Symantec™ Network Access Control 12.1.5 Installation and Administration Guide
Technical Support

Symantec Technical Support maintains support centers globally. Technical Support’s primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online 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 and Symantec Security Response to provide alerting services and virus definition updates.

Symantec’s support offerings include the following:

■ A range of support options that give you the flexibility to select the right amount of service for any size organization
■ Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
■ Upgrade assurance that delivers software upgrades
■ Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
■ Premium service offerings that include Account Management Services

For information about Symantec’s support offerings, you can visit our website at the following URL:

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

■ Product release level
■ Hardware information
Available memory, disk space, and NIC information

Operating system

Version and patch level

Network topology

Router, gateway, and IP address information

Problem description:

- Error messages and log files
- Troubleshooting that was performed before contacting Symantec
- Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as 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 about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec’s technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs, DVDs, or manuals

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:
Asia-Pacific and Japan	customercare_apac@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America
supportsolutions@symantec.com
Technical Support ................................................................................................................................. 4

Chapter 1  Introducing Symantec Network Access Control ........ 21

What is Symantec Network Access Control? ......................................................... 21
What's new in Symantec Network Access Control 12.1.5 ....................... 22
System requirements for Symantec Network Access Control .................. 24
    System requirements for Symantec Endpoint Protection
        Manager ............................................................................................................................. 25
    System requirements for the Symantec Network Access Control
        client for Windows ........................................................................................................... 27
    System requirements for the Symantec Network Access Control
        On-Demand Client for Windows ................................................................................... 27
    System requirements for the Symantec Network Access Control
        On-Demand Client for Mac ......................................................................................... 28
About the types of enforcement in Symantec Network Access
    Control ................................................................................................................................. 29
Deploying Symantec Network Access Control ........................................... 30
Components of Symantec Network Access Control ............................... 32
    Optional components for Symantec Network Access Control ............... 32

Section 1  Installing Symantec Endpoint Protection Manager ................ 34

Chapter 2  Planning the installation ................................................................. 35

Getting up and running on Symantec Endpoint Protection Manager for
    the first time ......................................................................................................................... 35
About Symantec Endpoint Protection Manager compatibility with other
    products ................................................................................................................................. 41
Network architecture considerations .............................................................. 41
About choosing a database type ................................................................. 42
About basic management server settings ............................................. 43
About SQL Server configuration settings ............................................. 45
About SQL Server database authentication modes ............................. 49
Chapter 3 Installing Symantec Endpoint Protection Manager ........................................... 51

Installing Symantec Endpoint Protection Manager ....................................................... 51
Configuring Symantec Endpoint Protection Manager during installation ................................................................. 52
Uninstalling Symantec Endpoint Protection Manager ..................................................... 53
Logging on to the Symantec Endpoint Protection Manager console .............................. 53
About accepting the self-signed server certificate for Symantec Endpoint Protection Manager ................................................................. 56
Displaying a message for administrators to see before logging on to the Symantec Endpoint Protection Manager console ............... 57
Granting or blocking access to remote Symantec Endpoint Protection Manager consoles ................................................................. 57
Unlocking an administrator's account after too many logon attempts ................................................................. 59
Changing the time period for staying logged on to the console ........................................ 60

Chapter 4 Managing product licenses ........................................................................... 61

Licensing Symantec Endpoint Protection ......................................................................... 61
About purchasing licenses ............................................................................................. 63
Activating or importing your Symantec Endpoint Protection 12.1.x product license ................................................................................................. 65
Required licensing contact information ............................................................................ 67
About the Symantec Licensing Portal ............................................................................ 68
About product upgrades and licenses .............................................................................. 68
About renewing your Symantec Endpoint Protection license ........................................... 69
Checking the license status in Symantec Endpoint Protection Manager ................................................................. 69
About the licensing enforcement rules .............................................................................. 70
Backing up your license files .......................................................................................... 71
Recovering a deleted license .......................................................................................... 71
Purging obsolete clients from the database to make more licenses available ................................................................. 72
About multi-year licenses ............................................................................................. 73

Chapter 5 Installing the Symantec Network Access Control client ....................................... 74

Preparing for client installation ....................................................................................... 74
Preparing Windows and Mac computers for remote deployment ................................................................. 76
| Chapter 6 | Upgrading Symantec Endpoint Protection .................................................. 91 |
| Chapter 7 | Managing groups of client computers ...................................................... 102 |
| Chapter 8 | Managing clients .............................................................................. 107 |
Password-protecting the client ................................................................. 111

Chapter 9 Managing administrator accounts and passwords ......................................................... 113

Managing administrator accounts .......................................................... 113
About administrator account roles and access rights .............................. 115
Adding an administrator account ......................................................... 117
Configuring the access rights for a limited administrator ...................... 118
Changing the authentication method for administrator accounts .......... 119
Best practices for testing whether a directory server authenticates an administrator account .............. 120
Changing the password for an administrator account ......................... 124
Allowing administrators to reset forgotten passwords ......................... 125
Sending a temporary password to an administrator ............................ 126
Displaying the Remember my user name and Remember my password check boxes on the logon screen ................................. 127

Section 3 Configuring Host Integrity and managing policies in Symantec Endpoint Protection Manager .......................................................... 129

Chapter 10 Configuring Host Integrity to enforce security compliance ........................................... 130

How Host Integrity works ................................................................. 131
How the Enforcers work with Host Integrity policies ............................ 132
Setting up Host Integrity ................................................................. 133
About Host Integrity requirements ..................................................... 135
Adding predefined requirements to a Host Integrity policy .................... 136
   Enabling and disabling Host Integrity requirements .......................... 137
   Setting up remediation for a predefined Host Integrity requirement ........... 137
   Allowing users to delay or cancel Host Integrity remediation ............... 138
Configuring the frequency of Host Integrity check settings .................... 140
Allowing the Host Integrity check to pass if a requirement fails .............. 140
Configuring notifications for Host Integrity checks .............................. 141
Creating a Quarantine policy for a failed Host Integrity check ............... 142
Adding a custom requirement from a template ................................... 143
Writing a customized requirement script .......................................... 143
   About registry conditions .............................................................. 145
   Writing a custom requirement to run a script on the client ............ 146
Writing a custom requirement to set the timestamp of a file ........... 147
Writing a custom requirement to increment a registry DWORD value ............................................................................ 148
Creating a test Host Integrity policy with a custom requirement script .................................................................................. 149

Chapter 11 Managing policies ............................................................. 151
Performing the tasks that are common to all policies ....................... 151
About shared and non-shared policies ............................................ 154
Adding a policy ............................................................................ 155
Editing a policy ............................................................................ 156
Copying and pasting a policy on the Policies page ......................... 157
Copying and pasting a policy on the Clients page .......................... 157
Assigning a policy to a group ......................................................... 158
Replacing a policy ........................................................................ 159
Exporting and importing individual policies ................................. 161
Converting a shared policy to a non-shared policy .......................... 162
Withdrawing a policy from a group ................................................. 163
How the client computers get policy updates ................................. 164
Configuring push mode or pull mode to update client policies and content ............................................................................ 165
Using the policy serial number to check client-server communication ............................................................................ 167
Manually updating policies on the client ....................................... 167

Section 4 Installing the Enforcers .......................................... 169

Chapter 12 Installing Enforcer appliances ........................................ 170
About the Symantec Network Access Control Enforcer appliances ............................................................................ 170
What you can do with Symantec Enforcer appliances .................. 171
About installing an Enforcer appliance ......................................... 172
Installing an Enforcer appliance .................................................. 173
About the Enforcer appliance indicators and controls .................. 173
Setting up an Enforcer appliance ................................................ 174
Logging on to an Enforcer appliance ......................................... 175
Configuring an Enforcer appliance ............................................. 176
Chapter 16: Installing the Symantec Network Access Control
Integrated Enforcer for Microsoft DHCP Servers

Process for installing the Symantec Network Access Control Integrated
Enforcer for Microsoft DHCP Server ........................................ 202
How to get started with the installation of an Integrated Enforcer for
Microsoft DHCP servers ..................................................... 203
System requirements for an Integrated Enforcer for Microsoft DHCP
Servers .................................................................................. 205
Components for an Integrated Enforcer for Microsoft DHCP
servers .................................................................................. 206
Placement requirements for an Integrated Enforcer for Microsoft DHCP
Servers .................................................................................. 206
Installing an Integrated Enforcer for Microsoft DHCP Servers ......... 208
Uninstalling the Symantec Network Access Control Integrated
Enforcer for Microsoft DHCP servers ..................................... 210
Upgrading the Integrated Enforcer for Microsoft DHCP
Servers .................................................................................. 210

Chapter 17: Installing the Symantec Integrated Enforcer for
Microsoft Network Access Protection ....................................... 212

Before you install the Symantec Integrated Enforcer for Microsoft
Network Access Protection ..................................................... 212
Process for installing the Symantec Network Access Control Integrated
Enforcer for Microsoft Network Access Protection ...................... 213
System requirements for an Integrated Enforcer for Microsoft Network
Access Protection .................................................................. 214
Components of a Symantec Integrated Enforcer for Microsoft Network
Access Protection .................................................................. 216
Installing the Integrated Enforcer for Microsoft Network Access
Protection ............................................................................. 217
Uninstalling the Integrated Enforcer for Microsoft Network Access
Protection ............................................................................. 218
Stopping and starting the Network Access Protection server
manually .............................................................................. 219
Section 5  Configuring the Enforcers ............................................. 220

Chapter 18  Configuring the Gateway Enforcer appliance from the Symantec Endpoint Protection Manager ......................................................... 221

How the Gateway Enforcer appliance works .................................................. 221
About configuring the Symantec Gateway Enforcer appliance on the Symantec Endpoint Protection Manager Console ........................................ 223
Changing Gateway Enforcer appliance configuration settings in Symantec Endpoint Protection Manager .............................................. 223
About authentication settings on a Gateway appliance .................................. 226
Authentication settings on a Gateway appliance .............................................. 226
About authentication sessions on a Gateway Enforcer appliance .......... 229
About client authentication on a Gateway Enforcer appliance ..................... 230
Specifying the maximum number of challenge packets during an authentication session ................................................................. 231
Specifying the frequency of challenge packets to be sent to clients .............. 231
Specifying the time period for which a client is blocked after it fails authentication ......................................................................................... 232
Specifying the time period for which a client is allowed to retain its network connection without reauthentication ................................................. 233
Allowing all clients with continued logging of non-authenticated clients ................................................................................................. 234
Allowing non-Windows clients to connect to a network without authentication .......................................................................................... 235
Checking the policy serial number on a client ............................................. 235
Sending a message from a Gateway Enforcer appliance to a client about non-compliance ............................................................................. 237
Redirecting HTTP requests to a Web page .................................................. 238
Authentication range settings ....................................................................... 239
Client IP address ranges compared to trusted external IP addresses .................. 240
When to use client IP address ranges .......................................................... 240
About trusted IP addresses ................................................................. 241
Adding client IP address ranges to the list of addresses that require authentication ......................................................................................... 243
Editing client IP address ranges on the list of addresses that require authentication .......................................................................................... 244
Chapter 19 Configuring the LAN Enforcer appliance on the Symantec Endpoint Protection Manager

Removing client IP address ranges from the list of addresses that require authentication ...................................................... 245
Adding a trusted internal IP address for clients on a management server ........................................................................ 245
Specifying trusted external IP addresses ........................................ 246
Editing trusted internal or external IP address ........................................ 247
Removing a trusted internal or trusted external IP address ............ 248
IP address range checking order ............................................. 248
About advanced Gateway Enforcer appliance settings .................. 249
Specifying packet types and protocols ....................................... 250
Allowing a legacy client to connect to the network with a Gateway Enforcer appliance .......................................................... 251
Enabling local authentication on a Gateway Enforcer appliance ........................................................................ 251
Enabling system time updates for the Gateway Enforcer appliance using the Network Time Protocol .......................... 252
Using the Gateway Enforcer appliance as a Web server ............... 252
Using the Gateway Enforcer as a DNS spoofing server ........ 253

Chapter 19 Configuring the LAN Enforcer appliance on the Symantec Endpoint Protection Manager

How the LAN Enforcer appliance works ........................................ 256
About configuring the Symantec LAN Enforcer on the Symantec Endpoint Protection Manager Console .............................. 257
About configuring RADIUS servers on a LAN Enforcer appliance .... 258
About configuring 802.1x wireless access points on a LAN Enforcer appliance ............................................................... 259
Changing LAN Enforcer configuration settings in Symantec Endpoint Protection Manager .................................................... 260
Using general settings ................................................................ 262
Adding or editing the name of a LAN Enforcer appliance group with a LAN Enforcer ....................................................... 263
Specifying a listening port for communication between a VLAN switch and a LAN Enforcer .................................................. 263
Adding or editing the description of an Enforcer group with a LAN Enforcer ................................................................. 264
Adding or editing the IP address or host name of a LAN Enforcer ............................................................................... 264
Adding or editing the description of a LAN Enforcer ..................... 264
Connecting the LAN Enforcer to Symantec Endpoint Protection Manager ........................................................................ 265
Using RADIUS server group settings ........................................ 266
Adding a RADIUS server group name and RADIUS server .......... 266
Editing the name of a RADIUS server group .......................... 268
Editing the friendly name of a RADIUS server ....................... 269
Editing the host name or IP address of a RADIUS server ......... 270
Editing the authentication port number of a RADIUS server .......... 270
Editing the shared secret of a RADIUS server ......................... 271
Enabling support for Windows Network Policy Server (NPS) on the LAN Enforcer ............................................................ 272
Deleting the name of a RADIUS server group ......................... 272
Deleting a RADIUS server ...................................................... 273
Using switch settings ................................................................... 273
Switch settings ..................................................................... 274
About the support for attributes of switch models ....................... 275
Adding an 802.1x switch policy for a LAN Enforcer appliance with a wizard ................................................................. 277
Editing basic information about the switch policy and 802.1x-aware switch ........................................................................... 285
Editing information about the 802.1x-aware switch .................. 290
Editing VLAN information for the switch policy ..................... 291
Editing action information for the switch policy ...................... 294
Using advanced LAN Enforcer appliance settings ....................... 298
  Allowing a legacy client to connect to the network with a LAN Enforcer appliance .......................................................... 299
  Enabling local authentication on the LAN Enforcer appliance ... 299
  Enabling system time updates for the Enforcer appliance using the Network Time Protocol .................................................. 300
Configuring MAC addresses and MAC authentication bypass (MAB) on the LAN Enforcer .......................................................... 300
Using 802.1x authentication ......................................................... 301
  About reauthentication on the client computer ......................... 304

Chapter 20 Configuring the Integrated Enforcers on the Enforcer console .......................................................... 306
What you can do with Symantec Integrated Enforcers ................. 307
About configuring Integrated Enforcers on an Enforcer console .... 307
Establishing or changing communication between an Integrated Enforcer for Microsoft DHCP servers and a Symantec Endpoint Protection Manager .................................................. 310
Configuring automatic quarantine ............................................. 312
Editing a Symantec Endpoint Protection Manager connection ........ 313
Configuring Integrated Enforcer communication settings in Symantec Endpoint Protection Manager ........................................ 313
Chapter 21 Configuring the Integrated Enforcer for Microsoft DHCP Server on the Symantec Endpoint Protection Manager ................................................. 319

About the Symantec Network Access Control Integrated Enforcer for Microsoft DHCP Servers ........................................................ 320

About configuring the Symantec Network Access Control Integrated Enforcer for Microsoft DHCP Server on the Symantec Endpoint Protection Manager ........................................................ 321

Configuring Symantec Network Access Control Integrated Enforcer basic settings ........................................................................... 322

Adding or editing the name of an Enforcer group for Symantec Network Access Control Integrated Enforcer ........................ 322

Adding or editing the description of an Enforcer group with a Symantec Network Access Control Integrated Enforcer ........ 323

Adding or editing the description of a Symantec Network Access Control Integrated Enforcer ......................................................... 323

Connecting the Symantec Network Access Control Integrated Enforcer to a Symantec Endpoint Protection Manager ............... 324

Configuring Symantec Network Access Control Integrated Enforcer advanced settings ................................................................. 325

Enabling servers, clients, and devices to connect to the network as trusted hosts without authentication ........................................ 325

Enabling local authentication on the Integrated Enforcer ............... 326

Configuring Symantec Network Access Control Integrated Enforcer authentication settings .......................................................... 327

About using authentication settings .............................................. 327

About authentication sessions ....................................................... 329

Specifying the maximum number of challenge packets during an authentication session ............................................................ 330

Specifying the frequency of challenge packets to be sent to clients ......................................................................................... 331

Allowing all clients with continued logging of non-authenticated clients ................................................................................. 332
Chapter 24 Configuring the Symantec Network Access Control On-Demand Clients ..................................................... 351
How the On-Demand Client works ................................................ 351
Before you configure Symantec Network Access Control On-Demand Clients on the console of a Gateway Enforcer ........................................ 352
Setting up guest access challenge using the Symantec Network Access Control DHCP Integrated Enforcer ........................................... 354
Enabling Symantec Network Access Control On-Demand clients to temporarily connect to a network ........................................ 358
Disabling Symantec Network Access Control On-Demand clients ......... 360
Setting up authentication on the Gateway Enforcer console for Symantec Network Access Control On-Demand clients .......... 360
Setting up user authentication with a local database ................. 361
Setting up user authentication with a Microsoft Windows 2003 Server Active Directory .................................................... 362
Setting up user authentication with a RADIUS server .......... 362
Setting up the On-Demand client on Windows for authentication with the dot1x-tls protocol ................................................. 363
Setting up the On-Demand client on Windows for authentication with the dot1x-peap protocol ............................................... 364
Editing the banner on the Welcome page ......................................... 365

Chapter 25 Performing basic tasks on the console of all types of Enforcer appliances ............................................... 366
About performing basic tasks on the console of an Enforcer appliance ............................................................... 366
Communication between an Enforcer appliance and a Symantec Endpoint Protection Manager .................................................. 367
Communication between the Enforcer appliance and clients .......... 368
Configuring a connection between an Enforcer appliance and a Symantec Endpoint Protection Manager .................................... 369
configure spm ........................................................................ 370
Checking the communication status of an Enforcer appliance on the Enforcer console ............................................................... 371
Remote access to an Enforcer appliance ........................................ 372
About the Enforcer appliance CLI command hierarchy ................. 372

Chapter 26 Managing Enforcers on the Symantec Endpoint Protection Manager .................................................... 374
About managing Enforcers on the management server console .......... 374
About managing Enforcers from the Servers page ..................... 375
Chapter 27 Troubleshooting the Enforcer appliance .................. 387

Troubleshooting communication problems between an Enforcer appliance and the Symantec Endpoint Protection Manager ........ 387
Troubleshooting an Enforcer appliance ........................................... 388
Frequently asked questions for the Enforcer appliances .................. 389
  Which virus protection and antivirus software is managed by Host Integrity? ................................................................. 390
  What happens if Enforcer appliances cannot communicate with Symantec Endpoint Protection Manager? ......................... 390
  Is a RADIUS server required when a LAN Enforcer appliance runs in transparent mode? ...................................................... 391
  How does Host Integrity enforcement manage computers without Symantec clients installed? ........................................... 392
Troubleshooting the connection between the Enforcer and the On-Demand Clients ......................................................... 394
Introducing Symantec Network Access Control

This chapter includes the following topics:

- What is Symantec Network Access Control?
- What’s new in Symantec Network Access Control 12.1.5
- System requirements for Symantec Network Access Control
- About the types of enforcement in Symantec Network Access Control
- Deploying Symantec Network Access Control
- Components of Symantec Network Access Control

What is Symantec Network Access Control?

Symantec Network Access Control ensures that a company’s client computers are compliant with the company’s security policies before the computers are allowed to access your protected network.

When enforcement controls are not in place, your organization’s data is vulnerable to intended loss or inadvertent loss. Recovering the data can result in down time and the financial losses that are associated with lost productivity. To prevent these losses, Symantec Network Access Control controls on site and remote access to protected network resources. Symantec Network Access Control provides a complete end-to-end network access control solution.

Symantec Network Access Control uses a Host Integrity policy and an optional Symantec Enforcer to discover and evaluate which computers are compliant. The clients that are not compliant are directed to a quarantine server for remediation. The remediation server provides downloads of the necessary software, patches,
virus definition updates, and so on, to make the client computer compliant. The Host Integrity policy on the client also continually monitors endpoints for changes in their compliance status.

Symantec Network Access Control is a companion product to Symantec Endpoint Protection. Both products include Symantec Endpoint Protection Manager, which provides the infrastructure to install and manage the Symantec Network Access Control and Symantec Endpoint Protection clients.

See “About the types of enforcement in Symantec Network Access Control” on page 29.

See “How Host Integrity works” on page 131.

## What's new in Symantec Network Access Control 12.1.5

Symantec Network Access Control 12.1.5 includes new features for Symantec Endpoint Protection Manager and Host Integrity policies.

### Table 1-1 New features in Symantec Network Access Control 12.1.5

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System requirements</td>
<td>You can now access Symantec Endpoint Protection Manager on the following browsers:</td>
</tr>
<tr>
<td></td>
<td>■ Microsoft Internet Explorer 10.2, 11</td>
</tr>
<tr>
<td></td>
<td>■ Mozilla Firefox 5.x through 31.0</td>
</tr>
<tr>
<td></td>
<td>■ Google Chrome through 37.0.2062.94</td>
</tr>
<tr>
<td></td>
<td>For the complete list of system requirements:</td>
</tr>
<tr>
<td></td>
<td>See the knowledge base article:</td>
</tr>
<tr>
<td></td>
<td><strong>Release Notes and System Requirements for all versions of Symantec Endpoint Protection and Symantec Network Access Control</strong></td>
</tr>
</tbody>
</table>
### Table 1-1  
New features in Symantec Network Access Control 12.1.5  
(continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Management server updates</strong></td>
<td>- Symantec Protection Center 1 was removed in Symantec Endpoint Protection 12.1.4. You can still integrate Symantec Endpoint Protection Manager with Symantec Protection Center 2, but the feature is no longer tested. Protection Center lets you manage Symantec Endpoint Protection together with other Symantec products in a single environment.</td>
</tr>
<tr>
<td><strong>Client password settings</strong></td>
<td>- The client password protection settings now appear in a more accessible location in Clients &gt; Policies &gt; Password Settings. This dialog also provides a new option to enable password protection globally for all clients. You can also access the Password Settings dialog box when you log on to Symantec Endpoint Protection Manager. See &quot;Password-protecting the client&quot; on page 111.</td>
</tr>
<tr>
<td></td>
<td>- You can no longer set to the console timeout to Never. For security reasons, the maximum timeout period is one hour. See &quot;Changing the time period for staying logged on to the console&quot; on page 60.</td>
</tr>
<tr>
<td></td>
<td>- After an administrator's failed logon attempts trigger an account lockout, the lockout interval now doubles with each subsequent lockout. Symantec Endpoint Protection Manager reverts to the original lockout interval after a successful logon, or after 24 hours since the first lockout. See &quot;Unlocking an administrator's account after too many logon attempts&quot; on page 59.</td>
</tr>
<tr>
<td><strong>Management server and client performance</strong></td>
<td>The management server and the client include the following performance improvements:</td>
</tr>
<tr>
<td></td>
<td>- Bandwidth control for client communication</td>
</tr>
<tr>
<td></td>
<td>- The management server now includes an Apache module that you can enable and configure to control network bandwidth. The module reduces the network load between Symantec Endpoint Protection Manager and the client computers, especially when the clients download content definitions or client installation packages.</td>
</tr>
<tr>
<td></td>
<td>- The client startup time has improved by more than 10%.</td>
</tr>
<tr>
<td></td>
<td>- The client service needs fewer processes to run.</td>
</tr>
<tr>
<td><strong>Host Integrity policy changes</strong></td>
<td>The Host Integrity policy is now included with both Symantec Endpoint Protection as well as Symantec Network Access Control. The Host Integrity policy evaluates the client computers and ensures that they meet the security policies you have modified and downloaded to those client computers. See &quot;How Host Integrity works&quot; on page 131.</td>
</tr>
</tbody>
</table>
Table 1-1: New features in Symantec Network Access Control 12.1.5
(continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Documentation</td>
<td>Symantec Network Access Control provides the following documentation changes:</td>
</tr>
<tr>
<td></td>
<td>■ All main PDF files are now on the Technical Support site. You can now look for and download the most current PDF files from a single location:</td>
</tr>
<tr>
<td></td>
<td>- Product guides for all versions of Symantec Network Access Control (English)</td>
</tr>
<tr>
<td></td>
<td>- Symantec Network Access Control (other languages)</td>
</tr>
<tr>
<td></td>
<td>- The tools documents remain in the same folder as the associated tool.</td>
</tr>
<tr>
<td></td>
<td>■ The Symantec Endpoint Protection Installation and Administration Guide no longer includes Network Access Control topics. A new Symantec Network Access Control Installation and Administration Guide includes the Network Access Control topics. The documents for specific tools remain in the same folder as the associated tool.</td>
</tr>
</tbody>
</table>

System requirements for Symantec Network Access Control

In general, the system requirements for Symantec Endpoint Protection Manager and the Symantec Network Access Control clients are the same as those of the operating systems on which they are supported.

