perform only limited actions on compressed files.

Table 7-3 lists and describes Threat History icons.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1" alt="Icon1" /></td>
<td>The file is infected with a virus or the file is another threat type, such as adware or spyware.</td>
</tr>
<tr>
<td><img src="image2" alt="Icon2" /></td>
<td>The file is not infected. The file was never infected, or it has been cleaned. See the action that was taken on the file for more information.</td>
</tr>
<tr>
<td><img src="image3" alt="Icon3" /></td>
<td>An error occurred in association with this file.</td>
</tr>
<tr>
<td><img src="image4" alt="Icon4" /></td>
<td>Close the Threat History window.</td>
</tr>
</tbody>
</table>

Table 7-4 lists and describes the actions available for viruses and blended threats in the Threat History window.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Undo Action Taken</td>
<td>Symantec Client Security can undo the last action that was taken on an infected file, including removing a file from the Quarantine and removing the .vbn extension from a renamed file. Symantec Client Security cannot restore a file that has been permanently deleted. You cannot undo actions on compressed files.</td>
</tr>
</tbody>
</table>
In the Threat History window, detected non-viral threats appear. You handle these threats differently than viruses and blended threats.

In a Threat History, you can perform a different set of actions for viruses than you can for other threats, such as adware and spyware.

**Work with Threat Histories**

For viruses, you can undo the last action that was taken on a file, clean a file, delete it permanently, or move the file to the Central Quarantine.

For other threats, you can access a Symantec Security Response web page to learn how to handle the threat.

You can also export the Threat History data.

**To undo the last action that was taken**

1. Right-click a file, and then click **Undo Action Taken**.
2. In the Take Action dialog box, click **Start Undo**.

**To clean an infected file**

1. Right-click a file, and then click **Clean**.
2. In the Take Action dialog box, click **Start Clean**.

### Table 7-4: Threat History actions for viruses and blended threats

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clean</td>
<td>Symantec Client Security virus definitions files are frequently updated. A file that you could not clean yesterday or a few weeks ago might be able to be cleaned when the virus definitions file is updated. You cannot perform this action on compressed files.</td>
</tr>
<tr>
<td>Delete Permanently</td>
<td>You can permanently delete any infected file (including a compressed file) that is stored in the Quarantine or Threat History. Permanently deleted files cannot be recovered.</td>
</tr>
<tr>
<td>Move To Quarantine</td>
<td>If you determine that Symantec Client Security has left an infected file alone, you should move the file to the Quarantine, where the virus will be unable to spread. You can move compressed files to the Quarantine.</td>
</tr>
<tr>
<td>Export</td>
<td>You can export information about a specific Threat History or Event Log item as a CSV or Microsoft Access database file.</td>
</tr>
</tbody>
</table>
To delete an infected file permanently
1  Right-click the file, and then click **Delete Permanently**.
2  In the Take Action dialog box, click **Start Delete**.
   Permanently deleted files cannot be recovered.

To move a file to the Central Quarantine
1  Right-click the file, and then click **Move To Quarantine**.
2  In the Take Action dialog box, click **Quarantine**.

To handle a threat in an expanded threat category
1  Double-click the file.
   A Symantec Security Response web page appears that describes the threat
   in detail and provides information about removal methods.
2  Take the recommended actions to remove the threat.

To export the Threat History data
1  Right-click the file, and then click **Export**.
2  In the Save as type list, select one of the following:
   ■  CSV
   ■  Access Database
3  In the File name box, type a file name.
4  Click **OK**.

**Working with Scan Histories**

In the Scan History window, icons display information about any viruses that
were found. You can also perform actions, such as saving the data as a CSV file.

---

**Note**: You cannot perform additional actions on email data and only limited
actions on compressed files.
Table 7-5 lists and describes the icons.

**Table 7-5**  
**Scan History icons**

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1" alt="Icon" /></td>
<td>The file is infected.</td>
</tr>
<tr>
<td><img src="image2" alt="Icon" /></td>
<td>The file is not infected. The file was never infected, or it has been cleaned. See the action taken on the file for more information.</td>
</tr>
<tr>
<td><img src="image3" alt="Icon" /></td>
<td>Close the Scan History window.</td>
</tr>
<tr>
<td><img src="image4" alt="Icon" /></td>
<td>Display item properties.</td>
</tr>
<tr>
<td><img src="image5" alt="Icon" /></td>
<td>Save the data that is shown in the Scan History as a comma separated value (.csv) file.</td>
</tr>
<tr>
<td><img src="image6" alt="Icon" /></td>
<td>Display Help for the Scan History.</td>
</tr>
</tbody>
</table>

Table 7-6 lists and describes the actions available in the Scan History window.

**Table 7-6**  
**Scan History actions**

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Undo Action Taken</td>
<td>Symantec Client Security can undo the last action that was taken on an infected file, including removing a file from the Quarantine, and removing the .vbn extension from a renamed file. Symantec Client Security cannot restore a file that has been permanently deleted. You cannot undo actions on compressed files.</td>
</tr>
<tr>
<td>Clean</td>
<td>Symantec Client Security virus definitions files are frequently updated. A file that you could not clean previously might be able to be cleaned when the virus definitions file is updated. You cannot perform this action on compressed files.</td>
</tr>
<tr>
<td>Delete Permanently</td>
<td>You can permanently delete any infected file (including a compressed file) that is stored in the Quarantine or Scan History. Permanently deleted files cannot be recovered.</td>
</tr>
<tr>
<td>Move To Quarantine</td>
<td>If you determine that Symantec Client Security has left an infected file alone, you should move the file to the Quarantine where the virus will be unable to spread. You can move compressed files to the Quarantine.</td>
</tr>
<tr>
<td>Export</td>
<td>You can export information about a specific Scan History or Event Log item as a CSV or Microsoft Access database file.</td>
</tr>
</tbody>
</table>
**Work with Scan Histories**

In a Scan History, you can undo the last action that was taken on a file, clean a file, delete it permanently, or move the file to the Central Quarantine. You can also export Scan History data.

**To undo the last action that was taken**
1. Right-click a file, and then click **Undo Action Taken**.
2. In the Take Action dialog box, click **Start Undo**.

**To clean an infected file**
1. Right-click a file, and then click **Clean**.
2. In the Take Action dialog box, click **Start Clean**.

**To delete an infected file permanently**
1. Right-click a file, and then click **Delete Permanently**.
2. In the Take Action dialog box, click **Start Delete**.
   Permanently deleted files cannot be recovered.

**To move a file to the Central Quarantine**
1. Right-click a file, and then click **Move To Quarantine**.
2. In the Take Action dialog box, click **Quarantine**.

**To export the Scan History data**
1. Right-click the file, and then click **Export**.
2. In the Save as type list, select one of the following:
   - CSV
   - Access Database
3. In the File name box, type a file name.
4. Click **OK**.

**Understanding Event Log icons**

In the Event Log window, icons display information about any viruses that were found, and allow you to perform actions, such as saving the data as a CSV file.
Table 7-7 lists and describes Event Log icons.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="Icon" /></td>
<td>Get information about an event.</td>
</tr>
<tr>
<td><img src="image2.png" alt="Icon" /></td>
<td>An error occurred in association with this event.</td>
</tr>
<tr>
<td><img src="image3.png" alt="Icon" /></td>
<td>Close the Event Log window.</td>
</tr>
<tr>
<td><img src="image4.png" alt="Icon" /></td>
<td>View item properties.</td>
</tr>
<tr>
<td><img src="image5.png" alt="Icon" /></td>
<td>Save the data shown in the Event Log window as a CSV or Microsoft Access database file.</td>
</tr>
</tbody>
</table>
| ![Icon](image6.png) | Filter the Event Log by the following categories:  
  - Configuration change  
  - Symantec Client Security startup/shutdown  
  - Virus definitions file  
  - Scan Omissions  
  - Forward to Quarantine  
  - Deliver to Symantec Security Response |
| ![Icon](image7.png) | Display Help for the Event Log. |

**Forwarding client logs to parent servers**

Symantec Client Security managed and sometimes managed clients forward log data to their parent servers. Log forwarding runs continually on managed clients. Log data accumulates between connections to parent servers for sometimes managed clients, such as roaming clients.

Symantec Client Security monitors and provides fault tolerant forwarding of the client logs. The client logs are located in the following directory:

C:\Documents and Settings\All Users\Application Data\Symantec\Symantec AntiVirus\7.5\Logs

Symantec Client Security tracks a client log throughout the forwarding process and handles delivery failures by resending the log when necessary.

**Configuring log forwarding options**

You can edit the client log forwarding registry values using a registry editor such as Regedit or Regedt32. You can reset values to achieve a balance between
the log delivery speed and network performance. You can also set the amount of data that Symantec Client Security forwards from clients.

Log forwarding behavior is controlled by the registry keys under the following path:

HKLM\SOFTWARE\INTEL\LANDesk\VirusProtect6\CurrentVersion\Common\ForwardEvents

Table 7-8 describes the registry values for client log forwarding.

### Table 7-8 Client log forwarding registry key values

<table>
<thead>
<tr>
<th>Registry value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interval</td>
<td>Number of seconds between log record processing intervals. There is no minimum or maximum number.</td>
</tr>
<tr>
<td>Count</td>
<td>The number of records to process in each polling interval. The default is 10 records. There is no minimum or maximum number.</td>
</tr>
</tbody>
</table>

#### Configuring log events to forward

You can configure the events that you want Symantec Client Security to forward. Table 7-9 lists the client and server events in the order in which they appear in the Log Event Forwarding dialog box.

### Table 7-9 Client and server events

<table>
<thead>
<tr>
<th>Event name</th>
<th>Forwarding Required</th>
<th>Forwarded by Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan stopped</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Scan started</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Virus definition update information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Virus infections</td>
<td></td>
<td></td>
</tr>
<tr>
<td>File not scanned</td>
<td></td>
<td></td>
</tr>
<tr>
<td>New virus defs applied</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Configuration change</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service shutdown</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service startup</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 7-9  
Client and server events

<table>
<thead>
<tr>
<th>Event name</th>
<th>Forwarding Required</th>
<th>Forwarded by Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virus definitions downloaded from parent</td>
<td></td>
<td></td>
</tr>
<tr>
<td>File forwarded to Quarantine Server</td>
<td></td>
<td></td>
</tr>
<tr>
<td>File forwarded to Symantec</td>
<td></td>
<td></td>
</tr>
<tr>
<td>File backed-up/restored to/from Quarantine</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Scan aborted</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Error loading services</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Services loaded</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Services unloaded</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client removed from parent server</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Scan delayed</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Scan restarted</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Client roamed to new parent server</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client roamed from parent server</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unauthorized communication</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Log forwarding error</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Configure log events to forward

You can configure the events to forward from a client to its parent server or from a secondary server to its primary server.

**Note:** If you change primary servers, the log from the former primary server is not forwarded to the new primary server.

To configure events to forward from clients to their parent servers

1. In the Symantec System Center console, right-click a server, server group, or client, and then click All Tasks > Symantec AntiVirus > Logs > Client Log Forwarding.
2. Check the events that you want the clients to forward to their parent servers.
3. Click OK.

To configure events to forward from secondary servers to their primary servers

1. In the Symantec System Center console, right-click a server or server group, and then click All Tasks > Symantec AntiVirus > Logs > Server Log Forwarding.
2. Check the events that you want the secondary servers to forward to their primary server.
3. Click OK.

**Best practice: Configuring events to forward for sometimes managed clients**

For sometimes managed clients, as a best practice, you can create a separate client group. See “Creating new client groups” on page 58. You can then set log forwarding Windows registry values to do the following:

- Forward the Virus definition update information event only.
- Poll at a high interval.
- Count at a low value.

See Table 7-8, “Client log forwarding registry key values,” on page 204.
Reviewing the forwarding status file

You can verify that a client log was forwarded and received by reviewing Fwdstatus.log, the default status log.

To verify that a client log was forwarded and received
1. Open the following folder:
   C:\Documents and Settings\All Users\Application Data\Symantec\Symantec AntiVirus\7.5\Logs
2. Use a standard text editor, such as Notepad, to open Fwdstatus.log.

Deleting Histories and Event Logs

You can configure Symantec Client Security to automatically remove data from Histories and Event Logs that is older than a specified date.

To set the delete frequency
1. In the Symantec System Center console, right-click a server, server group, or client, and then click All Tasks > Symantec AntiVirus > Configure History.
2. In the History Options dialog box, select the time period after which the Histories or Event Logs will be deleted.
3. Check Apply settings to clients not in Groups to apply the settings to the selected client or clients under the selected server or server group that are not members of client groups.
4. Click OK.

This does not permanently remove data, but hides it in the History and Event Log views. To permanently delete History or Event Log records, delete the .log files that contain the event records. Events are recorded in .log files for each day of the week in a Logs directory. These files are named according to the day on which they were created.
Section 3

Configuring Symantec Client Security firewall protection

- Managing policies
- Using Location Awareness and Zones
- Creating and testing rules
- Using pRules
- Customizing Intrusion Detection
- Configuring Client Settings and Web Content settings
- Managing client log data
- Creating network rulebases
Managing policies

This chapter includes the following topics:

- About policies
- Configuring policies and updates
- Importing and exporting policies and updates
- About importing and exporting
- Merging rules and pRules in policy files
- Distributing policies

About policies

Centralized firewall management lets you provide the maximum amount of firewall protection while minimizing maintenance and client user involvement. This is achieved by rolling out Symantec Client Security firewall client policies, which are sets of configured firewall rules and settings to govern firewall operation.

Policy management lets you do the following:

- Customize Symantec Client Security firewall clients to better accommodate your organization’s needs.
- Configure Symantec Client Security clients differently for different groups, departments, or users in your organization.
- Configure Symantec Client Security clients differently depending on client location and network connection information using one policy file.
- Update firewall rules to accommodate changing conditions on your corporate intranet and threats on the Internet.
Policies, which are .xml or compressed .cfp (Client Firewall Policy) files, contain all of the firewall rules, Intrusion Detection signatures, and configuration settings for a given policy. Updates, which are compressed .cfu (Client Firewall Update) files, contain firewall rules and Zones to add to policy files installed on Symantec Client Security firewall clients.

Policy components

Key components of a firewall policy include the following:

- Policy properties
- Rules
- pRules
- Zones
- Locations
- IDS signatures
- IDS settings
- Macros
- Client Settings
- Web Content settings
- Profiling settings
- File type settings

Policy properties

Policy properties are text that you add to identify the policy.

Rules

Firewall rules include General, Program, and Trojan rules.

General firewall rules apply to all network traffic. These rules are based on port numbers and IP addresses rather than specific programs or Trojan horses, which are handled separately.

Program rules apply to specific client program traffic. You can configure a Program rule that is specific to traffic on a particular port or IP address, or one that applies to multiple ports and IP addresses.

Trojan horses are malicious programs that are disguised as useful programs. Symantec Client Firewall Administrator Trojan rules examine the network traffic of Symantec Client Security firewall clients that access the Internet,
looking for signs of these malicious programs. If one is detected, the firewall rule takes immediate action against this type of threat.

See “About rules” on page 259.

**pRules**

Program rules are created when the firewall policy is rolled out. If all clients are similarly configured, this is an efficient method of providing uniform protection. If client workstations use widely divergent sets of programs, pRules are appropriate.

With pRules, or potential rules, data about programs is installed on the client workstation, but the rules themselves are not created. When a program first attempts to access the Internet, the pRule is invoked. If the program matches the pRule criteria, then a new Program rule is created from the pRule data on the client workstation.

See “About pRules” on page 287.

**Zones**

With Zones, you can identify computers that you trust, and those that you want to restrict from accessing a client computer. You identify computers using IP addresses.

- Computers that are in the Trusted Zone are not regulated by Symantec Client Security firewall client, and have total access to the client computer.
- Computers that are in the Restricted Zone are prevented from accessing client computers.
- Computers that are not placed in any Zone are regulated by all other settings of the firewall policy.

Use the Trusted Zone to list computers on your local network with which you need to share files and printers. Add computers to the Restricted Zone that have attempted to attack computers in your organization. The Restricted Zone provides the highest level of protection provided by Symantec Client Security. Clients cannot interact with any computers that are in the Restricted Zone.

Settings for Rules, IDS monitoring, Web Content, Privacy Control, and Ad Blocking are ignored for Web sites with IP addresses that fall into Trusted Zones.

See “Using Network Zones” on page 254.
Locations

Locations are named collections of rules, Zones, and settings. One Location is associated with one or more network connection specifications. Network specifications include gateway IP addresses for Ethernet connections, dial-up phone numbers for modem connections, and service set identifiers (SSIDs) for wireless connections. When a client computer accesses a network in a way that matches a specified network connection, Symantec Client Security firewall client immediately enforces the Location rules, Zones, and settings associated with that connection.

For example, many corporate computer users travel with laptop computers. They access networks locally when they are in the office, and they access networks remotely over VPNs when they travel. Typically, a policy for remote access is fairly restrictive for security reasons, and a policy for local access is relatively permissive because users need access to a variety of servers, printers, and so forth.

To support traveling users who access corporate networks both locally and remotely over VPNs, you can configure two Locations in one policy file, and name them, for example, Local and Remote VPN. When the client connects to the network locally, Symantec Client Security firewall client detects the network activity specified for that access point and filters traffic using the Local rules, Zones, and settings. When the client connects to the network over a VPN, Symantec Client Security firewall client detects the network activity specified for that access point, and filters traffic using the Remote VPN rules, Zones, and settings.

See “Using Locations” on page 241.

IDS signatures

Symantec Client Security Intrusion Detection is based on signatures. A signature defines or describes a network traffic pattern. Intrusion Detection System (IDS) signatures detect traffic patterns that are derived from previously detected exploits or attacks, or an anomalous pattern that is outside of the realm of expected traffic patterns and could be destructive.

See “About the Intrusion Detection System” on page 315.

IDS settings

You can exclude specified signatures from being processed. For example, you may not need protection against certain attack signatures because your environment does not contain the systems or components that they are known to attack. Once you exclude an IDS attack signature, the signature can cross the firewall and is not logged. You can also exclude specific IP addresses for a
signature. For example, the addresses may already be specified for automatic blocking by the firewall or it is possible that the threat from an IP address has been eliminated, and you want information from the IP to flow across the firewall.

See “About the Intrusion Detection System” on page 315.

**Macros**

The term macros is used to identify named port groups and named IP address groups that can be used for rules, pRules, Zones, and IDS exclusions. Symantec Client Firewall Administrator lets you create a group, name it, and then add a list of ports or IP addresses. You can select this group when configuring rules or Zones to quickly add ports or IP addresses without having to retype numbers for ports and IP addresses.

See “Using port groups” on page 273.
See “Using address groups” on page 276.

**Client Settings**

You can customize Client Settings for each firewall policy to enable or disable specific components of firewall protection, which include the following:

- **User access level:** Determines the extent to which users can modify firewall rules, configure firewall behavior outside of administrator control, and view firewall data

- **Degree of firewall protection:** Protects against potential Internet threats, such as ActiveX controls, Java applets, and traffic aimed at unused ports

- **Intrusion Detection:** Monitors inbound and outbound network traffic for packet patterns that are characteristic of an attack

- **Privacy Control:** Protects confidential information, blocks cookies, enforces browser privacy, and forces secure traffic (HTTPS)

- **Ad Blocking:** Stops ads from appearing in Web browsers based on originating source HTML strings

- **Custom alerts:** Supports customizable text that appears in alert messages for IDS events, cookies, and so forth

See “About Client Settings” on page 321.
Web Content settings
You can customize Web Content settings for each firewall policy to control how
the client handles interactive online content, ads, and possible privacy
intrusions. Web Content options are arranged on three tabs.

- Global Settings
- User Settings
- Ad Blocking

Note: All Web Content filtering is performed on ports that are specified in the
HTTP Port List on the Client Settings tab. If this list is blank, the firewall does
not enforce Web Content settings because all Web Content filtering is
performed on ports that are specified in this list. Further, Web Content settings
are ignored for computers placed in Trusted Zones.

See “Web Content settings” on page 333.

Profiling options
Symantec Client Firewall Administrator lets you export a policy file that causes
Symantec Client Security firewall clients to permit and log, or block and log,
traffic that does not match a rule. You can then import these logs and create
pRules with data that you select.

See “Using Profiling to generate pRules and NetSpecs” on page 302.

File version settings
Symantec Client Firewall Administrator lets you save policy files in .cfp and .xml
formats to support the following firewall versions:

- Symantec Client Firewall version 5.x
- Symantec Client Firewall version 7.0

Note: Location Awareness is not supported in versions earlier than 7.0. If you
are creating policy files for use in versions earlier than 7.0, save them using the
version 5.x option, do not enable Location Awareness, use the Default Location
only, and configure required Location information only.

See “Configuring required Location information” on page 242.
Configuring policies and updates

Symantec Client Firewall Administrator is a policy configuration tool used for tuning, customizing, and setting user-level settings. It is a separate program with its own user interface for use by firewall and system administrators. You use Symantec Client Firewall Administrator to create or import policy files for modification, and then save the policy files for distribution to Symantec Client Security firewall clients. The most efficient method to create firewall policies is to install both Symantec Client Security firewall client and Symantec Client Firewall Administrator on the same computer.

Typically, to prepare a policy, you install the software on a computer used by a specific user group or used at different locations. Different user groups and locations generally require different protection settings. For example, members of the accounting group may require different protection settings than members of the administrators group, and computers accessing the network remotely may require different protection settings than computers accessing the network locally.

To create a new policy, you can begin by creating a policy in Symantec Client Firewall Administrator and exporting it to Symantec Client Security firewall client, overwriting the default policy file (be sure to import and save the default policy file before overwriting it). You can create different policies for rollout as necessary.

**Note:** To use a firewall installation as the basis for creating a policy, do not use a computer that runs Symantec System Center. A Symantec System Center computer requires firewall rules that are not appropriate for client workstations.

From Symantec Client Firewall Administrator, you can save a policy for distribution in one of three formats:

- **.cfp:** Stores all configuration information in a compressed policy file. If a policy contains IDS settings, use the .cfp format.
- **.xml:** Stores all configuration information except IDS signatures in an .xml format file. If you create custom policies that are integrated during installation, use the .xml format.
- **.cfu:** Stores configuration information about pRules, General rules, and Trojan rules in a compressed update file. You can export this file to Symantec Client Security firewall client to insert new rules and pRules without affecting other settings.
Creating and opening policies and updates

Customizing a policy with Symantec Client Firewall Administrator includes the following actions:

■ Opening an existing policy for modification or creating an entirely new policy in Symantec Client Firewall Administrator.

■ Customizing the policy within Symantec Client Firewall Administrator to add, modify, or delete rules, pRules, Zones, Locations, IDS settings, Client Settings, and Web Content settings.

■ Saving the modified policy as a .cfp, .xml, or .cfu file for distribution to firewall installations.

The Active Client is the local instance of Symantec Client Security firewall client that is installed on the same computer as Symantec Client Firewall Administrator. You can use the Active Client to help develop, test, and clarify the rules and configuration settings of a policy package.

Note: As long as you import and export unlocked rules only, you can create rules on the Active Client and import them into Symantec Client Firewall Administrator.

See “About importing and exporting” on page 230.

Create and open policies and updates

New policies are created from the ScfaDefaultPolicy.cfp template, which contains IDS signatures and Client Settings only. New update files are empty. The file extension for updates is .cfu.

Updates only support General rules, Trojan rules, and pRules. Updates are applied to all Locations, and are designed to provide a quick way to provide protection against an active threat. After exporting an update, you should add the updated information to your regular policy files maintained by Symantec Client Firewall Administrator.

The initial firewall policy that is installed with the firewall is copied to the \Program Files\Symantec\Symantec Client Firewall Administrator\Policies folder on the computer on which Symantec Client Firewall Administrator is installed. The policy is called ScfaDefaultPolicy.cfp.

To create a new policy

◆ In Symantec Client Firewall Administrator, on the File menu, click New Policy.
To create a new update
◆ In Symantec Client Firewall Administrator, on the File menu, click **New Update**.

To open an existing policy or update
1 In Symantec Client Firewall Administrator, on the File menu, click **Open**.
2 Navigate to the .xml, .cfp, or .cfu file.
3 Click **Open**.

Adding and editing policy descriptions

Symantec Client Firewall Administrator lets you describe policy files and display the description in the About Symantec Client Firewall Help dialog box. The description is limited to 250 characters, and supports ASCII characters 32-126 only. **Figure 8-1** shows the description location in Symantec Client Security firewall client.

**Figure 8-1** Policy description

---

**Note:** Policy descriptions are disabled for .cfu policy update files. After an update, the text (Update) is appended to the policy description on the client.
To add or edit a policy description
1. In Symantec Client Firewall Administrator, on the File menu, click Policy Properties.
2. In the Properties window, under Description, do one of the following:
   ■ Type a policy description.
   ■ Edit the existing policy description.
3. Click OK.

Saving policies and updates
After you finish configuring a policy or update file, save it for later distribution to Symantec Client Security firewall clients.

Save policies or updates
By default, policy files are saved to the \Program Files\Symantec\Symantec Client Firewall Administrator\Policies folder on the computer on which Symantec Client Firewall Administrator is installed. You can, however, save in any location. With the Save As option, you can specify whether to save the policy as an .xml or .cfp policy file.

Note: The procedure for saving update files is the same as saving policy files, but you can only save to .cfu files.
To save a policy to the same policy file name

1. In Symantec Client Firewall Administrator, on the File menu, click **Save**.

2. In the File Save Data Selection dialog box, select the configuration data categories that you want the policy to contain.

3. Click **OK**.
   
   Only the selected categories are saved.

To save a policy to a new policy file name

1. In Symantec Client Firewall Administrator, on the File menu, click **Save As**.

2. In the File Save Data Selection dialog box, select the configuration data categories that you want the policy to contain.

3. Click **OK**.
   
   Only the selected categories are saved.

4. In the Save dialog box, type the location and file name for the policy.

5. In the Files of Type drop-down list, select one of the following file types:
   
   - Policy Packages (*.cfp)
   - XML files (*.xml)

6. Click **Save**.
Importing and exporting policies and updates

When importing a policy, you have the option of importing all settings categories or selected settings categories. This convenience lets you build a new policy using existing settings that do not require change and configure only those categories that do require change. If you want to use Symantec Client Security firewall client to test and customize a policy or update that was created in Symantec Client Firewall Administrator, you must export the policy data.

**Note:** After exporting an update, you should add the updated information to your regular policy files maintained by Symantec Client Firewall Administrator.

Import and export policies and updates

Make sure to install Symantec Client Security firewall client on the same computer as Symantec Client Firewall Administrator before using the Export to Active Client option.

When importing rules created on Symantec Client Security firewall client, rules associated with two or more Locations are identified on the Rules tab as being associated with Multiple Locations. This is also true for rules associated with all Locations on Symantec Client Security firewall client.

When importing settings from the Active Client, IDS signatures are not available.
To import data from an existing policy into Symantec Client Firewall Administrator

1. In Symantec Client Firewall Administrator, on the File menu, click Import.

2. In the File Import Data Selection dialog box, select the categories of configuration data that you want to import.

3. Click OK.

4. In the Open dialog box, navigate to the policy file that contains the data you want to import.

5. Click Open.

To import policy data from the Active Client

1. In Symantec Client Firewall Administrator, on the File menu, click Import from Active Client.

2. In the File Import Data Selection dialog box, select the categories of configuration data that you want to import.

3. Click OK.

4. In the Open dialog box, navigate to the policy file that contains the data you want to import.

5. Click Open.
To export policy or update data to the Active Client
1. In Symantec Client Firewall Administrator, on the File menu, click Export to Active Client.
2. In the Export Data Selection dialog box, select the categories of configuration data that you want to export.
3. Click OK.