For the most current system requirements, see:

Release Notes and System Requirements for all versions of Symantec Endpoint Protection and Symantec Network Access Control

■ System requirements for Symantec Endpoint Protection Manager
  See “System requirements for Symantec Endpoint Protection Manager” on page 25.

■ System requirements for the Symantec Network Access Control client for Windows
  See “System requirements for the Symantec Network Access Control client for Windows” on page 27.

■ System requirements for the Symantec Network Access Control On-Demand Client for Windows
  See “System requirements for the Symantec Network Access Control On-Demand Client for Windows” on page 27.

■ System requirements for the Symantec Network Access Control On-Demand Client for Mac
System requirements for Symantec Endpoint Protection Manager

Table 1-2 displays the minimum requirements for Symantec Endpoint Protection Manager.

Table 1-2  Symantec Endpoint Protection Manager system requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirements</th>
</tr>
</thead>
</table>
| Processor   | ■ 32-bit processor: Intel Pentium 4 or equivalent (minimum dual core or hyper-threading recommended)  
               ■ 64-bit processor: Intel Pentium 4 with x86-64 support or equivalent (minimum dual core or hyper-threading recommended)  
               **Note:** Intel Itanium IA-64 processors are not supported. |
| Physical RAM| 2 GB RAM available minimum; 4 GB or more available recommended.  
               **Note:** Your Symantec Endpoint Protection Manager server may require additional RAM depending on the RAM requirements of other applications that are already installed. |
<p>| Hard drive  | 16 GB available minimum (100 GB recommended) for the management server. 40 GB available minimum (200 GB recommended) for the management server and a locally installed database. |
| Display     | 1024 x 768                                                                   |</p>
<table>
<thead>
<tr>
<th>Component</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating system</td>
<td>■ Windows XP (32-bit, SP2 or later; 64-bit, all SPs; all editions except Home)</td>
</tr>
<tr>
<td></td>
<td>■ Windows 7 (32-bit, 64-bit; RTM and SP1; all editions except Home)</td>
</tr>
<tr>
<td></td>
<td>■ Windows 8 (32-bit, 64-bit)</td>
</tr>
<tr>
<td></td>
<td>■ Windows 8.1 (32-bit, 64-bit)</td>
</tr>
<tr>
<td></td>
<td>■ Windows 8.1 Update 1 (32-bit, 64-bit)</td>
</tr>
<tr>
<td></td>
<td>■ Windows 8.1 Update 2 (32-bit, 64-bit)</td>
</tr>
<tr>
<td></td>
<td>■ Windows Server 2003 (32-bit, 64-bit; R2, SP1 or later)</td>
</tr>
<tr>
<td></td>
<td>■ Windows Server 2008 (32-bit, 64-bit; R2, RTM, SP1 and SP2)</td>
</tr>
<tr>
<td></td>
<td>■ Windows Server 2012</td>
</tr>
<tr>
<td></td>
<td>■ Windows Server 2012 R2</td>
</tr>
<tr>
<td></td>
<td>■ Windows Server 2012 R2 Update 1</td>
</tr>
<tr>
<td></td>
<td>■ Windows Server 2012 R2 Update 2</td>
</tr>
<tr>
<td></td>
<td>■ Windows Small Business Server 2003 (32-bit)</td>
</tr>
<tr>
<td></td>
<td>■ Windows Small Business Server 2008 (64-bit)</td>
</tr>
<tr>
<td></td>
<td>■ Windows Small Business Server 2011 (64-bit)</td>
</tr>
<tr>
<td></td>
<td>■ Windows Essential Business Server 2008 (64-bit)</td>
</tr>
<tr>
<td>Web browser</td>
<td>■ Microsoft Internet Explorer 8, 9, 10, 10.2, 11</td>
</tr>
<tr>
<td></td>
<td>■ Mozilla Firefox 3.6 through 31.0</td>
</tr>
<tr>
<td></td>
<td>■ Google Chrome, through 37.0.2062.94</td>
</tr>
</tbody>
</table>

**Note:** This Symantec Endpoint Protection Manager version manages clients earlier than version 12.1, regardless of the client operating system.

The Symantec Endpoint Protection Manager includes an embedded database. You may also choose to use one of the following versions of Microsoft SQL Server:

■ SQL Server 2005, SP4
■ SQL Server 2008, through SP3
■ SQL Server 2008 R2, through SP2
■ SQL Server 2012, through SP1
■ SQL Server 2014
System requirements for the Symantec Network Access Control
client for Windows

Table 1-3 displays the minimum requirements for the Symantec Network Access
Control Windows client.

Table 1-3  Symantec Network Access Control client for Windows system
requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirement</th>
</tr>
</thead>
</table>
| Processor       | - 32-bit processor: 1 GHz Intel Pentium III or equivalent minimum (Intel Pentium 4 or equivalent recommended)  
                  - 64-bit processor: 2 GHz Pentium 4 with x86-64 support or equivalent minimum  
                  **Note:** Itanium processors are not supported. |
| Operating system| - Windows XP (32-bit, SP2 or later; 64-bit, all SPs)  
                  - Windows XP Embedded  
                  - Windows Vista (32-bit, 64-bit)  
                  - Windows 7 (32-bit, 64-bit)  
                  - Windows 8 (32-bit, 64-bit)  
                  - Windows 8.1 (32-bit, 64-bit)  
                  - Windows 8.1 Update 1 (32-bit, 64-bit)  
                  - Windows Server 2003 (32-bit, 64-bit; R2, SP1 or later)  
                  - Windows Server 2008 (32-bit, 64-bit)  
                  - Windows Server 2012  
                  - Windows Server 2012 R2  
                  - Windows Server 2012 R2 Update 1  
                  - Windows Small Business Server 2008 (64-bit)  
                  - Windows Essential Business Server 2008 (64-bit) |
| Physical RAM    | 512 MB of RAM, or higher if required by the operating system                |
| Hard disk       | 32-bit: 300 MB; 64-bit: 400 MB                                              |
| Display         | 800 x 600                                                                   |

System requirements for the Symantec Network Access Control
On-Demand Client for Windows

Table 1-4 lists the minimum requirements for the computers on which the Symantec
Network Access Control On-Demand Client needs to be installed.
Table 1-4  System requirements for the Symantec Network Access Control On-Demand Client for Windows

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>Intel Pentium II 550 MHz (1 GHz for Windows Vista) or faster</td>
</tr>
<tr>
<td>Operating System</td>
<td>The following operating systems are supported:</td>
</tr>
<tr>
<td></td>
<td>■ Windows XP Home or Professional (32-bit; SP2 and SP3)</td>
</tr>
<tr>
<td></td>
<td>■ Windows Vista (32-bit, 64-bit)</td>
</tr>
<tr>
<td></td>
<td>■ Windows 7 (32-bit, 64-bit)</td>
</tr>
<tr>
<td></td>
<td>■ Windows 8 (32-bit, 64-bit)</td>
</tr>
<tr>
<td></td>
<td>■ Windows 8.1 (32-bit, 64-bit)</td>
</tr>
<tr>
<td></td>
<td>■ Windows Server 2003 (32-bit, 64-bit; R2, SP1 or later)</td>
</tr>
<tr>
<td></td>
<td>■ Windows Server 2008 (32-bit, 64-bit; R2)</td>
</tr>
<tr>
<td></td>
<td>■ Windows Server 2012</td>
</tr>
<tr>
<td></td>
<td>■ Windows Server 2012 R2</td>
</tr>
<tr>
<td></td>
<td>■ Windows Small Business Server 2008 (64-bit)</td>
</tr>
<tr>
<td></td>
<td>■ Windows Essential Business Server 2008 (64-bit)</td>
</tr>
<tr>
<td>Memory</td>
<td>512 MB RAM</td>
</tr>
<tr>
<td>Hard disk</td>
<td>Download size: 9 MB</td>
</tr>
<tr>
<td></td>
<td>The amount of free disk space that is needed to run the client: 100 MB</td>
</tr>
<tr>
<td>Display</td>
<td>Super VGA (1,024 x 768) or higher resolution video adapter and monitor</td>
</tr>
<tr>
<td>Browser</td>
<td>You can use one of the following browsers:</td>
</tr>
<tr>
<td></td>
<td>■ Microsoft Internet Explorer 6.0 or later</td>
</tr>
<tr>
<td></td>
<td>■ Mozilla Firefox 3.0 or later</td>
</tr>
</tbody>
</table>

System requirements for the Symantec Network Access Control On-Demand Client for Mac

You may want to check your system requirements before you try to connect to an organization's protected network.

*Table 1-5* lists the minimum requirements for the computers on which the Symantec Network Access Control On-Demand Client installs.
Table 1-5 System requirements for Symantec Network Access Control On-Demand Downloader and Client on a Mac

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>Mac computer with an Intel CPU</td>
</tr>
<tr>
<td>Operating system</td>
<td>Mac OS X 10.6 or 10.7</td>
</tr>
<tr>
<td>Memory</td>
<td>512 MB of RAM</td>
</tr>
<tr>
<td>Hard disk</td>
<td>Download size: 9 MB</td>
</tr>
<tr>
<td></td>
<td>The amount of free disk space that is needed to run the client: 100 MB</td>
</tr>
<tr>
<td>Display and connectivity</td>
<td>■ Super VGA (1,024 x 768) or higher resolution video adapter and monitor</td>
</tr>
<tr>
<td></td>
<td>■ At least one Ethernet adapter (with TCP/IP installed)</td>
</tr>
<tr>
<td>Browser</td>
<td>Apple Safari 4.0 and 5.0; Mozilla Firefox 3.0 or later.</td>
</tr>
</tbody>
</table>

About the types of enforcement in Symantec Network Access Control

Symantec Network Access Control provides different methods of enforcement to control access to your network.

Table 1-6 describes the differences between host-based enforcement and network-based enforcement.
### Table 1-6 Types of enforcement

<table>
<thead>
<tr>
<th>Type of enforcement</th>
<th>Description</th>
</tr>
</thead>
</table>
| Host-based enforcement | Allows the client computers to obtain and run the software they need to automatically remediate compliance failures. This is usually done through assigning the client computer to a quarantine server, where the client can download needed remediation files. When the client computer is remediated, it can safely access your protected network resources. Host-based enforcement can selectively allow or block access to the protected network, or can use the Symantec firewall to allow or block access. The firewall is included as part of the Symantec Endpoint Protection product. Host-based enforcement includes the following methods:  
  - Host Integrity alone uses your Host Integrity policy to police network access, providing the easiest and fastest enforcement deployment option. You can implement Host Integrity more easily if the organization has already deployed the Symantec Endpoint Protection product.  
    See “How Host Integrity works” on page 131. 
    See “How the Enforcers work with Host Integrity policies” on page 132.  
  - Peer-to-peer authentication ensures that client-to-client communication occurs only between the company computers and Host Integrity-compliant computers outside the company. Compliant computers have passed their Host Integrity check.  
    You must have Symantec Endpoint Protection installed with Symantec Network Access Control to use peer-to-peer enforcement. |
| Network-based enforcement | Uses the Symantec Enforcer appliances and integrated software Enforcers to enable you to control network access. Network-based enforcement authenticates and allows network access only to the clients that meet the requirements in the Host Integrity policy. Network-based enforcement also checks that the policy is current.  
  Additionally, if your deployment includes a Gateway Enforcer appliance, you can allow guests without compliant software to access your network temporarily. These Enforcers enable guest access by installing On-Demand Clients on guest computers and dissolving them when guests log off. Guest access works with both Windows and Mac clients. This type of enforcement requires an Enforcer appliance.  
  See “Deploying Symantec Network Access Control” on page 30. |

### Deploying Symantec Network Access Control

It is best to deploy Symantec Network Access Control in phases. This approach allows your organization to evolve an implementation that fits your needs. You build on each previous phase instead of completely redoing your entire security infrastructure to make changes or enhancements.
### Table 1-7 Phases for deploying Symantec Network Access Control

<table>
<thead>
<tr>
<th>Phase</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phase 1</td>
<td>Install Symantec Endpoint Protection Manager and Symantec Network Access Control clients, and configure Host Integrity policies</td>
<td>You can control access for the laptops, desktops, and servers in your organization with Host Integrity and self-enforcement. With self-enforcement, computers can obtain the software they need to comply with your security policy. Use Symantec Endpoint Protection Manager to configure Host Integrity policies. See “Getting up and running on Symantec Endpoint Protection Manager for the first time” on page 35. See “How Host Integrity works” on page 131. See “Upgrading Symantec Endpoint Protection to include Symantec Network Access Control” on page 94.</td>
</tr>
</tbody>
</table>
| Phase 2 | Install and configure a Gateway Enforcer appliance                       | For partial network protection, control wired and wireless access to the network for managed clients and for guest computers.  
- Managed clients are those that run the Symantec Network Access Control client.  
- Guest clients are the laptops, desktops, and servers that do not meet your security requirements for items such as installed software and secure passwords. These are devices owned by guests such as contractors, consultants, and partners. You can allow these guest clients to safely and temporarily connect to your network with On-Demand clients. See “About installing an Enforcer appliance” on page 172. See “Installing an Enforcer appliance” on page 173. See “How the Gateway Enforcer appliance works” on page 221. See “How the On-Demand Client works” on page 351. |
| Phase 3 | Install and configure a LAN Enforcer appliance                           | For complete network protection, you can control LAN access for client computers and guest computers.  
See “About installing an Enforcer appliance” on page 172.  
See “Installing an Enforcer appliance” on page 173.  
See “How the LAN Enforcer appliance works” on page 256. |

See “About the types of enforcement in Symantec Network Access Control” on page 29.
**Components of Symantec Network Access Control**

Table 1-8 lists the product's components and describes their functions.

**Table 1-8  Symantec Network Access Control product components**

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symantec Endpoint Protection Manager</td>
<td>Symantec Endpoint Protection Manager is a management server that manages the client computers that connect to your company's network. Symantec Endpoint Protection Manager includes the following software:</td>
</tr>
<tr>
<td></td>
<td>■ The management server software provides secure communication to and from the client computers and the console.</td>
</tr>
<tr>
<td></td>
<td>■ The console is the interface to the management server. The console software coordinates and manages security policies, client computers, reports, logs, roles and access, administrative functions, and security. You can also install a remote console and use it to log on to the management server from any computer with a network connection.</td>
</tr>
<tr>
<td></td>
<td>■ The database stores security policies and events. You install the embedded database on the computer that hosts Symantec Endpoint Protection Manager. You can also separately install the Microsoft SQL Server database to use instead of the embedded database.</td>
</tr>
<tr>
<td></td>
<td>See “About choosing a database type” on page 42.</td>
</tr>
<tr>
<td></td>
<td>See “Installing Symantec Endpoint Protection Manager” on page 51.</td>
</tr>
<tr>
<td>Symantec Network Access Control Windows client</td>
<td>The Host Integrity policy enforces security policy compliance on the client computers by using Host Integrity checks and self-enforcement capabilities. The client reports its Host Integrity compliance status to the management server and a Symantec Enforcer. For more information about using the client, see the Symantec Endpoint Protection and Symantec Network Access Control Client Guide.</td>
</tr>
<tr>
<td></td>
<td>See “What is Symantec Network Access Control?” on page 21.</td>
</tr>
</tbody>
</table>

See “Optional components for Symantec Network Access Control” on page 32.

**Optional components for Symantec Network Access Control**

Table 1-9 lists the additional components that you can download and use with Symantec Network Access Control.
### Table 1-9 Symantec Network Access Control product subcomponents

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Symantec Enforcer** | An Enforcer ensures that the clients that try to connect to the network comply with configured security policies. You can restrict non-compliant computers to specific network segments for remediation and you can completely prohibit access to non-compliant computers.  
  Symantec Network Access Control includes the following types of Enforcers:  
  - The Gateway Enforcer appliance provides in-line enforcement at network choke points.  
  - The LAN 802.1X Enforcer appliance provides an out-of-band standards-based approach for LAN and wireless networks.  
  - The DHCP Integrated Enforcer provides a DHCP-based approach for LAN and wireless networks over any infrastructure.  
  - The Microsoft Network Access Protection Integrated Enforcer provides a Microsoft NAP-based approach for LAN and wireless networks.  
  See "About the Symantec Network Access Control Enforcer appliances" on page 170.  
  See "About the Symantec Network Access Control Integrated Enforcer for Microsoft DHCP Servers" on page 320.  
  See "About the Symantec Network Access Control Integrated Enforcer for Microsoft Network Access Protection" on page 337. |
| **Symantec Network Access Control On-Demand clients for Windows and Mac** | On-Demand Clients are the temporary clients that you provide to users when they are unauthorized to access your network. Unauthorized client computers do not have the software that is compliant with your security policy. Once the Enforcer has installed an on-demand client, it temporarily connects to your enterprise network as a guest.  
  See "How the On-Demand Client works" on page 351. |
| **IT Analytics server** | The IT Analytics tool expands upon the built-in reports in Symantec Endpoint Protection Manager by enabling you to create custom reports and custom queries. The tool also offloads the reporting burden from the management server to another server. IT Analytics keeps information for a longer period of time, enforces compliance, reduces costs, and provides summaries.  
  The IT Analytics tool and documentation is located in the Tools\ITAnalytics folder. |
Installing Symantec Endpoint Protection Manager

- Chapter 2. Planning the installation
- Chapter 3. Installing Symantec Endpoint Protection Manager
- Chapter 4. Managing product licenses
- Chapter 5. Installing the Symantec Network Access Control client
- Chapter 6. Upgrading Symantec Endpoint Protection
Planning the installation

This chapter includes the following topics:

- Getting up and running on Symantec Endpoint Protection Manager for the first time
- About Symantec Endpoint Protection Manager compatibility with other products
- Network architecture considerations
- About choosing a database type
- About basic management server settings
- About SQL Server configuration settings
- About SQL Server database authentication modes

Getting up and running on Symantec Endpoint Protection Manager for the first time

Table 2-1 lists the tasks that you should perform to install and protect the computers in your network immediately.
Table 2-1  Tasks to install and configure Symantec Endpoint Protection Manager

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plan your installation architecture</td>
<td>Before you install the product, consider the size and geographical distribution of your network to determine the installation architecture.</td>
</tr>
<tr>
<td></td>
<td>To ensure good network and database performance, you need to evaluate several factors. These factors include how many computers need protection, whether any of those computers connect over a wide-area network, or how often to schedule content updates.</td>
</tr>
<tr>
<td></td>
<td>■ If your network is small, is located in one geographic location, and has fewer than 500 clients, you need to install only one Symantec Endpoint Protection Manager.</td>
</tr>
<tr>
<td></td>
<td>■ If the network is very large, you can install additional sites with additional databases and configure them to share data with replication. To provide additional redundancy, you can install additional sites for failover or load balancing support. Failover and load balancing can only be used with Microsoft SQL Server databases.</td>
</tr>
<tr>
<td></td>
<td>■ If your network is geographically dispersed, you may need to install additional management servers for load balancing and bandwidth distribution purposes.</td>
</tr>
<tr>
<td></td>
<td>To help you plan medium to large-scale installations, see: Symantec Endpoint Protection Sizing and Scalability Best Practices White Paper.</td>
</tr>
</tbody>
</table>
Table 2-1  Tasks to install and configure Symantec Endpoint Protection Manager (continued)

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Prepare for and then install Symantec Endpoint Protection Manager | 1  Make sure the computer on which you install the management server meets the minimum system requirements.  
   See: Release Notes and System Requirements for all versions of Symantec Endpoint Protection and Symantec Network Access Control  
  
  2  Decide on whether to install the embedded database or use a Microsoft SQL Server database.  
   If you use a Microsoft SQL Server database, the installation requires additional steps. These include, but are not limited to, configuring or creating a database instance that is configured to use mixed mode or Windows authentication mode. You also need to provide database server administration credentials to create the database and the database user. These are specifically for use with the management server.  
   See “About SQL Server configuration settings” on page 45.  
  
  3  You install Symantec Endpoint Protection Manager first. After you install, you immediately configure the installation with the Management Server Configuration Wizard.  
   Decide on the following items when you configure the management server:  
   ■ A password for your login to the management console  
   ■ An email address where you can receive important notifications and reports  
   ■ An encryption password, which may be needed depending on the options that you select during installation  
   See “Installing Symantec Endpoint Protection Manager” on page 51.  
   See “About basic management server settings” on page 43.  
   See “Configuring Symantec Endpoint Protection Manager during installation” on page 52. |
Table 2-1  Tasks to install and configure Symantec Endpoint Protection Manager (continued)

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Add groups, locations, and policies         | **1** You use groups to organize the client computers, and apply a different level of security to each group. You can use the default groups, import groups if your network uses Active Directory or an LDAP server, or add new groups.  
If you add new groups, you can use the following group structure as a basis:  
- Desktops  
- Laptops  
- Servers  
See "How you can structure groups" on page 104.  
See “Adding a group” on page 105.  
**2** You use locations to apply different policies and settings to computers based on specific criteria. For example, you can apply different security policies to the computers based on whether they are inside or outside the company network. In general, the computers that connect to your network from outside of your firewall need stronger security than those that are inside your firewall.  
You can set up a location that allows the mobile computers that are not in the office to update their definitions automatically from Symantec's LiveUpdate servers.  
See Best Practices for Symantec Endpoint Protection Location Awareness.  
**3** Disable inheritance for the groups or locations for which you want to use different policies or settings.  
By default, groups inherit their policies and settings from the default parent group, My Company. If you want to assign a different policy to child groups, or want to add a location, you must first disable inheritance. Then you can change the policies for the child groups, or you can add a location.  
See “Disabling and enabling a group’s inheritance” on page 105.  
**4** For the default Host Integrity policy, you must add requirements for the Host Integrity check to have an effect on the client computer. Before you deploy the policy to client computers, test that the policy works the way that it should. |
### Table 2-1  Tasks to install and configure Symantec Endpoint Protection Manager (continued)

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Change communication settings to increase performance | You can improve network performance by modifying the following client-server communication settings in each group:  
  - Use pull mode instead of push mode to control when clients use network resources to download policies and content updates.  
  - Increase the heartbeat interval. For fewer than 100 clients per server, increase the heartbeat to 15-30 minutes. For 100 to 1,000 clients, increase the heartbeat to 30-60 minutes. Larger environments might need a longer heartbeat interval. Symantec recommends that you leave Let clients upload critical events immediately checked.  
  - Increase the download randomization to between one and three times the heartbeat interval.  

See “Configuring push mode or pull mode to update client policies and content” on page 165. |
| Activate the product license                 | Purchase and activate a license within 60 days of product installation.  

See “Activating or importing your Symantec Endpoint Protection 12.1.x product license” on page 65. |
| Decide on a client deployment method         | Determine which client deployment method would work best to install the client software on your computers in your environment.  