About importing and exporting

Note: The information about importing and exporting focuses on locked and unlocked rules, pRules, Zones, and Locations, and assumes that you are proficient in creating rules, pRules, Zones, and Locations. If you are not proficient, you may want to skip this information for now and refer back to it later.

Symantec Client Firewall Administrator is designed to manage administrative policies. When Symantec Client Firewall Administrator opens a policy file and imports content, it is attempting to open the administrative content for the opened policy file. If you allow Symantec Client Security firewall client users to create rules, Zones, or Locations by giving them administrator privileges with Client Settings, the policy files may contain both administrative and user content.

See “Access level settings” on page 323.

Symantec Client Firewall Administrator lets you create locked and unlocked rules, pRules, and Zones. Symantec Client Security firewall client users, if permitted, can only create unlocked rules, Zones, and Locations. When you save a policy file with Symantec Client Firewall Administrator, the file contains the following:

- Administrative content only
- Locked or unlocked rules, not both
- Locked and unlocked Zones
- Locked Locations only

If the policy file being opened was imported from Symantec Client Security firewall client, the file may contain both administrative and user content. As a result, when Symantec Client Firewall Administrator imports policy fields, it must distinguish between administrative and user content, and import only the administrative content. Because Symantec Client Firewall Administrator lets
you edit and save an administrative policy only, user content will be lost in the imported file.

Therefore, to successfully use importing and exporting, you need to understand the logic behind locked and unlocked settings. Specifically, you must understand when rules and Locations are deleted and preserved, what type of Location information gets imported under certain conditions, what Location configuration settings allow users to select or create Locations, and the processing order of locked and unlocked Zones.

### About importing and exporting rules and pRules

If you permit Symantec Client Security firewall client users to create rules by giving them administrator privileges on the Client Settings tab, these rules are unlocked. A policy file that contains administrative and user content can have a combination of locked and unlocked rules.

When Symantec Client Firewall Administrator imports the rulebase, it uses the following logic:

- If it detects one or more locked rules, it assumes that there is a locked administrative rulebase configured in this policy. Symantec Client Firewall Administrator then imports the locked rulebase only.
- If it doesn't detect one or more locked rules but does detect unlocked rules, it assumes that there is an unlocked administrative rulebase configured in this policy. Symantec Client Firewall Administrator then imports the unlocked rulebase.

**Note:** If you are viewing a policy file with Symantec Client Firewall Administrator and you import settings, you overwrite the viewed policy. Typically, you should create a new policy and then import policy items from other files or computers.

Table 8-1 shows possible client configurations for rules and pRules and the results of importing these configurations to Symantec Client Firewall Administrator.

<table>
<thead>
<tr>
<th>Client configuration</th>
<th>Administrator result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contains locked rules only</td>
<td>Imports all rules</td>
</tr>
<tr>
<td>Contains locked and unlocked rules</td>
<td>Imports locked rules only</td>
</tr>
<tr>
<td>Contains unlocked rules only</td>
<td>Imports all rules</td>
</tr>
</tbody>
</table>
When you import unlocked rules from Symantec Client Security firewall client, the rule setting for Delete unlocked rules on policy integration is always enabled when importing completes. Be sure to verify that this setting is what you want before exporting the imported rulebase. If you subsequently create a locked rulebase, you can disable this function.

See “Configuring rule lock settings” on page 272.

Table 8-2 shows possible administrator configurations for rules and pRules, and shows the results of exporting these configurations to Symantec Client Security firewall client.

### Table 8-2 Exporting rules and pRules

<table>
<thead>
<tr>
<th>Administrator configuration</th>
<th>Client result</th>
</tr>
</thead>
<tbody>
<tr>
<td>One or more pRules</td>
<td>Deletes all existing pRules and adds the new pRules.</td>
</tr>
<tr>
<td>One or more unlocked rules</td>
<td>Deletes all existing locked and unlocked rules and adds the new unlocked rules.</td>
</tr>
<tr>
<td>One or more locked rules</td>
<td>Deletes all existing locked rules and adds the new rules. Administrators can enable or disable the setting for Delete unlocked rules on policy integration.</td>
</tr>
<tr>
<td>Locked rules that match unlocked rules on the client</td>
<td>Merges the locked rules with the unlocked rules and creates duplicates. Locked rules are processed first. <strong>Note:</strong> A setting exists for rules that deletes unlocked rules when exporting (policy integration).</td>
</tr>
</tbody>
</table>

About importing and exporting Locations

All Locations created with Symantec Client Firewall Administrator are locked after exporting to Symantec Client Security firewall client. Symantec Client Security firewall client users cannot delete locked Locations. If you permit client users to create Locations, these Locations are unlocked when created with Symantec Client Security firewall client. You can delete these Locations during export with a setting on the Locations Settings tab.
Table 8-3 shows possible client configurations for locked and unlocked Locations and the results of importing these configurations to Symantec Client Firewall Administrator.

**Table 8-3 Importing Locations**

<table>
<thead>
<tr>
<th>Client configuration</th>
<th>Administrator result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contains locked Locations only</td>
<td>Imports all Locations, associated network connections, and Zones.</td>
</tr>
<tr>
<td>Contains locked and unlocked Locations</td>
<td>Imports locked Locations, associated network connections, and Zones only. Imports network connections associated with unlocked Locations and places them in the Unassigned Connections Location.</td>
</tr>
</tbody>
</table>

About importing and exporting Location Awareness settings

You use Location Awareness to cause client computers to use different rulebases and Zones when they connect to networks from different locations. However, if you do not set a Primary Location and if you do not correctly set other Location settings, Symantec Client Security firewall client prompts users to select a Location when it detects a new network connection. As a result, users must be trusted to select the correct Location.

The Location-specific setting Allow New Connections affects whether users are prompted to select a Location. When you set a Primary Location, the Allow New Connections setting is disabled for all existing Locations. When you create a Location and enable this setting, the Primary Location disappears.

The following global settings affect whether users are prompted to create or select an unlocked Location that allows new connections:

- Allow user to create Locations.
- Delete unlocked Locations.

Table 8-4 shows a few setting combinations and what happens on the client when Symantec Client Security firewall client detects unrecognized network connections. This table does not list all possibilities but indicates where to focus...
when configuring Locations if you want to ensure that users cannot select or create Locations.

**Table 8-4** Exporting Locations

<table>
<thead>
<tr>
<th>Administrator configuration</th>
<th>Client result</th>
</tr>
</thead>
<tbody>
<tr>
<td>■ Allow New Connections: Yes (Location Specific)</td>
<td>Prompts users to select lockedLocations that allow new connections or create a new Location to associate with unrecognized network connections.</td>
</tr>
<tr>
<td>■ Allow user to create locations: Yes (Global)</td>
<td></td>
</tr>
<tr>
<td>■ Delete unlocked locations: Yes (Global)</td>
<td></td>
</tr>
<tr>
<td>■ Allow New Connections: Yes (Location Specific)</td>
<td>Prompts users to select locked or unlocked Locations that allow new connections or create a new Location to associate with unrecognized network connections.</td>
</tr>
<tr>
<td>■ Allow user to create locations: Yes (Global)</td>
<td></td>
</tr>
<tr>
<td>■ Delete unlocked locations: No (Global)</td>
<td></td>
</tr>
<tr>
<td>■ Allow New Connections: No (Location Specific)</td>
<td>Prompts users to create a new Location to associate with unrecognized network connections.</td>
</tr>
<tr>
<td>■ Allow user to create locations: Yes (Global)</td>
<td></td>
</tr>
<tr>
<td>■ Delete unlocked locations: Yes (Global)</td>
<td></td>
</tr>
<tr>
<td>■ Allow New Connections: No (Location Specific)</td>
<td>Does not prompt users to select or create Locations. Uses the Location associated with recognized network connections or the Default Location or Primary Location for unrecognized network connections.</td>
</tr>
<tr>
<td>■ Allow user to create locations: No (Global)</td>
<td></td>
</tr>
<tr>
<td>■ Delete unlocked locations: Yes (Global)</td>
<td></td>
</tr>
</tbody>
</table>

**About importing and saving the default client policy file**

The default Symantec Client Firewall Administrator policy file does not contain rules, pRules, or Locations like the default Symantec Client Security firewall client policy file. After you export a policy file to Symantec Client Security firewall client with a locked rule or Location, you lose the ability to import the default client policy information into Symantec Client Firewall Administrator. The first action that you should take with Symantec Client Firewall Administrator after installing Symantec Client Security firewall client is to import the client policy file and save it.
Merging rules and pRules in policy files

Symantec Client Firewall Administrator lets you merge rules and pRules that are contained in two policy files. The purpose of the merge feature is to let you modify rather than overwrite a rulebase. Specifically, merging modifies existing rules and inserts new rules. The act of merging affects General rules, Program rules, Trojan rules, and pRules only. No other policy settings are affected. Merging rules does not create a third policy file. Instead, it updates the currently viewed file using the contents of a second file.

For example, two policy files, A and B, both contain five identical rules. You modify two of the five rules in B, add three rules to B, and then merge B into A. The merge modifies policy file A by changing two rules and adding three rules, reflecting the changes made to policy file B. Furthermore, rules are never deleted during a merge. So if policy file A in this example had contained an additional 15 rules not contained in B, the merge would have modified file A the same way by changing two rules and adding three rules only.

Note: During a merge, confirmation prompts appear before rules are added and modified.

To modify rules, you must understand how the merge utility determines rule identity, which differs across the rule types. If you change rule identity, the rule is considered new and is not modified in the destination file during a merge.

For example, suppose that policy files A and B contain one identical General rule. You modify the rule in B by changing the description field, and then merge B into A. The merge modifies policy file A by inserting the rule contained in B, and A now contains two rules.

Table 8-5 shows the identifiers for the four rule types.

<table>
<thead>
<tr>
<th>Rule type</th>
<th>Identifiers</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>Description</td>
</tr>
<tr>
<td>Program</td>
<td>■ File Name and associated file location</td>
</tr>
<tr>
<td></td>
<td>■ File MD5 hash, which changes with different versions</td>
</tr>
<tr>
<td>Trojan</td>
<td>Description</td>
</tr>
<tr>
<td>pRule</td>
<td>■ File Name</td>
</tr>
<tr>
<td></td>
<td>■ Description</td>
</tr>
</tbody>
</table>
If you do not use different Locations and use the Default Location only, you do not need to understand how rules are merged for different Locations. If you do use different Locations, you need to understand this information.

Symantec Client Firewall Administrator handles rules and Locations in the following ways (the source file is the file being imported):

- If the source rule specifies All Locations, that setting is preserved for that rule in the target file.
- If a Location of the same name exists in the target file, Locations for source rules are preserved in target rules. If no matching Location exists in the source file, it is not created.
- If source rules have no matching Location assignments or no Location assignments at all, such as rules merged in from older versions, they are assigned to the Default Location in the target file.

You can use the merge utility to manage policy files distributed by Symantec. For example, if you customize the default policy file, receive an updated policy file, and then want to incorporate your customizations into the updated policy file, you can use the merge utility to accomplish this task.

A good way to explore how this utility works is to open two instances of Symantec Client Firewall Administrator, and then create, save, and modify policy files in both instances and practice merging.

**To merge rules and pRules in policy files**

1. In Symantec Client Firewall Administrator, click **File > Open**.
2. In the File Open dialog box, navigate to and select the policy file to modify, and then click **Open**.
3. Click **File > Merge**.
4. In the File Open dialog box, navigate to and select the policy file to merge into the displayed file.
5  Click Open.

6  In the Merge Options window, select one of the following:
   - All Rules
   - Modified Rules Only

7  In the Confirmation window, respond to the provided information as appropriate.
Distributing policies

Policy distribution is the process of rolling out a new policy to one or more groups of Symantec Client Security firewall clients.

Distribution mechanisms include the following:

- Symantec System Center
- Fio.exe policy import/export tool
- Web-based policy package distribution
- Login scripts
- Third-party distribution tools

How policy distribution affects Locations, rules, and settings

When a policy update is distributed to Symantec Client Security firewall client, the previous settings used by clients are modified by those in the new policy according to the following precedence rules:

- All Client and Web settings are replaced.
- All Intrusion Detection System exclusion data is replaced.
- All pRules are replaced.

Rules, Zones, and Locations may or may not be deleted depending on their deletion settings on the associated Settings tabs.

See “About importing and exporting” on page 230.

A policy may include only subsets of data from one or more of the policy categories. If a category is not included in the policy update, the existing client data for that category or group of categories is preserved.

Using the policy file import/export utility

Fio.exe is a command-line utility that is installed with Symantec Client Security firewall client. You can use it to import .cfp, .xml, and .cfu files. Additionally, you can use Fio.exe to export the policy to an .xml file only. Fio.exe must be run on the client computer. Policies exported to .xml files do not include IDS signatures.

Generally, you want to use the Symantec System Center as the distribution mechanism for updating policies. Use of the file import/export utility is usually restricted to special situations, such as when you want to save a policy and Symantec Client Firewall Administrator is not available, or when a policy needs to be updated and the Symantec Client Security firewall client is either
unmanaged or the Symantec System Center is not currently managing that Symantec Client Security firewall client.

The command syntax for the file import/export utility is as follows (parameters in brackets are optional):

```
fio.exe I | O [path] filename [/DisplayProgress] [/Log]
```

When Fio.exe is run, it updates Symantec Client Security firewall client automatically.

Table 8-6 describes the parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>Imports the specified .cfp, .xml, or .cfu file.</td>
</tr>
<tr>
<td>O</td>
<td>Exports the rules and configuration settings from the current Symantec Client Security firewall client to an .xml file.</td>
</tr>
<tr>
<td>path</td>
<td>Fully qualified path to the policy file. If any directory or file name contains spaces, enclose the path in quotation marks.</td>
</tr>
<tr>
<td>filename</td>
<td>Name of the .xml, .cfp, or .cfu file. Export supports .xml files only.</td>
</tr>
<tr>
<td>/DisplayProgress</td>
<td>Displays the Progress dialog box.</td>
</tr>
<tr>
<td>/Log</td>
<td>Creates a log file named Fio.log in the directory from which Fio.exe is run.</td>
</tr>
</tbody>
</table>

For example, to import all properties for a file named NewAdminPkg.cfp and display the Progress dialog box, you would type the following at a command prompt:

```
fio I c:\Admin\Packages\NewAdminPkg.cfp /DisplayProgress
```

To export Administrator properties for a file named NewAdminPkg.xml and not display the Progress dialog box, you would type the following at a command prompt:

```
fio O c:\Admin\Packages\NewAdminPkg.xml
```
Using Location Awareness and Zones

This chapter includes the following topics:

- Using Locations
- Using Network Zones

Using Locations

Locations let you configure rules, Zones, and Location settings for specific network connections made by Symantec Client Security firewall clients. For example, you may have a specific collection of rules, Zones, and Location settings that you want Symantec Client Security to enforce when a client connects to a network using a remote wireless connection, and you may have another collection that you want Symantec Client Security to enforce when a client connects to a network using a local Ethernet connection.

One policy file can be configured with different information for up to 32 Locations. You cannot associate pRules with Locations. When pRules become either General or Program rules, these rules are configured for the current Location only.

The following two primary activities are associated with using Locations:

- Configuring required Location information
- Implementing Location Awareness
Configuring required Location information

Location Awareness is the term used to describe the feature that lets you install different collections of rules and Zones automatically based on client network connection activity. All Symantec Client Firewall Administrator users must understand how to configure required Location information, even if Location Awareness is disabled.

One Location exists after initial Symantec Client Firewall Administrator installation and is called Default. The Default Location is used when Location Awareness is disabled, and certain Global and specific settings for the Default Location are enforced on Symantec Client Security firewall client. The Default Location also plays a role when Location Awareness is enabled.

Furthermore, if you allow client users to create Locations, all rules and Zones associated with the Default Location are automatically created in the user-created Locations.

Note: If you are a new user of Symantec Client Firewall Administrator, do not enable Location Awareness until you are comfortable with configuring and testing rules and Zones (Location Awareness is disabled upon initial installation). If you do not enable Location Awareness, the information for configuring required Location information is all that you need to configure the Default Location for use with Symantec Client Firewall Administrator.

Configuring required Location information involves the following tasks:

■ Specifying Global Settings for Locations
■ Specifying Default Settings for Locations
■ Specifying Location-specific settings

Specifying Global Settings for Locations

Global Location settings specify whether Location Awareness is enabled or disabled, and specify Symantec Client Security firewall client user rights regarding Location manipulation. You use the Enable Network Detector check box on the Settings tab to enable and disable Location Awareness. Figure 9-1 shows the location of the check box.
When Location Awareness is enabled, all rules, Zones, and settings that are configured for Locations are enforced on Symantec Client Security firewall client. When Location Awareness is disabled, all rules, Zones, and settings that are configured for the Default Location are enforced on Symantec Client Security firewall client. If you enable Location Awareness and disable Symantec Client Security firewall client, Location Awareness remains enabled.

If you are not going to use Location Awareness, configure all rules, Zones, and Location settings for the Default Location. Additionally, the Default Location rules and Zones are copied to new Locations that the Symantec Client Security firewall client user creates. You can disable this feature on the Settings tab with the Allow user to create locations check box.

All Locations exported to Symantec Client Security firewall client are locked. The client user cannot delete the exported Locations.

See “About importing and exporting” on page 230.
Table 9-1 describes Global Settings for Locations.

Table 9-1  Global Settings for Locations

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| Enable Network Detector                | Checked: Enables Location Awareness, and the Location configuration installed in Symantec Client Security firewall client is based on network connectivity.  
|                                        | Unchecked: Disables Location Awareness, and the Default Location configuration is enforced on Symantec Client Security firewall client.         |
| Allow user to create locations         | Checked: Allows Admin users to create new Locations. New Locations that they create are created as copies of the Default Location configuration.  
|                                        | Unchecked: Does not allow any user to create new Locations.                                                                                  |
| Delete unlocked locations on policy integration | Checked: Deletes user-created Locations on Symantec Client Security firewall client when the new policy is installed. User-created Locations are always unlocked.  
|                                        | Unchecked: Does not delete user-created Locations on Symantec Client Security firewall client when the new policy is installed.                  |

To specify Global Settings for Locations

- In Symantec Client Firewall Administrator, on the Locations tab, on the Settings tab, check or uncheck the following options:
  - Enable Network Detector
  - Allow user to create locations
  - Delete unlocked locations on policy integration

Specifying default settings for Locations

The Default Settings for Locations populate a Location-specific setting that you can select for any Location that is created with Symantec Client Firewall Administrator. The setting that you select as a default appears in parentheses next to the words Use Default. For example, if you set Allow New Zones to No, the option Use Default (No) appears as a selection. When you change a Default Setting, the setting is automatically changed for all Locations that specify Use Default.
Table 9-2 describes the Default Settings for Locations.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Exception Handling</td>
<td>Prompt: Prompts the user to decide whether to permit or block network activity that is not covered with a rule or pRule.</td>
</tr>
<tr>
<td></td>
<td>Block: Blocks network activity that is not covered with a rule or pRule without prompting the user and without creating a rule.</td>
</tr>
<tr>
<td></td>
<td>Permit: Permits network activity that is not covered with a rule or pRule without prompting the user and without creating a rule.</td>
</tr>
<tr>
<td>Auto Rule Creation</td>
<td>Enabled: Creates a Program rule from a pRule when network activity is defined by a pRule but not covered with a rule.</td>
</tr>
<tr>
<td></td>
<td>Disabled: Does not create a rule from a pRule when network activity is defined by a pRule but not covered with a rule.</td>
</tr>
<tr>
<td>Enable Firewall</td>
<td>Yes: Enables the firewall when the settings for this Location are applied if the firewall is currently disabled.</td>
</tr>
<tr>
<td></td>
<td>No: Leaves the firewall in its current state, either enabled or disabled, when the settings for this Location are applied.</td>
</tr>
<tr>
<td>Allow New Connections</td>
<td>Yes: Lets users add and clear connections for this Location.</td>
</tr>
<tr>
<td></td>
<td>No: Does not let users add or clear connections for this Location.</td>
</tr>
<tr>
<td>Allow New Zones</td>
<td>Yes: Lets Admin users add and delete Zones for this Location.</td>
</tr>
<tr>
<td></td>
<td>No: Does not let users add or delete Zones for this Location.</td>
</tr>
</tbody>
</table>

**Note:** When you set Rule Exception Handling to permit, processing overhead on Symantec Client Security firewall clients may be unacceptable on computers that are slower than 1 GHz. Generally, you use this feature when Profiling only. See “Using Profiling to generate pRules and NetSpecs” on page 302.
To specify Default Settings for Locations

1. In Symantec Client Firewall Administrator, on the Locations tab, on the Connection Management tab, under Locations and Connections, click (Default).

2. Click Edit.

3. In the Edit Location window, click Edit Defaults.

4. In the Edit Defaults window, select the settings to apply to all Locations that use the Use Default setting.

5. Click OK.

Specifying Location-specific settings

Individual settings exist for each Location. Whether or not Location Awareness is enabled or disabled, you should specify settings for the Default Location because all Locations that are created with Symantec Client Security firewall client receive Default Location settings.

To specify Location-specific settings

1. In Symantec Client Firewall Administrator, on the Locations tab, on the Connection Management tab, under Locations and Connections, select a Location, and then click Edit.

2. In the Edit Location window, under Location-specific Settings, select the settings to apply to this Location, and then click OK.

If you select Use Default for any setting, the setting is changed whenever the default is changed in the Edit Defaults window.
Implementing Location Awareness

To implement Location Awareness, you associate rules and Zones with one or more Locations. Implementing and managing Location Awareness involves the following activities:

- Understanding NetSpecs
- Discovering NetSpecs
- Prioritizing NetSpecs
- Profiling NetSpecs
- Adding new Locations
- Adding NetSpecs to Locations
- Moving NetSpecs between Locations
- Selecting a Primary Location
- Enabling the Network Detector
- Deleting Locations

Symantec Client Firewall Administrator supports earlier versions of Symantec Client Security firewall client (earlier than version 7.0) that do not support Location Awareness and that use Default Location information only.

About NetSpecs

To activate the rules, Zones, and settings that are associated with new Locations, you must understand how the clients will access the network from the Locations. After you understand how the clients will access the network, you must associate network connection information with the Location, which acts as a triggering mechanism for loading the associated rules and Zones.
Table 9-3 lists and describes the connection options that you can associate with a Location. The Target column indicates where the NetSpec is located, either on the gateway or on the client.

Table 9-3  Connection options

<table>
<thead>
<tr>
<th>NetSpec</th>
<th>Target</th>
<th>Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gateway MAC Address</td>
<td>Gateway</td>
<td>MAC address</td>
<td>MAC address of the default gateway. Display using the command <code>arp-a</code>. For example: ac-de-48-0e-c6-ab</td>
</tr>
<tr>
<td>Gateway IP Address</td>
<td>Gateway</td>
<td>IP address</td>
<td>IP address of the default gateway. Display using the command <code>ipconfig /all</code>. For example: 192.168.134.5</td>
</tr>
</tbody>
</table>
| **Note:** Private IP addresses are not valid for this NetSpec and will not trigger Location Awareness if they are associated with a Location. (The IP address example of 192.168.134.5 is a private IP address.) Private addresses are not routable on the Internet, and fall into the following ranges:  
  - 10.0.0.0 to 10.255.255.255  
  - 172.16.0.0 to 172.31.255.255  
  - 192.168.0.0 to 192.168.255.255 |
| Subnet Address         | Client | IP address: subnet mask | Network address and subnet mask. Display current IP addresses and subnet mask using the command `ipconfig /all`. For example: 192.168.134.0:255.255.255.0  
This network address is the first address in the subnet. For example, the network address for IP address 192.168.2.63 with subnet mask 255.255.255.0 is 192.168.2.0. The network address for IP address 192.168.2.63 with subnet mask 255.255.255.248 is 192.168.2.56. |
| Domain                 | Client | String          | Connection-specific DNS suffix. Display using the command `ipconfig /all`. For example: symantec.com |
| SSID                   | Gateway, Client | String 32 character maximum | Identifier used for wireless networking. Display using Network Adapter Properties. For example: wireless |
Using Location Awareness and Zones

Using Locations

How to discover NetSpecs

You can display network information using a variety of Windows commands that are executable from the command prompt.

The following list contains some of the more useful commands and options:

- **arp -a**
- **netstat -r**
- **route show**
- **netsh**

Netsh is an interactive shell. Microsoft also provides a useful tool that you can run on Windows 2000 computers called netdiag.exe. When run in verbose, log mode, the tool creates a report file that lists extensive information about

<table>
<thead>
<tr>
<th>Table 9-3</th>
<th>Connection options</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NetSpec</strong></td>
<td><strong>Target</strong></td>
</tr>
<tr>
<td>Dialup Number</td>
<td>Gateway</td>
</tr>
<tr>
<td>Dialup Entry Description</td>
<td>Client</td>
</tr>
<tr>
<td>Interface Description</td>
<td>Client</td>
</tr>
<tr>
<td>Interface Type</td>
<td>Client</td>
</tr>
<tr>
<td>Interface Index</td>
<td>Client</td>
</tr>
</tbody>
</table>
networking and network interface cards (NICs). If you use this command, be aware that this utility provides decimal Interface Index values that you must convert to hexadecimal values before you can use them as NetSpecs if the value is greater than 10. Many Ethernet PCI NICs have Interface Indexes of decimal 16777219, which you must convert to hexadecimal 1000003.

Additionally, a variety of subnet calculators exist that can help identify network addresses for IP address and subnet mask associations, which are used in the Subnet Address network specification.

**Prioritizing NetSpecs**

Symantec Client Firewall Administrator lets you associate multiple connection assignments with Locations. However, the Location activates when the current connection matches the first valid NetSpec from a prioritized list. The list appears on the Location tab's Settings tab.

By default, the NetSpec list is prioritized from top to bottom as shown in Table 9-3. The gateway MAC address has first priority, and the client interface index has last priority. For example, suppose you associate two NetSpecs with a Location: gateway IP address and client subnet address. When the Symantec Client Security firewall client makes a connection, it first checks the gateway IP address. If it doesn’t match the configured NetSpec, the firewall checks the client subnet address.

The prioritized list affects all Locations. Again, using the gateway IP address and client subnet address NetSpecs, suppose you have three Locations. When the Symantec Client Security firewall client makes a connection, it first checks the gateway IP address for a match in all three Locations. If it doesn’t find a match, the firewall then checks the client subnet address in all three Locations.

You cannot type duplicate entries for NetSpecs. For example, you cannot type a gateway IP address of 192.168.2.3 for more than one Location.

**To prioritize NetSpecs**

1. In Symantec Client Firewall Administrator, on the Locations tab, on the Settings tab, under NetSpec Priority List, select the NetSpec to reprioritize.
2. Do one of the following:
   - To set the NetSpec to a higher priority, click **Move Up**.
   - To set the NetSpec to a lower priority, click **Move Down**.
   - To set the NetSpec to the default priority, click **Reset**.
About profiling NetSpecs

Symantec Client Firewall Administrator lets you generate a list of NetSpecs used by client computers running Symantec Client Security firewall client, and then add them to Unassigned Connections on the Profiling tab. This tab also allows you to create pRules using the same technique.

See “Using Profiling to generate pRules and NetSpecs” on page 302.

Adding new Locations

If you allow client computers to connect to your network from different access points, you can create rules and settings that will be installed on the clients before they gain access to your network from these different access points.

Symantec Client Firewall Administrator supports 32 Locations, and Symantec Client Security firewall client supports 64 Locations. For information on Location Settings, See Table 9-2, “Default Settings for Locations,” on page 245.

To add a new Location

1. In Symantec Client Firewall Administrator, on the Locations tab, on the Connection Management tab, click Add Location.
2. In the Add Location dialog box, in the Description box, type a Location description.
   The description is limited to 16 characters.
3. Under Location-specific Settings, select the settings to apply to this Location, and then click OK.

Adding NetSpecs to Locations

To trigger the installation of Location rules and Zones, you must add at least one NetSpec to the Location.

To add a NetSpec to a Location

1. In Symantec Client Firewall Administrator, on the Locations tab, on the Connection Management tab, select a Location.
2. Click Add Connection.
3. In the Add Connection dialog box, in the Description box, type a connection description.
4. In the Select column, select the NetSpec to add.
In the Value column, type the value associated with the NetSpec. See “Connection options” on page 248.

Click OK.

Moving NetSpecs to Locations

You can add NetSpecs at any time, and you can move NetSpecs from one Location to another. Symantec Client Firewall Administrator lets you add NetSpecs to the Unassigned Connections Location, and then when you want to use the NetSpec, you can move it to the desired Location.

If you have multiple NetSpecs for one Location, their priority is governed by the list shown on the Settings tab, not the order in which they appear under a Location.

To move NetSpecs to Locations

1. In Symantec Client Firewall Administrator, on the Locations tab, on the Connection Management tab, select the NetSpec to move.
2. Select one of the following:
   - Move Up
   - Move Down

Selecting a Primary Location

The Primary Location is a Location in which new connection assignments are placed when Symantec Client Security firewall client users are not allowed to make connection assignments. The Location setting for Allow New Connections controls whether or not users can make connection assignments. If you disable Location Awareness, you should make the Default Location the Primary Location. When Location Awareness is enabled, users can only add connections to the Default Location when it is configured as the Primary Location.

If you configure a Location as the Primary Location and then add a new Location that allows new connections, or if you enable Allow User to Create Locations, the Primary Location disappears, forcing you to reset the Primary Location if you still require one.

See “Specifying Global Settings for Locations” on page 242.

If you export policies that do not specify a Primary Location, you may allow Symantec Client Security firewall client users to select Locations that are not appropriate for new network connections.

See “About importing and exporting” on page 230.
To select a Primary Location
1. In Symantec Client Firewall Administrator, on the Locations tab, on the Connection Management tab, under Locations and Connections, select the Location to make Primary.
2. Click Set Primary Location.
3. In the Confirmation dialog box, click Yes.

Enabling the Network Detector
The Network Detector, when enabled, allows the implementation of different rules and Zones for different Locations on Symantec Client Security firewall client.

To enable the Network Detector
◆ In Symantec Client Firewall Administrator, on the Locations tab, on the Settings tab, check Enable Network Detector.

Deleting Locations
When you delete a Location, you need to decide what to do with connections and rules associated with the Location. For example, you can move connections associated with the Location to Unassigned Connections, or you can delete them. You can delete rules associated with only one Location, or you can keep these rules in an unassigned state. Deleting Locations always deletes the associated Zones.

Table 9-4 describes the Location deletion options.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Options</th>
</tr>
</thead>
</table>
| Connections | Move Connections to Unassigned Connections: Moves the connection specifications associated with the Location to the Unassigned Connections on the Connection Management tab.  
Delete Connections: Deletes the connection specifications associated with the Location. |
| Rules       | Keep Orphaned (Unassigned) Rules: Keeps rules associated with the Location in an unassigned state.                                      
Delete Orphaned (Unassigned) Rules: Deletes rules associated with the Location.         |
To delete a Location

1. In Symantec Client Firewall Administrator, on the Locations tab, on the Connection Management tab, select the Location to delete.

2. Click Delete.

3. In the Confirmation dialog box, next to Connections, select one of the following:
   - Move Connections to Unassigned Connections
   - Delete Connections

4. Next to Rules, select one of the following:
   - Keep Orphaned (Unassigned) Rules
   - Delete Orphaned (Unassigned) Rules

5. Click Yes.

Editing Locations and NetSpecs

You can edit Locations and NetSpecs at any time.

To edit a Location or NetSpec

1. In Symantec Client Firewall Administrator, on the Locations tab, on the Connection Management tab, select one of the following:
   - Location
   - Connection

2. Click Edit.

3. Edit the settings.

4. When you are finished editing the settings, click OK.

Using Network Zones

Symantec Client Security firewall client lets you organize IP addresses on your network and the Internet into two Zones: Trusted and Restricted. The firewall permits all traffic to and from IP addresses listed in the Trusted Zone. The firewall blocks all traffic to and from IP addresses listed in the Restricted Zone. The firewall does not block traffic to and from an IP address in the Restricted Zone if the address is the default gateway. The client can still access the Internet.

Settings for rules, IDS monitoring, Web Content, Privacy Control, and Ad Blocking are ignored for Web sites with IP addresses that fall into Trusted
Using Location Awareness and Zones

Additionally, Zones are attributes of Locations only. You cannot create a Zone and make it an attribute of multiple Locations. You can, however, copy Zones to other Locations.

See “Copying Zones to other Locations” on page 256.

**Adding computers to Zones**

If you trust your network completely and do not want to create a Program or General rulebase that supports network activity, you can create a Trusted Zone of IP addresses. All computers with IP addresses that are in the Trusted Zone are free to conduct all client/server communications without being blocked at the firewall.

It is not possible to create overlapping Trusted and Restricted Zones using network addresses and ranges. If you attempt to create overlapping Zones, the system prompts you to decide whether to delete the previously entered Zone.

**To add one or more computers to a Zone**

1. In Symantec Client Firewall Administrator, on the Zones tab, next to Location, select the Location in which to add the Zone.
2. On the Trusted or Restricted Zone tab, click **Add**.
3. In the Add Computer dialog box, select one of the following:
   - Single address: An IP address that identifies the computer
   - Host name: A host name that identifies the computer
   - Network address: A range of IP addresses, created by typing one IP address and a subnet mask
■ Address range: A range of IP addresses, created by typing a beginning and ending IP address
■ Named address group: A collection of IP addresses that may contain single addresses as well as ranges

4 Do one of the following:
■ In the Address boxes, type the necessary information.
■ From the drop-down list, select a Named address group.

5 Click **OK**.

**Copying Zones to other Locations**

Symantec Client Firewall Administrator lets you copy Zones to other Locations. You can copy Zones to the Default Location.

**To copy Zones to other Locations**

1 In Symantec Client Firewall Administrator, on the Zones tab, do one of the following:
   ■ On the Trusted Zone tab, select the Zone to copy.
   ■ On the Restricted Zone tab, select the Zone to copy.

2 In the Copy Zone Address window, do one of the following:
   ■ Select one or more Locations in which to copy the Zone.
   ■ Click **All**.

3 Click **OK**.

**About locking Zones**

Unless you lock a Zone, Symantec Client Security firewall client users can delete the Zone. Padlock icons in the Lock column identify locked settings. No icons in the Lock column identify unlocked settings. You can toggle the setting.
Table 9-5 lists the tabs that contain lockable items and describes the functionality when locked and unlocked.

**Table 9-5** Tabs that contain lockable items

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trusted Zone</td>
<td>Locked: Client users cannot delete the IP address.</td>
</tr>
<tr>
<td></td>
<td>Unlocked: Client users can delete the IP address.</td>
</tr>
<tr>
<td>Restricted Zone</td>
<td>Locked: Client users cannot delete the IP address.</td>
</tr>
<tr>
<td></td>
<td>Unlocked: Client users can delete the IP address.</td>
</tr>
</tbody>
</table>

Table 9-6 shows the processing order for locked and unlocked Trusted and Restricted Zones. To verify that Restricted Zones are always processed, be sure to create locked Restricted Zones.

**Table 9-6** Processing order

<table>
<thead>
<tr>
<th>Zone</th>
<th>Processing order</th>
</tr>
</thead>
<tbody>
<tr>
<td>Locked Restricted</td>
<td>First</td>
</tr>
<tr>
<td>Locked Trusted</td>
<td>Second</td>
</tr>
<tr>
<td>Unlocked Restricted</td>
<td>Third</td>
</tr>
<tr>
<td>Unlocked Trusted</td>
<td>Fourth</td>
</tr>
</tbody>
</table>

Deleting locked and unlocked Zones when exporting policies

Symantec Client Firewall Administrator lets you delete locked and unlocked Zones on Symantec Client Security firewall client when exporting policies. This feature allows you to delete user-created Zones, along with any locked and unlocked Zones that you previously exported to clients. If you allow users to create Zones, these Zones are unlocked.

These settings affect all Locations. Deleting unlocked Zones also deletes unlocked IP addresses from the IDS Exclusions list, and deleting locked Zones deletes locked IP addresses from the IDS Exclusions list.

See “Excluding computers from AutoBlock” on page 318.
**Warning:** Users who can create Zones may decide to create a Trusted Zone range of IP addresses from 0.0.0.0 to 255.255.255.255, where the firewall would permit all traffic to and from all computers on the Internet. This Trusted Zone, however, would not override IP addresses in a Restricted Zone.

To delete locked and unlocked Zones when exporting policies

1. In Symantec Client Firewall Administrator, on the Zones tab, on the Settings tab, do one of the following:
   - Check **Delete locked Zone address on policy integration**.
   - Uncheck **Delete locked Zone addresses on policy integration**.

2. Do one of the following:
   - Check **Delete unlocked Zone address on policy integration**.
   - Uncheck **Delete unlocked Zone addresses on policy integration**.
Creating and testing rules

This chapter includes the following topics:

- About rules
- Working with firewall rules
- Using port groups
- Using address groups
- Incorporating Secure Port
- Testing firewall rules

About rules

Rules are policy components that control how Symantec Client Security firewall client protects computers from malicious incoming traffic, programs, and Trojan horses. The firewall automatically checks all incoming and outgoing packets against these rules, and permits or blocks the packets based on information specified in rules.

Rules are ordered sequentially, from highest to lowest priority, and are inspected in this order. For example, if the first rule does not specify how to handle a packet, the second rule is inspected for information on how to handle a packet. This process continues until a match is found. Once a rule is invoked, the firewall takes the action that the rule specifies, and subsequent lower priority rules are not inspected. If no match is found, the firewall blocks the packet by default.

Symantec Client Security firewall client automatically creates rules for a client computer as it communicates over the Internet, either silently (with the Automatic Program Control setting enabled) or by prompting the user. Firewall
administrators can also create new firewall rules manually using Symantec Client Firewall Administrator.

**Rule categories**

Rules are classified into the following three categories:

- **General rules**: Apply to all client traffic. These rules inspect every inbound and outbound packet for protocols, ports, and source and destination IP addresses.

- **Program rules**: Apply to specific client program traffic. These rules are essentially General rules tailored to specific program executable files.

- **Trojan rules**: Apply to malicious applications disguised as useful applications. These rules typically block traffic on ports associated with Trojan horses. Symantec Client Security firewall client supplies a set of Trojan rules that apply to the characteristics of known Trojan horse threats.

**Rule types**

Rules are categorized as either Locked rules or Unlocked rules. Table 10-1 describes the characteristics of both categories.

<table>
<thead>
<tr>
<th>Rule type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Locked</td>
<td>Symantec Client Security firewall client users cannot modify or delete Locked rules. You can select whether to lock or unlock rules created with Symantec Client Firewall Administrator.</td>
</tr>
<tr>
<td>Unlocked</td>
<td>Symantec Client Security firewall client users with Administrator and Normal privileges create Unlocked rules if permitted with the Global Location Setting. pRules created with Symantec Client Firewall Administrator become Locked or Unlocked rules, depending on how the pRules are configured.</td>
</tr>
</tbody>
</table>

**Rule processing order**

Rules are processed using a priority based on category and type. Packets are inspected with rules until the conditions specified in a rule are met. When the first match occurs, the action specified by the rule is triggered and all further rule evaluation stops, unless the rule is configured to monitor traffic.
Table 10-2 shows how rules are prioritized.

**Table 10-2**  Rule processing priority

<table>
<thead>
<tr>
<th>Priority</th>
<th>Rule category</th>
<th>Rule type</th>
</tr>
</thead>
<tbody>
<tr>
<td>First</td>
<td>Firewall state table</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Second</td>
<td>General</td>
<td>Locked</td>
</tr>
<tr>
<td>Third</td>
<td>Program</td>
<td>Locked</td>
</tr>
<tr>
<td>Fourth</td>
<td>General</td>
<td>Unlocked</td>
</tr>
<tr>
<td>Fifth</td>
<td>Program</td>
<td>Unlocked</td>
</tr>
<tr>
<td>Sixth</td>
<td>Trojan</td>
<td>Locked</td>
</tr>
<tr>
<td>Seventh</td>
<td>Trojan</td>
<td>Unlocked</td>
</tr>
</tbody>
</table>

Symantec Client Security firewall client implements stateful inspection, which automatically permits inbound traffic that is replying to permitted outbound traffic. Information about the outbound traffic is maintained in the firewall state table.

See “About stateful inspection” on page 266.

The firewall administrator may want to order rules within priority categories so that evaluation occurs in a logical sequence. Order rules so that they are evaluated according to exclusivity, with the most restrictive rules evaluated first and the most general rules evaluated last. For example, if you decide to create rules that block traffic, you should place these rules near the top because other rules may permit the traffic.

The Secure Port utility secures ports defined with Trojan rules so completely that all Trojan rules configured as Block take first priority for outbound traffic only.

See “Incorporating Secure Port” on page 279.

**Elements of a rule**

A rule is a collection of settings that characterize network traffic and specify what to do with the traffic when it appears at the firewall. The following list summarizes the settings that you specify when creating a rule:

- Description
- Action to take when matched, such as permit, block, or monitor
- Protocols of TCP, UDP, and ICMP
About rules

- Position of client rulebase insertion after exporting (available for policy updates only)
- Inbound and outbound port numbers
- Source and destination computers
- Tracking options, if any
- Locations

See “About updating rulebases on Symantec Client Security firewall client” on page 272.

General and Trojan rules apply these settings to all traffic. Program rules and pRules apply these settings to traffic that is generated by a specific executable file. pRules do not support Locations.

Figure 10-1 shows the dialog box that you use to configure the rule settings.

**Figure 10-1** Edit Firewall Rule dialog box

**Description**

Description lets you specify the name of the rule so that you can distinguish it from other rules.
Action options

Action options let you specify whether the rule permits, blocks, or monitors the type of network communication defined within the rule.

Table 10-3 describes the available Action options.

Table 10-3  Action options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permit</td>
<td>Allows communication of this type to take place.</td>
</tr>
<tr>
<td>Block</td>
<td>Prevents communication of this type from taking place.</td>
</tr>
<tr>
<td>Monitor</td>
<td>Updates the Firewall tab in the Symantec Client Security firewall client Event Log. Rule processing then continues until a match is found. If there is no match, the communication is either blocked by default or an Automatic Program Control alert appears.</td>
</tr>
</tbody>
</table>

Connection options

Connection options let you specify whether the rule applies to inbound network traffic, outbound network traffic, or network traffic in both directions.

Table 10-4 describes the available Connection options.

Table 10-4  Connection options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outbound</td>
<td>The rule applies to outbound traffic from your computer to other computers.</td>
</tr>
<tr>
<td>Inbound</td>
<td>The rule applies to inbound traffic from other computers to your computer.</td>
</tr>
<tr>
<td>Both</td>
<td>The rule applies to both inbound and outbound traffic.</td>
</tr>
</tbody>
</table>

To simplify rulebase management, specify both inbound and outbound traffic in a rule whenever possible.
Protocol options

Protocol options let you specify the protocols that a rule controls. 

*Table 10-5* describes the available Protocol options.

**Table 10-5**  Protocol options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>The rule applies to Transmission Control Protocol (TCP) traffic.</td>
</tr>
<tr>
<td>UDP</td>
<td>The rule applies to User Datagram Protocol (UDP) traffic.</td>
</tr>
<tr>
<td>TCP and UDP</td>
<td>The rule applies to both TCP and UDP traffic.</td>
</tr>
<tr>
<td>ICMP</td>
<td>The rule applies to Internet Control Message Protocol (ICMP) traffic. ICMP</td>
</tr>
<tr>
<td></td>
<td>applies to General rules and Trojan rules only.</td>
</tr>
</tbody>
</table>

Ports options

Ports options let you specify the ports that are controlled by a rule. Typically, specific types of traffic occur on specific ports. For example, Web traffic generally occurs on ports 80 and 443.

*Table 10-6* describes the available Ports options.

**Table 10-6**  Ports options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single port</td>
<td>The rule applies to traffic on one port. Requires you to type one port number.</td>
</tr>
<tr>
<td>Port range</td>
<td>The rule applies to traffic on a range of ports. Requires you to type a beginning and ending port number.</td>
</tr>
<tr>
<td>List of ports</td>
<td>The rule applies to traffic on a list of ports. Requires you to type and add ports one at a time.</td>
</tr>
<tr>
<td>Named ports</td>
<td>The rule applies to traffic on all ports listed in a named port group. Requires you to select a named port. See “Using port groups” on page 273.</td>
</tr>
<tr>
<td>Any port</td>
<td>The rule applies to traffic on all ports.</td>
</tr>
</tbody>
</table>
Computers options

Computers options let you specify the computers and network adapters to which a rule applies.

Table 10-7 describes the available Computers options.

Table 10-7  Computers options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Computers:</td>
<td>The rule applies to all remote computers.</td>
</tr>
<tr>
<td>Any computer</td>
<td></td>
</tr>
<tr>
<td>Remote Computers:</td>
<td>The rule applies to one IP address, a range of IP addresses, or to IP addresses in a named IP address group.</td>
</tr>
<tr>
<td>Computer list</td>
<td></td>
</tr>
<tr>
<td>Network Adapters:</td>
<td>The rule applies to all network adapters in the local computer. An Ethernet card is a network adapter.</td>
</tr>
<tr>
<td>Any adapter</td>
<td></td>
</tr>
<tr>
<td>Network Adapters:</td>
<td>The rule applies to one or more network adapters in the local computer, which are specified using IP addresses.</td>
</tr>
<tr>
<td>Adapter list</td>
<td></td>
</tr>
</tbody>
</table>

IP addressing options

IP addressing options let you specify the IP addresses of remote and local computers when you do not specify all computers.

Table 10-8 describes the available IP addressing options.

Table 10-8  IP Addressing options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single address</td>
<td>The rule applies to one IP address. Requires you to type one IP address only.</td>
</tr>
<tr>
<td>Host name</td>
<td>The rule applies to one host name. Requires you to type one host name only. Adding a host name generates a DNS query, so you must have a rule that permits DNS queries.</td>
</tr>
<tr>
<td>Network Address</td>
<td>The rule applies to a range of IP addresses. Requires you to type one IP address and a subnet mask. For example, typing an IP address of 192.168.1.0 and a subnet mask of 255.255.255.0 creates a range of IP addresses from 192.168.1.0-192.168.1.255. Using a subnet mask, you can define a range as small as two IP addresses, or as large as all IP addresses in the class C network.</td>
</tr>
<tr>
<td>Address Range</td>
<td>The rule applies to a range of IP addresses. Requires you to type a beginning IP address and an ending IP address.</td>
</tr>
</tbody>
</table>
About rules

Tracking options

Tracking options let you specify whether the program should notify you or create an Event Log entry when a network traffic event matches the criteria set for this rule.

Table 10-9 describes the available Tracking options.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Write an event log entry when this rule is matched</td>
<td>An entry is written in the firewall Event Log when this rule is matched.</td>
</tr>
<tr>
<td>Create Security Alert when this rule is logged</td>
<td>A Security Alert dialog box appears when this rule is matched.</td>
</tr>
</tbody>
</table>

Location options

Location options let you specify Locations to which this rule applies. Rules are not used unless they are assigned to a Location. You can assign rules to one, many, or all Locations.

About stateful inspection

Symantec Client Security firewall client uses stateful inspection, which creates a connection state table that tracks information about current connections such as IP addresses, ports, applications, and so forth. Symantec Client Security firewall client makes traffic flow decisions using this connection information before inspecting General and Program rules.
For example, if a firewall rule permits a client to connect to a Web server, the firewall logs connection information in the state table. When the server replies, the firewall checks the state table, discovers that a response from the Web server to the client is expected, and permits the Web server traffic to flow to the initiating client without inspecting the rulebase.

**Note:** A rule must permit the initial traffic before the firewall logs the connection in the state table.

Stateful inspection allows you to simplify rulebases because you don’t have to create rules that permit traffic in both directions for traffic typically initiated in one direction. Client traffic typically initiated in one direction includes Telnet (port 23), FTP (ports 20 and 21), HTTP (port 80), and HTTPS (port 443). Clients initiate this traffic outbound so you only have to create a rule that permits outbound traffic for these protocols. The firewall permits the return traffic when it inspects the state table.

By configuring outbound rules only, when possible, you increase client security in the following two ways:

- You reduce rulebase complexity.
- You eliminate the possibility that a worm or other malicious program can initiate connections to a client on ports configured for outbound traffic only.

You can also configure inbound rules only, for traffic to clients that clients do not initiate.

Stateful inspection supports all rules that filter TCP/UDP traffic, but does not support rules that filter ICMP traffic. For ICMP, you must create rules that permit traffic in both directions when necessary. For example, if you want clients to use the ping command and receive replies, you must create a rule that permits ICMP traffic in both directions.

**Working with firewall rules**

Firewall rules are created using Symantec Client Firewall Administrator, saved to a new policy, and distributed to firewalls. Firewall rules can also be created on Symantec Client Security firewall client, if the user has the proper access level.
Creating rules

To simplify rulebase management, specify both inbound and outbound traffic in one rule whenever possible. Additionally, you do not need to create inbound rules for traffic such as HTTP and FTP because Symantec Client Security firewall client uses stateful inspection and does not need a rule to filter return traffic initiated by clients.

See “About stateful inspection” on page 266.

If you are not yet familiar with Locations, or if you do not want to use Location Awareness, you can apply the rule to the Default Location only. Another option is to assign the rule to All Locations.

See “Using Locations” on page 241.

Note: The ICMP protocol is available for General and Trojan rules only.

To create a rule

1. Do one of the following:
   - If you are creating a Program rule, begin with step 2.
   - If you are creating a General or Trojan rule, select the appropriate tab, and begin with step 7.

2. In Symantec Client Firewall Administrator, on the Rules tab, on the Program Rules tab, under Program, click Add.

3. In the Add Program dialog box, on the Program tab, in the Description box, type a rule description.

4. Do one of the following:
   - In the File Name box, type the path to a program executable file.
   - Click Browse, and then locate and select an executable file.

5. On the Locations tab, do one of the following:
   - Click Apply rule to all locations.
   - Click Apply rule to the following selected locations, and then select the Locations to associate with this Program rule.

6. Click OK.
7 Under Rules, click **Add**.

![Add Firewall Rule dialog box](image)

8 In the Add Firewall Rule dialog box, in the Action list, select one of the following:
- Block
- Permit
- Monitor

9 In the Connection list, select one of the following:
- Inbound
- Outbound
- Both

10 In the Protocol list, select one of the following:
- UDP
- TCP
- TCP and UDP

11 On the Ports tab, under Remote Ports and Local Ports, select one of the following:
- Single port
- Port range
- List of ports
Creating and testing rules

Working with firewall rules

- Named ports
- Any ports

12. On the Computers tab, under Remote Computers, select one of the following:
   - Any computer
   - Computer list

13. Under Network Adapters (on the local computer), select one of the following:
   - Any computer
   - Computer list

14. On the Tracking tab, specify none, one, or both of the following:
   - Write an event log entry when this rule is matched
   - Create Security Alert when this rule is logged

15. On the Locations tab, select one of the following:
   - Apply rule to all locations
   - Apply rule to the following selected locations, and then select the Locations to associate with this rule

   If you are creating a Program rule, these Locations can be a subset of the Locations that you selected for the Program executable file in step 4. You can use this subset to enable and disable certain program features at different Locations that permit the program to execute.

16. Click OK.

Displaying rules by Location

Symantec Client Firewall Administrator lets you display the rules configured for specific Locations. To display rules used at all Locations, select the Master list Location.

To display rules for specific Locations

1. In Symantec Client Firewall Administrator, on the Rules tab, in the Locations list, select the Location for which to display rules.

2. Click the General Rules, Program Rules, and Trojan Rules tabs.
Adding rules to different Locations

Symantec Client Firewall Administrator lets you add existing rules to Locations.

**To add a rule to a Location**

1. In Symantec Client Firewall Administrator, on the Rules tab, select one of the following rule types:
   - General Rules
   - Program Rules
   - Trojan Rules
2. Select the rule to add to a Location, and then click **Edit**.
3. On the Locations tab, select one of the following:
   - Apply rule to all locations: To select all Locations.
   - Apply rule to the following selected locations, and then select the Locations to associate with this rule.
4. Click **OK**.

Deleting rules

Symantec Client Firewall Administrator lets you delete rules from one Location or all Locations.

**To delete a rule**

1. In Symantec Client Firewall Administrator, next to Location, do one of the following:
   - Select a Location that contains the rule to delete.
   - To delete rules from all Locations, click **Master list**.
2. On one of the following tabs, select the rule to delete:
   - General Rules
   - Program Rules
   - Trojan Rules
3. Click **Delete**.
4. If you did not click Master list, in the Delete Rule window, select one of the following:
   - Remove selected rules from the <selected> location
   - Delete selected rules from all locations
5. Click **OK**.
Creating and testing rules

Working with firewall rules

Configuring rule lock settings

Symantec Client Firewall Administrator lets you lock and unlock all rules before you export the policy to Symantec Client Security firewall client. You can also delete all unlocked rules on Symantec Client Security firewall client when you export locked rules.

After you import an unlocked rulebase from Symantec Client Security firewall client, the setting for Delete unlocked rules on policy integration is always enabled. Be sure to verify that this setting is what you want before you export the imported rulebase.

See “About importing and exporting rules and pRules” on page 231.

To lock or unlock rules

1. In Symantec Client Firewall Administrator, on the Rules tab, on the Settings tab, next to Rule set is, select one of the following:
   - Locked
   - Unlocked

2. If you selected Locked, to delete unlocked client rules during export, check Delete unlocked rules on policy integration.

About updating rulebases on Symantec Client Security firewall client

Symantec Client Firewall Administrator lets you update rules for All Locations on Symantec Client Security firewall client. This feature is useful if you have client ports that may be transmitting or receiving worms and you want to restrict all network traffic from those subnets that are attacking your clients. You can only add rules and pRules to update files, and you can only update All Locations.

When you create rules for updates, you can select whether updated rules are positioned at the top or bottom of the rulebase. If you position them at the top, the ordering in Symantec Client Security firewall client is the reverse of what you see in Symantec Client Firewall Administrator. If you position them at the bottom, the ordering in Symantec Client Security firewall client does not change. If you are exporting an update to block traffic, you should insert the rules at the top of the rulebase.

See “Configuring policies and updates” on page 223.

See “About importing and exporting” on page 230.
Using port groups

Symantec Client Firewall Administrator supports using port groups. A port group is a collection of port numbers grouped under one name. The purpose of port groups is to eliminate the retyping of port numbers.

For example, Table 10-10 shows three pRules that support Windows 2000 networking in an Active Directory environment. All rules are permitted, bidirectional rules.