See “Installing clients with Web Link and Email” on page 80.  
See “Installing clients with Remote Push” on page 82.  
See “Installing clients with Save Package” on page 84.  
See “Exporting client installation packages” on page 85.  
If you use Remote Push, you may need to do the following task:  
If the client computers are part of an Active Directory domain, you must be logged on to the computer that hosts Symantec Endpoint Protection Manager with an account that grants local administrator access to the client computers. You should have administrator credentials available for each client computer that is not part of an Active Directory domain.  

See “Preparing Windows and Mac computers for remote deployment” on page 76. |
### Table 2-1  Tasks to install and configure Symantec Endpoint Protection Manager (continued)

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Prepare and deploy the client software for installation** | 1 Make sure that the computers on which you install the client software meet the minimum system requirements.  
See: *Release Notes and System Requirements for all versions of Symantec Endpoint Protection and Symantec Network Access Control*  
2 Do the following tasks:  
  ■ Make sure that you keep computer mode and not user mode.  
  ■ Update custom client install settings to determine installation options on the client computer. These options include the target installation folder and the restart behavior after installation completes. You can also use the default client install settings.  
3 With the Client Deployment Wizard, create a client installation package with selections from the available options, and then deploy it to your client computers.  
See “Exporting client installation packages” on page 85. |
| **Check that the computers are listed in the groups that you expected and that the client communicates with the management server** | In the management console, on the Clients > Clients page:  
1 Change the view to **Client status** to make sure that the client computers in each group communicate with the management server.  
Look at the information in the following columns:  
  ■ The **Name** column displays a green dot for the clients that are connected to the management server.  
   See “How to determine whether the client is connected in the console” on page 108.  
  ■ The **Last Time Status Changed** column displays the time that each client last communicated with the management server.  
  ■ The **Restart Required** column displays the client computers you need to restart to enable protection.  
  ■ The **Policy Serial Number** column displays the most current policy serial number. The policy might not update for one to two heartbeats. You can manually update the policy on the client if the policy does not update immediately.  
   See “Using the policy serial number to check client-server communication” on page 167.  
   See “Manually updating policies on the client” on page 167.  
2 On the client, check that the client is connected to a server, and check that the policy serial number is the most current one. |
About Symantec Endpoint Protection Manager compatibility with other products

Some products may cause conflicts with Symantec Endpoint Protection Manager when they are installed on the same server. You need to configure the Symantec Endpoint Protection Manager installation if one or more of the following products is installed on the same server:

- Symantec Backup Exec 10, 10D, or 11D
- Symantec Brightmail
- Symantec Enterprise Vault
- Symantec Ghost Solution Suite 2.0
- Symantec Mail Security for Exchange
- Symantec NetBackup
- Microsoft Outlook Web Access
- Microsoft SharePoint
- Microsoft Windows Update Services

In most cases, port changes are required to allow these programs to run concurrently with Symantec Endpoint Protection Manager.

For information about any necessary configuration changes, see Addressing Symantec Endpoint Protection compatibility issues.

For the most current system requirements, see Release Notes and System Requirements for all versions of Symantec Endpoint Protection and Symantec Network Access Control.

Network architecture considerations

You can install Symantec Endpoint Protection for testing purposes without considering your company network architecture. You can install Symantec Endpoint Protection Manager with a few clients, and become familiar with the features and functions.

When you are ready to install the production clients, you should plan your deployment based on your organizational structure and computing needs.

You should consider the following elements when you plan your deployment:

- Symantec Endpoint Protection Manager
Administrators use Symantec Endpoint Protection Manager to manage security policies and client computers. You may want to consider the security and availability of the computer on which Symantec Endpoint Protection Manager is installed.

■ Remote console
Administrators can use a remote computer that runs the console software to access Symantec Endpoint Protection Manager. Administrators may use a remote computer when they are away from the office. You should ensure that remote computers meet the remote console requirements.

■ Local and remote computers
Remote computers may have slower network connections. You may want to use a different installation method than the one you use to install to local computers.

■ Portable computers such as notebook computers
Portable computers may not connect to the network on a regular schedule. You may want to make sure that portable computers have a LiveUpdate policy that enables a LiveUpdate schedule. Any portable computers that do not check in regularly do not get other policy updates.

■ Computers that are located in secure areas
Computers that are located in secure areas may need different security settings from the computers that are not located in secure areas.

You identify the computers on which you plan to install the client. Symantec recommends that you install the client software on all unprotected computers, including the computer that runs Symantec Endpoint Protection Manager.

About choosing a database type
Symantec Endpoint Protection Manager uses a database to store information about clients and settings. The database is created as part of the configuration process. You must decide which database to use before you install the management server. You cannot use the console until you have configured the management server to use a database.
### Table 2-2  Databases that Symantec Endpoint Protection Manager uses

<table>
<thead>
<tr>
<th>Database type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Embedded database</td>
<td>The embedded database is included with Symantec Endpoint Protection Manager. The embedded database does not require configuration and is easier to install. The embedded database supports up to 5,000 clients. See “About basic management server settings” on page 43.</td>
</tr>
</tbody>
</table>
| SQL Server database   | If you choose to use this option, you must install SQL Server and SQL Server Native Client before you install Symantec Endpoint Protection Manager. For optimal compatibility, you install the version of SQL Server Native Client equal to your version of SQL Server. You should consider purchasing and installing SQL Server for the following reasons:  
  - You must support more than 5,000 clients. Each management server that uses SQL Server can support up to 50,000 clients. If your organization has more than 50,000 clients, you can install another management server.  
  - You want to support failover and load balancing.  
  - You want to set up additional management servers as site partners.  
  If you create a SQL Server database, you must first install an instance of SQL Server. You must then configure it for communication with the management server.  
  See “About SQL Server configuration settings” on page 45. |

### About basic management server settings

The following values represent the default settings when you install the Symantec Endpoint Protection Manager.

You can configure some of the following values only when you install the Symantec Endpoint Protection Manager using a custom configuration.

See “Installing Symantec Endpoint Protection Manager” on page 51.
<table>
<thead>
<tr>
<th>Setting</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site Name</td>
<td>My Site (default)</td>
<td>The name of the site as it appears in Symantec Endpoint Protection Manager. Site name is the highest level container under which all features are configured and run within Symantec Endpoint Protection Manager.</td>
</tr>
<tr>
<td></td>
<td>Site <em>local host name</em> (custom)</td>
<td></td>
</tr>
<tr>
<td>Server name</td>
<td><em>local host name</em></td>
<td>The name of the computer that runs Symantec Endpoint Protection Manager.</td>
</tr>
<tr>
<td>Server data folder</td>
<td>C:\Program Files\Symantec\Symantec Endpoint Protection Manager\data (32-bit operating system)</td>
<td>The directory in which the Symantec Endpoint Protection Manager places data files including backups, replicated logs, and other files. The installer creates this directory if it does not exist.</td>
</tr>
<tr>
<td></td>
<td>C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\data (64-bit operating system)</td>
<td></td>
</tr>
<tr>
<td>Encryption password</td>
<td>None</td>
<td>This password encrypts communication between Symantec Endpoint Protection Manager and clients.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You can also encrypt communication between a management server and an Enforcer.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If you choose the default configuration, the system automatically generates the encryption password for you. From the summary screen, you can print or copy this information to the clipboard.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If you choose a custom configuration, you can have the system automatically generate a random password, or you can create your own password. The password can be from 6-32 alphanumeric characters.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Document this password and put it in a secure location. You cannot change or recover the password after you create the database. You must also enter this password for disaster recovery purposes if you do not have a backed-up database to restore.</td>
</tr>
<tr>
<td>User name</td>
<td>admin</td>
<td>The name of the default user that is used to log on to the Symantec Endpoint Protection Manager console for the first time. This value is not configurable.</td>
</tr>
</tbody>
</table>
Table 2-3  Basic server settings (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>None</td>
<td>The password that is specified for the admin account during server configuration. You need the original admin password to reconfigure the management server at a later time. Document this password and put it in a secure location.</td>
</tr>
<tr>
<td>Email address</td>
<td>None</td>
<td>System notifications are sent to the email address specified.</td>
</tr>
</tbody>
</table>

About SQL Server configuration settings

If you install Symantec Endpoint Protection Manager with a SQL Server database, there are specific configuration requirements for SQL Server.

See "Installing Symantec Endpoint Protection Manager" on page 51.

Before you create the database, Symantec recommends that you install a new instance of SQL Server that conforms to Symantec installation and configuration requirements. You can install a database in an existing instance, but the instance must be configured properly or your database installation fails. For example, if you select a case-sensitive SQL collation, your installation fails.

**Warning:** Symantec Endpoint Protection Manager authenticates to SQL Server with a clear text database owner user name and password. To maximize the security posture of remote SQL Server communications, place both servers in the same secure subnet.

Table 2-4  Required SQL Server configuration settings

<table>
<thead>
<tr>
<th>Configuration setting</th>
<th>Installation requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance name</td>
<td>Do not use the default instance name. Create a name such as SEPM. By default, a database named Sem5 is created in the SQL Server instance when you install Symantec Endpoint Protection Manager. The default name is supported, but can cause confusion if you install multiple instances on one computer.</td>
</tr>
</tbody>
</table>
Table 2-4  Required SQL Server configuration settings (continued)

<table>
<thead>
<tr>
<th>Configuration setting</th>
<th>Installation requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication configuration</td>
<td>Mixed mode or Windows Authentication mode</td>
</tr>
<tr>
<td></td>
<td>See “About SQL Server database authentication modes” on page 49.</td>
</tr>
<tr>
<td>sa password</td>
<td>Set this password when you set Mixed Mode authentication.</td>
</tr>
<tr>
<td>Enabled protocol</td>
<td>TCP/IP</td>
</tr>
<tr>
<td>IP addresses for TCP/IP</td>
<td>Enable IP1 and IP2</td>
</tr>
<tr>
<td>TCP/IP port numbers for IP1, IP2, and</td>
<td>Set TCP Dynamic Ports to blank, and specify a TCP port number. The default port is</td>
</tr>
<tr>
<td>IPALL</td>
<td>typically 1433.</td>
</tr>
<tr>
<td></td>
<td>You specify this port number when you create the database.</td>
</tr>
<tr>
<td></td>
<td>The Symantec Endpoint Protection Manager database does not support dynamic ports.</td>
</tr>
<tr>
<td>Remote connections</td>
<td>Must be enabled. TCP/IP protocol must also be specified.</td>
</tr>
</tbody>
</table>

If your database is located on a remote server, you must also install SQL Server client components on the computer that runs Symantec Endpoint Protection Manager. SQL Server client components include BCP.EXE. The version number of the SQL Server client components should be the same as the version number of SQL Server that you use. Refer to your SQL Server documentation for installation instructions.

During the Symantec Endpoint Protection Manager database configuration phase of the installation, you select and enter various database values. Understand the decisions you must make to correctly configure the database.

Table 2-5 displays the settings that you might need to know before you begin the installation process.

Table 2-5  SQL Server database settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server name</td>
<td>local host name</td>
<td>Name of the computer that runs Symantec Endpoint Protection Manager.</td>
</tr>
<tr>
<td>Setting</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Server data folder</td>
<td>C:\Program Files\Symantec Endpoint Protection Manager\data</td>
<td>Folder in which the Symantec Endpoint Protection Manager places data files including backups, replication, and other Symantec Endpoint Protection Manager files. The installer creates this folder if it does not exist.</td>
</tr>
<tr>
<td>Encryption password</td>
<td>None</td>
<td>The password that encrypts communication between Symantec Endpoint Protection Manager and clients. The password can be from 6-32 alphanumeric characters and is required. You can also encrypt the communication between a management server and an Enforcer hardware device. Document this password and put it in a secure location. You cannot change or recover the password after you create the database. You must also enter this password for disaster recovery purposes if you do not have a backed-up database to restore.</td>
</tr>
<tr>
<td>Databaseserver</td>
<td>local host name</td>
<td>Name of the computer where SQL Server is installed, and the optional instance name. If the database server was installed with the default instance, which is no name, type either host name or the host's IP address. If the database server was installed with a named instance, type either host name\instance_name or IP address\instance_name. The use of host name only works with properly configured DNS. If you install to a remote database server, you must first install the SQL Server client components on the computer that runs Symantec Endpoint Protection Manager.</td>
</tr>
<tr>
<td>SQL Server Port</td>
<td>1433</td>
<td>The port that is used to send and receive traffic to the SQL Server. The use of port 0 is not supported. Port 0 specifies a random, negotiated port.</td>
</tr>
<tr>
<td>Database Name</td>
<td>sem5</td>
<td>Name of the database that is created.</td>
</tr>
<tr>
<td>Setting</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>Database user name</td>
<td>sem5</td>
<td>Name of the database user account that is created. The user account has a standard role with read and write access. The name can be a combination of alphanumeric values and the special characters `~ # % _ + =</td>
</tr>
<tr>
<td>Database password</td>
<td>None</td>
<td>The password that is associated with the database user account. The name can be a combination of alphanumeric values and the special characters `~ # % _ + =</td>
</tr>
<tr>
<td>SQL Server client folder</td>
<td>SQL Server 2005: Install Directory\90\Tools\Binn SQL Server 2008: Install Directory\100\Tools\Binn SQL Server 2012: Install Directory\110\Tools\Binn SQL Server 2014: Install Directory\Client SDK\ODBC\110\Tools\Binn</td>
<td>Location of the local SQL Client Utility directory that contains bcp.exe. Installation Directory represents the installation location of Microsoft SQL Server. By default, this location is C:\Program Files\Microsoft SQL Server.</td>
</tr>
<tr>
<td>Server user name</td>
<td>None</td>
<td>Name of the database server administrator account, which is typically sa.</td>
</tr>
<tr>
<td>Server password</td>
<td>None</td>
<td>The password that is associated with the database server administrator account, which is typically sa.</td>
</tr>
</tbody>
</table>
Table 2-5  SQL Server database settings (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database data folder</td>
<td>Automatically detected after you click Default. SQL Server 2005: Install Directory\MSSQL.1\MSSQL\Data</td>
<td>Location of the SQL Server data folder. If you install to a remote server, the volume identifier must match the identifier on the remote server. Installation Directory represents the installation location of Microsoft SQL Server. By default, this location is C:\Program Files\Microsoft SQL Server.</td>
</tr>
</tbody>
</table>
| SQL Server 2005          | Install Directory\MSSQL10.MSSQLSERVER\MSSQL\Data                     | If you install to a named instance on SQL Server 2005, the instance name is appended to MSSQL with a dot numeric identifier. For example, \MSSQL.n|MSSQL\Data

| SQL Server 2008 R2       | Install Directory\MSSQL10_50.MSSQLSERVER\MSSQL\Data                  | If you install to a named instance on SQL Server 2008, the instance name is appended to MSSQL10. For example, \MSSQL10.instance name|MSSQL\Data

| SQL Server 2012          | Install Directory\MSSQL11.MSSQLSERVER\MSSQL\Data                      | If you install to a named instance on SQL Server 2012, the instance name is appended to MSSQL11. For example, \MSSQL11.instance name|MSSQL\Data

| SQL Server 2014          | Install Directory\MSSQL12.MSSQLSERVER\MSSQL\Data                      | If you install to a named instance on SQL Server 2014, the instance name is appended to MSSQL12. For example, \MSSQL12.instance name|MSSQL\Data

Note: Clicking Default displays the correct installation folder if you entered the database server and instance name correctly. If you click Default and the correct installation folder does not appear, your database creation fails.

About SQL Server database authentication modes

The Symantec Endpoint Protection Manager supports two modes of SQL Server database authentication:

- Windows Authentication mode
- Mixed mode

SQL Server can be configured to use either Windows Authentication or mixed mode authentication. Mixed mode authentication allows the use of either Windows or SQL Server credentials. When SQL Server is configured to use mixed mode, Symantec Endpoint Protection Manager may be set to use either Windows Authentication or mixed mode authentication. When SQL Server is set to use Windows Authentication
mode, Symantec Endpoint Protection Manager must also be configured to use Windows Authentication mode.

For the remote database connections that use the Windows Authentication mode, be aware of the following requirements:

- For deployments in an Active Directory environment, Symantec Endpoint Protection Manager and SQL Server must be located in the same Windows domain.

- For deployments in a Workgroup environment, the Windows account credentials must be the same for the local computers and the remote computers.

See “About SQL Server configuration settings” on page 45.
Installing Symantec Endpoint Protection Manager

This chapter includes the following topics:

- Installing Symantec Endpoint Protection Manager
- Configuring Symantec Endpoint Protection Manager during installation
- Uninstalling Symantec Endpoint Protection Manager
- Logging on to the Symantec Endpoint Protection Manager console
- Changing the time period for staying logged on to the console

Installing Symantec Endpoint Protection Manager

You perform several tasks to install the management server and the console. In the installation wizard, a green check mark appears next to each completed task.

**Note:** Symantec Endpoint Protection Manager requires full access to the system registry for installation and normal operation. To prepare a Windows Server 2003 computer on which you plan to remotely install Symantec Endpoint Protection Manager, you must first allow remote control on the computer. When you connect with Remote Desktop, you must also use a console session or shadow the console session in Remote Desktop.
For the most current system requirements, see: Release Notes and System Requirements for all versions of Symantec Endpoint Protection and Symantec Network Access Control

See “About client installation methods” on page 80.

See “Preparing for client installation” on page 74.

## Configuring Symantec Endpoint Protection Manager during installation

The Management Server Configuration Wizard automatically starts after the Symantec Endpoint Protection Manager installation.

See “Installing Symantec Endpoint Protection Manager” on page 51.

You can also start the Management Server Configuration Wizard at any time after installation from **Start > All Programs > Symantec Endpoint Protection Manager > Symantec Endpoint Protection Manager Tools**.

To configure the server, you specify the following information:

- The configuration type, which is **Default configuration** or **Custom configuration**. The wizard provides information about each type.
- Whether you want to use a recovery file.

---

**Note:** If this installation is the first installation of Symantec Endpoint Protection Manager, there is no recovery file.

- The password for the default administrator account.
- The email address that receives important notifications and reports.
- The mail server name and port number.
- The Symantec Sales Partner information, if a partner manages your Symantec licenses.

Each configuration type has a separate configuration process. Follow the instructions that are provided in the Management Server Configuration Wizard to complete the configuration.
Uninstalling Symantec Endpoint Protection Manager

Uninstalling Symantec Endpoint Protection Manager uninstalls the server and console. You can optionally remove the database and the database backup files during uninstallation.

If you plan to reinstall Symantec Endpoint Protection Manager, you should back up the database before you uninstall it.

You must turn off replication before you attempt to uninstall an installation of Symantec Endpoint Protection Manager that is set up for replication.

To uninstall Symantec Endpoint Protection Manager

The text that you see depends on the operating system of the server computer.

1. On the server computer, on the Start menu, click Control Panel > Add or Remove Programs (or Control Panel > Programs > Uninstall a program).

2. In the Add or Remove Programs (or Uninstall or change a program) dialog box, click Symantec Endpoint Protection Manager, and then click Change, Remove, or Uninstall.

3. Follow the onscreen prompts to remove Symantec Endpoint Protection Manager.

In some cases, you may have to uninstall Symantec Endpoint Protection Manager manually.

For more information, see Methods for uninstalling Symantec Endpoint Protection.

Logging on to the Symantec Endpoint Protection Manager console

You can log on to the Symantec Endpoint Protection Manager console after you install Symantec Endpoint Protection Manager. You can log on to the console in either of two ways:

- Locally, from the computer on which you installed the management server.
- Remotely, from any computer that meets the system requirements for a remote console and has network connectivity to the management server. You can log on to the remote web console or the remote Java console.

To log on remotely, you need to know the IP address or the host name of the computer on which the management server is installed. You should also ensure that your web browser Internet options let you view content from the server you log on to.
When you log on remotely, you can perform the same tasks as administrators who log on locally. What you can view and do from the console depends on the type of administrator you are. Most administrators in smaller organizations log on as a system administrator.

Note: If you installed the remote Java console with an earlier version of the product, you must reinstall it when you upgrade to a later version.

You can also access the reporting functions from a standalone web browser that is connected to your management server.

For security, the console logs you out after a maximum of one hour. You can decrease this period of time. In version 12.1.4 and earlier, you can disable the timeout period.

See “Changing the time period for staying logged on to the console” on page 60.

To log on to the console locally

1 Go to Start > Programs > Symantec Endpoint Protection Manager > Symantec Endpoint Protection Manager.

2 In the Symantec Endpoint Protection Manager logon dialog box, type the user name (admin by default) and the password that you configured during the installation.

   If the console has more than one domain, click Options and type the domain name.

3 Optionally check Remember my user name, Remember my password or both, if available, and then click Log On.
To log on to the console remotely

1. Open a supported web browser and type the following address in the address box:

   http://host name:9090

   where host name is the host name or IP address of the management server. For a list of supported web browsers, see Release Notes and System Requirements for all versions of Symantec Endpoint Protection and Symantec Network Access Control.

2. On the Symantec Endpoint Protection Manager console Web Access page, click the desired console type.

   If you click Symantec Endpoint Protection Manager Web Console, a secure webpage loads so you log on remotely without the use of the Java Runtime Environment (JRE).

   If you click Symantec Endpoint Protection Manager Console, the computer from which you log on must have the JRE installed to run the Java client. If it does not, you must download and install it. Follow the prompts to install the JRE, and follow any other instructions provided.

   The other option is not a remote management solution. You can click Symantec Endpoint Protection Manager Certificate to prompt you to download the management console’s certificate file. You can then import this file into your web browser if needed.

3. If a host name message appears, click Yes.

   This message means that the remote console URL that you specified does not match the Symantec Endpoint Protection Manager certificate name. This problem occurs if you log on and specify an IP address rather than the computer name of the management server.

   If the webpage security certificate warning appears, click Continue to this website (not recommended) and add the self-signed certificate.
4 Follow the prompts to complete the logon process.

When you log on for the first time after installation, use the account name admin.

Depending on the logon method, you may need to provide additional information. For instance, if the console has multiple domains, click Options and provide the name of the domain to which you want to log on.

5 If you use the Java-based console, you may have the option to save the user name and password. Click Log On.

You may receive one or more security warning messages as the remote console starts up. If you do, click Yes, Run, Start, or their equivalent, and continue until the console appears.

You may need to accept the self-signed certificate that the Symantec Endpoint Protection Manager console requires.

See “Granting or blocking access to remote Symantec Endpoint Protection Manager consoles” on page 57.

See “Displaying a message for administrators to see before logging on to the Symantec Endpoint Protection Manager console” on page 57.

See “About administrator account roles and access rights” on page 115.

See “About accepting the self-signed server certificate for Symantec Endpoint Protection Manager” on page 56.

About accepting the self-signed server certificate for Symantec Endpoint Protection Manager

When you install Symantec Endpoint Protection Manager, a self-signed certificate for the pages that are rendered in a browser is included as part of the installation. When you first access these pages from a remote console, you must accept the self-signed certificate for the pages to display.

The certificates are stored separately for each user. Each administrator account must accept the certificate for each remote location from which they connect to the management server.

For instructions to add the security certificate to the web browser, see the Symantec Technical Support knowledge base article, How to install the certificate for Symantec Endpoint Protection Manager for Web console access.

See “Logging on to the Symantec Endpoint Protection Manager console” on page 53.
Displaying a message for administrators to see before logging on to the Symantec Endpoint Protection Manager console

You can create and display a customizable message that all administrators see before they can log on to the console. The main purpose is to display a legal notice to tell the administrators that they are about to log on to a proprietary computer.

The message appears in the console after administrators type their user name and password and click Log On. After administrators have read the message, they can acknowledge the notice and click OK, which logs on the administrators. If administrators click Cancel, the logon process is canceled, and the administrator is taken back to the logon window.

The message also appears if the administrator runs the reporting functions from a standalone web browser that is connected to the management server.