### Table 10-10  Sample program rulebase

<table>
<thead>
<tr>
<th>pRule executable</th>
<th>Description</th>
<th>Protocol</th>
<th>Remote ports</th>
<th>Local ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lsass.exe</td>
<td>Kerberos</td>
<td>UDP</td>
<td>88</td>
<td>1024-5000</td>
</tr>
<tr>
<td></td>
<td>EPmap</td>
<td>TCP</td>
<td>135</td>
<td>1024-5000</td>
</tr>
<tr>
<td></td>
<td>LDAP</td>
<td>TCP, UDP</td>
<td>389</td>
<td>1024-5000</td>
</tr>
<tr>
<td></td>
<td>Nterm</td>
<td>TCP</td>
<td>1026</td>
<td>1024-5000</td>
</tr>
<tr>
<td>Explorer.exe</td>
<td>LDAP</td>
<td>TCP, UDP</td>
<td>389</td>
<td>1024-5000</td>
</tr>
<tr>
<td>Winlogon.exe</td>
<td>LDAP</td>
<td>TCP, UDP</td>
<td>389</td>
<td>1024-5000</td>
</tr>
</tbody>
</table>

An LDAP rule is required for each pRule executable. To create each rule without using port groups, you must type the LDAP port numbers for remote and local ports three times, once for each pRule executable. Using port groups, you could configure two groups for LDAP ports, and then select them from a drop-down list. Table 10-11 shows two groups that support this operation.

### Table 10-11  Sample port groups

<table>
<thead>
<tr>
<th>Group name</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP Remote</td>
<td>389</td>
</tr>
<tr>
<td>Range 1024-5000</td>
<td>1024-5000</td>
</tr>
</tbody>
</table>

The group named Range 1024-5000 can also be selected for each pRule shown in Table 10-10.

Adding named port groups

You can add port groups in all windows that let you create firewall rules. Port groups do not support mixed lists of ports, such as two specific ports along with a port range. You can enter one port, multiple ports, or a port range only. As you incorporate port groups into rules, you should consider documenting the rules and the group names. If you decide later to delete a port group, you must first
remove the port group from all rules that reference the group. Having the documentation makes deleting groups easier. You can add a named port group from either the Rules or pRules tab.

**To add a named port group**

1. In Symantec Client Firewall Administrator, on the Rules tab, select any rule on one of the following tabs:
   - General Rules
   - Program Rules
   - Trojan Rules
2. Click **Edit**.
3 In the Edit Firewall Rule window, on the Ports tab, do one of the following:
   ■ Under Remote Ports, check **Named ports**, and then click **Edit**.
   ■ Under Local Ports, check **Named ports**, and then click **Edit**.

4 In the Edit Named Ports window, click **New**.

5 In the New Port Group window, in the Named port box, type a name for the port group, and then click **OK**.

6 In the Edit Named Ports window, add one or more ports to the new group, and then click **Close**.

7 In the Edit Firewall Rule window, click **OK**.

---

**Deleting named port groups**

You can delete port groups from all windows that let you create firewall rules. However, before you can delete a port group, you must remove the port group from all rules that reference the group. You can delete a named port group from either the Rules or pRules tab.

**To delete a named port group**

1 In Symantec Client Firewall Administrator, on the Rules tab, select any rule on one of the following tabs:
   ■ General Rules
   ■ Program Rules
   ■ Trojan Rules

2 Click **Edit**.
3 In the Edit Firewall Rule window, on the Ports tab, do one of the following:
   ■ Under Remote Ports, check Named ports, and then click Edit.
   ■ Under Local Ports, check Named ports, and then click Edit.

4 In the Edit Named Ports window, in the Named port(s) drop-down list, select the group to delete, and then click Delete.

5 If the named group is referenced by one or more rules or pRules, in the Message window, click OK.

6 In the Edit Named Ports window, click Close.

7 In the Edit Firewall Rule window, click OK.

8 If you completed step 5, locate the rules or pRules that reference the port group that you tried to delete, deselect the port group, then repeat steps 1 through 7.

Using address groups

Symantec Client Firewall Administrator supports using address groups. An address group is a collection of IP addresses or host names grouped under one name. For example, if you have multiple IP addresses configured for the Trusted Zone, you can add these IP addresses to an address group, and then select the group from a drop-down list. The purpose of address groups is to eliminate the retyping of IP addresses.

Address groups are available for the following:
   ■ Rules
   ■ Zones
   ■ IDS IP addresses
Adding named address groups

Address groups support mixed lists of addresses or host names. As a result, you can add two specific IP addresses, an IP address range, and a network address to the same group.

As you incorporate address groups, you should consider documenting where the groups are used. If you decide later to delete an address group, you must first remove the address group from all rules, Zones, and IDS IP addresses that reference the group. Having the documentation makes deleting groups easier.

When you add a named address group, you can use the user interface for Zones or any other interface that supports adding IP addresses for rules and IDS AutoBlock Exclusions.

To add a named address group

1. In Symantec Client Firewall Administrator, on the Zones tab, click Add.
2 In the Add Computer window, click **Named address group**, and then click **Edit**.

![Edit Address Groups window](image)

3 In the Edit Address Groups window, click **New**.

4 In the New Address Group window, in the Group name box, type a name for the address group, and then click **OK**.

5 In the Edit Address Groups window, in the Address group drop-down list, select the new group, and then click **Add**.

6 In the Add Computer window, add the appropriate IP addresses, and then click **OK**.

7 Repeat step 6 until you finish adding IP addresses to the group, and then click **Close**.

### Deleting named address groups

You can delete address groups from all windows that let you create rules, Zones, and IDS IP addresses. However, before you can delete an address group, you must remove the address group from all rules, Zones, and IDS IP addresses that reference the group.

When you delete a named address group, you can use the user interface for Zones or any other interface that supports adding IP addresses for rules and IDS AutoBlock Exclusions.
To delete a named address group
1. In Symantec Client Firewall Administrator, on the Zones tab, click Add.
2. In the Add Computer window, click Named address group, and then click Edit.
3. In the Edit Address Groups window, in the Address group drop-down list, select the address group to delete, and then click Delete.
4. If the named group is referenced by one or more rules, pRules, Zones, or AutoBlock Exclusions, in the Message window, click OK.
5. In the Edit Address Groups window, click Close.
6. In the Edit Computer window, click OK.
7. If you completed step 4, locate the rules, Zones, or IDS IP addresses that reference the address group that you tried to delete, deselect the address group, and then repeat steps 1 through 6.

Incorporating Secure Port

Secure Port blocks TCP and UDP outbound traffic on local ports defined in Trojan rules and ports defined by users running Symantec Client Security firewall client. Secure Port secures the ports so completely that outbound traffic originating from these ports never triggers firewall rulebase inspection. Because the rulebase is not inspected for these ports for outbound traffic, firewall alert messages for outbound traffic never appear for these ports even when the Always Display Security Alerts feature is enabled. The rulebase is inspected for inbound traffic destined for these ports. You can enable and disable Secure Port on the Client Settings tab.

See “Global settings” on page 323.

Secure Port secures all local ports configured as Block in Trojan rules. If the local ports are also configured as Permit in General rules, the ports are still
Creating and testing rules

Incorporating Secure Port

secured and override the General setting. For example, consider the General rules shown in Table 10-12, which support Windows networking.

**Table 10-12** Sample bidirectional, permitted, General rules

<table>
<thead>
<tr>
<th>Description</th>
<th>Protocol</th>
<th>Remote ports</th>
<th>Local ports</th>
<th>Remote addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>TCP</td>
<td>80</td>
<td>1024-5000</td>
<td>192.168.100.0/24</td>
</tr>
<tr>
<td>Kerberos</td>
<td>UDP</td>
<td>88</td>
<td>1024-5000</td>
<td>192.168.100.0/24</td>
</tr>
<tr>
<td>EPmap</td>
<td>TCP</td>
<td>135</td>
<td>1024-5000</td>
<td>192.168.100.0/24</td>
</tr>
<tr>
<td>NetBIOS</td>
<td>TCP, UDP</td>
<td>137, 138, 139</td>
<td>1024-5000</td>
<td>192.168.100.0/24</td>
</tr>
<tr>
<td>LDAP</td>
<td>TCP, UDP</td>
<td>389</td>
<td>1024-5000</td>
<td>192.168.100.0/24</td>
</tr>
</tbody>
</table>

Notice that the rules permit local clients to transmit and receive traffic with local ports 1024-5000, which is necessary because these protocols communicate with clients using random ports beginning with 1024. The rules limit this traffic to IP addresses between 192.168.100.0 and 192.168.100.255 (/24 is shorthand for subnet mask 255.255.255.0).

Because these rules are General and permitted, Trojan rules that are configured to block ports inside this range never get enforced. As a result, clients are exposed to attacks across local ports 1024-5000 from remote ports 80, 88, 135, 137, 138, 139, and 389 in the 192.168.100.x network.

**Note:** Port 5000 may not be an appropriate upper limit for client computers that are rarely restarted. Use packet capturing tools to discover appropriate upper limits for your organization.

To mitigate this exposure, Secure Port secures ports for outbound traffic so that Windows programs do not attempt to use the secured ports. When Secure Port is enabled, Windows programs that use random ports know that the ports are secured and skip them during random port sequencing. As a result, Secure Port protects clients against Trojan horses that use ports inside General permitted port ranges without interrupting networking traffic.

For example, the following traffic capture shows client/server HTTP traffic, where local client ports are randomly sequencing upwards beginning with port 1676. The remote server port 80 remains static. Before this packet capture, ports
1680 to 1720 were configured as blocked with a Trojan rule, and Secure Port was enabled.

Notice in the middle of the capture that the local ports jumped from 1676 to 1721, indicating that the local Web browser never attempted to use ports in the 1680 to 1720 range.

**Note:** Secure Port secures ports defined as Local Block in Trojan rules only, and also secures these ports in Trusted Zones.

### Testing firewall rules

After a program has been run several times on a Symantec Client Security firewall client and all of its features have been used, many rules will have been built. It is important to exercise every possible use, connection, port, and operation of the program to get the most complete characterization of the program. It is helpful if you can determine in advance how a program is accessing the Internet. For example, some programs call for the use of consecutive ports, while others use random ports.

The Test Rules dialog box lets Symantec Client Security administrators test firewall rules, pRules, and Zones for every Location and for all policy file types, including updates. Testing does not involve sending or receiving packets. The
Creating and testing rules

Testing firewall rules

The procedure for testing TCP and UDP rules is not the same as the procedure for testing ICMP rules.

Because Symantec Client Security firewall client is stateful, some rules may permit traffic even though they test negative. For example, if you configure an HTTP outbound rule only, the firewall permits inbound HTTP traffic, as long as the traffic is a reply to outbound traffic that the client initiated. If you have an HTTP rule configured for outbound traffic only, the test for inbound HTTP traffic will fail, indicating that Web servers cannot initiate inbound traffic to Web clients.

**Test inbound and outbound rules for TCP, UDP, and ICMP**

When testing inbound rules, you must type a port number for Local Port. When testing outbound rules, you must type a port number for Remote Port and a remote IP address. Additionally, ICMP uses command numbers, not port numbers. Common command numbers are 0 for echo reply, 3 for destination unreachable, 8 for echo request, and so forth.

**To test an outbound rule for TCP or UDP**

1. In Symantec Client Firewall Administrator, on the Rules tab, click **Test Rules**.

2. In the Test Rules dialog box, under Direction, click **Outbound**.

3. Under Protocol, select one of the following:
   - TCP
   - UDP

4. Under Remote Port, type a port number.
5. Under Remote Address, type the IP address or host name of a remote computer.

6. Under Local Port, do one of the following:
   - Check Any local port.
   - Uncheck Any local port and type a port number.

7. Under Local Adapter, do one of the following:
   - Check Any adapter.
   - Uncheck Any adapter, and then type an IP address.

8. Under Program, do one of the following:
   - Check Any program.
   - Uncheck Any program, and then type the fully qualified path to the program including the name of the executable.
   - Uncheck Any program, click Browse, and then navigate to and open the target executable.

9. Click Test.

10. In the Test Results dialog box, click Close.

To test an inbound rule for TCP or UDP

1. In Symantec Client Firewall Administrator, on the Rules tab, click Test Rules.

2. In the Test Rules dialog box, under Direction, click Inbound.

3. Under Protocol, select one of the following:
   - TCP
   - UDP

4. Under Remote Port, do one of the following:
   - Check Any remote port.
   - Uncheck Any remote port, and then type a port number.

5. Under Remote Address, do one of the following:
   - Check Any address.
   - Uncheck Any address, and then type an IP address or host name of a remote computer.

6. Under Local Port, type a port number.

7. Under Local Adapter, type an IP address.
8 Under Program, do one of the following:
   - Check Any program.
   - Uncheck Any program, and then type the fully qualified path to the program including the name of the executable.
   - Uncheck Any program, click Browse, and then navigate to and open the target executable.

9 Click Test.

10 In the Test Results dialog box, click Close.

To test an inbound rule for ICMP
1 In Symantec Client Firewall Administrator, on the Rules tab, click Test Rules.

2 In the Test Rules dialog box, under Direction, click Inbound.

3 Under Protocol, click ICMP.

4 Under ICMP Command, type an ICMP command number.

5 Under Remote Address, do one of the following:
   - Check Any address.
   - Uncheck Any address, and then type an IP address or host name of a remote computer.

6 Under Local Adapter, type an IP address.

7 Under Program, do one of the following:
   - Check Any program.
   - Uncheck Any program, and then type the fully qualified path to the program including the name of the executable.
   - Uncheck Any program, click Browse, and then navigate to and open the target executable.

8 Click Test.

9 In the Test Results dialog box, click Close.

To test an outbound rule for ICMP
1 At the top of the Symantec Client Firewall Administrator window, on the Rules tab, click Test Rules.

2 In the Test Rules dialog box, under Direction, click Outbound.

3 Under Protocol, click ICMP.

4 Under ICMP Command, type an ICMP command number.
5 Under Remote Address, type an IP address or host name of a remote computer.

6 Under Local Adapter, do one of the following:
   ■ Check **Any adapter**.
   ■ Uncheck **Any adapter** and type an IP address.

7 Under Program, do one of the following:
   ■ Check **Any program**.
   ■ Uncheck **Any program**, and then type the fully qualified path to the program including the name of the executable.
   ■ Uncheck **Any program**, click **Browse**, and then navigate to and open the target executable.

8 Click **Test**.

9 In the Test Results dialog box, click **Close**.
Creating and testing rules
Testing firewall rules
Using pRules

This chapter includes the following topics:

- **About pRules**
- **Symantec-supplied pRules**
- **Creating and editing pRules**
- **Configuring pRules to support Active Directory**
- **Using Profiling to generate pRules and NetSpecs**

**About pRules**

A pRule, or potential rule, contains the data required to validate an Internet-enabled program and then create a Program rule on the firewall client. The first time that a program is run, its corresponding pRule is processed. If the program matches the pRule criteria, Symantec Client Security firewall client creates a Program rule using information that is contained in the pRule.

Once a Program rule is generated from a pRule on a client computer, the pRule is never applied again because the Program rule has a higher processing priority than the pRule. If the Program rule is deleted, the pRule may be applied again. Using pRules lets Symantec Client Security firewall client generate Program rules as they are needed rather than creating a large number of Program rules that may never be used.

pRules are not used on a Symantec Client Security firewall client until a program is run on the client and one of the following exists:

- No Program rule for the program is in place.
- A rule is in place, but the rule does not cover all the access that the program needs; for example, the rule allows only outbound TCP access on remote
port 80 for Internet Explorer, but the program needs access to remote port 443.

A set of Symantec-supplied pRules, corresponding to many commonly used Internet-enabled programs, is installed on a firewall client when the default policy package is rolled out. This default set of pRules should be customized by an administrator using the Symantec Client Firewall Administrator or extended to include administrator-created, custom pRules for additional internal corporate or external programs and then rolled out to clients as part of a policy package.

**Note:** You cannot associate pRules with Locations. When pRules become Program rules, these rules are configured for the current Location only. If a program communicates from a new Location, the pRule becomes a Program rule for the new Location.

**pRules and user types**

By default, most pRules are configured to create Unlocked Program rules, but you can modify them to create Locked Program rules. To ensure client manageability, several Symantec Client Security firewall client pRules associated with Symantec components create Locked rules. Any Program rule generated from a pRule on the client is, by default, also of rule type Unlocked.

Unlike Locked rules, Unlocked rules are not replaced when a policy package is rolled out to a client. Any Program rules generated from pRules that are of type Unlocked remain in force on the client.

**Using a digest value to identify a program**

A pRule can include a digest, or program signature, that Symantec Client Security firewall client uses to validate the program’s executable file before applying any rule criteria. The digest is a hash value based on unique internal information about the program’s executable file.

For the set of pRules supplied with Symantec Client Security firewall client, the program digests are guaranteed to identify authentic copies of the program.

For pRules that you create for new programs with Symantec Client Firewall Administrator, you generate the digests, or program signatures, based on the executable files that you specify. Before creating a new pRule, make certain that the executable file referred to is the genuine program and has not been replaced or altered by a Trojan horse.
The digest is the most stringent means with which to securely identify a program. This capability is useful for preventing threats, such as malicious programs impersonating genuine programs from executing on the network.

Priority of pRule evaluation

A pRule is evaluated after all Zones, AutoBlock lists, and rules are evaluated, as shown in Table 11-1.

Table 11-1  Client program evaluation order

<table>
<thead>
<tr>
<th>Order</th>
<th>Process</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Match the IP address associated with the program against IP addresses in the Zones and AutoBlock lists.</td>
<td>If a match occurs, perform the action (permit, block, or monitor) and stop any further processing. If monitor or no match occurs, continue with rule processing.</td>
</tr>
<tr>
<td>2</td>
<td>Check all rules in the following order of priority:</td>
<td>The first time that a match occurs, perform the action (permit, block, or monitor) and stop any further rule processing. If monitor or no match occurs, continue with pRule processing.</td>
</tr>
<tr>
<td></td>
<td>■ General Locked rules</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Program Locked rules</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ General Unlocked rules</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Program Unlocked rules</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Trojan Locked rules</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Trojan Unlocked rules</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Check pRules.</td>
<td>If a matching pRule exists for the program, then create the Program rule defined from the pRule data on the client and perform the specified action (permit, block, or monitor).</td>
</tr>
</tbody>
</table>

Program rules and pRules

A pRule also contains information about the rules that determines the conditions under which a program is permitted to connect to the Internet.

In most cases, rule sets for pRules are designed to permit, rather than block, Internet access. The rule sets defined when creating a pRule are usually such that only expected behaviors by the program, such as communicating through the program’s default port, are permitted.
If a pRule exists for a program and the program is executed on a client, two possible courses of events can take place:

- If the Automatic Program Control setting is enabled on the client, Symantec Client Security firewall client silently creates a Program rule and a corresponding rule set that includes permitting the program to communicate over the Internet using the program's designated ports. In most cases, using the Automatic Program Control setting for firewalls is recommended. This minimizes the number of firewall alerts and firewall configuration requests that users receive. You can selectively override automatic rule creation for single pRules in the Add and Edit pRule dialog boxes.

- If the Automatic Program Control setting is not enabled on the client, a sequence of alerts and messages is displayed on the client that require user input for configuring the program. The client is queried as to whether to create a Program rule, and which rule settings to use when the program is executed.

  See “Specifying default settings for Locations” on page 244.
  See “Global settings” on page 323.

**Guidelines for using pRules**

Following are some guidelines and recommendations for using pRules:

- pRules are most useful when there are many computers in an organization using a divergent set of programs. When many clients in an organization are using the same small set of programs installed in the same volume and directory, using Program rules instead of pRules is simpler.

- When deciding whether to create a Program rule or a pRule, consider that in a Program rule you must specify the fully qualified path. Therefore, the location of the executable file must be correct on all the client computers that use the information. A pRule is path independent; that is, you only have to specify the executable file name.

- If a client user has access rights to create local rules on Symantec Client Security firewall client, and creates a rule for a program before its pRule is executed, the pRule will never be triggered. When the program is run on the client, the Program rule, being of a higher priority, will always be applied before the pRule can be used.

  In cases such as these, make certain there is no conflict of intent between the Program rule and the pRule. For example, the pRule specifying to block a communication and the Program rule created by the user specifying to permit a communication.
Any time that a version update is made to a program with a pRule, the pRule must be reconfigured through Symantec Client Firewall Administrator. If the pRule is not reconfigured, Symantec Client Security firewall client cannot match the pRule against the program executable and the firewall will block the program from running and will post alerts (users with an access level of Restricted will not receive alerts). When updating a program version, it is possible to retain information about earlier versions so that they can still execute.

If clients are using programs that are updated frequently, consider not creating a pRule digest entry for the program to simplify administration. If the program is updated occasionally, consider creating a pRule that applies to different program versions. If you use a digest match criterion in the pRule for the program, you can optionally use other rules along with the match criterion to regulate the program's Internet connection behavior. See “Digest match criteria” on page 298.

pRules are most useful for clients with an access level of Restricted. They are less useful for clients with an access level of Normal or Admin, because clients with those access levels can create their own rules. If a user creates, for example, a local Program rule for the same program covered by a pRule, the Program rule, being of a higher priority will always execute before the pRule, rendering the pRule irrelevant.

Symantec-supplied pRules

The default policy package for firewalls contains a set of pRules that provide coverage for many commonly used commercially available programs, as well as Windows subsystem executables. You can view the list of pRules in the current policy package loaded into Symantec Client Security firewall client by importing them to Symantec Client Firewall Administrator.

You can update pRules with LiveUpdate. When you use LiveUpdate, custom pRules that you added are deleted. Therefore, it is good practice to create new pRules in a separate policy file, and then merge that policy file with the newly updated policy file.

See “Merging rules and pRules in policy files” on page 235.

Note: You should import pRules from Symantec Client Security firewall client immediately after client installation and save them in a policy file. If you export a policy file to a Symantec Client Security firewall client that contains one pRule, you will delete all pRules on the client.
To view the pRules in the current policy package

1. In Symantec Client Firewall Administrator, on the File menu, click **Import from Active Client**.
2. On the pRules tab, scroll through the list to view the current pRules or see if a specific executable file for a program is secured by a pRule.

Creating and editing pRules

In addition to the Symantec-supplied set of pRules, you can create new pRules using Symantec Client Firewall Administrator. This capability lets you add protection for commercially available programs for which pRules are not supplied and for internal corporate programs.

You create or modify a pRule for distribution to firewalls by configuring the following four sets of options for the pRule:

- **Program identity**: Specify the program's executable file and supply a brief description of the program.
- **Match names**: Generate program match names, which label sets of match criteria that are used to authenticate a program's executable file. Each match name for the pRule has separate associated match criteria.
Using pRules

Creating and editing pRules

- Match criteria: Configure the values the pRule uses to verify the program before allowing it to communicate. You can configure one or more sets of match criteria for an individual pRule, with each match set containing one or more match criteria. You select from among the following match criteria:

  - **File Version**: Specify a version number or range of version numbers for the program to use as a match.
  - **Version Data**: Specify file resource property values to use as match criteria. After you select this option, you can select one of the following: Comments, Company name, File description, Internal name, Original file name, Product name, Product version, Legal copyright, or Legal trademarks.
  - **Required Digest**: Specify a pRule digest value to use for matching the Internet-enabled program.
    
    Using a required digest match means that the program executable must be authenticated by the digest or a security alert is triggered. It is the strongest method of verifying the authenticity of a program.
  - **Optional Digest**: Specify a pRule digest value to use for matching the program.
    
    Using an optional digest match means that if the program executable is not validated by the digest, other match criteria, such as company name, can be applied without triggering a security alert, for example.
  - **File Size**: Specify a program executable file size or a range of possible file sizes to use for matching the program.

- **Rules**: Configure the Program rule that will be created on Symantec Client Security firewall client once the executable file specified by the pRule has been validated.

**Create new pRules or edit existing pRules**

You can create new pRules or modify existing pRules.

**To create a new pRule**

- In Symantec Client Firewall Administrator, on the pRules tab, click **Add**.
To edit an existing pRule

- In Symantec Client Firewall Administrator, on the pRules tab, select an existing pRule, and then click **Edit**.

Selectively disabling auto-create

Symantec Client Firewall Administrator includes a pRule option to never auto-create Program rules from pRules without user intervention. Enable or disable this option under the Description field in the Add pRule and Edit pRule windows.

See “Specifying default settings for Locations” on page 244.

Ignoring file name matching

By default, Symantec Client Firewall Administrator verifies that the executable file name matches the internal name and original file name as match criteria for the program when a pRule is added. Enable or disable this option under the Description field in the Add pRule and Edit pRule windows.

Most executable files have internal names and original file names in headers. You can view these names by looking at file version properties. For security reasons, when you use the default Any Version match criteria, Symantec Client Security firewall client requires executable file headers to contain this
information. The file name matching feature prevents malicious code from overwriting a permitted pRule program file and executing on client computers, which would happen if the firewall checked for the correct .exe name only.

Specifying the program identity for a pRule

The program identity is the executable name of the program.

To specify the program identity for a pRule

1. In Symantec Client Firewall Administrator, on the pRules tab, select one of the following:
   - Add: Create a new pRule.
   - Edit: Open an existing pRule.

2. In the Add or Edit pRule dialog box, in the File name text box, type or confirm the executable name of the program.
   Do not type the path to the executable file (for example, NewApp.exe).

3. In the Description text box, type a description of the program.

4. Click **OK**.

Adding or editing match names for a pRule

Each match name for the pRule is associated with a set of match criteria that the pRule uses to validate the executable file including file size, file version, version information, and digest value.

To add or edit match names for a pRule

1. In Symantec Client Firewall Administrator, on the pRules tab, select one of the following:
   - Add: Create a new pRule.
   - Edit: Open an existing pRule.

2. In the Add or Edit pRule dialog box, under Matches, do one of the following:
   - To add a match name, click **Add**.
     By default, the Match name is the file name with a sequential number appended (for example, NewApp.exe-0). You can rename the Match name by clicking Edit and changing the name in the Edit Match Name dialog box.
     By default, the associated match criteria is set to Any Version. This value is overwritten when a new value is set.
To modify an existing match name, select the match name, and then click **Edit**.

3. Click **OK**.

### Configuring match criteria

Match criteria are the types of information used to validate a program and their values.

#### Configure match criteria

You begin working with match criteria by selecting from among five types of available criteria. Each of the match criteria types has a dialog box that requests appropriate information. For example, File Size allows you to enter one or more file sizes or a size range that the program must match when the pRule is processed on Symantec Client Security firewall client.

#### To specify new match criteria

1. In Symantec Client Firewall Administrator, on the pRules tab, select one of the following:
   - **Add**: Create a new pRule.
   - **Edit**: Open an existing pRule.

2. In the Add pRule or Edit pRule dialog box, under Matches, select a match name.

3. Under Match Criteria, click **Add**.

4. In the Add Match Criteria dialog box, select one of the five match criteria, and then click **OK**.
To modify existing match criteria
1  In Symantec Client Firewall Administrator, on the pRules tab, select one of the following:
   ■ Add: Create a new pRule.
   ■ Edit: Open an existing pRule.
2  In the Add pRule or Edit pRule dialog box, under Matches, select a match name.
3  Under Match Criteria, select the item, and then click Edit.

To specify the match criteria
1  In the Add or Edit pRule Match Criteria dialog box, type the requested information, and then click Add.
2  Do one of the following:
   ■ If this is the only value that you want validated, click OK to close the Add pRule Match Criteria dialog box.
   ■ To add additional values, in the Add or Edit pRule Match Criteria dialog box, type the information, and then click Add after each value.
3  When finished, click OK to close the Add pRule Match Criteria dialog box.