To display a message for administrators to see before logging on to the Symantec Endpoint Protection Manager console

1. In the console, click Admin, and then click Domains.
2. Select the domain for which you want to add a logon banner.
4. On the Logon Banner tab, check Provide a legal notice to administrators when they log on to Symantec Endpoint Protection Manager.
5. Type the banner title and text.
   Click Help for more information.
6. Click OK.

See “Adding an administrator account” on page 117.

Granting or blocking access to remote Symantec Endpoint Protection Manager consoles

By default, all consoles are granted access. Administrators can log on to the main console locally or remotely from any computer on the network.

You can secure a management console from remote connections by denying access to certain computers.

You may want to grant or deny access from the following types of users or computers:

- You should deny access to anyone on the Internet. Otherwise, the console is exposed to Internet attacks.
You should deny access to limited administrators who use consoles on a different network than the network they manage.

You should grant access to system administrators and IT administrators.

You should grant access to lab computers, such as a computer that is used for testing.

In addition to globally granting or denying access, you can specify exceptions by IP address. If you grant access to all remote consoles, the management server denies access to the exceptions. Conversely, if you deny access to all remote consoles, you automatically grant access to the exceptions. When you create an exception, the computer that you specified must have a static IP address. You can also create an exception for a group of computers by specifying a subnet mask. For example, you may want to grant access in all areas that you manage. However, you may want to deny access to a console that is located in a public area.

To grant or deny access to a remote console

1. In the console, click **Admin**, and then click **Servers**.
2. Under **Servers**, select the server for which you want to change the remote console access permission.
3. Under **Tasks**, click **Edit the server properties**.
4. On the **General** tab, click **Granted Access** or **Denied Access**.
5. If you want to specify IP addresses of the computers that are exempt from this console access permission, click **Add**.

   Computers that you add become exceptions. If you click **Granted Access**, the computers that you specify are denied access. If you click **Denied Access**, the computers that you specify are granted access. You can create an exception for a single computer or a group of computers.

6. In the **Deny Console Access** dialog box, click one of the following options:

   - **Single Computer**
     For one computer, type the IP address.
   
   - **Group of Computers**
     For several computers, type both the IP address and the subnet mask for the group.
7 Click **OK**.

The computers now appear in the exceptions list. For each IP address and mask, its permission status appears.

If you change **Granted Access** to **Denied Access** or vice versa, all exceptions change as well. If you have created exceptions to deny access, they now have access.

8 Click **Edit All** to change the IP addresses or host names of those computers that appear on the exceptions list.

The **IP Address Editor** appears. The **IP Address Editor** is a text editor that lets you edit IP addresses and subnet masks.

9 Click **OK**.

10 When you finish adding exceptions to the list or editing the list, click **OK**.

See “Adding an administrator account” on page 117.

See “Logging on to the Symantec Endpoint Protection Manager console” on page 53.

Unlocking an administrator's account after too many logon attempts

Symantec Endpoint Protection Manager locks out an administrator for a certain length of time after a number of unsuccessful logon attempts. By default, the management server locks out an administrator for 15 minutes after five failed attempts.

You cannot unlock the administrator account without waiting for the specified period of time to pass. However, you can disable the administrator account from locking. You can also change the number of unsuccessful logon attempts and wait time that is permitted before the account is locked.

For added security in 12.1.5, after the first lockout, the lockout interval doubles with each additional lockout. Symantec Endpoint Protection Manager reinstates the original lockout interval after a successful logon occurs or after 24 hours pass since the first lockout. For example, if the original lockout interval is 15 minutes, the second lockout triggers a 30-minute lockout interval. The third lockout triggers a 60-minute lockout interval. If the first lockout occurs at 2:00 P.M. on Thursday, then the 24-hour period ends 2:00 P.M. Friday, and Symantec Endpoint Protection Manager resets the lockout interval to 15 minutes.

If you are locked out of your account, you must wait for the specified length of time before you can log on again. A password change does not reset or otherwise affect the lockout interval.
To disable administrator account locking

1. In the console, click Admin > Administrators.
2. Under Administrators, select the administrator account that is locked.
3. Under Tasks, click Edit the administrator.
4. On the General tab, uncheck Lock the account after the specified number of unsuccessful logon attempts.

See “Sending a temporary password to an administrator” on page 126.
See “Changing the password for an administrator account” on page 124.

Changing the time period for staying logged on to the console

To help protect the console, the console requires you to reenter your user name and password after one hour. To increase security, you can decrease the timeout period before you must log on to the management console.

In version 12.1.4 and earlier, you can set the time period to Never.

To change the time period for staying logged on to the console

1. In the console, click Admin, and then click Servers.
2. Click Local Site or a remote site and click Edit Site Properties.
3. On the General tab, click the Console Timeout drop-down list and select one of the available options for length of time.
4. Click OK.
Managing product licenses

This chapter includes the following topics:

- Licensing Symantec Endpoint Protection
- About purchasing licenses
- Activating or importing your Symantec Endpoint Protection 12.1.x product license
- About product upgrades and licenses
- About renewing your Symantec Endpoint Protection license
- Checking the license status in Symantec Endpoint Protection Manager
- About the licensing enforcement rules
- Backing up your license files
- Recovering a deleted license
- Purging obsolete clients from the database to make more licenses available
- About multi-year licenses

Licensing Symantec Endpoint Protection

Symantec Endpoint Protection requires a paid license after the trial period expires or when your current license expires. You can apply an existing license to a product upgrade.

You use the License Activation Wizard to activate new or renewed licenses, or when you convert a trial license to a paid license. You license Symantec Endpoint Protection according to the number of clients that you need to protect the endpoints at your site.
Once you install Symantec Endpoint Protection Manager, you have 60 days to purchase enough license seats to cover all of your deployed clients.

**Note:** To administer licenses, you must log on to Symantec Endpoint Protection Manager with a management server system administrator account, such as the default account admin.

See “About administrator account roles and access rights” on page 115.

**Table 4-1** lists the tasks that are required to purchase, activate, and manage your Symantec product license.

### Table 4-1 Licensing tasks

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check the product license requirements</td>
<td>Understand the importance of the license requirements for the computers that you want to protect. A license lets you install the Symantec Endpoint Protection client on a specified number of computers. A license lets you download security content and product updates from LiveUpdate.</td>
</tr>
<tr>
<td></td>
<td>See “About the licensing enforcement rules” on page 70.</td>
</tr>
<tr>
<td></td>
<td>See “About multi-year licenses” on page 73.</td>
</tr>
</tbody>
</table>
| Purchase a license and save it to the management server | You need to purchase a license in the following situations:  
  - You want to purchase Symantec Endpoint Protection.  
  - Your trial license expired.  
  - Your paid license expired.  
  - Your license is over-deployed.  
  - Your upgrade license from 11.0 expired.  
You do not need to manually download a license file. After you purchase your license, you receive an email with a Symantec license file (.slf) or a license serial number. |
|                                           | See “About purchasing licenses” on page 63.                                                                                                                                                                                        |
|                                           | See “Checking the license status in Symantec Endpoint Protection Manager” on page 69.                                                                                                                                                |
### Table 4-1  Licensing tasks (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
</table>
| Import the license file and activate your purchased license | You use the License Activation Wizard in the Symantec Endpoint Protection Manager console to import and activate your Symantec product license. Before you activate the license, you must have one of the following items:  
- A Symantec license serial number  
- A Symantec license file (.slf)  
You receive one or the other of these when you purchase a license.  
See “Activating or importing your Symantec Endpoint Protection 12.1.x product license” on page 65.  
See “About the Symantec Licensing Portal” on page 68. |
| Back up your license files                      | Back up your license files to preserve them in case the database or the computer's hard disk becomes damaged.  
See “Backing up your license files” on page 71.  
See “Recovering a deleted license” on page 71.                                                   |
| Review the preconfigured license notifications   | Preconfigured license notifications alert administrators about expired licenses and other license issues.                                                                                                     |
| Keep track of when your licenses expire, and renew your licenses | Check the status for each license that you imported into the console to see whether you need to renew a license or purchase more licenses.  
See “Checking the license status in Symantec Endpoint Protection Manager” on page 69.  
See “About renewing your Symantec Endpoint Protection license” on page 69.                         |

### About purchasing licenses

You need to purchase a license in the following situations:

- Your trial license expired. Symantec Endpoint Protection comes with a trial license that lets you install and evaluate the product in your environment.
- Your current license is expired.
Your current license is over-deployed. Over-deployed means that you have deployed more clients than your current license allows.

You decide to keep the new version after the upgrade trial from 11.0 expires. If you use 11.0, Symantec sends you an email with an upgrade offer that includes a free upgrade trial. If you decide to keep the new version beyond the upgrade trial period of 90 days, you need to purchase a paid license.

Depending upon how you purchase your license, you receive by email either a product license serial number or a Symantec License file. The license file uses the file extension .slf. When you receive the license file by email, it is attached to the email as a .zip file. You must extract the .slf file from the .zip file.

Save the license file to a computer that can be accessed from the Symantec Endpoint Protection Manager console. Many users save the license on the computer that hosts Symantec Endpoint Protection Manager. Many users also save a copy of the license to a different computer or removable storage media for safekeeping.

**Warning:** To prevent corruption of the license file, do not open or alter the file contents in any way. However, you may copy and store the license as desired.

Table 4-2 displays where to learn more about purchasing licenses.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Determine your licensing requirements</td>
<td>See “About the licensing enforcement rules” on page 70.</td>
</tr>
<tr>
<td>Find out where to buy product licenses</td>
<td>You can purchase a Symantec product license from the following sources:</td>
</tr>
<tr>
<td></td>
<td>■ The Symantec online store:</td>
</tr>
<tr>
<td></td>
<td><a href="http://store.symantec.com/">http://store.symantec.com/</a></td>
</tr>
<tr>
<td></td>
<td>■ Your preferred Symantec reseller:</td>
</tr>
<tr>
<td></td>
<td>To find a reseller, use the <a href="http://www.symantec.com/partners/index.jsp">Partner locator</a>.</td>
</tr>
<tr>
<td></td>
<td>To find out more about Symantec partners, go to</td>
</tr>
<tr>
<td></td>
<td><a href="http://www.symantec.com/partners/index.jsp">http://www.symantec.com/partners/index.jsp</a></td>
</tr>
<tr>
<td></td>
<td>■ The Symantec sales team:</td>
</tr>
<tr>
<td></td>
<td>Visit the <a href="http://www.symantec.com/orders">Symantec Ordering website</a> for</td>
</tr>
<tr>
<td></td>
<td>sales contact information.</td>
</tr>
<tr>
<td>Get help with purchasing licenses or</td>
<td><a href="http://customercare.symantec.com/">http://customercare.symantec.com/</a></td>
</tr>
<tr>
<td>learn more about licenses</td>
<td>See “Licensing Symantec Endpoint Protection” on page 61.</td>
</tr>
</tbody>
</table>
Activating or importing your Symantec Endpoint Protection 12.1.x product license

You can use the License Activation Wizard workflow to perform the following tasks:

- Activating a new paid license.
- Converting a trial license to a paid license.
- Renewing a license.
- Activating an additional paid license in response to an over-deployment status.
- Activating a license after you upgrade from a previous version, such as 11.0.

You can import and activate a license file that you received from the following sources:

- Symantec Licensing Portal
- Symantec partner or preferred reseller
- Symantec sales team
- Symantec Business Store

**Note:** You can only import your Symantec Network Access Control 12.1.x license into a Symantec Network Access Control-enabled management server.

You can start the License Activation Wizard in the following ways:

- The Welcome screen that appears after you install the product.
- From the **Common Tasks** menu on the **Home** page.
- The **Admin** page of the Symantec Endpoint Protection Manager console.

If you activate or import your license from the Welcome screen or the **Common Tasks** menu, you can skip to step 3.

To activate or import your Symantec Endpoint Protection 12.1.x product license

1. In Symantec Endpoint Protection Manager, click **Admin > Licenses**.
2. Under **Tasks**, click **Activate license**.
3. Click **Activate a new license**, and then click **Next**. If you do not see this panel, continue to the next step.
4 On the **License Activation** panel, select the option that matches your situation, and then click **Next**.

The following table describes each option:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>I have a serial number</td>
<td>You may receive a license serial number when you or your Symantec Partner purchased the license. If you have a license serial number, select this option. If you are an eFlex (Symantec Enterprise Options) customer and have an eFlex-generated serial number, select <strong>I have a Symantec License File</strong>.</td>
</tr>
</tbody>
</table>
| I have a Symantec License File (.slf) | In most cases, you receive a Symantec license file (.slf file) in an email from Symantec shortly after you complete the purchase process. The file arrives attached to the notification email as a .zip file. If you have received a .slf file, select this option.  
  **Note:** You must extract the .slf file from the .zip file before you can use it to activate your product license.  
  **Warning:** The .slf file contains the information that is unique to your license. To avoid corrupting the license file, do not alter its contents. You may copy the file for your records. |

You can find information about eFlex at the following webpage:

**Enterprise Options**

5 Do one of the following tasks based on the selection that you made in the previous step:

- If you selected **I have a serial number**, enter the serial number, and then click **Submit**. Review the information about the license you added, and then click **Next**.

- If you selected **I have a Symantec License File (.slf)**, click **Add File**. Browse to and select the .slf file you extracted from the .zip file that came with your Symantec notification email. Click **Open**, and then click **Next**.
6 Enter information about your technical contacts and primary contacts, and about your company. Click to acknowledge the disclosure statement, and then click Submit.

If you provided this information when you purchased your license, this panel does not display.

7 Click Finish.

See “About renewing your Symantec Endpoint Protection license” on page 69.
See “About purchasing licenses” on page 63.
See “Licensing Symantec Endpoint Protection” on page 61.

Required licensing contact information

The activation process prompts you to provide any missing license contact information. Privacy statements are provided in the wizard to describe how this information is used. You must indicate that the privacy conditions are acceptable before you can complete the activation process.

Table 4-3 includes the information you need.

<table>
<thead>
<tr>
<th>Type of information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical Contact</td>
<td>Contact information for the person who is in charge of the technical activities that are concerned with installing or maintaining your endpoint security infrastructure. The contact's name, email address, and phone number are required.</td>
</tr>
<tr>
<td>Primary Contact</td>
<td>Contact information for the person who represents your company. The contact's name, email address, and phone number are required.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: Click the check box to indicate when the Technical Contact and Primary Contact are the same person.</td>
</tr>
<tr>
<td>Company Information</td>
<td>Includes the company name, location, phone number, and email address.</td>
</tr>
</tbody>
</table>

See “Licensing Symantec Endpoint Protection” on page 61.
About the Symantec Licensing Portal

You can use the Symantec Licensing Portal to activate product licenses. However, you can activate licenses from the Symantec Endpoint Protection Manager console, which is simpler and faster.

The Symantec Licensing Portal is now part of MySymantec. You can access the Licensing Portal through the following website:

https://licensing.symantec.com

Note: If you have existing credentials for MySymantec, you can use those credentials to access licensing information. If you do not have a MySymantec account, you must create one before you can use the Licensing Portal. To create an account, go to the Licensing Portal website and then click Register Now.

The Symantec Customer Care website has additional information about using the Symantec Licensing Portal to manage licenses:

http://customersupport.symantec.com/

See “Activating or importing your Symantec Endpoint Protection 12.1.x product license” on page 65.

See “Licensing Symantec Endpoint Protection” on page 61.

About product upgrades and licenses

When Symantec releases a new version of Symantec Endpoint Protection, you may apply your existing active license to the new version. You receive an email notification that a new release is available that includes instructions for downloading the new version of Symantec Endpoint Protection.

For more information about licensing product upgrades, see the Version Upgrade FAQ at the following webpage:


See “Upgrading to a new release” on page 91.

See “Licensing Symantec Endpoint Protection” on page 61.
About renewing your Symantec Endpoint Protection license

When your current license is about to expire, the Symantec Endpoint Protection Manager sends license expiration notifications to the Symantec Endpoint Protection administrator. Symantec highly recommends that you renew your license before it expires.

When you renew a license, the management server removes and replaces the expired license with a new license. To purchase renewal licenses, visit the Symantec Store, or contact your Symantec partner or preferred Symantec reseller.

In the event that you accidentally delete a license, you can recover it from the Symantec Endpoint Protection Manager console.

See “About purchasing licenses” on page 63.

See “Activating or importing your Symantec Endpoint Protection 12.1.x product license” on page 65.

See “Recovering a deleted license” on page 71.

Checking the license status in Symantec Endpoint Protection Manager

You can find out whether the management server uses a trial license or a paid license. You can also obtain the following license information for each paid license that you imported into the console:

- License serial number, total seat count, expiration date
- Number of valid seats
- Number of deployed seats
- Number of expired seats
- Number of over-deployed clients

The trial license status only provides limited information that is related to the expiration date.

To determine if your installation uses a paid license or a trial license

1. In the console, click Admin.
2. On the Admin page, click Licenses.
To check license status for paid licenses

1. In the console, click **Home**.

2. On the **Home** page, click **Licensing Details**.

See “Licensing Symantec Endpoint Protection” on page 61.

See “Activating or importing your Symantec Endpoint Protection 12.1.x product license” on page 65.

### About the licensing enforcement rules

Symantec Endpoint Protection licenses are enforced according to the following rules:

#### Table 4-4 Licensing enforcement rules

<table>
<thead>
<tr>
<th>Where applies</th>
<th>Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>Term of license</td>
<td>The term of the license starts from the time and date of activation until midnight of the last day of the licensing term. If you have multiple sites, the license expires on the day and the time of the westernmost Symantec Endpoint Protection Manager database.</td>
</tr>
<tr>
<td>License coverage: Symantec Endpoint Protection components</td>
<td>A Symantec Endpoint Protection license applies to the Symantec Endpoint Protection clients. For instance, in a network with 50 endpoints, the license must provide for a minimum of 50 seats. Instances of Symantec Endpoint Protection Manager do not require a license.</td>
</tr>
<tr>
<td>License coverage: sites and domains</td>
<td>A Symantec Endpoint Protection product license is applied to an entire installation regardless of the number of replicated sites or domains that compose the installation. For instance, a license for 100 seats covers a two-site installation where each site has 50 seats. If you have not implemented replication, you may deploy the same .sif file to multiple Symantec Endpoint Protection management servers. The number of clients reporting to your management servers must not exceed the total number of licensed seats.</td>
</tr>
<tr>
<td>License coverage: platforms</td>
<td>Licensing seats apply to all clients.</td>
</tr>
</tbody>
</table>
Table 4-4  Licensing enforcement rules (continued)

<table>
<thead>
<tr>
<th>Where applies</th>
<th>Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>License coverage: products and</td>
<td>License seats apply equally across product versions. For example, a license covers both version 11.0 and 12.1.x clients within the same site.</td>
</tr>
<tr>
<td>versions</td>
<td></td>
</tr>
</tbody>
</table>

See “Licensing Symantec Endpoint Protection” on page 61.

Backing up your license files

Symantec recommends that you back up your license files. Backing up the license files preserves the license files in case the database or the console computer’s hard disk becomes damaged.

By default, when you import the license file using the Licensing Activation Wizard, Symantec Endpoint Protection Manager places a copy of the license file in the following location: `\Symantec Endpoint Protection Manager installation directory\Inetpub\license`

If you misplaced the license files you originally downloaded or received by email, you can download the files again from the Symantec Licensing Portal website.

To back up your license files

- Using Windows, copy the .slf license files from the directory where you saved the files to another computer of your choice.

  See your company’s procedure for backing up files.

See “Activating or importing your Symantec Endpoint Protection 12.1.x product license” on page 65.

See “About the Symantec Licensing Portal” on page 68.

See “Licensing Symantec Endpoint Protection” on page 61.

Recovering a deleted license

If you accidentally delete a license file, you can recover it from the Symantec Endpoint Protection Manager console.
**To recover a deleted license**

1. On the Symantec Endpoint Protection Manager console Admin page, click Licenses and then under Tasks, click Recover a deleted license.

2. On the License recovery panel, check the box next to the deleted license you want to recover, and then click Submit.

---

**Purging obsolete clients from the database to make more licenses available**

Symantec Endpoint Protection Manager can incorrectly display an over-deployed license status due to obsolete clients. These are database entries for the clients that no longer communicate with Symantec Endpoint Protection Manager in the protected environment. Clients can be rendered obsolete for many reasons, such as when you upgrade the operating system, decommission a computer, or change the hardware configuration.

If your license reports show more seats are licensed than known to be deployed, you should purge the database of obsolete clients. Obsolete clients count against the product license, so it is important to purge obsolete clients as soon as they are created. By default, purging occurs every 30 days. You can shorten the interval between purge cycles to more quickly purge the obsolete clients. You reset the interval as needed to suit your long-term needs after the purge cycle completes.

In non-persistent Virtual Desktop Infrastructures (VDIs), you can set a separate time period for purging the non-persistent clients. This setting purges the offline clients that have not connected during the time period that you set. Non-persistent offline clients do not affect the license count.

**To purge obsolete clients from the database to make more licenses available**

1. In the console, on the Admin page, click Domains, right-click the domain, and click Edit Domain Properties.

2. On the General tab, change the Delete clients that have not connected for specified time setting from the default of 30 to 1.

   You do not need to set the option to purge the non-persistent clients for licensing purposes. The non-persistent clients that are offline do not count toward the license total.

3. Click OK.

4. Wait 24 hours and then revert the settings to 30 days or to another interval that suits your requirements.

See "Licensing Symantec Endpoint Protection" on page 61.
About multi-year licenses

When you purchase a multi-year license, you receive a set of license files equal to the number of years your license is valid. For instance, a three-year license consists of three separate license files. When you activate a multi-year license, you import all of the license files during the same activation session. Symantec Endpoint Protection Manager merges the separate license files into a single activated license that is valid for the purchased duration.

While not recommended, it is possible for you to activate fewer than the full complement of license files. In this case, Symantec Endpoint Protection Manager merges the files and applies the duration of the license file that expires last. For instance, a three-year license that is activated with only the first two files indicates a duration of only two years. When you activate the third file at a later date, Symantec Endpoint Protection Manager accurately reports the full duration of the license as three years. In all cases, the number of seats remains consistent with the number of seats that you purchased.

When Symantec Endpoint Protection Manager merges files, it deletes the shortest duration files and keeps the longest duration file for internal license-keeping functions. If you think that Symantec Endpoint Protection Manager inappropriately deleted a license, recover and reactivate the deleted license.

You can see the license serial numbers of shorter duration that are associated with the active license. On the Admin page, click Licenses and then click the activated license. The associated licenses appear in the Associated Licenses column.

See “Recovering a deleted license” on page 71.

See “Licensing Symantec Endpoint Protection” on page 61.
Installing the Symantec Network Access Control client

This chapter includes the following topics:

- Preparing for client installation
- About client installation methods
- Exporting client installation packages
- About the Windows client installation settings
- Uninstalling the Symantec Endpoint Protection client for Windows
- Managing client installation packages
- Adding client installation package updates

Preparing for client installation

You must install a Symantec Endpoint Protection client on every computer you want to protect, whether the computer is physical or virtual.