File version match criteria
File version match criteria can include specific file versions for the program as well as file version ranges. When you configure version match criteria, you can specify one of the following for file matching:
■ A single version number
■ A list of nonconsecutive version numbers
■ A range of version numbers
You can use either the standard four-part version naming convention for version data (four numbers separated by three periods, for example, 8.0.0.1) or as few digits as are necessary to specify the version or versions that you want.
If you specify fewer than four digits, the remaining digits are wildcards. For example, if you specify a value of 2.0, it matches any value from 2.0.0.0 to 2.0.9.9.
**Version data match criteria**

Version data match criteria includes the following resource properties that are associated with the program:

- **Comments**: Use the value of the comments property that is associated with the program’s executable file.
- **Company name**: Use the value of the company name property that is associated with the program executable, if one exists.
- **File description**: Use the value for the description property of the program’s executable file.
- **Internal name**: Use the value of the internal name property of the program executable, if one exists. If no internal file name value was specified before the program was compiled, this value defaults to the program file name without the file suffix.
- **Original file name**: Use the name that the program executable was created with, before any renaming of the file happened.
- **Product name**: Use the product name that was distributed with this version of the program’s executable file.
- **Product version**: Use the version of the product with which the program’s executable file is distributed. A product version number is a 64-bit number displayed according to the format major number.minor number.build number.private part number, such as the value 9.0.3517.0.
- **Legal copyright**: Use the property value that represents the legal copyright of the program.
- **Legal trademarks**: Use the property value that represents the trademarks of the program.

A file property that is listed under Resource Name may or may not exist for a given executable file. Examine the Version page of a program’s property box, viewable in Windows Explorer, to check which file properties are available.

**Digest match criteria**

A pRule digest is a program signature that is derived from a scan of the code sections of a program’s executable file. A digest value uniquely identifies a program’s executable file. When the pRule is invoked on Symantec Client Security firewall client, the program’s digest value is recomputed and compared to the stored digest value of the pRule. For a match to occur, the digest of the executed program on Symantec Client Security firewall client must exactly match that of its digest entry.
Creating and editing pRules

Using a digest as a match criterion provides high-level security for verifying the authenticity of a program. A required digest provides the maximum level of security possible, while an optional digest provides a lower level of security, but greater flexibility in handling different versions of a program. To enable rules to be automatically generated on a client computer the first time that a program is run, you need to have already defined a pRule for the program with a digest.

The executable file name used in a pRule can be associated with more than one program. The same file name can correspond to different programs on a client (for example, Setup.exe) or different versions of a program (for example, Internet Explorer). In this case, you can create several match names, each with a required digest value corresponding to a different executable.

Note: There can be up to six digest values per program match name. Whenever a program is updated, either the pRule digest value must also be updated or a new digest must be added to the pRule. If this is not done, the new version of the program will be blocked from executing.

Required digest match criteria

When you use the required digest match selection, and the program associated with the pRule is run, Symantec Client Security firewall client checks the required digest value for each match name according to the match name order:

■ If a match occurs with a required digest value the first time that a program is executed on a client, the Program rule is created automatically on the client computer.

■ If Symantec Client Security firewall client is unable to match the program against any required digest value in the pRule, a security alert is posted, and a sequence of dialog boxes prompts the user to configure rules for the program.

Note: Restricted users cannot configure Program rules.

Note that once a pRule becomes a Program rule, the path locations for the executable files associated with the pRule cannot be changed, or the Program rule will not work.

Optional digest match criteria

The optional digest match selection works similarly to the required digest match selection. However, if the optional digest match fails, other match criteria in the same set are checked. If another criterion in the match set containing the optional digest is matched, no security alert is triggered.
You can use the optional digest value as the only match criterion in a match set. When you do so, and the associated program is run, one of the following behaviors can occur:

- If a match occurs between the program and the optional digest value, the rules for the program auto-create on the client.
- If a match does not occur, the user receives a prompt, and can select whether to allow Symantec Client Security firewall client to automatically configure a rule for the program (using the pRule data), or manually configure the rule by completing the Symantec Client Security firewall client prompts.

**File size match criteria**

You can specify either a list of nonconsecutive file size values, or a range of file sizes to use for matching.

**Adding a rule to a pRule**

After a pRule is triggered and the corresponding program runs, the pRule becomes a Program rule and is governed by the rules associated with the program. You can selectively lock and unlock the rules that you associate with the pRule.

See “Configuring rule lock settings” on page 272.

**To add a rule to a pRule**

1. In Symantec Client Firewall Administrator, on the pRules tab, select a rule, and then click **Edit**.
2. In the Add pRules dialog box, under Rules, click **Add**.
3. In the Add Firewall Rule dialog box, enter the necessary information to create the rule.
4. Click **OK**.
5. In the Edit pRule dialog box, click **OK**.
Configuring pRules to support Active Directory

Typically, a Windows 2000/NT client in a Windows 2000 network uses the following processes for networking in an Active Directory environment:

- `C:\Winnt\System32\Lsass.exe` supports Kerberos, LDAP, EPmap, and Nterm
- `C:\Winnt\System32\Services.exe` supports NTP, Bootp, Kerberos, DNS, and EPmap
- `C:\Winnt\Explorer.exe` supports LDAP
- `C:\Winnt\System32\Winlogon.exe` supports LDAP

Windows Subsystem supports NetBIOS and SMB.

Table 11-2 shows a rulebase that supports Windows 2000 networking in an Active Directory environment. All rules are permitted bidirectional rules unless indicated in the Description column.

**Table 11-2** Sample program rulebase

<table>
<thead>
<tr>
<th>Executable</th>
<th>Description</th>
<th>Protocol</th>
<th>Remote ports</th>
<th>Local ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lsass.exe</td>
<td>Kerberos, EPmap, LDAP, Nterm</td>
<td>UDP</td>
<td>88</td>
<td>1024-5000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TCP</td>
<td>135</td>
<td>1024-5000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TCP, UDP</td>
<td>389</td>
<td>1024-5000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TCP</td>
<td>1026</td>
<td>1024-5000</td>
</tr>
<tr>
<td>Services.exe</td>
<td>DNS, Bootp, Kerberos, NTP, EPmap</td>
<td>TCP, UDP</td>
<td>53</td>
<td>1024-5000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>UDP</td>
<td>67, 68</td>
<td>1024-5000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>UDP</td>
<td>88</td>
<td>1024-5000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>UDP</td>
<td>123</td>
<td>1024-5000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TCP</td>
<td>135</td>
<td>1024-5000</td>
</tr>
<tr>
<td>Explorer.exe</td>
<td>LDAP</td>
<td>TCP, UDP</td>
<td>389</td>
<td>1024-5000</td>
</tr>
<tr>
<td>Winlogon.exe</td>
<td>LDAP</td>
<td>TCP, UDP</td>
<td>389</td>
<td>1024-5000</td>
</tr>
<tr>
<td>System</td>
<td>NetBIOS, NetBIOS to 139 (inbound only), SMB (microsoft-ds)</td>
<td>TCP, UDP</td>
<td>137, 138, 139</td>
<td>0, 139, 1024-5000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TCP</td>
<td>445</td>
<td>1024-5000</td>
</tr>
</tbody>
</table>

Additionally, be sure to verify that locked, General rules are not blocking protocols, such as SMB and EPmap, and that the upper port range of 5000 is satisfactory in your environment.
Using Profiling to generate pRules and NetSpecs

Symantec Client Firewall Administrator lets you gather information about network traffic and connections that occur on managed Symantec Client Security firewall clients. You can then use the Profiling feature to view the traffic generated and received by clients and quickly create pRules and NetSpecs to support the traffic. Profiled network connections are used with Location Awareness.

See “About NetSpecs” on page 247.

To retrieve the information from Symantec Client Security firewall clients, you must use Symantec System Center. You retrieve the information in the same way that you retrieve firewall logs.

Profiling overview

Profiling pRules and NetSpecs involves using several Symantec Client Security components in a specific order. Table 11-3 provides an overview of the components, settings, and activities used in Profiling.

Table 11-3  Profiling overview

<table>
<thead>
<tr>
<th>Component</th>
<th>Settings and activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symantec Client Firewall Administrator</td>
<td>Configure the following settings:</td>
</tr>
<tr>
<td></td>
<td>■ Enable Profiling for programs.</td>
</tr>
<tr>
<td></td>
<td>■ Enable Profiling for connections.</td>
</tr>
<tr>
<td></td>
<td>■ Specify the amount of time to profile.</td>
</tr>
<tr>
<td></td>
<td>■ For Locations, set Rule Exception Handling to Permit, Block, or Prompt.</td>
</tr>
<tr>
<td>Select one of the following components:</td>
<td>Export the policy file to Symantec Client Security firewall client.</td>
</tr>
<tr>
<td>■ Symantec Client Firewall Administrator</td>
<td></td>
</tr>
<tr>
<td>■ Symantec System Center</td>
<td></td>
</tr>
</tbody>
</table>
Table 11-3 Profiling overview

<table>
<thead>
<tr>
<th>Component</th>
<th>Settings and activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symantec Client Security firewall client</td>
<td>Perform a variety of networking activity such as the following:</td>
</tr>
<tr>
<td></td>
<td>■ Display network servers in a window.</td>
</tr>
<tr>
<td></td>
<td>■ Connect to the Internet.</td>
</tr>
<tr>
<td></td>
<td>■ Connect to an Internet email account or secure Web site over HTTPS.</td>
</tr>
<tr>
<td></td>
<td>■ Perform LiveUpdate from Symantec Client Security firewall client.</td>
</tr>
<tr>
<td></td>
<td>■ Print.</td>
</tr>
<tr>
<td></td>
<td>■ Execute the following DHCP commands from the DOS command line:</td>
</tr>
<tr>
<td></td>
<td>ipconfig /release</td>
</tr>
<tr>
<td></td>
<td>ipconfig /renew</td>
</tr>
<tr>
<td></td>
<td>■ Restart your computer, and log on and authenticate to a domain.</td>
</tr>
<tr>
<td></td>
<td>■ Send and receive email.</td>
</tr>
<tr>
<td>Symantec System Center</td>
<td>Perform the following activities:</td>
</tr>
<tr>
<td></td>
<td>■ Right-click the client computer.</td>
</tr>
<tr>
<td></td>
<td>■ Using All Tasks, view the profiled firewall exceptions and then the profiled firewall connections.</td>
</tr>
<tr>
<td></td>
<td>■ Save each profile as a .csv comma-delimited file.</td>
</tr>
<tr>
<td>Symantec Client Firewall Administrator</td>
<td>Perform the following activities:</td>
</tr>
<tr>
<td></td>
<td>■ Retrieve the .csv file that contains the profiled firewall exceptions.</td>
</tr>
<tr>
<td></td>
<td>■ Select an exception and process it. A pRule either gets created or updated.</td>
</tr>
<tr>
<td></td>
<td>■ Open the .csv file that contains the profiled connections.</td>
</tr>
<tr>
<td></td>
<td>■ Select a connection and process it. A NetSpec is added to the user-specified Location.</td>
</tr>
<tr>
<td>Select one of the following components:</td>
<td>Export the policy file to Symantec Client Security firewall client.</td>
</tr>
<tr>
<td>■ Symantec Client Firewall Administrator</td>
<td></td>
</tr>
<tr>
<td>■ Symantec System Center</td>
<td></td>
</tr>
<tr>
<td>■ Fio.exe</td>
<td></td>
</tr>
</tbody>
</table>
If you have pRules in the policy, traffic matching these rules is not profiled. The Program rule is created and is not treated as an exception.

### Enabling Profiling in policy files

Symantec Client Firewall Administrator lets you enable Profiling in policy files.

**To enable Profiling in policy files**

1. In Symantec Client Firewall Administrator, on the Locations tab, on the Connection Management tab, select a Location that may be used during Profiling.
2. Click **Edit**.
3. In the Edit Location window, next to Rule Exception Handling, click **Permit**, and then click **OK**.
4. Repeat steps 1 through 3 for each Location that may be used during Profiling.
5. On the Profiling tab, click **Options**.
6. In the Profiling Options window, check one or both of the following:
   - Enable application profiling
   - Enable connection profiling
7. In the Profiling Options window, do one of the following:
   - Check **Continuous profiling**.
   - Check **Suspend profiling after**, and then type the number of days.
8. Click **OK**.
9. Click **File > Save**.

### About exporting the policy file to clients

To enable Symantec Client Security firewall clients to save profiled data, you must export the policy file to one or more clients. You can use a variety of tools and ways to export the policy file, including Symantec System Center and Symantec Client Firewall Administrator.

See “Importing and exporting policies and updates” on page 228.

See “Distributing policies” on page 238.
Viewing and saving profiled data with Symantec System Center

Symantec System Center lets you view and save profiled data from Symantec Client Security firewall clients to files with .csv extensions. Also, consider using Symantec System Center to sort large amounts of data because Symantec Client Firewall Administrator does not support sorting.

See “About sorting with Symantec System Center” on page 312.

To view and save profiled data with Symantec System Center

1. In Symantec System Center, in the right pane, right-click the client that contains profiled information, and then do one of the following:
   - Click All Tasks > Symantec Client Firewall > View Profiled Firewall Exceptions.
   - Click All Tasks > Symantec Client Firewall > View Profiled Connections.

2. In the Environmental Profiling Firewall Exceptions window, drag the window edges sideways to enlarge it and inspect the data, and click column headings to sort the data.
Most likely you will want to sort the File Information column.

3 To save the sorted data, do the following:
   ■ Click the floppy disk icon.
   ■ In the Save As window, next to File name, type a file name.
   ■ Click Save.

Retrieving profiled information

You should open a policy file to update before retrieving (opening) .csv files, which contain update information to integrate with a policy file.

To retrieve profiled information

1 In Symantec Client Firewall Administrator, on the Profiling tab, click Retrieve.

2 In the File Open window, browse to and select the .csv file to open.

3 Click Open.
Processing profiled firewall rule exceptions

You process profiled firewall rule exceptions to create pRules or update existing pRules with the same digest. When you begin processing information, Symantec Client Firewall Administrator prompts you to decide whether to update the existing policy file or open a new one. Table 11-4 lists and describes the options.

Table 11-4  Policy file choices

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Close/save the current policy file and open the “&lt;profiled policy&gt;” policy file before processing “&lt;profiled policy&gt;” events.</td>
<td>Gives you the option to open and update the policy file that you pushed to the Symantec Client Security firewall client for Profiling</td>
</tr>
<tr>
<td>Process “&lt;profiled policy&gt;” events using the current “&lt;currently opened&gt;” policy file.</td>
<td>Gives you the option to update the policy file that you are currently viewing</td>
</tr>
<tr>
<td>Close/save the current policy file and create a new, empty policy file before processing “&lt;profiled policy&gt;” events.</td>
<td>Gives you the option to update a new, default policy file</td>
</tr>
</tbody>
</table>

If you are unfamiliar with Profiling, select the last option to create a new policy file so that you can become familiar with creating and updating pRules. Then, process an exception to create a pRule, and then reprocess the exception but add a different port number when prompted to see how the pRule that you created the first time was updated with the additional port number.

After processing one entry, Symantec Client Firewall Administrator compares all entries against the pRules. If a pRule does not match the executable file, a new pRule is created. If a pRule is matched but the program digest is different, a new program digest is added to the pRule. If a pRule is matched but does not contain the rule for the port number and IP addresses processed, a new rule is added to the pRule. Furthermore, all profiled exceptions that match pRule entries are marked as processed so you do not waste time processing those entries.

See “Refreshing profiled data” on page 310.
When you use the Processing Wizard, the local and remote ports that you see on the Profiling tab are not what will be configured in one of the connection directions, because the wizard does not support specific local and remote ports. In one direction, the ports are always configured as Any. In the other direction, you can enter specific ports. You can also enter Any ports for both local and remote ports. Table 11-5 shows which port setting, local or remote, defaults to Any, based on the connection type that you select.

Table 11-5  Inbound and outbound port processing

<table>
<thead>
<tr>
<th>Connection type</th>
<th>Ports that default to Any</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connections to other computers</td>
<td>Local ports</td>
</tr>
<tr>
<td>Connections from other computers</td>
<td>Remote ports</td>
</tr>
<tr>
<td>Connections to and from other computers</td>
<td>Local ports</td>
</tr>
</tbody>
</table>

**Note:** The buttons for Mark Processed and Mark Unprocessed are used as visual indicators only. They do not provide processing functionality.

To process profiled firewall rule exceptions

1. In Symantec Client Firewall Administrator, on the Profiling tab, select an exception to process.
2. Click **Process**.

3. In the Select Policy for Profile Event Processing window, select one of the options, and then click **OK**.
   
   See Table 11-4, “Policy file choices,” on page 307.
4 In the Add Rule window, select one of the following rule actions, and then click **Next**:
   - Permit
   - Block
   - Monitor

5 To log when this rule is matched, under Do you want to track new connections, check **Write an event log entry when a connection matches this rule**.

6 Click **Next**.

7 Select one of the following connection options, and then click **Next**:
   - Connections to other computers
   - Connections from other computers
   - Connections to and from other computers

8 Select the computers and adapters to permit, block, or monitor, and then click **Next**.
   - If you select a specific adapter IP address that conflicts with Location connection specifications, the rule may never be enforced.

9 Select the protocols and ports to permit, block, or monitor, and then click **Next**.

10 Type a description for the rule, and then click **Finish**.
   - A check appears on the left side of the profiled selection, indicating that it was processed.

11 On the pRule tab, verify that the pRule was created, and edit as necessary.

**Processing profiled connections**

The purpose of processing profiled firewall connections is to add them to Unassigned Connections on the Location tab’s Connection Management tab, where you can move and associate the profiled connections with Locations. When you begin processing connections, Symantec Client Firewall Administrator prompts you to decide whether to update the existing policy file or open a new one. **Table 11-4** lists and describes the options in the prompt.

If you are unfamiliar with Profiling, select the last option to create a new policy file so that you can become familiar with how processing works to create connections for Locations.
**Note:** The buttons for Mark Processed and Mark Unprocessed are used as visual indicators only. They do not provide processing functionality.

### To process profiled connections

1. In Symantec Client Firewall Administrator, on the Profiling tab, select an exception to process.
2. Click **Process**.
3. In the Select Policy for Profile Event Processing window, select one of the options, and then click **OK**. See Table 11-4, “Policy file choices,” on page 307.
4. In the Edit Connection window, next to Description, type a description.
5. Next to Location, select a Location.
6. Click **OK**.
7. On the Locations tab, on the Connection Management tab, verify that the connection was assigned to the desired Location.
8. To move the connection to a Location, click **Move Up** until the connection is associated with the desired Location.

### Refreshing profiled data

You can refresh profiled data to display the profiled data that is and is not contained in pRules, rules, Zones, or NetSpecs. The Refresh feature allows you to quickly reveal which profiled data to work with. After you refresh data, entries that are contained in pRules, rules, Zones, or NetSpecs contain a check mark in the left column. Data entries that are not contained in pRules, rules, Zones, or NetSpecs do not contain a check mark in the left column.

#### To refresh profiled data

- In Symantec Client Firewall Administrator, on the Profiling tab, click **Refresh Status**.

### About working with .csv files

To better understand the Profiling process, you may want to export a core set of rules and pRules that support corporate networking, and then profile the exceptions. Profiled data viewed with Symantec System Center may also grow quite large after a few days, so you need to know how to extract relevant information and manage growth.
The purpose of Profiling firewall exceptions is to generate a list of connection activity with which to create pRules. Exporting a policy file full of rules may defeat this purpose, depending on your situation. Additionally, you typically do not want to profile programs performing loopback operations because loopback operations are internal communications only.

Local Ethernet adapters have an internal IP address of 127.0.0.1, which is not routable. When you see both local and remote IP addresses as 127.0.0.1 in profiled data, the program is performing a loopback operation, which is common for some programs. You do not want to create pRules for specific executable files that support traffic to or from any address of 127.0.0.1. Rather, you should create a loopback General rule that permits all TCP/UDP traffic to and from local remote address 127.0.0.1.

A good starting point is to create a policy file with the Program rules that support Symantec client products, and a few General rules. To get the Program rules, import a recently installed Symantec Client Security firewall client policy, and then delete all rules and pRules with the exception of Program rules. After importing, be sure to set Firewall Exception handling to Permit for all Locations.

Then, create three General rules, one for loopback, one for ICMP, and one for Rtvscan.exe to support Symantec System Center communications. Table 11-6 shows information necessary to create these rules. Be sure to set the local address for Loopback to 127.0.0.1 to prevent attacks from spoofed remote addresses.

**Table 11-6** Sample Profiling General rulebase

<table>
<thead>
<tr>
<th>Description</th>
<th>Protocol</th>
<th>Remote ports</th>
<th>Local ports</th>
<th>Remote addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loopback</td>
<td>TCP, UDP</td>
<td>Any</td>
<td>Any</td>
<td>127.0.0.1</td>
</tr>
<tr>
<td>ICMP</td>
<td>ICMP</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
</tr>
<tr>
<td>Rtvscan.exe</td>
<td>UDP</td>
<td>2967, 53</td>
<td>2967</td>
<td>Any</td>
</tr>
</tbody>
</table>

Next, on the Client Settings tab, disable as many features as possible to increase performance if performance is an issue. Be sure to disable stealthing blocked ports. Finally, you may also want to create pRules to support Active Directory. The resulting rulebase should allow your client computer to operate in a relatively normal manner, while generating exception data for a small number of programs in a strict corporate environment. pRules that become Program rules do not appear in profiled data.

See “Configuring pRules to support Active Directory” on page 301.
About sorting with Symantec System Center

For programs that use random ports, such as Web browsers, your profiled firewall exception list may contain quite a few entries for a single application. Each time that the program uses a new random port, the firewall profiles the exception. In these cases, you may find that you need to sort data. Two of the more beneficial attributes to sort on are IP destination address and file information.

Sorting on IP destination address is useful because it allows you to separate exceptions that are performing loopback operations to address 127.0.01. Sorting on file information is useful because it allows you to separate exceptions that are using random ports for a single executable file.

If you find it necessary to sort data, you can use Symantec System Center before saving and importing the .csv file into Symantec Client Firewall Administrator.

Reducing the amount of profiled data

The data profiled on Symantec Client Security firewall clients is logged by the antivirus client. Each time that you view the profiled data with Symantec System Center, the data that appears may be as old as the oldest log file, which is typically configured to remain on clients for 31 days. If you have a large amount of profiled data, you may want to delete it and start over.

Warning: When you delete logs, you delete information generated by Symantec AntiVirus client, including infection and scanning histories.

Reduce the amount of profiled data

You have the following two options for reducing the amount of profiled data:

■ Filter the logs when viewing them with Symantec System Center.
■ Reduce the antivirus client history configuration time, which actually deletes log files.

To filter the logs

1. In Symantec System Center, in the right pane, right-click the client that contains profiled information, and then click All Tasks > Symantec Client Firewall > View Profiled Firewall Exceptions.

2. In the Environmental Profiling Firewall Exceptions window, in the drop-down list, select a time value that is smaller than the current setting.
To reduce the history configuration time

1. On the client computer that is profiling data, on the Windows taskbar, click **Start > Programs > Symantec Client Security > Symantec AntiVirus client**.

2. In the Symantec AntiVirus window, on the File menu, click **Configure Histories**.

3. Next to Delete After, do one of the following:
   - Select a lesser number of days to keep log data.
   - To purge all logs, select 1 day.

4. Click **OK**.
Using pRules

Using Profiling to generate pRules and NetSpecs
Customizing Intrusion Detection

This chapter includes the following topics:

- About the Intrusion Detection System
- Excluding attack signatures from being blocked
- Configuring AutoBlock
- Locking IDS exclusions and IP addresses

About the Intrusion Detection System

The Intrusion Detection System (IDS) used in Symantec Client Security firewall client scans each packet that enters and exits its host computer for attack signatures (packet sequences that identify an attacker’s attempt to exploit a known operating system or program vulnerability).

The IDS examines packets in two different ways. It scans each packet individually looking for patterns that do not adhere to specifications and that can crash the TCP/IP stack. It also monitors the packets as a stream of information, looking for commands directed at a particular service to exploit or crash the system.

If the information matches a known attack, the IDS automatically discards the packet and severs the connection with the computer that sent the data. This feature is called AutoBlock, and protects computers on your network from being affected in any way. AutoBlock does not use Location Awareness, so the IP address of the attacking computer is blocked for all Locations.
The IDS relies on an extensive list of attack signatures to detect and block suspicious network activity. This list appears in Symantec Client Firewall Administrator, and you can control whether or not to exclude attack signatures from blocking, and whether or not to lock signatures to prevent users from changing the signatures. Symantec supplies the known threat list, which you can update on Symantec Client Security firewall client using Symantec LiveUpdate. You can also exclude and lock specific IP addresses from AutoBlock, which also affects all Locations.

**Note:** Symantec Client Firewall Administrator supports signatures for all supported versions of Symantec Client Security firewall client. However, not all versions of Symantec Client Security firewall client support the same signature versions. When working with earlier versions, you may discover that Symantec Client Firewall Administrator may contain some signatures that do not appear in Symantec Client Security firewall client. This behavior is normal.

The default IDS settings should provide your Symantec Client Security firewall client computers with adequate protection against a wide variety of threats. If the default settings do not completely address the needs of your network, or if you want to prevent users from excluding particular signatures, you can customize IDS settings in one or more of the following ways:

- Enable and disable.
- Exclude specific attack signatures from being monitored.
- Enable and disable AutoBlock.
- Exclude specific computers from AutoBlock.
- Lock attack signatures and excluded computers to prevent user modification.

**Excluding attack signatures from being blocked**

You might want to disable firewall protection for the following reasons:

- In some cases, benign network activity may appear similar to a Symantec Client Security firewall client attack signature. If you receive repeated warnings about possible attacks, and you know that these attacks are being triggered by safe behavior, you can exclude the attack signature that matches the benign activity.

- Lowering the number of attack signatures checked for by Symantec Client Security firewall client lowers the amount of resource consumption by the
firewall. However, you must be certain that an attack signature poses no threat before excluding it from blocking.

**To exclude an IDS attack signature from being blocked**

- In Symantec Client Firewall Administrator, on the IDS tab, on the Signatures tab, under Exclude, check the attack signatures that you want to exclude from firewall blocking.

### Configuring AutoBlock

When Symantec Client Security firewall client detects an attack, it automatically blocks the connection to ensure that your computer is safe. The program can also activate AutoBlock, which automatically discards all incoming communication from the attacking computer for a set period of time, even if the incoming communication does not match an attack signature. By default, AutoBlock stops all inbound traffic from the attacking computer for 30 minutes. Symantec Client Security firewall client Admin users can extend this time up to 48 hours.
To configure AutoBlock

1. In Symantec Client Firewall Administrator, on the Client Settings tab, under Intrusion Detection, click the Value cell for Intrusion Detection - AutoBlock.

2. In the drop-down list, select one of the following:
   - Enable
   - Disable
   - Keep Existing Selection: Do Not Change

Excluding computers from AutoBlock

Some normal Internet activities will be repeatedly recognized by Symantec Client Security firewall client as attacks. For example, some Internet service providers scan the ports of your computer to ensure that you are within their service agreements.

If client computers can't communicate with computers they should be able to connect to, the destination computers may be blocked by AutoBlock. Depending on the circumstances, you can disable the AutoBlock setting on clients, preventing attacking computers from being added to the AutoBlock list, or you can exclude specific computers from AutoBlock.
Note: Zone settings allow you to delete locked and unlocked Zones when exporting policy files. If you decide to delete locked Zones, you will also delete locked computers that are excluded from AutoBlock. If you decide to delete unlocked Zones, you will also delete unlocked computers that are excluded from AutoBlock.

See “Deleting locked and unlocked Zones when exporting policies” on page 257.

To exclude computers from being blocked

1. In Symantec Client Firewall Administrator, on the IDS tab, on the AutoBlock Exclusions tab, click Add.

2. In the Add Computer dialog box, select whether the rule applies to one IP address, a host name, a network address, a range of IP addresses, or a named address group.

3. Click OK.

The addresses that you added appear on the AutoBlock tab, under Internet Addresses to be Excluded from IDS AutoBlock.
Locking IDS exclusions and IP addresses

Unless you lock IDS attack signatures and IP address exclusions, Symantec Client Security firewall client users can modify the settings. Padlock icons in the Lock column identify locked settings.

Table 12-1 lists the tabs that contain lockable items and describes the functionality when they are locked and unlocked.

**Table 12-1** Tabs that contain lockable items

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Addresses</td>
<td>Locked: Client users cannot delete the IP address.</td>
</tr>
<tr>
<td></td>
<td>Unlocked: Client users can delete the IP address.</td>
</tr>
<tr>
<td>Signatures</td>
<td>Locked and Excluded: Client users cannot include the signature in the monitored signature list.</td>
</tr>
<tr>
<td></td>
<td>Unlocked and Excluded: Client users can include the signature in the monitored signature list.</td>
</tr>
<tr>
<td></td>
<td>Locked and Included: Client users cannot exclude the signature from being monitored.</td>
</tr>
<tr>
<td></td>
<td>Unlocked and Included: Client users can exclude the signature from being monitored.</td>
</tr>
</tbody>
</table>

**To lock IDS exclusions and IP addresses**

1. In Symantec Client Firewall Administrator, on the IDS tab, in the Lock column, click anywhere.

2. Click **Locked**.
Configuring Client Settings and Web Content settings

This chapter includes the following topics:

- About Client Settings
- Setting user access levels
- Web Content settings

About Client Settings

Symantec Client Firewall Administrator includes settings for overall operation of Symantec Client Security firewall client. These settings specify user access levels, enable or disable automatic rule generation, control security levels for various Internet traffic, and so on. **Figure 13-1** shows the user interface for the Client Settings tab.
A subset of the Client Settings has a relationship with the Web Content settings. Web Content settings may override some Client Settings on a URL basis. For example, if the Client Setting for Java Applet Security is set to High, which prevents all Java applets from running, and if a Web Content setting exists that permits Java applets to run from the site www.spammersRus.com, the firewall permits www.spammersRus.com to run Java applets on the client computer.

See “Web Content settings” on page 333.

Web Content settings may override the following Client Settings:

- Custom Security Level - Java Applet Security
- Custom Security Level - ActiveX Control Security
- Custom Privacy Level - Confidential Information Level
- Custom Privacy Level- Cookie Blocking Level
- Custom Privacy Level - Browser Privacy
- Ad Blocking
- Popup Window Blocking
The HTTP Port List Client Setting under Options - Advanced affects all Web Content settings. If the Value for HTTP Port List is blank, the firewall does not enforce Web Content settings, and does not enforce Client Settings that may be overridden by Web Content settings.

**Note:** The selection Keep User Selection: Do Not Change is available for many Client Settings. This selection retains whatever value (for example, Enabled or Disabled) is already selected in the client user interface.

### Access level settings

**Table 13-1** describes the Access level settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| User Type | Sets the permissions for a Symantec Client Security firewall client.  
Admin: All Symantec Client Security firewall client product features and configuration options are available to users.  
Normal: Users have a limited subset of permissions that includes viewing firewall data and modifying privacy control settings.  
Restricted: Users cannot configure rules or change settings. For the most part, the firewall is invisible to a user with this setting. |

See “Setting user access levels” on page 331.

### Global settings

**Table 13-2** describes the Global settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symantec Client Firewall Protection</td>
<td>Enables and disables the firewall, IDS, and Privacy Control.</td>
</tr>
</tbody>
</table>
Table 13-2  Global settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symantec Secure Port protection</td>
<td>Enable: Secures all local ports defined in Trojan rules in a way that no program can use the ports for outbound traffic even if permitted with rules, and disables all pop-up messages relating to outbound traffic access alerts. Does not affect inbound traffic. Disable: Removes the Secure Port override and permits the firewall to process Trojan rules normally. See “Incorporating Secure Port” on page 279.</td>
</tr>
<tr>
<td>Ignore pRule Digest Values</td>
<td>Yes: Ignores all digest settings when creating Program rules from pRule data. No: Requires digest matching when creating Program rules from pRule data (all pRules do not necessarily require digest matching).</td>
</tr>
</tbody>
</table>

Status settings

Table 13-3 describes the Status settings.

Table 13-3  Status settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Firewall</td>
<td>Enables and disables firewall rulebase inspection and IDS AutoBlock, and uses the Default Location only. When disabled, the firewall still runs but is in a default-permit condition, disabling all client firewall settings. See “Implementing Location Awareness” on page 247.</td>
</tr>
<tr>
<td>Privacy Control</td>
<td>Enables and disables Privacy Control.</td>
</tr>
</tbody>
</table>
Client firewall settings

Table 13-4 describes the client firewall settings. If the Client Firewall Status setting is disabled, these settings are not enforced.

See Table 13-3, “Status settings,” on page 324.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| Custom Security Level-Client Firewall Level | **Medium:** Blocks many ports used by harmful programs. However, it can also block useful programs when they use the same ports.  
**High:** Blocks all traffic that is not specifically allowed. Firewall rules for every program that requests Internet access must be created. Rules are often created by a Symantec Client Security firewall client program scan. |
| Custom Security Level-Java Applet Security | **None:** Lets all Java applets run.  
**Medium:** Prompts for permission each time that a Java applet attempts to run. Do not use the Medium setting if the client access level is set to Restricted.  
**High:** Prevents all Java applets from running. |
| Custom Security Level-ActiveX Control Security | **None:** Lets all ActiveX controls run.  
**Medium:** Prompts for permission each time that an ActiveX control attempts to run. If the client access level is Restricted, do not use the Medium setting.  
**High:** Prevents all ActiveX controls from running. |
| Custom Security Level-Access Control Alerts | **Enable:** Prompts to permit or block a program from accessing the Internet when no firewall rule exists for it.  
**Disable:** Blocks programs from accessing the network when there are no specific firewall rules in place for them. Make sure to disable Access Control Alerts if the user access setting is Restricted. |
| Custom Security Level-Unused port Access Alert | **Enable:** Alerts are generated when an attempt is made to access an unused port. Enabling this option significantly increases the number of alerts displayed.  
**Disable:** Alerts are not generated for unsolicited connection attempts. |
## Intrusion Detection settings

Table 13-5 describes the Intrusion Detection settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intrusion Detection</td>
<td>Enable: Monitors Internet traffic for patterns that are typical of a hacker attack, for example, a port scan or attempts to connect to ports used by remote-access Trojan horse programs. Disable: Does not scan packets for intrusion behavior.</td>
</tr>
<tr>
<td>Intrusion Detection-AutoBlock</td>
<td>Enable: Stops all inbound traffic from attacking computers for 30 minutes. Disable: Does not use AutoBlock. In some cases, normal activity might be recognized as an attack. For example, some Internet service providers scan the ports of client computers to ensure that they are within their service agreements. To prevent normal activities from interrupting your Internet use, specified computers can be excluded from AutoBlock. Computers in the Trusted and Restricted Zones are not subject to AutoBlock. Computers in the Trusted Zone are never blocked, while computers in the Restricted Zone are permanently blocked. AutoBlock is disabled if the firewall is disabled.</td>
</tr>
<tr>
<td>Always display alerts for Intrusion Detection</td>
<td>Enable: Displays pop-up alerts for all Intrusion Detection events. Disable: Does not display pop-up alerts for Intrusion Detection events.</td>
</tr>
</tbody>
</table>
Privacy Control settings

Table 13-6 describes the Privacy Control settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom Privacy Level-Confidential Information Level</td>
<td>High: Blocks all specified confidential information entered in a Web page from being sent to nonsecured (HTTP) Web sites.</td>
</tr>
<tr>
<td></td>
<td>Medium: Prompts each time that specified confidential information entered in a Web page is sent to a nonsecured (HTTP) Web site. Do not use this setting if the user access level is set to Restricted.</td>
</tr>
<tr>
<td></td>
<td>None: Disables the monitoring of confidential information sent to Web sites.</td>
</tr>
<tr>
<td>Custom Privacy Level-Cookie Blocking Level</td>
<td>High: Blocks all cookies.</td>
</tr>
<tr>
<td></td>
<td>Medium: Prompts each time that a Web site requests a cookie. Do not use this setting if the user access level is set to Restricted.</td>
</tr>
<tr>
<td></td>
<td>None: Allows all cookies.</td>
</tr>
<tr>
<td>Custom Privacy Level-Browser Privacy</td>
<td>Enable: Prevents a Web site from retrieving the user's email address or the address of the last Web site visited.</td>
</tr>
<tr>
<td></td>
<td>Disable: Permits the sending of the user's email address or address of the last Web site visited.</td>
</tr>
<tr>
<td>Custom Privacy Level-Secure Connections (https)</td>
<td>Enable: Permits communication via HTTPS protocol. If enabled, confidential information is sent.</td>
</tr>
<tr>
<td></td>
<td>Disable: Blocks HTTPS traffic, including most credit card and financial transactions.</td>
</tr>
</tbody>
</table>

Ad Blocking settings

Symantec Client Firewall Administrator includes a Client Settings category called Ad Blocking. Table 13-7 describes the Ad Blocking settings.

Table 13-7 Ad Blocking settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ad Blocking</td>
<td>Enable: Blocks ads using the Ad Blocking settings on the Web Content tab. Disables: Permits all Web pages to display all banner ads, and disables the Ad Blocking settings on the Web Content tab.</td>
</tr>
</tbody>
</table>
### Configuring Client Settings and Web Content settings

#### About Client Settings

**General options settings**

Table 13-8 describes the General options settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run at System Startup</td>
<td>Yes: Symantec Client Security firewall client runs when the computer is started.</td>
</tr>
<tr>
<td></td>
<td>No: Symantec Client Security firewall client must be started manually.</td>
</tr>
<tr>
<td>Show Taskbar Icon</td>
<td>Yes: Displays the Symantec Client Security firewall client icon in the Windows system tray, which can be right-clicked to log on and off, exit the program, or perform other tasks.</td>
</tr>
<tr>
<td></td>
<td>No: The Symantec Client Security firewall client icon is not displayed in the Windows system tray.</td>
</tr>
</tbody>
</table>

**Tray Menu options settings**

Table 13-9 describes the Tray Menu options settings. These are menu selections that become available when a client user right-clicks the Symantec Client Security firewall client icon in the Windows system tray.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Options</td>
<td>Yes: Displays the Options selection on the Windows system tray menu, which allows you to display the Symantec Client Security firewall client Options dialog box for access to General, Firewall, and Secure Port settings, and to Settings Manager.</td>
</tr>
<tr>
<td></td>
<td>No: Does not display the Options selection on the Windows system tray menu.</td>
</tr>
</tbody>
</table>
Table 13-9  Tray Menu options settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| Display View Event Log   | **Yes:** Displays the View Event Log selection on the Windows system tray menu, which allows you to view the Event Log. The Event Log contains information on content blocking, connections, firewall activity, and other events.  
**No:** Does not display the View Event Log selection on the Windows system tray menu. |
| Display View Statistics  | **Yes:** Displays the View Statistics selection on the Windows system tray menu, which allows you to view real-time, detailed protection statistics.  
**No:** Does not display the View Statistics selection on the Windows system tray menu. |

Advanced options settings

Table 13-10 describes the Advanced options settings.

Table 13-10  Advanced options settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| HTTP Port List           | Specifies the list of ports to filter for Java and ActiveX blocking, script blocking, confidential information, cookies, and so on. The client computer must be restarted for this setting to take effect.  
**Note:** When this option is selected, all ports listed here will overwrite any ports listed on a client through the Symantec Client Security firewall client user interface. |
| Block IGMP Protocol      | Enable: Blocks the use of the Internet Group Management Protocol (IGMP), a standard for IP multicasting on the Internet. Attackers sometimes exploit this protocol to freeze a computer once they obtain its IP address.  
Disable: Does not block IGMP. |
| Stealth Block Ports      | Enable: Blocked ports do not respond to inquiries from the Internet.  
Disable: Blocked ports respond that they are closed. |
Alert Customization settings

Alert Customization settings let you customize the text that appears in Alert prompts. The customized text is added to the default text, and the limit is 250 characters. Table 13-11 describes the Alert Customization settings.

**Table 13-10** Advanced options settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block Fragmented IP Packets</td>
<td>Block All: Blocks IP packets that have severely fragmented headers and contain data areas that are too small to be useful for legitimate network traffic. Permit All Except Suspected Attacks: Permits all fragmented IP packets except those associated with suspected attacks. Note: This setting affects computers that run Windows 98 only. Windows 2000/XP computers automatically reassemble fragmented packets.</td>
</tr>
<tr>
<td>Program Component Monitoring</td>
<td>Enable: Checks access settings for external modules that programs use to connect to the Internet. Disable: Does not check access settings for external modules.</td>
</tr>
<tr>
<td>Program Launch Monitoring</td>
<td>Enable: Checks Internet access settings for each program launched by another program. Disable: Does not check access settings for each program.</td>
</tr>
</tbody>
</table>

**Alert Customization settings**

Alert Customization settings let you customize the text that appears in Alert prompts. The customized text is added to the default text, and the limit is 250 characters. Table 13-11 describes the Alert Customization settings.

**Table 13-11** Alert Customization settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expand Alert Details</td>
<td>Yes: Automatically displays details for program and security alerts such as protocol, remote address, and so forth. No: Does not automatically display details for all alerts.</td>
</tr>
<tr>
<td>Custom Alert Text - ActiveX</td>
<td>Appears when Web pages contain ActiveX controls.</td>
</tr>
<tr>
<td>Custom Alert Text - Privacy Control</td>
<td>Appears when users attempt to send confidential information to a Web site.</td>
</tr>
<tr>
<td>Custom Alert Text - Cookie</td>
<td>Appears when a Web site attempts to create or read a cookie on a computer.</td>
</tr>
<tr>
<td>Custom Alert Text - IDS</td>
<td>Appears when the IDS engine detects an intrusion attempt.</td>
</tr>
</tbody>
</table>
Setting user access levels

The extent of individual customization of Symantec Client Security firewall client and available information is determined by the client’s user access level. As the firewall administrator, you set the user access level for firewalls in Symantec Client Firewall Administrator. The user access level setting is saved when you save the policy. The user access level setting is implemented for firewalls after the policy is rolled out.

Admin users have all permissions associated with Normal and Restricted users. Normal users have all permissions associated with Restricted users. The

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom Alert Text - IP</td>
<td>Appears when an unknown program attempts to access the Internet.</td>
</tr>
<tr>
<td>Custom Alert Text - Java</td>
<td>Appears when a Web site attempts to run a Java applet.</td>
</tr>
<tr>
<td>Custom Alert Text - Launcher</td>
<td>Appears when one program attempts to access the Internet using another program.</td>
</tr>
<tr>
<td>Custom Alert Text - Listen</td>
<td>Appears when a new program, such as a Trojan horse, begins listening for connections from other computers.</td>
</tr>
<tr>
<td>Custom Alert Text - Location</td>
<td>Appears when Location Awareness is enabled and Symantec Client Security firewall client prompts users to select a Location.</td>
</tr>
<tr>
<td>Custom Alert Text - Module</td>
<td>Appears when a known program attempts to access the Internet with an unknown module.</td>
</tr>
<tr>
<td>Custom Alert Text - Security</td>
<td>Appears when security alerts are enabled with rule tracking.</td>
</tr>
<tr>
<td>Custom Alert Text - Service Monitor</td>
<td>Appears when certain Symantec Client Security firewall client services are disabled, such as Symantec Event Manager, Symantec Secure Port, and Symantec Proxy Service.</td>
</tr>
</tbody>
</table>

Various Client Settings control whether alerts appear. For example, if Custom Security Level - ActiveX Control Security is set to None, the alert for ActiveX would never appear, even if you created custom alert text for this alert.
Symantec Client Security firewall client user levels are listed and described in Table 13-12.

Table 13-12  Symantec Client Security firewall client user access levels

<table>
<thead>
<tr>
<th>User level</th>
<th>Description</th>
</tr>
</thead>
</table>
| Admin      | Users with Admin access rights have the following permissions:  
  ■ Adding, modifying, and deleting Unlocked rules  
  ■ Changing all Client Settings, including enabling and disabling the firewall  
  ■ Adding and deleting IP addresses to Trusted and Restricted Zones if unlocked  
  ■ Editing the Intrusion Detection Signature Exclusion list if unlocked  
  ■ Running program scans  
  ■ Enabling and disabling automatic rule creation  
  ■ Enabling and disabling Network Detector  
  ■ Modifying Privacy Control settings  
  ■ Backing up and restoring policy files |
| Normal     | Users with Normal access rights have the following permissions:  
  ■ Viewing statistics; deciding which data to view  
  ■ Limited viewing of Zone IP addresses  
  ■ Modifying Privacy Control settings but not adding private information  
  ■ Modifying Ad Blocking settings |
| Restricted | Users with Restricted access rights have limited access to Symantec Client Security firewall client, and have the following permissions:  
  ■ Running LiveUpdate and using Help  
  ■ Viewing the Log Viewer  

Once a user is classified as Restricted, that user will be unable to run any Internet programs unless there are specific rules permitting access to Internet programs in the same policy file. |

When you assign an access level of Restricted, you need to configure the following client configuration settings:

■ Use a setting other than Medium for the Symantec Client Security firewall client or Privacy Control settings.

A setting of Medium means that the user will be prompted about allowing or blocking communication each time that there is a cookie, Java applet, ActiveX control, and so forth, on a Web site. Since Restricted users do not
have permission to respond to alerts, and will not see the alerts, the Medium setting is not applicable.

- Disable the Access Control Alerts setting, because restricted users are neither able to receive nor respond to alerts.

**To set Symantec Client Security firewall client user access levels**
- In Symantec Client Firewall Administrator, on the Client Settings tab, under Access Level, in the Value column, on the User Type row, select one of the following:
  - Admin
  - Normal
  - Restricted
  - Keep Existing Selection - Do Not Change

---

**Web Content settings**

Web Content settings let you control how Symantec Client Security firewall client handles interactive online content, ads, and possible privacy intrusions. When these settings are exported to Symantec Client Security firewall client, all Client Settings are deleted and overwritten. Web Content options are arranged on three tabs:

- Global Settings
- User Settings
- Ad Blocking

**Note:** All Web Content filtering is performed on ports that are specified in the HTTP Port List on the Client Settings tab. If this list is blank, the firewall does not enforce Web Content settings because all Web Content filtering is performed on ports that are specified in this list. Further, Web Content settings are ignored for computers placed in Trusted Zones.
Global Settings

Global Settings let you control the default actions Symantec Client Security firewall client takes when Web sites attempt to get information about your browser and browsing history, or use animated images, JavaScripts, and other active content. Table 13-13 describes the settings.

Table 13-13  Global Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information about your browser</td>
<td>Block or allow Web sites from requesting information about your computer and Web browser.</td>
</tr>
<tr>
<td>Information about visited sites</td>
<td>Block or allow Web sites from requesting information about the last Web site that you visited during this session online.</td>
</tr>
<tr>
<td>Animated images</td>
<td>Block or allow animated images from running. The images still appear but are not animated.</td>
</tr>
<tr>
<td>Scripts</td>
<td>Block or allow Java and Visual Basic scripts. Some scripts write cookies.</td>
</tr>
<tr>
<td>Flash Animation</td>
<td>Block or allow content created with Macromedia Flash.</td>
</tr>
</tbody>
</table>

Note: If the Privacy Control Client Setting is disabled, the Global Settings for Information about your browser and Information about visited sites are ignored.
User Settings

User Settings let you customize Cookie Blocking, Popup Window Blocking, and ActiveX and Java settings for individual sites. If the Client Settings for User Settings is set to None, these values are ignored. Table 13-14 describes the settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cookies</td>
<td>Block or allow Web sites from creating and reading cookie files on your computer.</td>
</tr>
<tr>
<td>Java Applets</td>
<td>Block or allow Java applets from running.</td>
</tr>
<tr>
<td>ActiveX Controls</td>
<td>Block or allow ActiveX controls from running.</td>
</tr>
<tr>
<td>Popup Ads</td>
<td>Block or allow pop-up ads.</td>
</tr>
</tbody>
</table>

Note: Two types of cookies exist, persistent and nonpersistent. Symantec Client Security firewall client treats both types the same way.

Ad Blocking settings

Ad Blocking settings let you specify individual ad banners or groups of ad images you want to block or allow on individual sites. Symantec Client Security firewall client detects and blocks ads based on two criteria: their dimensions and their locations.

Note: If the Banner Blocking Client Setting is disabled, Ad Blocking is disabled.

Blocking by dimensions

Most online advertisers use one or more standard sizes for their ads. Symantec Client Security firewall client now includes the ability to block images, Flash animations, and other HTML elements that have the same dimensions as these common ad sizes.
Blocking by location

Every file on the Internet has a unique address or URL. When you view a Web page, your computer connects to a URL and displays the file that is stored there. If the page points to graphics, audio files, and other multimedia content, your browser displays the files as part of the page.

When Ad Blocking is enabled and you connect to a Web site, Symantec Client Security firewall client scans Web pages and compares their contents to two lists:

- A default list of ads that Symantec Client Security firewall client blocks automatically. Use LiveUpdate to keep the list of blocked ads current.
- A list that you create as you block specific ads. You can add to and change this list.

If the page includes files from a blocked domain, Symantec Client Security firewall client removes the link and downloads the rest of the page.

Creating text strings to identify ads to block or permit

You can control whether Symantec Client Security firewall client displays specific ads by creating a list of text strings that identify individual ad banners. Ad Blocking strings are sections of HTML addresses. If any part of a file’s address matches the text string, Symantec Client Security firewall client automatically blocks the file. Symantec Client Security firewall client provides an Ad Blocking list (Defaults) that is used to determine which images should be blocked when displaying Web pages.

You can also create permit strings that allow Web sites to display images that match the string. This allows you to override the blocking effect of any string in the (Defaults) block list for individual sites. Permit rules take precedence over Block rules on any site.

When Ad Blocking is enabled, all Web pages are scanned for the HTML strings specified in the (Defaults) list. Symantec Client Security firewall client looks for the blocked strings within HTML tags that are used to present advertising. The HTML structures that contain matching strings are removed from the page by Symantec Client Security firewall client before the page appears in the Web browser.

Make sure that the strings that you place in the (Defaults) block list are not too general. For example, www by itself is not a good string to block because almost every URL includes www. A string like www.slowads is more effective because it only blocks graphics from the slowads domain without affecting other sites.
The way that you define Ad Blocking strings affects how restrictive or unrestrictive Symantec Client Security firewall client is when filtering data. For example, if you add the string spammersRus.com to the (Defaults) block list, you block everything in the spammersRus.com domain. If you are more specific and add the string /images/image7.gif to the site-specific block list maintained for www.spammersRus.com, you block only that particular image.

**Note:** When exporting policy files to Symantec Client Security firewall client, all user-defined strings are deleted.

## Adding Ad Blocking strings

You can add strings to the Ad Blocking list for all sites or for individual sites. Ad Blocking supports lowercase characters only.

### To add an Ad Blocking string

1. In Symantec Client Firewall Administrator, on the Web Content tab, on the Ad Blocking tab, do one of the following:
   - To block a string on all Web sites, click **(Defaults)**.
   - To block a string on a Web site in the list, select the site's name.
   - To block a string on a Web site not in the list, click **Add Site**, and then in the New Site/Domain dialog box, type the site's address.

2. On the Ad Blocking tab, click **Add**.

3. In the Add New HTML String dialog box, select one of the following:
   - **Block**  Block ads matching this string.
   - **Permit**  Allow ads matching this string.

4. Type an HTML string to block or permit.

5. Click **OK**.

## Modifying or removing Ad Blocking strings

If you later decide that an Ad Blocking string is too restrictive, not broad enough, or not appropriate, you can change or remove it.
To modify or remove an Ad Blocking string

1. In Symantec Client Firewall Administrator, on the Web Content tab, on the Ad Blocking tab, do one of the following:
   - To modify or remove a string in the (Defaults) list, click (Defaults).
   - To modify or remove a site-specific string, select the site’s name.

2. In the HTML string list, select the string that you want to change.

3. Do one of the following:
   - To modify a string, click Modify, and then type your changes.
   - To remove a string, click Remove.

4. Click OK.
Managing client log data

This chapter includes the following topics:
- About logging
- Saving client log data to text files
- Viewing Event Logs from the Symantec System Center

About logging

The Symantec Client Security firewall client Event Logs contain information about activity permitted and blocked by the firewall for each client and data on various aspects of firewall functioning. You can examine the specifics of problem traffic, or assess patterns of overall firewall activity.

Data for the Event Log is organized into categories. Table 14-1 lists the Event Log tabs and their descriptions.

<table>
<thead>
<tr>
<th>Tab</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content Blocking</td>
<td>Details about Java applets and ActiveX controls blocked by Symantec Client Security firewall client.</td>
</tr>
<tr>
<td>Connections</td>
<td>A history of all TCP/IP network connections made with the Symantec Client Security firewall client computer. Connections are logged when the connection is closed.</td>
</tr>
<tr>
<td>Firewall</td>
<td>Traffic intercepted by the firewall, including rules that were processed, alerts displayed, unused ports blocked, and AutoBlock events.</td>
</tr>
</tbody>
</table>
There may be cases in which you want to save individual Symantec Client Security firewall client Event Log data for later inclusion in spreadsheets and reports.

You can save firewall log data for any Symantec Client Security firewall client Event Log category by using the Log Export command-line utility. The Log Export utility (LogExprt.exe) is supplied with Symantec Client Security firewall client and lets you create a delimited text file that contains log data from a single Event Log category. Each possible log corresponds to a tab in the Event Log dialog box (for example, System or Alerts).

By default, the Log Export (LogExprt.exe) program is located in the \Program Files\Symantec Client Security\Symantec Client Firewall\directory.

### Table 14-1 Event Log tabs

<table>
<thead>
<tr>
<th>Tab</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intrusion Detection</td>
<td>Whether Intrusion Detection is active, the attack signatures being monitored, and the number of intrusions blocked. Also lists any IDS attacks that occurred and were blocked.</td>
</tr>
<tr>
<td>Privacy</td>
<td>The cookies that have been permitted or blocked, including the name of the cookie and the Web site that requested the cookie. The information listed is dependent on the cookie settings.</td>
</tr>
<tr>
<td>Private Information</td>
<td>Private information sent or blocked.</td>
</tr>
<tr>
<td>System</td>
<td>When the Symantec Client Security firewall client has been enabled or disabled, connection activity, and administrator updates to rules, pRules, and IDS settings.</td>
</tr>
<tr>
<td>Configuration</td>
<td>Information regarding configuration changes and updates to rules and IDS signatures.</td>
</tr>
<tr>
<td>Web History</td>
<td>URLs visited by the computer, providing a history of Web activity.</td>
</tr>
<tr>
<td>Alerts</td>
<td>All alert activity, including normal Internet Access Control alerts and security alerts triggered by possible attacks on the Symantec Client Security firewall client computer.</td>
</tr>
</tbody>
</table>
Log Export utility syntax

The Log Export (LogExprt.exe) command-line utility has the following syntax:

`LogExprt [-v][-l<LogID>][-x<File>][-d<Delimiter>][-f<+|-,Col,Data>]`

Each of the parameters and a description of its use is provided in Table 14-2.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description and usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>-v</td>
<td>Used by itself, -v lists the log IDs of the individual Symantec Client Security firewall client Event Log files. Using the -v parameter together with the -l parameter with a log ID returns the column names of the specified Event Log file.</td>
</tr>
<tr>
<td>-l&lt;LogID&gt;</td>
<td>Used in conjunction with other commands, specifies which log file the other commands process. Paths that contain spaces must be enclosed in double quotation marks.</td>
</tr>
<tr>
<td>-x&lt;File&gt;</td>
<td>Used with the -l parameter, exports the log data from the specified Event Log file. If an export file name is not specified, the Event Log file name is used with a file suffix of .txt. Paths that contain spaces must be enclosed in double quotation marks.</td>
</tr>
<tr>
<td>-d&lt;Delimiter&gt;</td>
<td>Specifies the single character to be used as a delimiter when exporting the Event Log data to a text file. If this parameter is omitted, the default delimiter used is the comma character (,). Do not use quotation marks or any DBCS character as the delimiter.</td>
</tr>
</tbody>
</table>
Managing client log data

Saving client log data to text files

Using wildcard characters in filters with LogExprt.exe

You can use the wildcard characters shown in Table 14-3 when using filters with a LogExprt.exe command.