Table 5-1 lists the actions that you must perform to install the client software on the computers in your network.
Table 5-1  Client computer preparation

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Identify client computers           | Identify the computers on which you want to install the client software. Check that all the computers run a supported operating system.  
Note: Symantec recommends that you also install the client on the computer that hosts Symantec Endpoint Protection Manager.  
For the most current system requirements, see: Release Notes and System Requirements for all versions of Symantec Endpoint Protection and Symantec Network Access Control |
| Identify computer groups (optional) | Identify the computer groups to which you want the clients to belong. For example, you can group clients based on type of computer, to conform to your corporate organization, or to the security level required. You can create these groups before or after you install the client software.  
You can also import an existing group structure such as an Active Directory structure.  
See "Managing groups of clients" on page 102.                                                                                                                                                                                                 |
| Prepare client computers for deployment and installation | Prepare the computers for remote client deployment and for successful communication with Symantec Endpoint Protection Manager after installation.  
- Modify any existing firewall settings to allow communication during Remote Push deployment, and between Symantec Endpoint Protection components after installation.  
If your users do not have administrative rights for their computers, then you should remotely install the client software using Remote Push. The Remote Push installation requires you to enter the credentials that have local administrative rights for the computers.  
See "About the communication ports that Symantec Endpoint Protection uses" on page 78.  
See "Installing clients with Remote Push" on page 82.  
See "Preparing Windows and Mac computers for remote deployment" on page 76. |
Table 5-1  Client computer preparation (continued)

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Determine features and deploy client software | You deploy the client software using one of the available methods. You can also export a customized client package to deploy later or with a third-party tool.  
See “About client installation methods” on page 80.  
See “Exporting client installation packages” on page 85.  
- You decide which features to install to the client computers. You configure custom client feature sets and installation settings before you export or deploy an installation package. Installation settings include the installation folder and the restart settings. You can also use the default client install feature sets and installation settings.  
See “About the Windows client installation settings” on page 86.  
- For Windows clients, you can choose to automatically uninstall existing third-party security software when you configure client installation settings. |
| Verify installation status                  | Confirm that the client installation succeeded and that clients communicate with Symantec Endpoint Protection Manager. Managed clients may not appear in the console until after they are restarted. |

After installation, you can take additional steps to optimize the performance of your Symantec Endpoint Protection installation.

Preparing Windows and Mac computers for remote deployment

Table 5-2 lists the tasks that you must do on Windows operating systems to successfully install the client remotely. See your Windows documentation for more information on any tasks you do not know how to perform.

Note: You use this method to deploy the Symantec Endpoint Protection Mac client, and not the Symantec Network Access Control On-Demand Mac client.
### Table 5-2  Windows remote deployment preparation tasks

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Tasks</th>
</tr>
</thead>
</table>
| Prepare Windows XP computers and Windows Server 2003 servers that are installed in workgroups | Windows XP computers and Windows Server 2003 servers that are installed in workgroups do not accept remote deployment by default. To permit remote deployment, disable Simple File Sharing.  
  
**Note:** This limitation does not apply to computers that are part of an Active Directory domain.  

You may also need to perform the following tasks:  
- Ensure that the Administrator account does not have a blank password.  
- Disable the Windows Firewall, or allow the required ports for communication between the client and Symantec Endpoint Protection Manager. |
| Prepare Windows Vista, Windows 7, or Windows Server 2008 / 2008 R2 computers | Windows User Account Control blocks local administrative accounts from remotely accessing remote administrative shares such as C$ and Admin$. You do not need to fully disable User Account Control on the client computers during the remote deployment if you disable the registry key `LocalAccountTokenFilterPolicy`.  

To disable UAC remote restrictions, see:  
[http://support.microsoft.com/kb/951016](http://support.microsoft.com/kb/951016)  

If the Windows client computer is part of an Active Directory domain, you should use domain administrator account credentials for a remote push installation.  

Perform the following tasks:  
- Disable the Windows Firewall, or configure the firewall to allow the required traffic.  
- Disable the Sharing Wizard.  
- Enable network discovery by using the Network and Sharing Center.  
- Enable the built-in administrator account and assign a password to the account.  
- Verify that the account has administrator privileges.  
- Disable or remove Windows Defender. |
| Prepare Windows 8 / 8.1 / 8.1 Update 1 or Windows Server 2012 / 2012 R2 / 2012 R2 Update 1 computers | Before you deploy, perform the following tasks:  
- Disable the Windows Firewall, or configure the firewall to allow the required traffic.  
- Disable the registry key `LocalAccountTokenFilterPolicy`.  

To disable UAC remote restrictions, see:  
[http://support.microsoft.com/kb/951016](http://support.microsoft.com/kb/951016)  

- Enable and start the Remote Registry service.  
- Disable or remove Windows Defender. |

See “About the communication ports that Symantec Endpoint Protection uses” on page 78.

See “Installing clients with Remote Push” on page 82.
About the communication ports that Symantec Endpoint Protection uses

If the Symantec Endpoint Protection Manager computer and Symantec Endpoint Protection client computers run firewall software, you must open certain ports for remote deployment and for communication between the management server and clients. See your firewall software product documentation for instructions to open ports or allow applications to use ports.

**Warning:** The firewall in the Symantec Endpoint Protection client is disabled by default at initial installation. To ensure firewall protection, leave the Windows firewall enabled on the clients until the software is installed and the client is restarted. The Symantec Endpoint Protection client firewall automatically disables the Windows firewall when the computer restarts.

### Table 5-3  Ports for client and server installation and communication

<table>
<thead>
<tr>
<th>Function</th>
<th>Component</th>
<th>Protocol and port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Push deployment</td>
<td>Management server and client</td>
<td>TCP 139 and 445 on management servers and clients</td>
</tr>
<tr>
<td></td>
<td></td>
<td>UDP 137 and 138 on management servers and clients</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TCP ephemeral ports on management servers and clients</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TCP 22 on Mac clients</td>
</tr>
<tr>
<td>General communication</td>
<td>Management server and client</td>
<td>For management servers and clients:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- TCP 8014 for management servers, by default.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You can change TCP 8014 (HTTP) to TCP 443 (HTTPS).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- TCP ephemeral port on clients.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For remote management servers and consoles:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- TCP 8443 for remote management servers and console</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- TCP ephemeral ports and 9090 on consoles</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- TCP 8445 for remote reporting consoles</td>
</tr>
<tr>
<td>Replication communication</td>
<td>Site to site between database servers</td>
<td>TCP 8443 between database servers</td>
</tr>
</tbody>
</table>
Table 5-3  Ports for client and server installation and communication (continued)

<table>
<thead>
<tr>
<th>Function</th>
<th>Component</th>
<th>Protocol and port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Symantec Endpoint Protection Manager console installation</td>
<td>Management server and remote management server console</td>
<td>TCP 9090 on remote management servers&lt;br&gt;TCP ephemeral ports on remote consoles&lt;br&gt;Note: You can change the port.</td>
</tr>
<tr>
<td>Web services</td>
<td>Remote Monitoring and Management (RMM) Symantec Protection Center</td>
<td>TCP 8446 for RMM Web services&lt;br&gt;TCP 8444 for Symantec Protection Center Web services</td>
</tr>
<tr>
<td>External database communication</td>
<td>Remote SQL Server and management server</td>
<td>TCP 1433 on remote SQL Server&lt;br&gt;TCP ephemeral ports on management servers&lt;br&gt;Note: Port 1433 is the default port.</td>
</tr>
<tr>
<td>Symantec Network Access Control Enforcer communication</td>
<td>Management server and Enforcer</td>
<td>TCP 1812 on management servers&lt;br&gt;TCP ephemeral ports on Enforcers&lt;br&gt;Note: RADIUS servers also use port 1812; do not install the management server on the same server. You cannot change the port on the management server.</td>
</tr>
<tr>
<td>LiveUpdate</td>
<td>LiveUpdate client and server</td>
<td>TCP ephemeral ports on clients&lt;br&gt;TCP 80 on LiveUpdate servers</td>
</tr>
</tbody>
</table>

- Windows Vista and later contain a firewall that is enabled by default. If the firewall is enabled, you might not be able to install or deploy the client software remotely. If you have problems deploying the client to computers running these operating systems, configure their firewalls to allow the required traffic.

- If you decide to use the Windows firewall after deployment, you must configure it to allow file and printer sharing (port 445).

For more information about configuring Windows firewall settings, see the Windows documentation.

See “Preparing for client installation” on page 74.
About client installation methods

After you install Symantec Endpoint Protection Manager, you install the Symantec Endpoint Protection client with the Client Deployment Wizard.

Table 5-4 displays the client installation methods that you can use.

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Link and Email</td>
<td>Users receive an email message that contains a link to download and install the client software. The users then install the client software, so they must have local administrator rights to their computers. See “Installing clients with Web Link and Email” on page 80.</td>
</tr>
<tr>
<td>Remote Push</td>
<td>Remote push installation pushes the client software to the computers that you specify. The installation begins automatically on the client computers. Remote push installation does not require the user to have local administrator rights to their computers. See “Installing clients with Remote Push” on page 82. See “Preparing Windows and Mac computers for remote deployment” on page 76.</td>
</tr>
<tr>
<td>Save Package</td>
<td>This installation option creates an executable installation package that you save on the management server and then distribute to the client computers. The users then install the client software, so they must have local administrator rights to their computers. See “Installing clients with Save Package” on page 84.</td>
</tr>
</tbody>
</table>

Before you run the Client Deployment Wizard, you review the installation options, optionally customize them, and then select those options during installation. Installation options include the protection technologies to install, the installation destination folder, and the restart behavior after installation.

See “About the Windows client installation settings” on page 86.
See “Preparing for client installation” on page 74.

Installing clients with Web Link and Email

The Web Link and Email option creates the installation package and the URL for the installation package, and then sends the link to users in an email. The users
download the package and install the Symantec Endpoint Protection client. Users must have administrator privileges to install the package.

Web Link and Email comprises the following tasks:

■ You select, configure, and then create the client installation package.
  You choose the options that appear for the configuration of the client installation package. All client installation packages are stored on the computer that runs Symantec Endpoint Protection Manager.

■ Email from Symantec Endpoint Protection Manager notifies the computer users that they can download the client installation package.
  You provide a list of users to receive an email message, which contains instructions to download and install the client installation package. Users follow the instructions to install the client software.

Before you begin the client installation with Web Link and Email, make sure that you correctly configure the connection from the management server to the mail server.

To install clients with Web Link and Email

1  In the console, on the Home page, in the Common Tasks menu, select Install protection client to computers.

2  In the Client Deployment Wizard, click New Package Deployment, and then click Next. Web Link and Email only sends a new installation package.

3  Make selections from the available options, which vary depending on the installation package type, and then click Next.
  See “About the Windows client installation settings” on page 86.

4  Click Web Link and Email, and then click Next.

5  In the Email Recipients and Message panel, specify the email recipients and the subject.
  To specify multiple email recipients, type a comma after each email address. A management console System Administrator automatically receives a copy of the message.
  You can accept the default email subject and body, or edit the text. You can also copy the URL and post it to a convenient and secure online location, like an intranet page.
To create the package and deliver the link by email, click **Next**, and then click **Finish**.

Confirm that the computer users received the email message and installed the client software.

Client computers may not appear within the management console until after they restart. Depending on the client restart settings of the installed client, you or the computer users may need to restart the client computers.

See “About client installation methods” on page 80.

See “Preparing for client installation” on page 74.

### Installing clients with Remote Push

Remote Push pushes the client software to the computers that you specify. Using Remote Push requires knowledge of how to search networks to locate computers by IP address or computer names. Once the package copies to the target computer, the package installs automatically. The computer user does not need to begin the installation or to have administrator privileges.

Remote Push comprises the following tasks:

- You select an existing client installation package, create a new installation package, or create a package to update communication settings.
- For new installation packages, you configure and create the installation package.
- You specify the computers on your network to which Symantec Endpoint Protection Manager sends a package.
  
  Remote Push locates either specific computers for which you provide an IP number or range, or all computers that are visible by browsing the network.
- Symantec Endpoint Protection Manager pushes the client software to the specified computers.
  
  The installation automatically begins on the computers once the package successfully copies to the target computer.

#### To install clients with Remote Push

1. In the console, on the **Home** page, in the **Common Tasks** menu, click **Install protection client to computers**.

2. In the **Client Deployment Wizard**, do one of the following tasks:
   - Click **New Package Deployment** to create a new installation package, and then click **Next**.
   - Click **Existing Package Deployment** to use a package that was previously created, and then click **Browse** to locate the package to install.
The Client Deployment Wizard uploads the package and directs you to the Computer Selection panel (step 5).

- Click Communication Update Package Deployment if you want to update Windows client communication settings on the computers that already have the Symantec Endpoint Protection client installed. Follow the on-screen instructions, and then go to step 4.

---

Note: While the Communication Update Package option appears for Mac, there is no Mac client for Symantec Network Access Control.

---

3 For a new package, in the Select Group and Install Feature Sets panel, make selections from the available options, which vary depending on the installation package type. Click Next.

See “About the Windows client installation settings” on page 86.

4 Click Remote Push, and then click Next.

5 In the Computer Selection panel, locate the computers to receive the software using one of the following methods:

- To browse the network for computers, click Browse Network.
- To find computers by IP address or computer name, click Search Network, and then click Find Computers.

You can set a timeout value to constrain the amount of time that the server applies to a search.

6 Click >> to add the computers to the list, and authenticate with the domain or workgroup if the wizard prompts you.

The remote push installation requires elevated privileges. If the client computer is part of an Active Directory domain, you should use a domain administrator account.

7 Click Next, and then click Send to push the client software to the selected computers.

Once the Deployment Summary panel indicates a successful deployment, the installation starts automatically on the client computers.

The installation takes several minutes to complete.
Click Next, and then click Finish.

Confirm the status of the installed clients on the Clients page.

For new Symantec Endpoint Protection installations, the client computers may not appear within the management console until after they are restarted. Depending on the client restart settings of the client, you or the computer users may need to restart the client computers.

See “Preparing for client installation” on page 74.
See “Preparing Windows and Mac computers for remote deployment” on page 76.
See “About client installation methods” on page 80.

Installing clients with Save Package

Save Package creates the installation packages that you can install either manually, with third-party deployment software, or with a login script.

Save Package comprises the following tasks:

- You make your configuration selections and then create the client installation packages.
- You save the installation package to a folder on the computer that runs Symantec Endpoint Protection Manager.
  For Windows, the installation package can be for 32- or 64-bit operating systems. The installation package comprises one setup.exe file or a collection of files that includes a setup.exe file. Computer users often find one setup.exe file easier to use.

Either you or the end user can install the installation package on the client computer. Alternately, you can use third-party deployment software to perform the installation.

To install clients with Save Package

1. In the console, on the Home page, in the Common Tasks menu, click Install protection client to computers.

2. In the Client Deployment Wizard, do one of the following tasks:
   - Click New Package Deployment, and then click Next. Save Package only installs a new installation package.
   - Click Communication Update Package Deployment if you want to update Windows client communication settings on the computers that already have the Symantec Endpoint Protection client installed. Follow the on-screen instructions, and then go to step 4.
Note: While the Communication Update Package option appears for Mac, there is no Mac client for Symantec Network Access Control.

3 Make selections from the available options, which vary depending on the installation package type, and then click **Next**.

See “About the Windows client installation settings” on page 86.

4 Click **Save Package**, and then click **Next**.

5 Click **Browse** and specify the folder to receive the package.

For Communication Update Package Deployment, go to step 6.

For new Windows packages, check **Single .exe file (default)** or **Separate files (required for .MSI)**.

Note: Use **Single .exe file** unless you require separate files for a third-party deployment program.

6 Click **Next**.

7 Review the settings summary, click **Next**, and then click **Finish**.

8 Provide the exported package to the computer users.

For example, you can save the package to a secure shared network location, or email the package to the computer users. You can also use a third-party program to install the package.

9 Confirm that the user downloads and installs the client software, and confirm the installation status of the clients.

Client computers may not appear within the management console until after they restart. Depending on the client restart settings of the installed client, you or the computer users may need to restart the client computers.

See “About client installation methods” on page 80.

See “Preparing for client installation” on page 74.

Exporting client installation packages

You might want to export a client install package if you need those options that are not available when you use **Save Package** in the **Client Deployment Wizard**. For example, you may only need 32-bit installation packages for Windows.
Once you export the client install package, you deploy it. Remote Push in the Client Deployment Wizard can deploy the packages that you export. Alternately, you can install an exported package directly on to the client, or use a third-party program to deploy it.

**Note:** If you export client installation packages from a remote console, the packages are created on the computer from which you run the remote console. Furthermore, if you use multiple domains, you must export the packages for each domain, or the clients do not appear in the correct domain groups.

To export client installation packages

1. In the console, click Admin, and then click Install Packages.
2. Under Install Packages, click Client Install Package.
3. In the Client Install Package pane, under Package Name, right-click the package you want to export and then click Export.
4. Click Browse to navigate to and select the folder to contain the exported package, and then click OK.

**Note:** Export Package does not support directories with double-byte or high-ASCII characters, and blocks their selection.

5. Set the other options according to your installation goals. The options vary depending on the type of installation package you export.

   For details about the export options in this dialog box, click Help.

6. Click OK.

See “Managing client installation packages” on page 88.

See “Installing clients with Save Package” on page 84.

See “Installing clients with Remote Push” on page 82.

See “Preparing for client installation” on page 74.

### About the Windows client installation settings

The Client Deployment Wizard prompts you to specify the client installation settings for Windows clients. The client installation settings define the options of the installation process itself. You can define the target installation folder, whether to disable installation logging, and the post-installation restart settings, among other options.
You can choose the default client installation settings, or you can add a custom **Client Install Settings** under **Admin > Install Packages > Client Install Settings**. The contextual Help provides details about the settings that you can configure.

**Note:** You should use silent installations for remote deployment to minimize user disruption.

If you use unattended installations (*Show progress bar only*), Windows may display to users one or more pop-up windows. However, the installation should not fail even if the user does not notice them.

You should not use an interactive installation for remote deployment. This installation type fails unless the user interacts with it. Security features (such as Windows Session 0 isolation) on some operating systems may cause the interactive installation wizard to not appear. You should only use the interactive installation type for local installations. These recommendations apply to both 32- and 64-bit operating systems.

See “Installing clients with Remote Push” on page 82.

See “Preparing for client installation” on page 74.

---

**Uninstalling the Symantec Endpoint Protection client for Windows**

You uninstall the Windows client by using the appropriate Windows control panel, such as Add or Remove Programs.

See your Windows documentation for more information.

**To uninstall the Symantec Endpoint Protection client for Windows**

The text that you see depends on the operating system of the client computer.

1. On the client computer, on the **Start** menu, click **Control Panel > Add or Remove Programs** (or **Control Panel > Programs > Uninstall a program**).

2. In the **Add or Remove Programs** (or **Uninstall or change a program**) dialog box, click **Symantec Endpoint Protection**, and then click **Change, Remove** or **Uninstall**.

3. Follow the onscreen prompts to remove the client software.

See “About client installation methods” on page 80.

If the standard Windows uninstall method fails, you may have to uninstall the client manually. For more information, see the knowledge base article: Methods for uninstalling Symantec Endpoint Protection.
Managing client installation packages

To manage computers with Symantec Endpoint Protection Manager, you must export a managed client installation package, and then install the files in the package onto client computers. You can export packages to deploy the client with Symantec Endpoint Protection Manager, or you can deploy them with a third-party deployment tool.

You can export these packages as a single executable file or as a series of files in a directory. The method that you choose depends on your deployment method and whether you want to upgrade client software in groups. Typically, if you use Active Directory Group Policy Object, you do not choose to export to a single executable file.

Symantec occasionally provides updated packages of installation files, usually when a new product version releases. You can automatically update the client software on all managed Windows clients in a group with the AutoUpgrade feature. You do not need to redepoly software with installation deployment tools.

Table 5-5  Client installation package-related tasks

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure client installation packages</td>
<td>You can specify how the installation interacts with end users. See &quot;About the Windows client installation settings&quot; on page 86.</td>
</tr>
<tr>
<td>Export client installation packages</td>
<td>You can export packages to install with Symantec Endpoint Protection Manager or with third-party deployment tools. See &quot;Exporting client installation packages&quot; on page 85.</td>
</tr>
<tr>
<td>Add client installation package updates</td>
<td>You can add updated client installation packages to the database to make them available for distribution from Symantec Endpoint Protection Manager. You can optionally export the packages during this procedure to make the package available for deployment to computers that do not have the client software. See &quot;Adding client installation package updates&quot; on page 89.</td>
</tr>
</tbody>
</table>
Table 5-5  Client installation package-related tasks (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upgrade Windows clients in one or more groups</td>
<td>You can install the exported packages to computers one at a time, or deploy the exported files to multiple computers simultaneously.</td>
</tr>
<tr>
<td></td>
<td>When Symantec provides updates to client installation packages, you first add them to Symantec Endpoint Protection Manager and make them available for exporting. However, you do not have to reinstall them with client deployment tools. The easiest way to update Windows clients in groups with the latest software is to use AutoUpgrade. You should first update a group with a small number of test computers.</td>
</tr>
<tr>
<td></td>
<td>See “Upgrading Windows clients by using AutoUpgrade in Symantec Endpoint Protection” on page 98.</td>
</tr>
<tr>
<td></td>
<td>You can also update clients with LiveUpdate if you permit clients to run LiveUpdate and if the LiveUpdate Settings policy permits updates.</td>
</tr>
<tr>
<td>Delete client installation packages</td>
<td>You can delete older client installation packages to save disk space. However, AutoUpgrade sometimes uses the older Windows client installation packages to build upgrade packages. The upgrade packages result in smaller downloads by clients.</td>
</tr>
<tr>
<td></td>
<td>See “Preparing for client installation” on page 74.</td>
</tr>
</tbody>
</table>

Adding client installation package updates

You can add a client installation package update to Symantec Endpoint Protection Manager to export and install. You can optionally export the packages during this procedure for installation at a later time.

For example, you can add a newer client installation package to an existing Symantec Endpoint Protection Manager installation if you cannot immediately upgrade Symantec Endpoint Protection Manager.

Note: An installation package that you import consists of two files. One file is named product_name.dat, and the other file is named product_name.info. These files automatically import during the installation or upgrade of Symantec Endpoint Protection Manager.
To add client installation package updates

1. Copy the package to a directory on the computer that runs Symantec Endpoint Protection Manager.

2. In the console, click Admin, and then click Install Packages.

3. Under Tasks, click Add a Client Install Package.

4. In the Add a Client Install Package dialog box, type a name and a description for the package.

5. Click Browse.

6. In the Select Folder dialog box, locate and select the product_name.info file for the new package, and then click Select.

7. When the Completed successfully prompt appears, do one of the following tasks:
   - If you do not want to export the installation files and make them available for deployment, click Close.
     You are finished with this procedure.
   - If you do want to export the installation files and make them available for deployment, click Export this Package, and then complete this procedure.

8. In the Export Package dialog box, click Browse.

9. In the Select Export Folder dialog box, browse to and select the directory to contain the exported package, and then click OK.

10. In the Export Package dialog box, select a group, and then set the other options according to your installation goals.
    For details about setting other options in this dialog box, click Help.

11. Click OK.

See “Managing client installation packages” on page 88.

See “Preparing for client installation” on page 74.
Upgrading Symantec Endpoint Protection

This chapter includes the following topics:

- Upgrading to a new release
- Upgrading Symantec Endpoint Protection to include Symantec Network Access Control
- Upgrading a management server
- Upgrading an environment that uses multiple embedded databases and management servers
- Stopping and starting the management server service
- About upgrading client software
- Upgrading Windows clients by using AutoUpgrade in Symantec Endpoint Protection

Upgrading to a new release

You can upgrade to the newest release of the product to take advantage of new features. To install a new version of the software, you must perform certain tasks to ensure a successful upgrade. You should also check the known issues that appear in the release notes for any late-breaking information relating to upgrades.

Before you upgrade, review the following information:

- System requirements
For the most current system requirements, see: Release Notes and System Requirements for all versions of Symantec Endpoint Protection and Symantec Network Access Control

- New features in this version
- Feature changes between the previous version and the newest version of the client, where applicable
- Compatible Symantec Endpoint Protection Manager and Symantec Endpoint Protection client upgrade paths

This section is specific to upgrading the software in environments where a compatible version of the product is already installed.

**Note:** If you upgrade from 11.0, remove any packages that are assigned to the client groups. The Maintain existing client features when upgrading option on the 11.0 package causes the upgrade to remove all protection technologies from the clients.

For more information, see: Clients show "No Symantec protection technologies are installed" after migrating the SEPM from 11.x to 12.1

Table 6-1 displays the steps you need to perform to upgrade to the latest version of Symantec Network Access Control.