<table>
<thead>
<tr>
<th>Wildcard</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Matches any sequence of characters (zero or more)</td>
</tr>
<tr>
<td>?</td>
<td>Matches any single character</td>
</tr>
<tr>
<td>\</td>
<td>Suppresses the syntactic significance of special characters</td>
</tr>
<tr>
<td>[SET]</td>
<td>Matches any character in the specified set</td>
</tr>
<tr>
<td>![SET] or [&gt;SET]</td>
<td>Matches any character that is not in the specified set</td>
</tr>
</tbody>
</table>

A set is composed of characters or ranges; a range looks like ‘<character-hyphen character>’, as in ‘0-9’ or ‘A-Z’. Any ASCII character can be used in a set or a range.

To suppress the special syntactic significance of the characters ‘] [ * ? ! ^ - \’ and match the character exactly, precede it with a ‘\’.  

Table 14-2 LogExprt.exe parameter descriptions

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description and usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>-f +</td>
<td>-, Col, Data</td>
</tr>
<tr>
<td></td>
<td>A plus (+) or minus (-) defines the filter type.</td>
</tr>
<tr>
<td></td>
<td>■ Plus (+) specifies that only Event Log entries will be exported that match the values specified for Col and Data.</td>
</tr>
<tr>
<td></td>
<td>■ The minus (-) character specifies that all Event Log entries will be exported except those that match the values specified for Col and Data.</td>
</tr>
<tr>
<td></td>
<td>Col specifies the column in the Event Log file to which the filter applies. You may use wildcards. Col is not case-sensitive.</td>
</tr>
<tr>
<td></td>
<td>Data specifies the values to search for in the specified column. This data must be matched for the filter to take effect. You may use wildcards. Data is not case-sensitive.</td>
</tr>
<tr>
<td></td>
<td>Filter specifications that contain spaces must be enclosed in double quotation marks.</td>
</tr>
</tbody>
</table>
The following command-line examples demonstrate typical wildcard filters:

- **10/2?/01**
  Matches all days between the 20th and the 29th in October 2001. 10/2[0-9]/01 generates the same match.

- **10/*/*01**
  Matches any day in October 2001.

- ***.domain.com**
  Matches any DNS entry that ended with domain.com.

- **192.168.*.***
  Matches all IP addresses that begin with 192.168. 192.168* generates the same match.

- **.*.1.100**
  Matches all IP address that end with 1.100. *.1.100 generates the same match.

- **192.168.23[012].***

- **192.168.10[0-6].***
  Matches all IP addresses between 192.168.100.000 and 192.168.106.255.

Log Export utility examples

The following command-line examples demonstrate typical LogExprt usage:

- **LogExprt.exe -v**
  List the available logs. The following is an example of the text output from this command:
  Available Logs:
  0001 - Content Blocking
  0002 - Connections
  0003 - Firewall
  0004 - Intrusion Detection
  0005 - Privacy
  0006 - Restrictions
  0007 - System
  0008 - Web History
  0009 - Alerts
  0011 - Confidential Info
  0012 - Spam
Viewing Event Logs from the Symantec System Center

The Symantec System Center allows you to display log data for one or more Symantec Client Security firewall clients. Using the Symantec System Center, you can do the following:

- View data at the server group, individual server, and individual managed workstation levels.
- Sort and filter Event Log data.
- Export data to Microsoft Access (as an .mdb file) or in comma-separated value (CSV) format.

Table 14-4 lists and describes the five types of Event Logs available with the Symantec System Center, reveals the data that appears in the Event Log.
columns, and indicates where in the console system hierarchy you can display Event Log data.

**Table 14-4**  Event Log types

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Data columns</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update Event Log</td>
<td>Provides information about Symantec Client Security firewall client configuration changes.</td>
<td>Date, Event, Description, Previous Version, Current Version, Computer, User</td>
</tr>
<tr>
<td>Configuration Change Log</td>
<td>Provides information about Symantec Client Security firewall client services that are started, stopped, enabled, and disabled.</td>
<td>Date, Description, Configuration, Type, Data, Computer, User</td>
</tr>
<tr>
<td>Firewall Violation Event Log</td>
<td>Provides information about Symantec Client Security firewall client events that are treated as security violations.</td>
<td>Date, Description, Network Protocol, IP Type, Computer, User, IP Source Address, IP Source Port, IP Destination Address, IP Destination Port, Violation, Action, Direction, Process Name</td>
</tr>
<tr>
<td>Intrusion Detection Status Log</td>
<td>Provides information about the Intrusion Detection engine, including version numbers and the number of monitored signatures.</td>
<td>Date, Description, IDS Version, Signature Count, Error Code, Computer, User</td>
</tr>
</tbody>
</table>
Displaying logs

You can display logs from the tree hierarchy in the Symantec System Center.

To display logs

1. In the Symantec System Center, in the right pane, right-click a server group, server, or client, and then click All Tasks > Symantec Client Firewall > Logs.

2. On the menu, select one of the following options:
   - Update Event Log
   - Configuration Change Log
   - Firewall Violation Event Log
Filtering log data

When viewing logs, you can filter data based on time.

To filter log data

- In the Event Log window, click the drop-down box, and select one of the following:
  - Today
  - Past 7 days
  - This month
  - All items
  - A selected range of days

Sorting log data

When viewing logs, you can sort the data by column.

To sort the data

- In the Event Log window, click a column header.
  The ascending sort icon appears within a column header the first time that you click it. The descending sort icon appears the next time that you click the column header.

Understanding Event Log icons

In all Event Log windows, icons allow you to perform actions, such as saving the data as a CSV file.
Table 14-5 lists and describes Event Log icons.

Table 14-5  

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Close the Event Log window.</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>View item properties.</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Save the data shown in the Event Log window as a CSV or Microsoft Access database file.</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Display Help for the Event Log.</td>
</tr>
</tbody>
</table>
Creating network rulebases

This chapter includes the following topics:
- Choosing an implementation approach
- Considering implementation options
- Implementing network rulebases
- Configuring an initial network rulebase
- Fine-tuning and troubleshooting rulebases
- Configuring a default-permit rulebase
- Configuring user interaction

Choosing an implementation approach

Network rulebases allow client/server traffic in computer networks, and support dynamic IP addressing, domain name resolution, printing, and so on. To create a network rulebase, you can either allow Symantec Client Security firewall client to create rules automatically on an as-needed basis, or you can create rules manually. The benefit of creating rules manually is that you gain a greater understanding of the protocols and programs that support network activity, which will make troubleshooting firewall problems easier.

How you configure a firewall to support networking depends on the diversity and size of your computer network, as well as the level of trust you place in the internal network components down to the client level.
Several approaches exist for configuring Symantec Client Security firewall client to support network activity:

- Create a Trusted Zone of specific server IP addresses.
- Create a General rulebase that specifies the protocols and port numbers over which local and remote computers can communicate, and restrict the communications to specific, remote IP addresses.
- Create a combination Program and General rulebase that specifies protocols and port numbers for the programs that the client uses for remote communications, and restrict the communications to specific, remote IP addresses.

Ultimately, you must decide which approach to use.

**Considering implementation options**

Each implementation option offers advantages and disadvantages that relate to your network size, configuration, and security features, as well as the workload shared by your technical support staff.

**Using the Trusted Zone approach**

If you trust your network completely and do not want to create a Program or General rulebase that supports network activity, you can create a Trusted Zone of IP addresses or domain names. All computers that fall into this Zone are Trusted in that they are free to conduct all client/server communications without being blocked at the firewall.

The advantage of this approach is that you can quickly configure firewall clients to support network activity and your support calls will be minimal. A disadvantage is that if a blended threat or other virus attacks the trusted network devices, firewall clients may be at risk of infection. Another disadvantage is that firewall clients may be compromised if the domain is hijacked through DNS cache poisoning, or if an IP address in the address range is spoofed.

Nevertheless, if your confidence is high that your perimeter firewalls and antivirus software will detect and mitigate blended threats, and if you have a small number of servers that perform network activity and you know their IP addresses, creating Trusted Zones may be the approach to take.
Creating network rulebases
Considering implementation options

Using the network-level firewall approach

If you do not trust your network completely, you can create a General rulebase that supports networking with specific IP addresses. This rulebase essentially creates a network-level firewall. This firewall inspects each inbound and outbound packet and makes decisions based on the local and remote ports, as well as the remote IP addresses.

The advantage of using network-level rules is that you can push a common rulebase onto a variety of clients running various operating systems. The disadvantage of using network-level rules is that Trojan horses and worms are free to use the permitted ports, potentially exposing your clients to infection. If, however, you know the IP addresses of your network devices that communicate with clients, and if these servers are hardened and secured, you can restrict the client ports to communicate with those IP addresses only.

Using the program-level firewall approach

To further harden the firewall, you can create Program rules and supplement these rules with two General rules for Loopback and ICMP. The resulting rulebase essentially combines a program-level firewall with a network-level firewall.

The advantage of using Program rules is that you can specify the protocols, ports, and IP addresses with which these programs are allowed to communicate, greatly reducing the threat of unknown programs communicating over a permitted port. Unless permitted with a rule, no other program can use the protocol and port to access the network.

The disadvantage of using Program rules is that you have to make an assumption about clients that may not be true in large organizations. The assumption is that all program locations and versions are identical on all clients. For example, if you create a rule that specifies a program that resides on drive C, install the rule on a client, and the client runs the program from drive D, the rule blocks the program from accessing the network. Nevertheless, if you have a tightly controlled network with program and version control, creating Program rules may be the approach to take.

An alternative to creating Program rules is to create pRules for the programs. While pRules are essentially Program rules that get generated automatically on clients, pRules allow you to tailor the degree with which the program executables must conform. If desired, you can require the executables to match a specific file version, or digest, which blocks program execution if a virus overwrites the file. On the other hand, you can create pRules with no file requirements other than that the file name must match.
The advantage of using this approach is that you can implement Program rules on clients running different operating systems, program versions, and executable file locations. The disadvantage of using this approach is that you cannot tailor the programs to communicate with IP address ranges. You can select one IP address, all IP addresses, or a domain name only. The workaround is to add an IP address range using Symantec Client Security firewall client for the rules that support networking.

Implementing network rulebases

After you have chosen the best approach for creating network rulebases, you need to implement the approach. Implementing network rulebases requires knowledge of networking concepts such as IP addressing, protocol functionality, port numbers, and so on.

Implementing Trusted Zones

If you decide to support networking with Trusted Zones, you need to decide whether to use specific IP addresses, a range of IP addresses, or a domain name.

If you have a small number of servers that support network activity, enter their IP addresses one at a time. If you have a relatively large number of servers and still decide to use Trusted Zones, decide whether to use a range of IP addresses or a domain name. Using a domain name is the least secure approach to enabling network traffic as any computer that authenticates to the domain is trusted.

If network operations policies and procedures are in place for assigning IP addresses to critical servers, consider using address ranges. Many times server network interface cards (NICs) are, for example, assigned static IP addresses that end in .1 through .50, reserving .51 to .254 for DHCP client addressing. In this case, you can trust IP addresses that end in .1 though .50, and implement the range by entering a beginning IP address of 192.168.100.0 and an ending IP address of 192.168.100.50.

You can also establish a range using a subnet mask. For example, assume that server NICs are assigned static IP addresses that end in .1 through .30. In this case, you can trust IP addresses that end in .1 through .30 by entering IP address 192.168.100.0 with a subnet mask of 255.255.255.224. This subnet mask creates the 192.168.100.0 subnet, which contains 30 assignable addresses from 192.168.100.1 to 192.168.100.30, reserving 192.168.100.31 as the broadcast address.
Creating network rulebases

Implementing network rulebases

You can enter any IP address between 192.168.100.0 and 192.168.100.30 to create the 192.168.100.0 subnet as long as you use subnet mask 255.255.255.224.

Implementing network-level firewalls

Symantec Client Security firewall client is a traditional packet filtering firewall in that it inspects all packets both inbound and outbound, looks for a rule that permits the packets to pass, and blocks packets that do not match rules—the default. As a result, rules must exist for both inbound and outbound packets. To configure a network-level firewall, you create General rules only.

When possible, try to configure inbound and outbound permissions for the same protocol and port combinations with one rule. As a firewall rulebase grows, it reaches a point where security diminishes because the rulebase gets increasingly complex and hard to understand. Combining inbound and outbound permissions reduces this growth.

After creating rules, consider ordering them so that commonly matched rules appear near the top of the rulebase, and rarely matched rules appear near the bottom. Placing commonly matched rules near the top maximizes performance. Two of the most commonly matched rules are for loopback and NetBIOS communications. To increase the security of a network rulebase, also consider limiting the number of IP addresses allowed for remote communications.

Some programs perform loopback during execution, which is an internal diagnostic test. Making loopback the first General Locked rule is a best practice and ensures optimum performance for programs that perform loopback.

Windows 2000 sample network-level rulebase

Table 15-1 shows a sample rulebase that supports Windows 2000 networking in an Active Directory environment. All rules are permitted, bidirectional rules unless noted under description. Be sure that the Loopback rule uses local address 127.0.0.1 to prevent IP address spoofing.

<table>
<thead>
<tr>
<th>Description</th>
<th>Protocol</th>
<th>Remote ports</th>
<th>Local ports</th>
<th>Remote addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loopback</td>
<td>TCP, UDP</td>
<td>Any</td>
<td>Any</td>
<td>127.0.0.1</td>
</tr>
<tr>
<td>ICMP</td>
<td>ICMP</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
</tr>
<tr>
<td>Description</td>
<td>Protocol</td>
<td>Remote ports</td>
<td>Local ports</td>
<td>Remote addresses</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>----------</td>
<td>--------------</td>
<td>-------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>Internal Symantec AntiVirus Discovery</td>
<td>UDP</td>
<td>Any</td>
<td>38293</td>
<td>192.168.100.0 (255.255.255.224)</td>
</tr>
<tr>
<td>FTP</td>
<td>TCP</td>
<td>20, 21</td>
<td>1024-5000</td>
<td>192.168.100.0 (255.255.255.224)</td>
</tr>
<tr>
<td>Telnet</td>
<td>TCP</td>
<td>23</td>
<td>1024-5000</td>
<td>192.168.100.0 (255.255.255.224)</td>
</tr>
<tr>
<td>DNS</td>
<td>TCP, UDP</td>
<td>53</td>
<td>1024-5000</td>
<td>192.168.100.0 (255.255.255.224)</td>
</tr>
<tr>
<td>Bootp</td>
<td>UDP</td>
<td>67, 68</td>
<td>67, 68</td>
<td>192.168.100.0 (255.255.255.224) 0.0.0.0 255.255.255.255</td>
</tr>
<tr>
<td>HTTP</td>
<td>TCP</td>
<td>80, 443</td>
<td>1024-5000</td>
<td>Any</td>
</tr>
<tr>
<td>Kerberos</td>
<td>UDP</td>
<td>88</td>
<td>1024-5000</td>
<td>192.168.100.0 (255.255.255.224)</td>
</tr>
<tr>
<td>NTP</td>
<td>UDP</td>
<td>123</td>
<td>1024-5000</td>
<td>192.168.100.0 (255.255.255.224)</td>
</tr>
<tr>
<td>EPmap</td>
<td>TCP</td>
<td>135</td>
<td>1024-5000</td>
<td>192.168.100.0 (255.255.255.224)</td>
</tr>
<tr>
<td>NetBIOS</td>
<td>TCP, UDP</td>
<td>137, 138, 139</td>
<td>0, 1024-5000</td>
<td>192.168.100.0 (255.255.255.224)</td>
</tr>
<tr>
<td>NetBIOS to 139 (inbound only)</td>
<td>TCP</td>
<td>1024-5000</td>
<td>139</td>
<td>192.168.100.0 (255.255.255.224)</td>
</tr>
<tr>
<td>LDAP</td>
<td>TCP, UDP</td>
<td>389</td>
<td>1024-5000</td>
<td>192.168.100.0 (255.255.255.224)</td>
</tr>
<tr>
<td>SrvLoc</td>
<td>UDP</td>
<td>427</td>
<td>427</td>
<td>192.168.100.0 (255.255.255.224)</td>
</tr>
<tr>
<td>SMB (microsoft-ds)</td>
<td>TCP</td>
<td>445</td>
<td>1024-5000</td>
<td>192.168.100.0 (255.255.255.224)</td>
</tr>
<tr>
<td>Nterm</td>
<td>TCP</td>
<td>1026</td>
<td>1024-5000</td>
<td>192.168.100.0 (255.255.255.224)</td>
</tr>
</tbody>
</table>
In the sample rulebase, many rules restrict communications to a remote address range using IP address 192.168.100.0 and subnet mask 255.255.255.224. This parameter restricts communications to remote computers with IP addresses between 192.168.100.0 and 192.168.100.31 only. The rulebase also reveals many rules with a local port range that falls between 1024 and 5000. These rules typically indicate protocols such as HTTP where clients transmit information on many different ports. For example, as clients communicate with remote port 80 on Web servers, client port numbers change over time and generally range between 1024 and 5000.

If you have a Windows 2000 network and decide to implement a network-level firewall only, this sample rulebase is a good place to start. The rulebase does not, however, contain a rule that supports email, but does support Web browsing and Symantec LiveUpdate operations.

Implementing program-level firewalls

Implementing a program-level rulebase is similar to implementing a network-level rulebase in that you still create network-level rules, and all information provided about implementing network-level rules applies to implementing program-level rules. The difference is that you create network-level rules for programs.

When implementing Program rules, you have two choices:

- Create one rule that permits all program traffic.
- Create one or more rules that permit specific program traffic only.

**Note:** Information for implementing program-level rules also applies to pRules.

The first approach is not as secure as the second approach. Nevertheless, if you tailor the Program rule so the program can communicate with specific internal IP addresses only, the approach may create a strong enough security posture to protect your internal network. The advantage of using this approach is that you can create a rulebase quickly. The disadvantage is that a Trojan horse or worm may overwrite trusted executable files, and if successful, potentially gain access to the internal network using any port and protocol. Using pRules with digest matching, however, mitigates this vulnerability.

The second approach creates the highest security posture possible. The advantage of using this approach is that if a Trojan horse or worm overwrites an executable file, the threat is restricted to communications over a limited number of ports and protocols. The disadvantage is that it takes time to discover all ports and protocols that a particular program uses. Also, using this approach with pRule digest matching creates the highest level of security.
Finally, you must create at least two network-level rules to support ICMP and loopback. Program-level rules do not support ICMP, and configuring loopback rules for all programs that use loopback adds additional complexity to the rulebase.

**Windows 2000 sample program-level rulebase**

Typically, a Windows 2000/NT client in a Windows 2000 network uses the following processes for networking in an Active Directory environment:

- C:\Winnt\System32\Lsass.exe
  Supports Kerberos, LDAP, Emap, and Nterm
- C:\Winnt\System32\services.exe
  Supports NTP, Bootp, DNS, and Emap
- C:\Winnt\Explorer.exe
  Supports LDAP
- C:\Winnt\System32\Winlogon.exe
  Supports LDAP
- Windows Subsystem
  Supports NetBIOS and SMB

In a Windows 2000 environment, you need to create rules for these processes. To support Web browsing and LiveUpdate in a Windows 2000 networking environment, you also need to configure the firewall to support the following additional processes:

- C:\Program Files\Internet Explorer\explore.exe
  Supports Internet Explorer
- C:\Program Files\Symantec\LiveUpdate\Lucomserver.exe
  Supports Symantec LiveUpdate
- C:\Program Files\Symantec Client Security\Symantec Client Firewall\Sympxsvc.exe
  Supports Symantec Client Security firewall client proxy server
You can create either Program rules or pRules for these processes. Table 15-2
shows a rulebase that supports Windows 2000 networking. All rules are
permitted, bidirectional rules.

Table 15-2  Sample program rulebase

<table>
<thead>
<tr>
<th>Executable</th>
<th>Description</th>
<th>Protocol</th>
<th>Remote ports</th>
<th>Local ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lsass.exe</td>
<td>Kerberos</td>
<td>UDP</td>
<td>88</td>
<td>1024-5000</td>
</tr>
<tr>
<td>EPmap</td>
<td>TCP</td>
<td>135</td>
<td>1024-5000</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>TCP, UDP</td>
<td>389</td>
<td>1024-5000</td>
<td></td>
</tr>
<tr>
<td>Nterm</td>
<td>TCP</td>
<td>1026</td>
<td>1024-5000</td>
<td></td>
</tr>
<tr>
<td>Services.exe</td>
<td>DNS</td>
<td>TCP, UDP</td>
<td>53</td>
<td>1024-5000</td>
</tr>
<tr>
<td>Bootp</td>
<td>UDP</td>
<td>67, 68</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kerberos</td>
<td>UDP</td>
<td>88</td>
<td>1024-5000</td>
<td></td>
</tr>
<tr>
<td>NTP</td>
<td>UDP</td>
<td>123</td>
<td>1024-5000</td>
<td></td>
</tr>
<tr>
<td>EPmap</td>
<td>TCP</td>
<td>135</td>
<td>1024-5000</td>
<td></td>
</tr>
<tr>
<td>Explorer.exe</td>
<td>LDAP</td>
<td>TCP, UDP</td>
<td>389</td>
<td>1024-5000</td>
</tr>
<tr>
<td>Winlogon.exe</td>
<td>LDAP</td>
<td>TCP, UDP</td>
<td>389</td>
<td>1024-5000</td>
</tr>
<tr>
<td>Lucomserver.exe</td>
<td>Internal Symantec AntiVirus</td>
<td>UDP</td>
<td>Any</td>
<td>38293</td>
</tr>
<tr>
<td>Discovery</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sympxsvc.exe</td>
<td>HTTP</td>
<td>TCP</td>
<td>80</td>
<td>1024-5000</td>
</tr>
<tr>
<td>Iexplore.exe</td>
<td>HTTP</td>
<td>TCP</td>
<td>80</td>
<td>1024-5000</td>
</tr>
</tbody>
</table>

Table 15-3 shows a pRule that typically supplements a program rulebase. Using
a pRule to configure the Windows Subsystem simplifies the program rulebase.
All rules are permitted, bidirectional rules unless indicated in the Description column.

Table 15-3  Sample pRule to supplement program rulebase

<table>
<thead>
<tr>
<th>Executable</th>
<th>Description</th>
<th>Protocol</th>
<th>Remote ports</th>
<th>Local ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>NetBIOS</td>
<td>TCP, UDP</td>
<td>137, 138, 139</td>
<td>0, 1024-5000</td>
</tr>
<tr>
<td></td>
<td>NetBIOS to 139 (inbound only)</td>
<td>TCP</td>
<td>1024-5000</td>
<td>139</td>
</tr>
<tr>
<td></td>
<td>SMB (microsoft-ds)</td>
<td>TCP</td>
<td>445</td>
<td>1024-5000</td>
</tr>
</tbody>
</table>

Finally, Table 15-4 shows four General rules that typically supplement a program rulebase. All rules are permitted, bidirectional rules. Be sure that the Loopback rule uses local address 127.0.0.1 to prevent IP address spoofing.

Table 15-4  Sample network rules to supplement a program rulebase

<table>
<thead>
<tr>
<th>Description</th>
<th>Protocol</th>
<th>Remote ports</th>
<th>Local ports</th>
<th>Remote addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loopback</td>
<td>TCP, UDP</td>
<td>Any</td>
<td>Any</td>
<td>127.0.0.1</td>
</tr>
<tr>
<td>ICMP</td>
<td>ICMP</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
</tr>
<tr>
<td>FTP</td>
<td>TCP</td>
<td>20, 21</td>
<td>1024-5000</td>
<td>192.168.100.0 (255.255.255.224)</td>
</tr>
<tr>
<td>Telnet</td>
<td>TCP</td>
<td>23</td>
<td>1024-5000</td>
<td>192.168.100.0 (255.255.255.224)</td>
</tr>
</tbody>
</table>

**Configuring an initial network rulebase**

To configure an initial firewall rulebase that supports Microsoft networking, you can start with one of the sample rulebases, or you can use various tools to discover the networking protocols that your network uses, and then begin implementing firewall rules based on your discoveries.

See Table 15-1, “Sample network rulebase,” on page 353.

See Table 15-2, “Sample program rulebase,” on page 357.

Symantec Client Security firewall client includes several tools that reveal network activity. The Connections tab in the Event Log window along with the Statistics window reveal port numbers and local/remote IP addresses. The Firewall tab in the Event Log window along with the Internet Access Control
alert window, which you enable and disable under Client Firewall Settings, reveal the processes that the firewall blocks from initiating outbound connections, along with protocols, port numbers, and local/remote IP addresses.

Other tools such as network protocol analyzers may also prove valuable when profiling network traffic, as well as shareware and freeware tools that show processes, connections, and protocols. Additionally, Windows includes a few DOS commands that may help, such as netstat and nbtstat. Various netstat and nbtstat command switches allow you to display local and remote connections, protocol statistics, and the route table.

The rule-creation process is a repetitive series of performing network activity, discovering and understanding network activity, and creating rules to support network activity. Then, after creating rules, you test the rules by performing the network activity that prompted you to create the rules.

The following list details network activity that you should perform, in no particular order, and then create rules to support this activity:

- Display network servers in a window.
- Display a network Directory in a window.
- Connect to the Internet.
- Connect to an Internet email account or secure Web site over HTTPS.
- Perform LiveUpdate from Symantec Client Security firewall client.
- Print.
- Execute the following DHCP commands from the DOS command line:
  - ipconfig /release
  - ipconfig /renew
- Restart your computer, and logon and authenticate to a domain.

If you are setting up a network-level firewall, you should not initially enable access control alerts because you may end up spending a large amount of time responding to access alert prompts. Rather, enable the firewall, and then in the Client Firewall Settings window, deselect Enable Security.

This configuration causes the firewall to permit all traffic, which you can view on the Connections tab in the Event Log and in the Network Connection pane in the Statistics window. These windows show remote and local connections, IP addresses, protocols, ports, and bytes sent and received. You can create an initial set of General rules based on this information.

If you are setting up a program-level firewall, first create two General rules for loopback and ICMP traffic. Then, one of the fastest ways to discover which programs to create rules for is to display Client Firewall Settings and enable the
Internet Access Control Alert window. When the alert window appears, gather the detailed information from the alert, disable the firewall (which stops further alert windows), create or modify a Program rule based on the details, enable the firewall, and repeat the sequence until the alert frequency drops significantly.