**Table 6-1** Process for upgrading Symantec Network Access Control

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Back up the database</td>
<td>Back up the database that Symantec Endpoint Protection Manager uses to ensure the integrity of your client information.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Turn off replication</td>
<td>If you upgrade from a Symantec Endpoint Protection 11.0 network, turn off replication on all sites that are configured as replication partners. Any attempts to replicate the database between Symantec Endpoint Protection versions during the upgrade corrupts the database. Symantec Endpoint Protection 12.1 and later does not allow replication if the product versions do not match.</td>
</tr>
<tr>
<td>Step</td>
<td>Action</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>---------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Step 3 | Enable local authentication              | Enforcers are not able to authenticate clients during an upgrade. To avoid problems with client authentication, Symantec recommends that you enable local authentication before you upgrade. After the upgrade is finished, you can return to your previous authentication setting.  
  See “Enabling local authentication on the Integrated Enforcer” on page 326.  
  See “Enabling local authentication on a Gateway Enforcer appliance” on page 251.  
  See “Enabling local authentication on the LAN Enforcer appliance” on page 299. |
| Step 4 | Stop the Symantec Endpoint Protection Manager service | You must stop the management server service before you install a newer version.  
  See “Stopping and starting the management server service” on page 96. |
| Step 5 | Upgrade the Symantec Endpoint Protection Manager software | Install the new version of Symantec Endpoint Protection Manager on all sites in your network. The existing version is detected automatically, and all settings are saved during the upgrade.  
  See “Upgrading a management server” on page 94. |
| Step 6 | Turn on replication after the upgrade       | Turn on replication when the installation is complete to restore your configuration. |
| Step 7 | Upgrade Symantec client software            | Prepare then upgrade your client software to the latest version.  
  See “About upgrading client software” on page 97.  
  See “Preparing for client installation” on page 74.  
  When Symantec provides updates to client installation packages, you add the updates to Symantec Endpoint Protection Manager and make them available for exporting. You do not, however, have to reinstall the client with client deployment tools. The easiest way to update Windows clients in groups with the latest software is to use AutoUpgrade. You should first update a group with a small number of test computers before you update your entire production network.  
  See “Upgrading Windows clients by using AutoUpgrade in Symantec Endpoint Protection” on page 98.  
  You can also update clients with LiveUpdate if you permit clients to run LiveUpdate and if the LiveUpdate Settings policy permits. |
Upgrading Symantec Endpoint Protection to include Symantec Network Access Control

If you already have installed Symantec Endpoint Protection Manager for Symantec Endpoint Protection, you can upgrade it to include Symantec Network Access Control. To upgrade to Symantec Network Access Control, you reinstall Symantec Endpoint Protection Manager to add the Symantec Network Access Control functionality.

To upgrade Symantec Endpoint Protection to include Symantec Network Access Control

1 Download the installation file or product disc for Symantec Network Access Control.
   If the installation program does not start immediately, locate and double-click setup.exe.

2 In the installation dialog box, click Install Symantec Network Access Control.

3 In the next installation dialog box, click Install Symantec Endpoint Protection Manager.

4 In the Welcome to the Management Server Upgrade Wizard dialog box, click Next.

5 After the wizard completes, in the Management Server and Console Installation Summary dialog box, click Next, and then click Finish.

6 After the upgrade, the Welcome to the Management Server Configuration Wizard dialog box appears. Provide the appropriate values, click Next, and then click Finish.

7 Deploy the Symantec Network Access Control client.
   See “About client installation methods” on page 80.

Upgrading a management server

You must upgrade all management servers before you upgrade any clients.

If you upgrade management servers in an environment that supports load balancing, failover, or replication, you must prepare and upgrade them in a specific order.

Warning: You must follow the scenario that applies to your type of installation, or your upgrade can fail.
The upgrade process is similar to a fresh installation.

See “Upgrading an environment that uses multiple embedded databases and management servers” on page 95.

Table 6-2 lists the tasks to upgrade Symantec Endpoint Protection Manager.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
</table>
| Upgrade the management server     | Upgrade the management server, and then configure it with the Management Server Configuration Wizard.  
Note: To upgrade the management server for Symantec Network Access Control, first apply the management server upgrade for Symantec Endpoint Protection, and then apply the management server upgrade for Symantec Network Access Control. The instructions are similar to installing the Symantec Network Access Control management server for the first time.  
See “Installing Symantec Endpoint Protection Manager” on page 51.  
See “Upgrading Symantec Endpoint Protection to include Symantec Network Access Control” on page 94. |
| Log onto the management server    | When the Symantec Endpoint Protection Manager logon panel appears, you can log on to the console by using your logon credentials.  
See “Logging on to the Symantec Endpoint Protection Manager console” on page 53. |

Note: You are not required to restart the computer after the upgrade, but you may notice performance improvements if you restart the computer and log on.

Upgrading an environment that uses multiple embedded databases and management servers

Upgrading an environment that uses multiple embedded database and management servers has the following implications:

- The management servers do not use failover or load balancing for Symantec Endpoint Protection because the embedded database does not support failover or load balanced servers.
- The management servers are Symantec Endpoint Protection replication partners.
All sites have a computer on which you first installed the management server. You must upgrade this management server first, because it contains critical site information such as the encryption key or encryption password. You then upgrade the other management servers that you installed for replication.

To upgrade an environment that uses multiple embedded databases and management servers

1. On all management servers, disable replication.
   
   This step is required for upgrades from Symantec Endpoint Protection Manager 11.0, because attempts to replicate during the upgrade process corrupt the database due to a product version mismatch. Symantec Endpoint Protection Manager 12.1 and later does not allow replication if the product versions do not match.

2. Authenticate to and log on to the computer on which you installed the first Symantec Endpoint Protection Manager.
   
   Do not log on to Symantec Endpoint Protection Manager.

3. Upgrade the management server.
   
   See “Upgrading a management server” on page 94.

4. Upgrade all additional management servers one by one.

5. After you upgrade the servers, enable replication on each server.

---

**Stopping and starting the management server service**

Before you upgrade from Symantec Endpoint Protection 11.0, you must manually stop the Symantec Endpoint Protection Manager service on every management server in your site. After you upgrade, the service starts automatically.

---

**Warning:** If you do not stop the Symantec Endpoint Protection Manager service before you upgrade the server, you risk corrupting your existing Symantec Endpoint Protection database.

---

**Note:** If you stop the management server service, clients can no longer connect to it. If clients are required to communicate with the management server to connect to the network, they are denied access until the management server service is restarted.

For example, a client must communicate with the management server to pass a Host Integrity check.
See “Upgrading to a new release” on page 91.

To stop the Symantec Endpoint Protection Manager service

2. In the Services window, under Name, scroll to and right-click Symantec Endpoint Protection Manager.
3. Click Stop.
4. Close the Services window.

**Warning:** Close the Services window or your upgrade can fail.

5. Repeat this procedure for all installations of Symantec Endpoint Protection Manager.

**Note:** To start the Symantec Endpoint Protection Manager service, follow the above procedure and click Start instead of Stop.

To stop the Symantec Endpoint Protection Manager service using the command line

- From a command prompt, type:

  ```
  net stop semsrv
  ```

To start the Symantec Endpoint Protection Manager service using the command line

- From a command prompt, type:

  ```
  net start semsrv
  ```

**About upgrading client software**

You can use several methods to upgrade Symantec client software. Some methods can take up to 30 minutes. Therefore, you may want to upgrade client software when most users are not logged on to their computers.
### Methods to upgrade the client software

<table>
<thead>
<tr>
<th>Upgrade method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AutoUpgrade</td>
<td>Use AutoUpgrade to update Windows clients in one or more groups from the Symantec Endpoint Protection Manager console. See “Upgrading Windows clients by using AutoUpgrade in Symantec Endpoint Protection” on page 98.</td>
</tr>
<tr>
<td>LiveUpdate</td>
<td>Configure a LiveUpdate Settings policy for a group that defines a LiveUpdate server and allows clients to run LiveUpdate to obtain product updates.</td>
</tr>
<tr>
<td>Installation file</td>
<td>Use the installation file you download from FileConnect to install a new version of the client.</td>
</tr>
<tr>
<td>Other methods</td>
<td>Use one of the other supported methods of installing client software. See “About client installation methods” on page 80.</td>
</tr>
</tbody>
</table>

If the Symantec Endpoint Protection client is also installed, you should upgrade both the Symantec Endpoint Protection client and the Symantec Network Access Control client. See “Upgrading to a new release” on page 91.

### Upgrading Windows clients by using AutoUpgrade in Symantec Endpoint Protection

The AutoUpgrade process lets you automatically upgrade the Symantec Endpoint Protection client software for all the Windows clients that are contained in a group. For example, you can use AutoUpgrade to upgrade clients to a new release update or product version.

Use the following best practices for using AutoUpgrade:

- You must test the AutoUpgrade process before you attempt to upgrade a large number of clients in your production network. If you do not have a test network, you can create a test group within your production network. For this kind of test, you add a few non-critical clients to the test group and then upgrade them by using AutoUpgrade.

- If you upgrade from 11.0 and use Application and Device Control, you must disable the Application Control rule Protect client files and registry keys. After the clients receive the new policy, you may upgrade using AutoUpgrade.
To reduce bandwidth during peak hours, in the Upgrade Clients with Package wizard, schedule AutoUpgrade for after hours. For wide area networks, you should also set up the remote clients to receive the upgrade package from a remote web server.

You confirm that the upgrade completed successfully by verifying the version number of the client software. The version number is displayed in the client's Help > About panel. The updated client version number is also displayed in Symantec Endpoint Protection Manager on the Clients page after a successful check-in. You click the group, then the Clients tab, and change the view to Client Status.

If both the Symantec Endpoint Protection client and the Symantec Network Access Control client are installed, you can assign both the Symantec Endpoint Protection package and the Symantec Network Access Control package to the same group. In this case, make sure that the Maintain Features option is selected.

See “About upgrading client software” on page 97.

To upgrade Windows clients by using AutoUpgrade in Symantec Endpoint Protection

1. In the Symantec Endpoint Protection Manager console, click Admin.
2. Click Install Packages.
3. Under Tasks, click Upgrade Clients with Package.
4. In the Upgrade Clients Wizard panel, click Next.
5. In the Select Client Install Package panel, select the appropriate client installation package, and then click Next.
6. In the Specify Groups panel, select the groups that contain the client computers that you want to upgrade, and then click Next.
7. In the Package Upgrade Settings panel, select Download from the management server.

To reduce bandwidth, stage and select a package on a web server that is local to the computers you upgrade.

8. Click Upgrade Settings.

You can optionally add or remove features when upgrading.

10. Optionally, on the Notification tab, customize the user notification settings. You can customize the message that is displayed on the client computer during the upgrade. You can also allow the user to postpone the upgrade by an amount of time you specify.

For more information about schedule and notification settings, click Help.

11. Click OK.
12 In the Upgrade Clients Wizard Complete panel, click Next.

13 Click Finish.
Section 2

Managing groups, clients, and administrators in Symantec Endpoint Protection Manager

- Chapter 7. Managing groups of client computers
- Chapter 8. Managing clients
- Chapter 9. Managing administrator accounts and passwords
Managing groups of client computers

This chapter includes the following topics:

■ Managing groups of clients
■ How you can structure groups
■ Adding a group
■ Disabling and enabling a group's inheritance
■ Moving a client computer to another group

Managing groups of clients

In Symantec Endpoint Protection Manager, groups function as containers for the endpoints that run the client software. These endpoints can be either computers, or users. You organize the clients that have similar security needs into groups to make it easier to manage network security.

Symantec Endpoint Protection Manager contains the following default groups:

■ The My Company group is the top-level, or parent, group. It contains a flat tree of child groups.

■ The Default Group is a subgroup of My Company. Clients are first assigned to the Default Group when they first register with Symantec Endpoint Protection Manager, unless they belong to a predefined group. You cannot create subgroups under the Default Group.

Note: You cannot rename or delete the default groups.
### Table 7-1: Group management actions

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
</table>
| Add groups                                    | See “How you can structure groups” on page 104.  
|                                               | See “Adding a group” on page 105.                                                                                                                                                                           |
| Import existing groups                        | If your organization already has an existing group structure, you can import the groups as organizational units.  
|                                               | **Note:** You cannot manage imported organizational units in the same ways that you can manage the groups that you create in Symantec Endpoint Protection Manager.                                           |
| Disable inheritance for subgroups             | The subgroups inherit the same security settings from the parent group by default. You can disable inheritance.  
|                                               | See “Disabling and enabling a group's inheritance” on page 105.                                                                                                                                             |
| Create locations within groups                 | You can set up the clients to switch automatically to a different security policy if the physical location of the client changes.  
|                                               | Some security settings are group-specific and some settings are location-specific. You can customize any settings that are location-specific.                                                                    |
| Assign clients to groups before you install the client software | You must apply the policy to the group for the policy to take effect.                                                                                                                                              |
| Manage security policies for groups            | You can create security policies based on the needs of each group. You can then assign different policies to different groups or locations.  
|                                               | See “Adding a policy” on page 155.  
|                                               | See “Assigning a policy to a group” on page 158.  
|                                               | See “Performing the tasks that are common to all policies” on page 151.                                                                                                                                     |
| Perform group maintenance                      | You can move groups for easier management and move clients between groups. You can also block clients from being added to a particular group.  
|                                               | See “Moving a client computer to another group” on page 106.                                                                                                                                                  |
How you can structure groups

You can create multiple groups and subgroups to match the organizational structure and security of your company. You can base your group structure on function, role, geography, or a combination of criteria.

Table 7-2 Criteria for creating groups

<table>
<thead>
<tr>
<th>Criterion</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Function</td>
<td>You can create groups based on the types of computers to be managed, such as laptops, desktops, and servers. Alternatively, you can create multiple groups that are based on usage type. For example, you can create a remote group for the client computers that travel and a local group for the client computers that remain in the office.</td>
</tr>
<tr>
<td>Role</td>
<td>You can create groups for department roles, such sales, engineering, finance, and marketing.</td>
</tr>
<tr>
<td>Geography</td>
<td>You can create groups based on the offices, cities, states, regions, or countries where the computers are located.</td>
</tr>
</tbody>
</table>
| Combination | You can create groups based on a combination of criteria. For example, you can use the function and the role. You can add a parent group by role and add child subgroups by function, as in the following scenario:  
  ▪ Sales, with subgroups of laptops, desktops, and servers.  
  ▪ Engineering, with subgroups of laptops, desktops, and servers. |

After you organize the client computers into groups, you can apply the appropriate amount of security to that group.

For example, suppose that a company has telemarketing and accounting departments. These departments have staff in the company's New York, London, and Frankfurt offices. All computers in both departments are assigned to the same group so that they receive virus and security risk definitions updates from the same source. However, IT reports indicate that the telemarketing department is more vulnerable to risks than the accounting department. As a result, the system administrator creates separate telemarketing and accounting groups. Telemarketing clients share configuration settings that strictly limit how users can interact with their virus and security risk protection.

If you have both Symantec Endpoint Protection clients and Symantec Network Access Control clients installed, keep the Symantec Endpoint Protection clients and Symantec Network Access Control clients in separate groups.

See the knowledge base article Best Practices for Creating Group Structure.
Adding a group

You can add groups after you define the group structure for your organization.

Group descriptions may be up to 1024 characters long. Group names may contain any character except the following characters: [" / * ? < > | :] Group descriptions are not restricted.

Note: You cannot add groups to the Default Group.

To add a group

1. In the console, click Clients.
2. Under Clients, select the group to which you want to add a new subgroup.
3. On the Clients tab, under Tasks, click Add Group.
4. In the Add Group for group name dialog box, type the group name and a description.
5. Click OK.

Disabling and enabling a group's inheritance

In the group structure, subgroups initially and automatically inherit the locations, policies, and settings from their parent group. By default, inheritance is enabled for every group. You can disable inheritance so that you can configure separate security settings for a subgroup. If you make changes and later enable inheritance, any changes that you made in the subgroup's settings are overwritten.

To disable or enable a group's inheritance

1. In the console, click Clients.
2. On the Clients page, under Clients, select the group for which you want to disable or enable inheritance.
   
   You can select any group except the top-level group, My Company.
3. In the group name pane, on the Policies tab, do one of the following tasks:
To disable inheritance, uncheck Inherit policies and settings from parent group "group name".

To enable inheritance, check Inherit policies and settings from parent group "group name", and then click Yes when asked to proceed.

Moving a client computer to another group

If your client computers are not in the correct group, you can move them to another group.

To move client from multiple groups into a single group, you can redeploy the client installation package.

To move a client computer to another group

1 In the console, click Clients.
2 On the Clients page, select a group.
3 On the Clients tab, in the selected group, select the computer, and then right-click Move.
   Use the Shift key or the Control key to select multiple computers.
4 In the Move Clients dialog box, select the new group.
5 Click OK.

See "Managing groups of clients" on page 102.
Managing clients

This chapter includes the following topics:

- Managing client computers
- How to determine whether the client is connected in the console
- Searching for information about client computers
- Password-protecting the client

Managing client computers

Table 8-1 lists the tasks you should perform with the computers after you install the client software.

Table 8-1 Tasks to manage client computers

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
</table>
| Check that the client software is installed on your computers | ■ You can display the computers in each group that do not have the client software installed yet.  
■ You can add a client to a group and install the client software later.  
See “About client installation methods” on page 80. |
| Check whether the client is connected to the management server | You can check the client status icons in the management console and in the client. The status icon shows whether the client and the server communicate.  
See “How to determine whether the client is connected in the console” on page 108. |
| Configure the connection between the client and the server | After you install the client software client computers automatically connect to the management server at the next heartbeat. You can change how the server communicates with the client computer.  
You can troubleshoot any connection issues. |
Table 8-1  Tasks to manage client computers (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
</table>
| Check that client computers have the right level of protection      | - You can view the status of each protection technology on your client computers. See "How to determine whether the client is connected in the console" on page 108.  
- You can run reports or view logs to see whether you need to increase protection or improve performance. For example, the scans may cause false positives. You can also identify the client computers that need protection.  
- You can modify protection based on specific attributes of the client software or the client computers. See “Searching for information about client computers” on page 110. |
| Move endpoints from one group to another to modify protection (optional) | To change a client computer's level of protection, you can move it to a group that provides more protection or less protection.  
See “Moving a client computer to another group” on page 106.  
When you deploy a client installation package, you specify which group the client goes in. You can move the client to a different group. But if the client gets deleted or disconnected and then gets added again and reconnected, the client returns to the original group. To keep the client with the group it was last moved to, configure the reconnection preferences. You configure these settings in the Communications Settings dialog box on the Clients > Policies tab. |
| Remove the Symantec Endpoint Protection client software from decommissioned computers (optional) | If you decommissioned a client computer and you want to use the license for a different computer, you can uninstall the Symantec Endpoint Protection client software. For the managed clients that do not connect, Symantec Endpoint Protection Manager deletes clients from the database after 30 days by default.  
You can change the period of time after which Symantec Endpoint Protection Manager deletes the client from the database. By deleting a client, you also save space in the database.  
See “Uninstalling the Symantec Endpoint Protection client for Windows” on page 87.  
See “Purging obsolete clients from the database to make more licenses available” on page 72. |

How to determine whether the client is connected in the console

In Symantec Endpoint Protection Manager, you can use the client status icons to check whether the client and the server communicate.
<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
</table>
| ![Icon 1](image1.png) | This icon indicates the following status:  
- The client software installation failed. |
| ![Icon 2](image2.png) | This icon indicates the following status:  
- The client can communicate with Symantec Endpoint Protection Manager.  
- The client is in computer mode. |
| ![Icon 3](image3.png) | This icon indicates the following status:  
- The client cannot communicate with Symantec Endpoint Protection Manager.  
- The client is in computer mode.  
- The client may have been added from the console, and may not have any Symantec client software installed. |
| ![Icon 4](image4.png) | This icon indicates the following status:  
- The client can communicate with Symantec Endpoint Protection Manager.  
- The client is in computer mode.  
- The client is an unmanaged detector. |
| ![Icon 5](image5.png) | This icon indicates the following status:  
- The client cannot communicate with Symantec Endpoint Protection Manager.  
- The client is in computer mode.  
- The client is an unmanaged detector. |
| ![Icon 6](image6.png) | This icon indicates the following status:  
- The client can communicate with Symantec Endpoint Protection Manager.  
- The client is in user mode. |
| ![Icon 7](image7.png) | This icon indicates the following status:  
- The client cannot communicate with Symantec Endpoint Protection Manager.  
- The client is in user mode.  
- The client may have been added from the console, and may not have any Symantec client software installed. |
Table 8-2  
Client status icons in the management console (continued)

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
</table>
| ![Icon] | This icon indicates the following status:  
- The client can communicate with Symantec Endpoint Protection Manager at another site.  
- The client is in computer mode. |
| ![Icon] | This icon indicates the following status:  
- The client can communicate with Symantec Endpoint Protection Manager at another site.  
- The client is in computer mode.  
- The client is an unmanaged detector. |
| ![Icon] | This icon indicates the following status:  
- The client can communicate with Symantec Endpoint Protection Manager at another site.  
- The client is in user mode. |

You can also look on the client to see whether or not it is connected to the management server.

**Searching for information about client computers**

You can search for information about the clients, client computers, and users to make informed decisions about the security of your network. For example, you can find which computers in the Sales group run the latest operating system. Or, you can find out which client computers in the Finance group need the latest virus definitions installed. You can view the information about each client in the group on the Clients page. You can narrow down the search if there are too many clients.

You can export the data that is contained in the query into a text file.

**Note:** To search for most of the information about the users, you must collect user information during the client software installation or later. This user information is also displayed on the General tab and the User Info tab in the client's Edit Properties dialog box.

**To search for information about client computers**

1. In the console, click **Clients**.
2. On the **Clients** tab, under **View Clients**, choose the group you want to search.
3 Under Tasks, click Search clients.

4 In the Search clients dialog box, in the Find drop-down list, click either Computers or Users.

5 Click Browse to select a group other than the default group.

6 In the Select Group dialog box, select the group, and then click OK.

7 Under Search Criteria, click in the Search Field to see the drop-down list, and then select the criteria by which you want to search.

8 Click the Comparison Operator drop-down list, and then select a comparison operator.

You can use standard Boolean operators in your search criteria.

9 In the Value cell, type the search string.

10 Click Search.

You can export the results into a text file.

11 Click Close.

**Password-protecting the client**

You can increase corporate security by requiring password protection on the client computer whenever users perform certain tasks.

You can require the users to type a password when users try to do one of the following actions:

- Open the client's user interface.
- Stop the client.
  The Network Access Control client can pass Enforcer authentication initially, while the client is running, and receive a normal network configuration and IP address. If the client later fails authentication, the Enforcer sends a message to the client. This failure causes the client to release and renew the IP address. However, if the end user stops the client on the client computer, the Enforcer is unable to enforce the release and renew. To ensure that the Enforcer can continue to quarantine or to block clients, you may want to restrict which users are allowed to stop a client. You can restrict users by requiring a password for the end user to stop the client.
- Uninstall the client.
- Import and export the security policy.

You can modify the password protection settings for any child group that does not inherit its settings from a parent.
To password-protect the client

1. In the console, click **Clients**.
2. Under **Clients**, select the group for which you want to set up password protection.
3. On the **Policies** tab, under **Location-independent Policies and Settings**, click **Password Settings**.
4. On the **Password Settings** tab, check any or all of the check boxes.
5. In the **Password** and **Confirm password** text boxes, type the same password. The password is limited to 15 characters or less.
6. Click **OK**.
Managing administrator accounts and passwords

This chapter includes the following topics:

- Managing administrator accounts
- About administrator account roles and access rights
- Adding an administrator account
- Configuring the access rights for a limited administrator
- Changing the authentication method for administrator accounts
- Best practices for testing whether a directory server authenticates an administrator account
- Changing the password for an administrator account
- Allowing administrators to reset forgotten passwords
- Sending a temporary password to an administrator
- Displaying the Remember my user name and Remember my password check boxes on the logon screen

Managing administrator accounts

You can use administrator accounts to manage Symantec Endpoint Protection Manager datacenters. Administrators log on to Symantec Endpoint Protection Manager to change policy settings, manage groups, run reports, and install client software, as well as other management tasks.
The default account is a system administrator account, which provides access to all features. You can also add a more limited administrator account, for administrators who need to perform a subset of tasks.