**Fine-tuning and troubleshooting rulebases**

Once you can perform network activity without the firewall blocking it, let the firewall run for a few days and look for traffic that the firewall may be mishandling. To see how the firewall is performing, use the Statistics window. The Firewall Rules pane shows permitted and blocked packets by rule, as well as unmatched packets as shown in Figure 15-1.

**Figure 15-1** Firewall Rules pane

<table>
<thead>
<tr>
<th>Rule</th>
<th>Permitted</th>
<th>Blocked</th>
<th>No Match</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loopback</td>
<td>1772</td>
<td>0</td>
<td>20332</td>
</tr>
<tr>
<td>NetBIOS</td>
<td>19743</td>
<td>0</td>
<td>589</td>
</tr>
<tr>
<td>NetBIOS Inbound : 39</td>
<td>0</td>
<td>0</td>
<td>589</td>
</tr>
<tr>
<td>FTP</td>
<td>8</td>
<td>0</td>
<td>581</td>
</tr>
<tr>
<td>ICMP</td>
<td>146</td>
<td>0</td>
<td>435</td>
</tr>
<tr>
<td>HTTP</td>
<td>77</td>
<td>0</td>
<td>350</td>
</tr>
<tr>
<td>DNS</td>
<td>98</td>
<td>0</td>
<td>260</td>
</tr>
<tr>
<td>Kerberos</td>
<td>96</td>
<td>0</td>
<td>164</td>
</tr>
<tr>
<td>Bootp</td>
<td>44</td>
<td>0</td>
<td>120</td>
</tr>
<tr>
<td>SMB</td>
<td>0</td>
<td>0</td>
<td>120</td>
</tr>
<tr>
<td>LDAP</td>
<td>56</td>
<td>0</td>
<td>64</td>
</tr>
<tr>
<td>Internal AntiVirus Host Discovery</td>
<td>6</td>
<td>0</td>
<td>58</td>
</tr>
<tr>
<td>FTP</td>
<td>0</td>
<td>0</td>
<td>58</td>
</tr>
<tr>
<td>HSRP</td>
<td>0</td>
<td>0</td>
<td>58</td>
</tr>
<tr>
<td>SrvLoc</td>
<td>0</td>
<td>0</td>
<td>58</td>
</tr>
<tr>
<td>Nterm</td>
<td>0</td>
<td>0</td>
<td>50</td>
</tr>
<tr>
<td>SunRPC</td>
<td>4</td>
<td>0</td>
<td>46</td>
</tr>
<tr>
<td>NTP</td>
<td>0</td>
<td>0</td>
<td>46</td>
</tr>
<tr>
<td>Telnet</td>
<td>0</td>
<td>0</td>
<td>46</td>
</tr>
<tr>
<td>Cleanup</td>
<td>0</td>
<td>46</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>22058</td>
<td>46</td>
<td>20332</td>
</tr>
</tbody>
</table>

This pane first shows locked, General rules in the order inspected, and then shows locked, Program rules in the order inspected. The firewall rules continue with unlocked, General and Program rules.

The No Match column shows packets that did not match a rule. If your network uses NetBIOS, and if your NetBIOS rule is not close to being the first rule in the list, you will see a large volume of No Match packets for the rules above the NetBIOS rule, and then notice that the numbers significantly drop after the NetBIOS rule. The reason for this drop is because NetBIOS is very chatty (provides functionality using a large number of packets). Placing the NetBIOS
rule near the top of the inspection order optimizes firewall processing, and is generally a best practice.

If you do not see a zero value for the last rule in the No Match column, the firewall is silently blocking packets and you may need to investigate what packets the firewall is blocking. You can find details about the blocked packets on the Firewall tab in the Event Log.

Another way to investigate blocked packets is to create an unlocked General Cleanup rule that blocks all TCP and UDP traffic to and from all computers, tracks the rule with an Event Log entry and security alert, and is the last rule inspected. When properly configured as the last rule inspected, this Cleanup rule logs information about all blocked packets on the Alert tab in the Event Log, and reveals the number of blocked packets on the Firewall Rules pane in the Statistics window.

**Note:** By default, the firewall blocks all packets not matching a rule and logs the information on the Firewall tab in the Event Log, but mixes this information with other firewall information. The Cleanup rule tracked with an Event Log entry and security alert isolates information about blocked packets only, on the Alert tab.

The key to using this technique is to configure the Cleanup rule as the last rule listed in the General rule list at the Unlocked level, which means that you must create the rule with Symantec Client Security firewall client, and to configure all other General and Program rules at the Locked level, meaning that you must export them using Symantec Client Firewall Administrator. The Cleanup rule must be the last rule inspected, which you can verify in the Statistics window.

If Program rules are configured at the Unlocked level, these rules can never be matched as the Cleanup rule blocks packets before they get inspected by the Program rules. Additionally, the Cleanup rule disables all pRule implementation, and disables all security alert prompts, which may or may not be beneficial. As a result, the Cleanup rule is best used when creating and fine-tuning rulebases to push to clients, and not for general client implementation.

**Note:** Using Profiling is another useful way to fine-tune network rulebases as it allows you to capture traffic information and convert it to pRules. See “Using Profiling to generate pRules and NetSpecs” on page 302.
Configuring a default-permit rulebase

By default, Symantec Client Security firewall client uses a default-deny rulebase. If traffic is not permitted with a rule, either the traffic is dropped, a pRule becomes a Program rule, or the user is prompted to create a rule depending on Client Settings. Some organizations, however, are only interested in blocking certain ports while permitting all other traffic. To support this configuration, you need to create a default-permit rulebase that supports selective port blocking.

To create a default-permit rulebase, create three General rules to permit loopback, ICMP, and TCP/UDP traffic. Then, after the Loopback rule but before the other two rules, insert the rules that block the desired ports. Table 15-5 shows this construction. All permit rules are bidirectional. Be sure that the Loopback rule uses local address 127.0.0.1 to prevent IP address spoofing.

Table 15-5 | Sample default-permit rulebase

<table>
<thead>
<tr>
<th>Description</th>
<th>Protocol</th>
<th>Remote ports</th>
<th>Local ports</th>
<th>Remote addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loopback</td>
<td>TCP, UDP</td>
<td>Any</td>
<td>Any</td>
<td>127.0.0.1</td>
</tr>
<tr>
<td>&lt;Insert Blocking Rules Here&gt;</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ICMP Permit All</td>
<td>ICMP</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
</tr>
<tr>
<td>TCP/UDP Permit All</td>
<td>TCP, UDP</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
</tr>
</tbody>
</table>

The logic is that rules that block ports are inspected after the Loopback rule to remove the potential that they might interfere with loopback operations. Then, the Blocking rules are inspected, and if there is no match, the traffic is permitted.

Because this configuration is not inherently secure, the best way to implement it is to use Secure Port to block all local ports defined with Trojan rules, and to only add remote ports to the General rules. The Permit All General rules stop Trojan rules from being inspected, so you need to use Secure Port to secure the local ports defined with Trojan rules, and add remote ports defined with Trojan rules to the General rule list.
Configuring user interaction

After you fine-tune and troubleshoot your rulebases, you have some decisions to make regarding user interaction with the firewall. One way to think about user interaction is to start with the configuration that offers the least user interaction, and then implement the exceptions that you want to allow. Table 15-6 lists and describes the various settings that limit user interaction with the firewall.

**Table 15-6 Settings that limit user interaction**

<table>
<thead>
<tr>
<th>Location</th>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Settings tab</td>
<td>Custom Security Level - Access Control Alerts</td>
<td>Disable</td>
<td>Does not display the alert.</td>
</tr>
<tr>
<td>Client Settings tab</td>
<td>Custom Security Level - Unused Port Access Alert</td>
<td>Disable</td>
<td>Does not display the alert.</td>
</tr>
<tr>
<td>Client Settings tab</td>
<td>Always display alerts for Intrusion Detection</td>
<td>Disable</td>
<td>Does not display the alert.</td>
</tr>
<tr>
<td>Client Settings tab</td>
<td>Symantec Secure Port protection</td>
<td>Enable</td>
<td>Disables alerts for local ports configured in Trojan rules.</td>
</tr>
<tr>
<td>Edit Location window</td>
<td>Rule Exception Handling</td>
<td>Permit</td>
<td>Does not prompt users to create rules for unknown traffic. Selecting permit is like creating a default-permit rulebase and is designed for use with Profiling. Use with caution.</td>
</tr>
<tr>
<td>Edit Location window</td>
<td>Auto Rule Creation</td>
<td>Enable</td>
<td>Does not prompt users to create Program rules from pRules. If you disable Auto Rule Creation, the firewall prompts users for unknown traffic handling selections.</td>
</tr>
<tr>
<td>Edit Location window</td>
<td>Allow New Connections</td>
<td>No</td>
<td>Does not prompt users to select a Location for an unrecognized network connection. If you enable Location Awareness and do not allow new connections, be sure that you have configured a Primary Location.</td>
</tr>
</tbody>
</table>
Generally, the appropriate level of user interaction is between complete freedom and no freedom. If you give users complete freedom, they may effectively disable Symantec Client Security firewall client. If you give users no freedom, you may experience an excessive amount of support calls.

<table>
<thead>
<tr>
<th>Location</th>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Settings</td>
<td>User Type</td>
<td>Normal</td>
<td>Users cannot create rules, Zones, or Locations, and have limited access to most functionality.</td>
</tr>
<tr>
<td>Client Settings</td>
<td>Symantec Secure Port protection</td>
<td>Enable</td>
<td>Reduces alerts for Trojan rules and IDS signatures.</td>
</tr>
</tbody>
</table>

Table 15-6
Settings that limit user interaction
Symbols
.cf files 223
.cfu files 223
.csv files 310
.xml files 223

Numerics
32-bit and 16-bit operating systems, running virus sweeps 182
64-bit operating systems
using Continuous LiveUpdate 153
virus definitions files 153

A
access levels
Admin 332
configuring for clients 323
Normal 332
Restricted 332
access list
reloading 56
using to enhance server group security 53
values for IP and IPX addresses 55
Action Status for alerts 89
actions, for firewall rules 263
Active Client, exporting policies to 228
Active Directory
configuring pRules to support 301
requirement for Discovery 26
sample network-level rulebase 353
sample program-level rulebase 356
Ad Blocking
adding strings to 337
creating text strings to filter 336
setting in Web Content settings 335
setting levels 327
address cache discovery 27
address groups
adding 277
deleting 278
address groups (continued)
using 276
adware 96
alert actions
configuring messages 70
viewing export status 85
Alert Log
Action Status 89
copying contents to Clipboard 88
deleting entries 87
displaying alerts in 86
filtering display list 89
viewing detailed information 88
Alert Management System
about 67
alert forwarding for unmanaged clients 90
Alert Log 86
alert notification methods 67
configuring alert action messages 70
event threads 68
forwarding alerts to servers 91
limiting alert configuration network segments 72
speeding up alert configuration 72
alerts
actions
deleting actions from alerts 84
export status 85
exporting to other computers 84, 85
limiting to network segments 72
testing 84
configuring
Broadcast 75
default messages 71
paging services 79
SNMP traps 80
configuring actions
about 69
Broadcast 75
Load An NLM 76
Message Box 74
messages 70
alerts (continued)
  configuring actions (continued)
    Run Program 75
    Send Internet Mail 77
    Send Page 78
forwarding
  for roaming clients 198
  to AMS servers 91
message
  parameters 70
  size limitation 71
antivirus clients, configuring with Grc.dat 17
antivirus protection 17, 19, 42
antivirus servers, configuring using the Virus
  Definition Transport Method 154
attack signatures
  about 316
  excluding from firewall protection 316
audits
  determining network security 36
  labeling items and rerunning audits 39
  labeling items during 39
AutoBlock
  configuring 317
  excluding computers from 318
Auto-Protect
  advanced options 104, 109
  configuring 102
  email scanning 111
  preserving file times 106
  resetting options at different levels 115
  scanning
    about 98
    configuring for mail applications 102
    email support issues 114
    options 101
  SmartScan 104

B
backup files 107
blended threats 96
Block, action for rules 263
Bloodhound scanning 107, 110
Broadcast alert, configuring 75

C

  cache
    adding Windows NT/2000 server addresses to NetWare server address cache 157
    caching client information when filtering client groups 61
    discovering computers from 31
    Discovery Clear Cache Now setting 31
    file options 110
    finding computers in local cache 32, 33
    items
      server group passwords 48
      server names and IP addresses in Symantec System Center console 26
    Load from cache only discovery type 27
    Normal Discovery address cache comparisons 26
    client data, configuring policies using 223
    client groups
      adding clients to 58
      caching information when filtering 61
      changing settings 55
      configuration change priority 44
      configuring settings 59
      creating 58, 62
      deciding whether to manage with 44
      deleting 62
      dragging and dropping clients to add them 58
      dragging and dropping clients to move them 59
      filtering client group view 61
      finding settings 59
      icon 19
      moving clients between 59
      renaming 62
      running tasks 59
      scenario 46
      viewing 59

Client Settings
  about 221
  access level 323
  Ad Blocking settings 327
  advanced options settings 329
  alert customization settings 330
  configuring 321
  firewall client settings 325
  general options settings 328
  Global Settings 323
  IDS settings 326
Client Settings (continued)
  in policies 221
  overriding with Web Content settings 322
Privacy Control settings 327
relationship with Web Content settings 322
status settings 324
Tray Menu options 328

Clients
  about antivirus protection for 42
  adding to client groups 58
  assigned and unassigned 44
  Auto-Protect options for 102
  changing between unmanaged and managed 63
  check-in time 127
  configuring
    access levels 323
    Advanced options 329
    General options 328
    Global Settings 323
    Intrusion Detection 326
    Privacy Control 327
    Status settings 324
    user access levels 331
  configuring check-in intervals 127, 128
  configuring expiration 127, 128
  disabling scheduled scans 126
  dragging and dropping to add into client groups 58
  dragging and dropping to move between client groups 59
  enumerating in server groups 61
  forcing virus definitions files updates 168
  log forwarding, registry values 209
  moving between client groups 59
  overview of centralized scanning control for 102
  scheduling scans 122
  settings when the client group is deleted 62
  viewing virus list 173
  with intermittent connectivity 127

Compressed files, configuring scanning 147

Computers (continued)
  finding (continued)
    in local cache 32
    unprotected 36
    using computer names 32
    using IP addresses 34
    using IPX addresses 32
    using network search 33
    using TCP/IP 32
    with outdated virus definitions 173

Configuration
  change priority 44
  roaming client support, for servers 193
  scan options 129
    about 129
    on multiple selected computers 101
  sharing in server and client groups 43
  unauthorized change attempts log 56
Configuration settings, for clients 321
console
  refreshing 35
  starting 18
Continuous LiveUpdate
  changing registry values to enable 170
  configuring for managed clients 170
CPU utilization, setting for scheduled and manual scans 150

Data columns in console views 19, 20
Dates of virus definitions files, verifying 173
Delete frequency, setting for Histories and Event Logs 213
Deletion, alert actions 84
dialers 96
digest values
  match criteria 298
  using with pRules 288
Discovery Service
  address cache discovery 27
  changing the Discovery Cycle interval 27
Discovery Cycle configuration 26
  how it works 25
  how to find NetWare computers 26
Intense Discovery 28
  limitations 28
IP Discovery 28
Local Discovery 27
Normal Discovery 26
Discovery Service (continued)
running 28
why Discovery may not find computers 32
WINS or Active Directory requirement 26
within octets or subnet masks 72
without IP 30
drag-and-drop operation
   add a client to a client group 58
   move a client from one client group to
      another 59
   move a server between server groups 46, 51

E
e-mail, Lotus Notes, configuring scans for 102
Emergency Disk, recovering from boot virus 183
enhancement, server group security 53
event logs
   deleting 213
   filtering data 201
   icons 209
   setting delete frequency 213
   sorting data 201
   types 200
event threads 68
events, forward from clients and servers 210
expanded threat detection 95
export command for roaming client support 196
export status, viewing for alert actions 85

F
failover servers for roaming clients 191
files
   backing up before repairing 107
   cache options 110
   cleaning infected 205, 208
   deleting infected 206, 208
   excluding from scanning 138
   exclusions 139
   moving to Quarantine 206, 208
   undoing action taken 205, 208
filter, server group view 52
firewall clients
   adding to a client group 58
   handling virus outbreaks 177
firewall rules
   about 218, 259
   actions for 263
   adding to different Locations 271
firewall rules (continued)
categories of 260
   computer options 265
   connection options 263
   creating Program rules 268
   deleting from Locations 271
displaying by Location 270
   elements of 261
   for ICMP protocol 264
   for TCP protocol 264
   for UDP protocol 264
   General rules 260
   IP addressing options 265
   Locations 266
   locked and unlocked 260
   manually creating 267
   ordering 259
   port options 264
   processing order 260
   Program rules 260
   protocol options 264
   testing 281
   tracking options 266
   Trojan rules 260
forward log events 210
forward logs to parent servers 209
found items, locating in the Symantec System
   Center console 34
G
General options settings for clients 328
General rules
   about 260
   processing order 261
Global Settings
   for clients 323
   for Locations 242
GRC servers 193
Gr.dat 51
   changing parent servers 51, 63
   configuring antivirus clients 17
   enabling and configuring roaming clients 192
   forwarding alerts to AMS servers 91
Gr.csv 51

H
hack tools 96
heuristic scanning 110
Hierarchical Storage Management (HSM) settings, configuring 147
Histories
  about 199
  deleting 213
  filtering data 201
  Scan Histories 206
  Scan History actions 207
  Scan History icons 207
  setting delete frequency 213
  sorting data 201
  Threat History actions 204
  Threat History icons 204
  types 200
  viewing 203
History and Event Log data, filtering 201
History and Log data, exporting to Microsoft Access 205
HTTP port list, affecting Web Content settings 323

I
ICMP, setting rules for 264
  icons
    Scan History 206
    Symantec System Center 22
    Threat History 204
IDS
  about 220, 315
  configuring for clients 326
  exclusions in policies 220
importing and exporting
  about 230
  Location Awareness settings 233
  Locations 232
  rules and pRules 231
inbound connections 263
infected email message 136
infected files
  cleaning 205
  deleting 206
  deleting on creation 107
infections, managing 177
Intelligent Updater 172
Intense Discovery
  about 28, 31
  about Discovery types 25
Intrusion Detection System. See IDS
IP addresses, finding computers using 34
  IP Discovery 28
IPX addresses, finding computers using 32

J
joke programs 96

L
LiveUpdate
  configuring servers to retrieve from Symantec FTP site 160
  setting client policy for 171
  using with internal LiveUpdate server 161
LiveUpdate servers, configuring internally for managed clients 169
Load An NLM alert, configuring 76
load balancing for roam servers 192
Load from cache only discovery 25
Local Discovery 25, 27, 31
Location Awareness
  about 242
  implementing 247
Locations
  about 220, 241
  adding 251
  adding NetSpecs to 251
  configuring required information for 242
  default settings 244
  deleting 253
  Global Settings 242
  importing and exporting 232
  Location-specific settings 246
  moving NetSpecs to 252
  selecting a Primary 252
  used in firewall rules 266
Lock options, using with the IDS 320
Locked rules
  about 260
  access level 332
  processing order for 261
locking
  IDS exclusions 320
  Zones 256
locking server groups 47
log events, forward 210
log forwarding 209
log type comparisons 203
log unauthorized configuration change attempts 56
LogExport.exe utility 341
logging
about 339
saving firewall client logs 340
Lotus Notes, configuring scans for 102

M
macros, about 221
managed clients
changing to unmanaged clients 63
configuring Continuous LiveUpdate for 170
configuring for internal LiveUpdate servers 169
mobile clients 127
manual scans
configuring 116
options 98
merging rules and pRules in policy files 235
Message Box alert, configuring 74
mobile clients, managing 127
Monitor, action for rules 263

N
NetSpecs
discovering 249
moving to Locations 252
prioritizing 250
Profiling 251
Profiling to generate 302
understanding 247
NetWare
adding Windows NT/2000 server addresses to cache 157
finding NetWare servers 26
network auditing, setting options 39
Network detector, enabling 253
Normal, user level 332
Nsctop.exe 25

O
outbound traffic 263

P
pager message, entering 80
paging service alerting, configuring 79
paging services, configuring for AMS 80
parent server 51
See also servers

passwords
cached 48
changing 48
changing for server groups 49
saving or unsaving 48
Permit, action for rules 263
Ping Discovery Service 25
policies
about 217
adding and editing descriptions 225
Client Settings in 221
components 218
configuring using client data 223
creating 224
distributing 238
exporting to the Active Client 228
file type settings 222
IDS exclusions in 220
importing into Symantec Client Firewall Administrator 224
macros in 221
merging rules and pRules in 235
Profiling options in 222
pRules in 219
rules as components of 259
rules in 218
saving 226
Web Content settings in 222
Zones in 219
port groups
adding 273
deleting 275
using 273
ports 264
Primary Location, selecting 252
primary server 42, 51
Privacy Control, configuring 327
Profiling
about options 222
enabling in policy files 304
NetSpecs 251
overview 302
processing
profiled connections 309
profiled information 307
reducing the amount of profiled data 312
refreshing profiled data 310
retrieving profiled information 306
sorting data 312
Profiling (continued)
using to generate pRules and NetSpecs 302
viewing and saving data 305
working with .csv files 310
Program rules
about 260
and pRules 289
processing order 261
protocols, controlling communications with rules 264
pRules
about 219, 287
about digest match criteria 298
adding a rule to 300
and Program rules 289
configuring
match criteria 296
to support Active Directory 301
creating 293
creating and editing 292
disabling auto-create 294
evaluation priority 289
guidelines for using 290
ignoring
file name matching 294
the Digest Value 324
in policies 219
Profiling to generate 302
rule user types 288
silent creation 290
specifying data match criteria 298
specifying file version match criteria 297
Symantec supplied 291
using digest values 288
purge of suspicious files from local Quarantines automatically 180

Q
Quarantine
forwarding for roaming clients 198
moving files to 206, 208
purging suspicious files from 180

R
Refresh feature 35
registry value, for access list 55
registry values
changing to enable Continuous LiveUpdate 170
for client log forwarding 209
for roaming clients 197
remote access programs 96
Restricted, user level 332
roam servers 186
RoamAdmin.exe
about 186
command-line options 195
roaming client support
configuring
for clients 192
from Symantec System Center console 190
how it works 187
roaming clients
about 185
analyzing and mapping the antivirus network 188
components 186
configuring load balancing, failover servers, and alternate servers 195
creating hierarchical server list 190
difference between /nearest_parent and /nearest_GRC servers 195
export command 196
failover servers for 191
forwarding alerts for 198
forwarding to Quarantine 198
implementing 187
registry values 197
server list 186
specifying server types 190
roaming servers
configuring roaming support 193
example 194
identifying 188
sample registry values 194
rulebases
about network 349
choosing a network implementation approach 349
configuring
a default-permit 362
an initial network 358
user interaction 363
rulebases (continued)
  fine-tuning and troubleshooting 360
  implementing
    network 352
    network-level firewalls 353
    program-level firewalls 355
    Trusted Zones 352
  using
    the network-level firewall approach 351
    the program-level firewall approach 351
    the Trusted Zone approach 350
Windows 2000
  sample network-level 353
  sample program-level 356
rules, in policies 218
Run Program alert, configuring 75
running tasks at the client group level, configuring settings 59

S
SavRoam.exe 186, 187
  command-line options 195
Scan History
  icons 206
  sorting columns 201
Scan History data, exporting 208
scan with Bloodhound heuristics 110
scanning
  by program type 143
  configuring
    Auto-Protect scans 102
    manual scans 116
  email 111
  exclusions 114, 119
  for viruses 95
  History 200
  option precedence 101
  recommended file extensions 141
  scheduled scans, configuring 119
  selected files and folders 143
scans
  assigning actions 129
  Bloodhound 107, 110
  configuring for compressed files 147
  configuring manual scans 147
  deleting scheduled 125
  dimmed or missing options 101
  displaying warning message on client 134
scans (continued)
  manual, scheduled, and Auto-Protect scan options 129
  option precedence 101
  options
    Auto-Protect for files 102
    manual 147
    scheduled scans 119
    to exclude files from scanning 138
  scheduled scans
    deleting 125
    disabling 125
    editing 125
    running on demand 126
  selecting files and folders to scan 143
  setting
    Auto-Protect for files 102
    CPU utilization 150
    options on multiple selected computers 101
  scheduled scans
    configuring 119
    deleting 125
  secondary server 43
Secure Port
  securing ports in a random range 280
  using 279
security, enhancing for server groups 53
Send Internet Mail alert, configuring 77
Send Page alert, configuring 78
  paging service 80
server groups
  about 53
  cached passwords 48
  changing passwords 48, 49
  configuration change priority 44
  creating 47
  deciding whether to manage with 44
  deleting 53
  discovering servers and clients 18
  dragging and dropping servers to move them 46, 51
  enhancing security 53
  enumerating clients 61
  filtering views 52
  grouping servers into 46
  how to view 52
  locking and unlocking 47
  moving servers to a new server group 51
Symantec System Center (continued)
  product management snap-ins 19
  refreshing the console 35
  saving console settings 21
  sorting log data 347
  starting 18
  system hierarchy display 18
  viewing event logs 344
Symantec-supplied pRules 291
syncing to computers 36
System Hierarchy
  configuration change priority 44
  data columns in Console Default View 19
  description 18
  icon 22

T
TCP, setting rules for 264
threat 95
Threat History
  icons and actions 204
  sorting columns of data 201
  viewing 203
Threat History data, exporting 206
Threat Tracer 110
trace threats 110
tracking
  submissions to Symantec Security Response 183
  virus alerts 183
Trackware 97
traffic, controlling inbound and outbound 263
Tray Menu options settings 328
Trojan horses 96
Trojan rules
  about 260
  processing order 261
  using Secure Port with 280
troubleshooting, rulebases 360
Trusted Zones, Web Content settings not enforced in 333

U
UDP, setting rules for 264
Unlocked rules
  processing order for 261
  types 260
unlocking server groups 47
unmanaged clients
  alert forwarding 90
  changing to managed clients 63
  finding with network audits 36
  using creating a custom .hst file for
    LiveUpdate 169
unprotected computers, finding 36
updating virus definitions files 151
user access levels
  configuring 331
  Normal 332
  Restricted 332
  setting 323

V
viewing
  Alert Log 86
  client groups 59
  Histories 203
  server groups 52
  virus list 173
views
  changing 21
  Symantec System Center console 19

Virus Definition Transport Method
  configuring antivirus servers with 154
  implementation examples 174
  updating NetWare servers 156

virus definitions files
  finding computers with outdated
    definitions 173
  forcing updates
    on all unlocked servers 154
    on clients 169
    on servers 154
  Intelligent Updater 163
  LiveUpdate 160
  rolling back 173
  rollouts 172
  update methods 152
  verifying dates 173
  verifying version numbers 173
virus list 173
virus protection, how it works 95
virus sweep
  History 200, 203
  running in response to outbreaks 177
viruses 95

W
warning message
  adding to infected email message 136
  displaying on infected computer 134
  example 134
  for email scanning 111, 113
  variables 134
Web Content settings
  about 222, 333
  Ad Blocking settings 335
  conditions when not enforced 333
  Global Settings 334
  in policies 222
  overriding Client Settings 322
  user settings 335
WINS requirement for Discovery 26
worms 96

Z
Zones
  about 219, 254
  adding computers to 255
  copying 256
  deleting when exporting policies 257
  in policies 219
  locking 256
  Restricted 254
  Trusted 254
  using Network 254