For a small company, you may only need one administrator and one domain. For a large company with multiple sites and Windows domains, you most likely need multiple administrators, some of whom have more access rights than others. You may also need to add multiple domains within Symantec Endpoint Protection Manager.

You manage domains and administrator accounts and their passwords on the Admin page.

Table 9-1  Account administration

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decide whether to add</td>
<td>Decide whether to add domains.</td>
</tr>
<tr>
<td>multiple domains</td>
<td></td>
</tr>
<tr>
<td>Add administrator</td>
<td>Add accounts for administrators who need access to the Symantec Endpoint Protection Manager console.</td>
</tr>
<tr>
<td>accounts</td>
<td>- Learn about the administrator account roles that are available.</td>
</tr>
<tr>
<td></td>
<td>See “About administrator account roles and access rights” on page 115.</td>
</tr>
<tr>
<td></td>
<td>Create the types of administrator accounts that you need.</td>
</tr>
<tr>
<td></td>
<td>See “Adding an administrator account” on page 117.</td>
</tr>
<tr>
<td></td>
<td>See “Configuring the access rights for a limited administrator” on page 118.</td>
</tr>
<tr>
<td></td>
<td>Change the method that is used to authenticate administrator accounts (optional).</td>
</tr>
<tr>
<td></td>
<td>By default, the Symantec Endpoint Protection Manager database authenticates the administrator's credentials. You can also use RSA SecurID or an LDAP server or a Microsoft Active Directory Server for authentication.</td>
</tr>
<tr>
<td></td>
<td>See “Changing the authentication method for administrator accounts” on page 119.</td>
</tr>
<tr>
<td>Unlock or lock an</td>
<td>By default, Symantec Endpoint Protection Manager locks out an administrator after a user tries to log on to Symantec Endpoint Protection Manager using the administrator account too many times. You can configure these settings to increase the number of tries or time the administrator is locked out.</td>
</tr>
<tr>
<td>administrator account</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The lockout interval doubles with each subsequent lockout. Symantec Endpoint Protection Manager restores the original lockout interval after a successful logon, or 24 hours after the first failed logon attempt.</td>
</tr>
<tr>
<td></td>
<td>See “Unlocking an administrator's account after too many logon attempts” on page 59.</td>
</tr>
<tr>
<td></td>
<td>Note: If an administrator is locked out of their account, they must wait the specified time before logging on again. You cannot unlock an account during the lockout interval.</td>
</tr>
</tbody>
</table>
Table 9-1 Account administration (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reset passwords</td>
<td>You can perform the following tasks for passwords:</td>
</tr>
<tr>
<td></td>
<td>■ Change the password for an administrator account.</td>
</tr>
<tr>
<td></td>
<td>See “Changing the password for an administrator account” on page 124.</td>
</tr>
<tr>
<td></td>
<td>■ Make sure that the Forget your password? link appears so that administrators can reset their own forgotten passwords.</td>
</tr>
<tr>
<td></td>
<td>See “Allowing administrators to reset forgotten passwords” on page 125.</td>
</tr>
<tr>
<td></td>
<td>■ Send an administrator a temporary password so that they can reset their password.</td>
</tr>
<tr>
<td></td>
<td>Note: A password change does not unlock a locked account.</td>
</tr>
<tr>
<td></td>
<td>■ Display the Remember my user name and Remember my password check boxes on the management server logon screen.</td>
</tr>
<tr>
<td></td>
<td>See “Displaying the Remember my user name and Remember my password check boxes on the logon screen” on page 127.</td>
</tr>
<tr>
<td>Configure log on options for Symantec Endpoint Protection Manager</td>
<td>You can configure the following logon options for each type of administrator:</td>
</tr>
<tr>
<td></td>
<td>■ Display a message for administrators to read before they log on.</td>
</tr>
<tr>
<td></td>
<td>See “Displaying a message for administrators to see before logging on to the Symantec Endpoint Protection Manager console” on page 57.</td>
</tr>
<tr>
<td></td>
<td>■ Allow or block log on access to the management console, so that certain administrators can, or cannot, log on remotely.</td>
</tr>
<tr>
<td></td>
<td>See “Granting or blocking access to remote Symantec Endpoint Protection Manager consoles” on page 57.</td>
</tr>
<tr>
<td></td>
<td>■ By default, if an administrator tries to log on to Symantec Endpoint Protection Manager too many times, the administrator is locked out for 15 minutes. You can configure these settings for each administrator.</td>
</tr>
<tr>
<td></td>
<td>See “Unlocking an administrator's account after too many logon attempts” on page 59.</td>
</tr>
</tbody>
</table>

See “Logging on to the Symantec Endpoint Protection Manager console” on page 53.

About administrator account roles and access rights

When you install the Symantec Endpoint Protection Manager, a default system administrator account is created, called admin. The system administrator account gives an administrator access to all the features in Symantec Endpoint Protection Manager.

To help you manage security, you can add additional system administrator accounts, domain administrator accounts, and limited administrator accounts. Domain administrators and limited administrators have access to a subset of Symantec Endpoint Protection Manager features.
You choose which accounts you need based on the types of roles and access rights you need in your company. For example, a large company may use the following types of roles:

- An administrator who installs the management server and the client installation packages. After the product is installed, an administrator in charge of operations takes over. These administrators are most likely system administrators.

- An operations administrator maintains the servers, databases, and installs patches. If you have a single domain, the operations administrator could be a domain administrator who is fully authorized to manage sites.

- An antivirus administrator, who creates and maintains the Virus and Spyware Protection policies and LiveUpdate policies on the clients. This administrator is most likely to be a limited administrator.

- A desktop administrator, who is in charge of security and creates and maintains the Firewall policies and Intrusion Prevention policies for the clients. This administrator is most likely to be a domain administrator.

- A help desk administrator, who creates reports and has read-only access to the policies. The antivirus administrator and desktop administrator read the reports that the help desk administrator sends. The help desk administrator is most likely to be a limited administrator who is granted reporting rights and policy rights.

Table 9-2 describes the account type and the access rights that each role has.

<table>
<thead>
<tr>
<th>Administrator role</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>System administrator</td>
<td>System administrators can log on to the Symantec Endpoint Protection Manager console with complete, unrestricted access to all features and tasks. A system administrator can create and manage other system administrator accounts, domain administrator accounts, and limited administrator accounts. A system administrator can perform the following tasks: Manage all domains. Administer licenses. View and manage all console settings. Manage the databases and management servers. Manage Enforcers.</td>
</tr>
<tr>
<td>Administrator role</td>
<td>Responsibilities</td>
</tr>
<tr>
<td>--------------------</td>
<td>------------------</td>
</tr>
</tbody>
</table>
| **Administrator**  | Administrators are domain administrators who can view and manage a single domain. A domain administrator has the same privileges as a system administrator, but for a single domain only. By default, the domain administrator has full system administrator rights to manage a domain, but not a site. You must explicitly grant site rights within a single domain. Domain administrators can modify the site rights of other administrators and limited administrators, though they cannot modify the site rights for themselves. A domain administrator can perform the following tasks:  
  ■ Create and manage administrator accounts and limited administrator accounts within a single domain.  
  Domain administrators cannot modify their own site rights. System administrators must perform this function.  
  ■ Run reports, manage sites, and reset passwords. You must explicitly configure reporting rights to groups that are migrated from Symantec AntiVirus 10.x.  
  ■ Cannot administer licenses. Only system administrators can administer licenses.  
  ■ Cannot manage Enforcers. |
| **Limited administrator** | Limited administrators can log on to the Symantec Endpoint Protection Manager console with restricted access. Limited administrators do not have access rights by default. A system administrator role must explicitly grant access rights to allow a limited administrator to perform tasks. Parts of the management server user interface are not available to limited administrators when you restrict access rights. For example:  
  ■ Limited administrators without reporting rights cannot view the Home, Monitors, or Reports pages.  
  ■ Limited administrators without policy rights cannot view or modify the policy. In addition, they cannot apply, replace, or withdraw a policy. See “Configuring the access rights for a limited administrator” on page 118. |

See “Managing administrator accounts” on page 113.

See “Adding an administrator account” on page 117.

**Adding an administrator account**

As a system administrator, you can add another system administrator, administrator, or limited administrator. As an administrator within a domain, you can add other administrators with access rights equal to or less restrictive than your own. Administrators can add limited administrators and configure their access rights.
To add an administrator account

1. In the console, click Admin.
2. On the Admin page, click Administrators.
3. Under Tasks, click Add an administrator.
4. In the Add Administrator dialog box, on the General tab, enter the username and email address.
5. On the Access Rights and Authentication tabs, specify the administrator role, access rights, and authentication method.
   - See “About administrator account roles and access rights” on page 115.
   - See “Changing the authentication method for administrator accounts” on page 119.
   - Click Help for more information.
6. Click OK.

See “Managing administrator accounts” on page 113.

Configuring the access rights for a limited administrator

If you add an account for a limited administrator, you must also specify the administrator's access rights. Limited administrator accounts that are not granted any access rights are created in a disabled state and the limited administrator will not be able to log on to the management server.

To configure the access rights for a limited administrator

1. In the console, click Admin.
2. On the Admin page, click Administrators.
3. Select the limited administrator.
   - You can also configure the access rights when you create a limited administrator account.
   - See “Adding an administrator account” on page 117.
4. Under Tasks, click Edit Administrator.
5. On the Access Rights tab, check an option, and then click the corresponding button to set the access rights. Click Help for more information.
If you want to authorize the limited administrator to create only non-shared policies for a location, check Only allow location-specific policy editing.

Click OK.

See “About administrator account roles and access rights” on page 115.
See “Managing administrator accounts” on page 113.

Changing the authentication method for administrator accounts

After you add an administrator account, the user name and password are stored in the Symantec Endpoint Protection Manager database. When the administrator logs on to the management server, the management server verifies with the database that the user name and password are correct. However, if your company uses a third-party server to authenticate existing user names and passwords, you can configure Symantec Endpoint Protection Manager to authenticate with the server.

Table 9-3 displays the authentication methods the management server can use to authenticate administrator accounts.

<table>
<thead>
<tr>
<th>Table 9-3 Authentication methods</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symantec Endpoint Protection Manager authentication (default)</td>
</tr>
<tr>
<td>RSA SecurID authentication</td>
</tr>
<tr>
<td>Directory server authentication</td>
</tr>
</tbody>
</table>

For the third-party authentication methods, Symantec Endpoint Protection Manager has an entry in the database for the administrator account, but the third-party server validates the user name and password.

To change the authentication method for administrator accounts

1 Add an administrator account.
   See “Adding an administrator account” on page 117.

2 On the Authentication tab, select the authentication method.
To authenticate administrators who use an RSA SecurID mechanism, first install the RSA ACE server and enable encrypted authentication for RSA SecurID.

To authenticate administrators using an Active Directory or LDAP directory server, you need to set up an account on the directory server. You must also establish a connection between the directory server and Symantec Endpoint Protection Manager. If you do not establish a connection, you cannot import users from an Active Directory server or synchronize with it.

**Note:** Synchronization is only possible for Active Directory Servers. Synchronization with LDAP servers is not supported.

You can check whether the directory server authenticates the account name by clicking **Test Account**.

See “Best practices for testing whether a directory server authenticates an administrator account” on page 120.

3 Click **OK**.

4 In the **Confirm Change** dialog box, type the password that you use to log on to Symantec Endpoint Protection Manager, and then click **OK**.

When you switch between authentication methods, you must type the administrator account's password.

---

### Best practices for testing whether a directory server authenticates an administrator account

You can test whether an Active Directory or LDAP server authenticates the user name and password for an administrator account that you create. The test also ensures that you added the user name and password correctly.

You use the same user name and password for an administrator account in Symantec Endpoint Protection Manager as you do in the directory server. When the administrator logs on to the management server, the directory server authenticates the administrator's user name and password. The management server uses the directory server configuration that you added to search for the account on the directory server.

The **Test Account** option checks whether or not the account name exists on the directory server.

You can also test whether an Active Directory or LDAP server authenticates an administrator account with no user name and password. An account with no user...
name or password is anonymous access. You should create an administrator account with anonymous access so that the administrators are never locked out if the password changes on the directory server.

**Note:** In Windows 2003 Active Directory server, anonymous authentication is disabled by default. Therefore, when you add a directory server without a user name to an administrator account and click *Test Account*, an **Account Authentication Failed** error message appears. To work around this issue, create two directory server entries, one for testing, and one for anonymous access. The administrator can still log on to the management server using a valid user name and password.

Table 9-4  Steps to test directory server authentication for an administrator account

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 1 | Add multiple directory server connections | To make testing easier for anonymous access, add at least two directory server entries. Use one entry to test the authentication, and the second entry to test anonymous access. These entries all use the same directory server with different configurations.  
By default, most users reside in **CN=Users** unless moved to different organizational unit. Users in the LDAP directory server are created under **CN=Users, DC=<sampledomain>, DC=local**. To find out where a user resides in LDAP, use ADSIEdit.  
Use the following information to set up the directory servers for this example:  
- **CN=John Smith**  
- **OU=test**  
- **DC=<sampledomain>**  
- **DC=local**  
The example uses the default Active Directory LDAP (389) but can also use Secure LDAP (636). |
| Step 2 | Add multiple administrator accounts | You add multiple system administrator accounts. The account for anonymous access does not have a user name or password.  
See “To add the administrator accounts using the directory server entries” on page 123. |
To add the directory server connections to test Active Directory and LDAP server authentication

1. On the console, click **Admin > Servers**, select the default server, and click **Edit the server properties**.
2. On the **Directory Servers** tab, click **Add**.
3. On the **General** tab, add the following directory server configurations, and then click **OK**.

   **Directory server 1:**
   - **Name:** `<sampledomain>` Active Directory
   - **Server Type:** Active Directory
   - **Server IP Address or Name:** `server01.<sampledomain>.local`
   - **User Name:** `<sampledomain>\administrator`
   - **Password:** `<directory server password>`

   **Directory server 2:**
   - **Name:** `<sampledomain>` LDAP with User Name
   - **Server Type:** LDAP
   - **Server IP Address or Name:** `server01.<sampledomain>.local`
   - **LDAP Port:** 389
   - **LDAP BaseDN:** `DC=<sampledomain>, DC=localhost`
   - **User Name:** `<sampledomain>\administrator`
   - **Password:** `<directory server password>`

   **Directory server 3 (for anonymous authentication):**
   - **Name:** `<sampledomain>` LDAP without User Name
   - **Server Type:** LDAP
   - **Server IP Address or Name:** `server01.<sampledomain>.local`
   - **LDAP Port:** 389
   - **LDAP BaseDN:** `<empty>`
     Leave this field empty when you use anonymous access.
   - **User Name:** `<empty>`
   - **Password:** `<empty>`

   After you click **OK**, a warning appears. But the directory server is valid.
When you try to add a BaseDN without a user name and password, the warning appears.

To add the administrator accounts using the directory server entries

1. On the console, click **Admin > Administrators**, and on the **General** tab, add the administrator accounts in step 2.

   See “Adding an administrator account” on page 117.

   See “Changing the authentication method for administrator accounts” on page 119.

   After you add each administrator account and click the **Test Account** option, you see a message. In some cases, the message appears to invalidate the account information. The administrator can still log on to Symantec Endpoint Protection Manager, however.

2. **Administrator account 1:**

   - On the **General** tab, enter the following information:
     - **User Name:** john
     - **Full Name:** John Smith
     - **Email Address:** john@<sampledomain>.local
   
   - On the **Access Rights** tab, click **System Administrator**.
   
   - On the **Authentication** tab, click **Directory Authentication**.
     - In the **Directory Server** drop-down list, select `<sampledomain> Active Directory`.
     - In the **Account Name** field, type john.
     - Click **Test Account**.
     
     The system administrator john can log on to Symantec Endpoint Protection Manager with directory authentication.

   **Administrator account 2:**

   - On the **General** tab, enter the following information:
     - **User Name:** john
     - **Full Name:** John Smith
     - **Email Address:** john@<sampledomain>.local
   
   - On the **Access Rights** tab, click **System Administrator**.
   
   - On the **Authentication** tab, click **Directory Authentication**.
     - In the **Directory Server** drop-down list, select `<sampledomain> LDAP with User Name`. 
In the **Account Name** field, type `john`.

Click **Test Account**.

The system administrator `john` cannot log on into Symantec Endpoint Protection Manager with directory authentication.

**Administrator account 3:**

- On the **General** tab, enter the following information:
  - **User Name:** `john`
  - **Full Name:** John Smith
  - **Email Address:** `john@<sampledomain>.local`
- On the **Access Rights** tab, click **System Administrator**.
- On the **Authentication** tab, click **Directory Authentication**.
  - In the **Directory Server** drop-down list, select `<sampledomain> LDAP with User Name`.
  - In the **Account Name** field, type `John Smith`.
  - Click **Test Account**.

The system administrator `john` can log on into Symantec Endpoint Protection Manager with directory authentication.

**Administrator account 4, for anonymous access:**

- On the **General** tab, enter the following information:
  - **User Name:** `john`
  - **Full Name:** John Smith
  - **Email Address:** `john@<sampledomain>.local`
- On the **Access Rights** tab, click **System Administrator**.
- On the **Authentication** tab, click **Directory Authentication**.
  - In the **Directory Server** drop-down list, select `<sampledomain> LDAP without User Name`.
  - In the **Account Name** field, type `John Smith`.
  - Click **Test Account**.

The account authentication fails, but the system administrator `John Smith` can log on to Symantec Endpoint Protection Manager.

---

**Changing the password for an administrator account**

For security purposes, you may need to change the password for another administrator's account.
The following rules apply to changing passwords:

- System administrators can change the password for all administrators.
- Domain administrators can change the password for other domain administrators and limited administrators within the same domain.
- Limited administrators can change their own passwords only.

When you configure the management server in the Management Server Configuration Wizard, you select either the embedded database or a Microsoft SQL Server database. If you select the embedded database, the password you enter for the default administrator account admin also becomes the database password. If you change the default administrator's password, the database password does not change.

If the password is reset to fix an administrator account lockout, the administrator must still wait for the lockout period to expire. The default lockout period is 15 minutes.

**To change the password for an administrator account**

1. In the console, click **Admin > Administrators**.
2. Under **Administrators**, select the administrator account, and then click **Change password**.
   - Press **F1** to see the password restrictions.
3. Type both your password and the administrator's new password.
4. Click **Change**.

See “Unlocking an administrator's account after too many logon attempts” on page 59.

See “Managing administrator accounts” on page 113.

---

**Allowing administrators to reset forgotten passwords**

If you have a system administrator account, you can allow your administrators to reset passwords. If you enable this feature, administrators can click the **Forgot your password?** link on the logon panel to request a temporary password.

---

**Note:** You can allow this method to reset a password only for the administrator accounts that authenticate by using Symantec Management Server authentication. This method does not work for any administrator accounts that authenticate by using either RSA SecurID authentication or directory authentication.
To allow administrators to reset forgotten passwords

1. In the console, click Admin.
2. On the Admin page, click Servers.
3. Under Servers, select the local site.
   
   You control this setting only for the local site.
4. Click Edit Site Properties.
5. On the Passwords tab, check Allow administrators to reset the passwords.
6. Click OK.

See “Sending a temporary password to an administrator” on page 126.

See “Displaying the Remember my user name and Remember my password check boxes on the logon screen” on page 127.

See “Managing administrator accounts” on page 113.

Sending a temporary password to an administrator

If you have a system administrator account, you can allow your administrators to reset their own passwords. An email that contains a link to activate the temporary password is sent to the administrator. You must first make sure the Forgot your password? link appears on the Symantec Endpoint Protection Manager log on screen.

For security reasons, the management server does not store or verify the temporary passwords. To verify whether the administrator successfully reset the password, check that the administrator received the email message.

An administrator can request a temporary password from the management console only once per minute.

You must configure the mail server so that the mail server sends the notification.

You can use this method to reset a password only for the administrator accounts that authenticate by using Symantec Management Server authentication. This method does not work for any administrator accounts that authenticate by using either RSA SecurID authentication or directory authentication.

Warning: Do not use the tool resetpass.bat to reset the administrator password on Symantec Endpoint Protection 12.1.1.1 or later. This tool is intended for use with earlier versions, and is not supported for use with later versions. The use of resetpass.bat with later versions of Symantec Endpoint Protection may corrupt the installation.
To send a temporary password to an administrator

1. On the management server computer, click Start > All Programs > Symantec Endpoint Protection Manager > Symantec Endpoint Protection Manager.

   By default, the Forgot your password? link appears on the management server logon screen. If it does not, you must enable it.

   See “Displaying the Remember my user name and Remember my password check boxes on the logon screen” on page 127.

2. In the Logon screen, click Forgot your password?

3. In the Forgot Password dialog box, type the user name for the account for which to reset the password.

   For domain administrators and limited administrators, type the domain name for the account. If you did not set up domains, leave the domain field blank.

4. Click Temporary Password.

   As a security precaution, the administrator must change the temporary password immediately after logging on.

   See “Changing the authentication method for administrator accounts” on page 119.
   See “Managing administrator accounts” on page 113.

Displaying the Remember my user name and Remember my password check boxes on the logon screen

You can display the Remember my user name and Remember my password check boxes on the Symantec Endpoint Protection Manager logon screen. If you enable this feature, the administrator's user name and password is prepopulated on the logon screen.

To display the Remember my user name and Remember my password check boxes on the logon screen

1. In the console, click Admin.

2. On the Admin page, click Domains.

3. Under Domains, select the domain for which to allow administrators to save logon credentials.

4. Click Edit Domain Properties.
5 On the **Passwords** tab, check **Allow users to save credentials when logging on**.
6 Click **OK**.

See “**Managing administrator accounts**” on page 113.
Configuring Host Integrity and managing policies in Symantec Endpoint Protection Manager

- Chapter 10. Configuring Host Integrity to enforce security compliance
- Chapter 11. Managing policies
Chapter 10

Configuring Host Integrity to enforce security compliance

This chapter includes the following topics:

- How Host Integrity works
- How the Enforcers work with Host Integrity policies
- Setting up Host Integrity
- About Host Integrity requirements
- Adding predefined requirements to a Host Integrity policy
- Setting up remediation for a predefined Host Integrity requirement
- Configuring the frequency of Host Integrity check settings
- Allowing the Host Integrity check to pass if a requirement fails
- Configuring notifications for Host Integrity checks
- Creating a Quarantine policy for a failed Host Integrity check
- Adding a custom requirement from a template
- Writing a customized requirement script
- Creating a test Host Integrity policy with a custom requirement script
How Host Integrity works

Host Integrity ensures that client computers are protected and compliant with your company’s security policies. You use Host Integrity policies to define, enforce, and restore the security of clients to secure enterprise networks and data.

Table 10-1 describes the process to enforce security compliance on the client computer.

Table 10-1  Process for Host Integrity

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 1| The client computer runs a Host Integrity check on the client computer. | The management server downloads the Host Integrity policy to the client computers in the assigned group. The client computers run the Host Integrity check, which compares each computer’s configuration with the requirements that you add to the Host Integrity policy.  
  The Host Integrity policy checks for the existence for antivirus software, patches, hot fixes, and other security requirements. For example, the policy may check whether the latest patches have been applied to the operating system.  
  See “Setting up Host Integrity” on page 133. |
| Step 2| The Host Integrity check passes or fails    | ■ If the computer meets all of the policy’s requirements, the Host Integrity check passes.  
  ■ If the computer does not meet all of the policy’s requirements, the Host Integrity check fails. You can also set up the policy to ignore a failed requirement so that the check passes.  
  See “Allowing the Host Integrity check to pass if a requirement fails” on page 140. |
Table 10-1  Process for Host Integrity *(continued)*

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 3 | Non-compliant computers remediate a failed Host Integrity check (optional) | - If the Host Integrity check fails, you can configure the client to remediate. To remediate, the client downloads and installs the missing software. You can configure either the client to remediate or the end user to remediate in a predefined requirement or a custom requirement. Host Integrity then rechecks that the client computer installed the software.  
  See “Setting up remediation for a predefined Host Integrity requirement” on page 137.  
  - If the Host Integrity check that verifies remediation still fails, the client applies a Quarantine policy. You can use a Quarantine policy to apply stricter restrictions to the failed computers.  
  See “Creating a Quarantine policy for a failed Host Integrity check” on page 142.  
  - While the client is in the Quarantine location, the Host Integrity check continues to run and to try to remediate. The frequency of the check and remediation settings are based on how you configure the Host Integrity policy. Once the client is remediated and passes the Host Integrity check, the client moves out of the Quarantine location automatically. In some cases, you may need to remediate the client computer manually. |
| Step 4 | The client continues to monitor compliance | The Host Integrity check actively monitors each client's compliance status. If at any time the client's compliance status changes, so do the privileges of the computer.  
  - If you change a Host Integrity policy, it is downloaded to the client at the next heartbeat. The client then runs a Host Integrity check.  
  - If the client switches to a location with a different Host Integrity policy while a Host Integrity check is in progress, the client stops checking. The stop includes any remediation attempts. The user may see a timeout message if a remediation server connection is not available in the new location. When the check is complete, the client discards the results. Then the client immediately runs a new Host Integrity check based on the new policy for the location.  
  You can view the results of the Host Integrity check in the Compliance log. |

See “How the Enforcers work with Host Integrity policies” on page 132.  
See “About the Symantec Network Access Control Enforcer appliances” on page 170.  
See “How does Host Integrity enforcement manage computers without Symantec clients installed?” on page 392.

How the Enforcers work with Host Integrity policies

The security policy that all Enforcers direct Symantec Network Access Control clients to run on client computers is the Host Integrity policy. Host Integrity policies
specify the software that is required to run on a client. You can use an Enforcer to enforce Host Integrity policies. You can also run Host Integrity policies without an Enforcer.

You can configure the Enforcer to automatically do the following tasks:

- Verify that a client has been installed on a user’s computer.
- Prompt a client to retrieve updated Host Integrity policies, if available.
- Prompt the client to run a Host Integrity check.
- Verify that the client passes the Host Integrity check. The client sends the results of the check to the Enforcer. If the client passes the check, the Enforcer grants the client access to the protected network. If the client fails the Host Integrity check, the Enforcer blocks the client. The client tries to recover with remediation, and runs the Host Integrity check again until it passes.

Each type of Enforcer appliance implements the network access criteria differently.

A Windows or Mac On-Demand Client can be set up to automatically download and install the latest Host Integrity policies from the Symantec Endpoint Protection Manager. If the client cannot connect to the console, the On-Demand Client gets the Host Integrity policy from the Enforcer appliance when it connects for the first time. After that it gets the Host Integrity policy from the Symantec Endpoint Protection Manager.

The Enforcers control network access for client computers based on the results of a Host Integrity check.

See “How Host Integrity works” on page 131.

See “How the On-Demand Client works” on page 351.

See “How the Gateway Enforcer appliance works” on page 221.

See “How the LAN Enforcer appliance works” on page 256.

Setting up Host Integrity

Use Host Integrity policies to make sure that the client computers in your network meet your organization’s security policies.

Table 10-2 lists the steps you need to perform to set up security compliance using Host Integrity policies.
### Table 10-2  Tasks to set up Host Integrity policies

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 1 | Add a Host Integrity policy that checks for a requirement on the client computer and enforces a remediation action for non-compliant computers | When you add a new policy, perform the following tasks:  
1. Choose which types of requirements you want the client computer to check. Create a separate requirement for each type of software (such as applications, files, and patches).  
   See “About Host Integrity requirements” on page 135.  
   See “Adding predefined requirements to a Host Integrity policy” on page 136.  
2. Configure the remediation actions for non-compliant client computers.  
   Remediation requires that the client computer installs or requests the client user to install the required software.  
   See “Setting up remediation for a predefined Host Integrity requirement” on page 137.  
3. Set the order in which requirements are checked and the remediation is tried. For example, updates should be completed in a specific order so that all updates are applied before the user has to restart the client computer. |
| Step 2 | Set the options for the Host Integrity check and notifications | - Configure how often the Host Integrity check runs.  
   See “Configuring the frequency of Host Integrity check settings” on page 140.  
- Configure whether or not users can cancel remediation.  
   See "Allowing users to delay or cancel Host Integrity remediation" on page 138.  
- Set up a notification to appear on the client computer when the Host Integrity check either passes or fails. Use the notification to tell the end user what to do next. For example, the end user may need to allow a new patch to download and install on the client computer.  
   See “Configuring notifications for Host Integrity checks” on page 141. |
| Step 3 (optional) | Set up peer-to-peer enforcement | If the client computers being tested for Host Integrity compliance are on the same network as already-compliant client computers, you can set up peer-to-peer enforcement. You primarily use peer-to-peer enforcement for file sharing. |
| Step 4 (optional) | Set up a Quarantine policy for non-compliant and unremediated computers | If the client computer fails the Host Integrity check and does not perform remediation, you can quarantine the computer using a Quarantine policy.  
   See “Creating a Quarantine policy for a failed Host Integrity check” on page 142. |
About Host Integrity requirements

When you create a new Host Integrity policy, decide which type of requirements to add.

Each requirement specifies the following items:

- What conditions to check
  For example, a requirement would check whether the latest set of virus definitions is installed on the client computer.

- What remediation actions the client takes if the client fails to pass the condition’s requirements
  For example, the remediation action can include a URL where the client can download and install the missing virus definitions.

Table 10-3 lists the types of requirements you can use.

Table 10-3  
Requirement types for Host Integrity policies

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| Predefined requirements     | Use a predefined requirement to check that a specific application or file is installed and runs on the client. A predefined requirement checks for the status of any of the following types of applications: antivirus software, antispyware software, a firewall, a patch, or a service pack. For example, a patch requirement checks that the client computers run a specific operating system patch.  
  If the predefined requirement does not have enough detail, add a custom requirement and write a script.  
  See “Adding predefined requirements to a Host Integrity policy” on page 136. |
| Custom requirements from templates | Templates are predefined custom requirements that Symantec wrote for commonly performed tasks. For example, the client can check that a password has been changed in the last 42 days. You can also use the templates as a basis for writing a custom requirement script.  
  Template requirements are available through the Host Integrity policy LiveUpdate service. You must first set up LiveUpdate to download the Host Integrity templates to the management server.  
  See “Adding a custom requirement from a template” on page 143. |
Table 10-3  
Requirement types for Host Integrity policies (continued)

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom requirements</td>
<td>Use a custom requirement if neither a predefined requirement nor the templates provide the kind of check that you need. Custom requirements include the same fields as predefined requirements, but provide more flexibility. For example, you can include an antispyware application that is not included in the predefined list of antispyware applications. You can simplify the management of required applications by including similar applications in one custom requirement. For example, you can include Internet browsers such as Internet Explorer and Mozilla Firefox in one requirement. See “Writing a customized requirement script” on page 143.</td>
</tr>
</tbody>
</table>

Note: For Symantec Network Access Control, when you migrate from an older version to the current version of the Enforcer, the Host Integrity policies for the On-Demand Mac client do not migrate. You must add a new policy for the On-Demand Mac client. 
See “Setting up Host Integrity” on page 133.

Adding predefined requirements to a Host Integrity policy

A predefined requirement in a Host Integrity policy checks that the client computer runs any of several types of applications such as: antivirus, antispyware, firewall, and so on.

You determine the particular application, such as specific patches for the Windows 7 operating system. You then specify the path where the client computers should get the patch.

To add predefined requirements to a Host Integrity policy

1. In the console, open a Host Integrity policy.
2. On the Host Integrity policy page, click Requirements > Add.
3. In the Add Requirement dialog box, click either the Windows or Mac client platform.
4. In the Select requirement drop-down list, select a predefined requirement, and then click OK.
5 Configure the settings and remediation options for the requirement, and then click **OK**.

See “Setting up remediation for a predefined Host Integrity requirement” on page 137.

For more information, click **Help**.

6 Click **OK**.

7 Assign the policy to groups or locations.

8 Click **OK**.

See “Adding a custom requirement from a template” on page 143.

See “Writing a customized requirement script” on page 143.

### Enabling and disabling Host Integrity requirements

When you add requirements to a Host Integrity policy, the requirements are enabled by default. You must disable them from being used until they are needed. For example, you can disable a requirement temporarily while you test your Host Integrity policy.

**To enable and disable Host Integrity requirements**

1 In the console, open a Host Integrity policy and click **Requirements**.

2 On the **Requirements** page, do one of the following tasks:

   - To enable a requirement, check the **Enable** check box for the selected requirement.
   - To disable a requirement, uncheck the **Enable** check box for the selected requirement.

3 Click **OK**.

See “Setting up Host Integrity” on page 133.

### Setting up remediation for a predefined Host Integrity requirement

If the Host Integrity check on a client shows that a requirement failed, you can configure the policy to restore the necessary files. The client restores files by downloading, installing, or running the required applications to meet the requirement. The client computer can then pass the Host Integrity check.
You set up remediation in the same dialog box in which you add a predefined requirement. You specify both the path from which the client downloads the remediation files and how the remediation process is implemented.

You can also enable users to have some control over when they remediate their computers. For example, a restart may cause users to lose their work, so users may want to delay remediation until the end of the day.

After the download, installation, or execution of a command to restore a requirement, the client always retests the requirement. Also, the client logs the results as pass or fail.

To set up remediation for a predefined Host Integrity requirement

1. In the console, open a Host Integrity policy and add a predefined requirement. See “Adding predefined requirements to a Host Integrity policy” on page 136.

2. In the Add Requirement dialog box, click Install the <requirement type> if it has not been installed on the client.

3. Click Download the installation package.

4. In the Download URL text box, type the URL from where the installation file gets downloaded to the client computer.

5. In the Execute the command text box, do one of the following tasks:
   - If you want the client user to run the installation, leave the text box blank.
   - If you want the installation to run automatically, type %F%.
     The %F% variable represents the last downloaded file. You can use any command that can be run from Start > Run. For example, to install a patch for Vista, type the command %Systemroot%\system32\wusa.exe /quiet /norestart %F%.

6. Optionally set the options to delay or cancel remediation, and then click OK.
   See “Allowing users to delay or cancel Host Integrity remediation” on page 138.

7. Click OK.
   See “Allowing the Host Integrity check to pass if a requirement fails” on page 140.

Allowing users to delay or cancel Host Integrity remediation

You can allow the user to delay remediation to a more convenient time. If users must restart their computers after they install the software for a requirement, they may want to wait to restart their computers until later.

If the user delays remediation, any of the following events can happen:
- The client logs the event. The Host Integrity status is shown as failed because the requirement is not met. The user can manually run a new Host Integrity check at any time from the client.

- The Host Integrity check remediation message window does not appear again until the client runs another Host Integrity check. If the user has chosen to be reminded in five minutes, but the Host Integrity check runs every 30 minutes, the message window does not appear until 30 minutes. To avoid confusion for the user, you may want to synchronize the minimum time setting with the Host Integrity check frequency setting.

- If the user delays the remediation before the next Host Integrity check, the user selection is overridden.

- If the user delays a remediation action and the client receives an updated policy, the amount of time available for remediation is reset to the new maximum.

To allow users to delay or cancel Host Integrity remediation

1. In the console, open a Host Integrity policy and add a requirement.
   See “Adding predefined requirements to a Host Integrity policy” on page 136.

2. In the Add Requirement dialog box, set up remediation.
   See “Setting up remediation for a predefined Host Integrity requirement” on page 137.

3. On the dialog box for the requirement, do one of the following tasks, and then click OK:
   - To let the client user delay a file from being downloaded, check Specify wait time before attempting the download again if the download fails.
   - To let the client user cancel remediation, check Allow the user to cancel the download for Host Integrity remediation.

4. Click OK.

5. Click Advanced Settings.

6. On the Advanced Settings page, under Remediation Dialog Options, configure the options for canceling the remediation.

7. To add a custom message on the client computer, click Set Additional Text.
   The message you type appears on the client remediation window if the user clicks Details.

8. Click OK.
Configuring the frequency of Host Integrity check settings

You can configure how the Host Integrity check is carried out and how the results are handled.

After you add or update a Host Integrity policy, the policy is downloaded to the client at the next heartbeat. The client then runs the Host Integrity check.

If the user switches to a location with a different policy while a Host Integrity check is in progress, the client stops the check. The stop includes remediation attempts, if required by the policy. The user may get a timeout message if a remediation server connection is not available in the new location. When the check is complete, the client discards the results. Then the client immediately runs a new Host Integrity check based on the new policy for the location.

If the policy is the same in the new location, the client maintains any Host Integrity timer settings. The client runs a new Host Integrity check only when required by the policy settings.

To configure the frequency of Host Integrity check settings

1. In the console, open a Host Integrity policy, and click Advanced Settings.
2. On the Advanced Settings page, under Host Integrity Checking Options, set the Host Integrity check frequency.
3. Click OK.

See “Adding predefined requirements to a Host Integrity policy” on page 136.
See “Allowing the Host Integrity check to pass if a requirement fails” on page 140.

Allowing the Host Integrity check to pass if a requirement fails

Users may need to continue working even if their computers fail the Host Integrity check. You can let the Host Integrity check pass even if a specific requirement fails. The client logs the results but ignores the results.

You apply this setting for a specific requirement. If you want to apply this setting to all requirements, you must enable the setting on each requirement separately. The setting is disabled by default.
To allow the Host Integrity check to pass if a requirement fails

1. In the console, open a Host Integrity policy.
2. Add a predefined requirement or a custom requirement, and then click OK.
   
   See “Adding predefined requirements to a Host Integrity policy” on page 136.
   
   See “Writing a customized requirement script” on page 143.
3. On the dialog box for the requirement, check **Allow the Host Integrity check to pass even if this requirement fails**, and then click OK.
4. Click OK.

Configuring notifications for Host Integrity checks

When the client runs a Host Integrity check, you can configure notifications to appear when the following conditions occur:

- A Host Integrity check fails.
- A Host Integrity check passes after it previously failed.

The results of the Host Integrity check appear in the client's Security log. They are uploaded to the Compliance log on the **Monitors** page of the management server.

The client's Security log contains several panes. If you select a Host Integrity check event type, the lower left-hand pane lists whether the individual requirement has passed or failed. The lower right-hand pane lists the conditions of the requirement. You can configure the client to suppress the information in the lower right-hand pane. Although you may need this information when troubleshooting, you may not want users to view the information. For example, you may write a custom requirement that specifies a registry value or a file name. The details are still recorded in the Security log.

You can also enable a notification that gives the user the choice to download the software immediately or delay the remediation.

See “Allowing users to delay or cancel Host Integrity remediation” on page 138.

To configure notifications for Host Integrity checks

1. In the console, open a Host Integrity policy.
2. On the **Host Integrity** page, click **Advanced Settings**.
3. On the **Advanced Settings** page, under **Notifications**, to show detailed requirement information, check **Show verbose Host Integrity Logging**.
   
   The lower right-hand pane of the client's Security log displays complete information about a Host Integrity requirement.
4 Check any of the following options:
   ■ Display a notification message when a Host Integrity check fails.
   ■ Display a notification message when a Host Integrity check passes after previously failing.

5 To add a custom message, click Set Additional Text, type up to 512 characters of additional text, and then click OK.

6 When you are finished with the configuration of this policy, click OK.

Creating a Quarantine policy for a failed Host Integrity check

You use a Quarantine policy for the client computers that fail the Host Integrity check, try to remediate, and then fail remediation again. After the client computer fails remediation, it automatically switches to a Quarantine location, where a Quarantine policy is applied to the computer. You use a Quarantine policy to apply stricter restrictions to the failed computers. You can use any type of protection policy for the Quarantine policy. For example, you can apply a Quarantine Firewall policy that blocks a computer's access to the Internet.

While the client computer is in the Quarantine location, you can configure the Host Integrity check to continue to run and try to remediate the computer. You may also need to remediate the computer manually.

To create a Quarantine policy for a failed Host Integrity check

1 In the console, click Clients, and then click the Policies tab.

2 On the Policies tab, next to Quarantine Policies when Host Integrity Fails, click Add a policy.

3 In the Add Quarantine Policy dialog box, choose a policy type and then click Next.

4 Choose whether to use an existing policy, create a new policy, or import a policy file, and then click Next.

5 Do one of the following tasks:
   ■ In the Add Policy dialog box, choose the policy, and click OK.
   ■ In the Policy Type dialog box, configure the policy, and click OK.
   ■ In the Import Policy dialog box, locate the .dat file and click Import.

See “Setting up remediation for a predefined Host Integrity requirement” on page 137.
See “About Host Integrity requirements” on page 135.
Adding a custom requirement from a template

Instead of writing custom requirements from scratch, you can add common custom requirements that Symantec created. You use LiveUpdate to download Host Integrity content to the management server. The Host Integrity content includes templates. You then add the custom requirements from the templates to the Host Integrity policy.

To get the latest Host Integrity templates, you must configure a LiveUpdate Content policy to download Host Integrity content.

If you import a requirement a second time and a requirement with the same name exists, the imported requirement does not overwrite the existing requirement. Instead, the imported requirement is shown with the number 2 next to its name on the Requirements table.

To add a custom requirement from a template

1. In the console, open a Host Integrity policy.
2. On the Host Integrity policy page, click Requirements > Add.
3. In the Add Requirement dialog box, click either the Windows or Mac client platform.
4. In the Select requirement drop-down list, click Use existing templates, and then click OK.
5. In the Host Integrity Online Updating dialog box, expand Templates, and then select a template category.
6. Next to each template you want to add, click Add.
7. Click Import.
8. Click OK.

See “About Host Integrity requirements” on page 135.

Writing a customized requirement script

Custom requirements provide more flexibility than a predefined requirement. For example, you can add an application that is not included in the predefined lists of applications.

To build a custom requirement, you add one or more functions or IF..THEN statements to a script. When you run the script, the Host Integrity check looks for the condition that is listed under the IF node. Depending upon the condition, the action that is listed under the THEN node is executed. The result (pass or fail) is returned.
When you add many different conditions in one script to check for, this setting applies to the entire custom requirement script. This choice may affect whether you want to create several small custom requirements or a longer one that includes multiple steps.

**To write a customized requirement script**

1. In the console, open a Host Integrity policy.
2. On the Host Integrity policy page, click Requirements > Add.
3. In the Add Requirement dialog box, click either the Windows or Mac client platform.
4. In the Select requirement drop-down list, select Custom requirement, and then click OK.
5. In the Custom Requirement dialog box, type a name for the requirement. The requirement name appears on the client computer. The name notifies the user whether the requirement has passed or the requirement has failed or prompts the user to download the software.
6. To add a condition, under Customized Requirement Script, click Add, and then click IF..THEN.

   __Note:__ If you first add a function or an IF..THEN statement without filling out the fields, an error appears. If you do not want to add the statement, right-click the statement and click Delete.

7. With the highlight on the empty condition under the IF node, in the right pane, select a condition. The Host Integrity check looks for the condition on the client computer.
8. Under the Select a condition drop-down list, specify the additional information that is required.
9. Under Customized Requirement Script, click THEN, and then click Add. The THEN statement provides the action that should be taken if the condition is true.
10. Click any of the following options:
    - **IF..THEN**
      Use a nested IF..THEN statement to define conditions to check and actions to take if the condition is evaluated as true.
    - **Function**
      Use a function to define a remediation action, such as downloading a file.
Return
Use a return statement to specify whether the results of the evaluation of the condition pass or fail. Every custom requirement must end with a pass or fail statement.

Comment (optional)
Use a comment to explain the functionality of the conditions, functions, or statements that you add.

11 In the right-hand pane, define the criteria that you added.
   For more information on these options, click Help.
12 To add more nested statements, conditions, or functions, under Customized Requirement Script, right-click the node, and then click Add.
13 Repeat steps 10 to 12 as needed.
14 To allow the Host Integrity check to pass no matter what the result, check Allow the Host Integrity check to pass even if this requirement fails.
15 Click OK.
See “Creating a test Host Integrity policy with a custom requirement script” on page 149.
See “Adding predefined requirements to a Host Integrity policy” on page 136.

About registry conditions
You can specify which Windows registry settings to check as part of an IF..THEN statement for a customized requirement. You can also specify ways to change registry values. Only HKEY_CLASSES_ROOT, HKEY_CURRENT_USER, HKEY_LOCAL_MACHINE, HKEY_USERS, and HKEY_CURRENT_CONFIG are supported registry settings.

When you specify registry keys, remember the following considerations:

- The key name is limited to 255 characters.
- If the registry key has a backslash (\) at the end, it is interpreted as a registry key. For example: HKEY_LOCAL_MACHINE\SOFTWARE\ActiveTouch
- If the registry key has no backslash at the end, then it is interpreted as a registry name. For example: HKEY_LOCAL_MACHINE\SOFTWARE\ActiveTouch

When you specify registry values, remember the following considerations:

- The value name is limited to 255 characters.
- You can check for values as DWORD (decimal), Binary (hexadecimal), or String.
For DWORD values, you can check whether the value is less than, equal to, not equal to, or greater than the specified value.

For string values, you can check whether the value data equals or contains a given string. If you want the string comparison to be case-sensitive, check the Match case check box.

For binary values, you can check whether the value data equals or contains a given piece of binary data. Hexadecimal bytes represent the data. If you specify value contains, you can also specify the offset for this data. If the offset is left blank, it searches the value for the given binary data. Allowed values for the hexadecimal edit box are 0 through 9 and a through f.

The following are examples of registry values:

- DWORD 12345 (in decimal)
- Binary 31 AF BF 69 74 A3 69 (in hexadecimal)
- String ef4adf4a9d933b747361157b8ce7a22f

Writing a custom requirement to run a script on the client

In a custom Host Integrity requirement, you can specify a function that causes the client to run a script. You can use a scripting language, such as JScript or VBScript, which you can run with the Microsoft Windows Script Host.

To write a custom requirement to run a script on the client

1. In the console, open a Host Integrity policy.
2. On the Host Integrity policy page, click Requirements > Add.
3. In the Add Requirement dialog box, click either the Windows or Mac client platform.
4. In the Select requirement drop-down list, select Custom requirement, and then click OK.
   
   See "Writing a customized requirement script" on page 143.
5. In the Custom Requirement dialog box, under Customized Requirement Script, select the node where you want to add the function.
6. Click Add, and then click Function.
7. Click Utility: Run a script.
8. Enter a file name for the script, such as myscript.js.
9. Type the content of the script.
10 In the **Execute the command** text field, type the command to use to execute the script.

Use `%F` to specify the script file name. The script executes in system context.

11 To specify the amount of time to allow the **Execute** command to complete, select one of the following options:

  - **Do not wait**
    The action returns true if the execution is successful but it does not wait until the execution is completed.
  - **Wait until execution completes**
  - **Enter maximum time**
    Enter a time in seconds. If the **Execute** command does not complete in the specified time, the file execution is terminated.

12 Optionally, uncheck **Delete the temporary file after execution is completed or terminated** if you no longer need it.

This option is disabled and unavailable if **Do not wait** is selected.

13 Optionally, uncheck **Show new process window** if you do not want to see a window that shows the requirement running the script.

**Writing a custom requirement to set the timestamp of a file**

In the custom Host Integrity requirement, you can specify the **Set Timestamp** function to create a Windows registry setting to store the current date and time.

You can then use the **Check Timestamp** condition to find out if a specified amount of time has passed since that timestamp was created.

For example, if the Host Integrity check runs every 2 minutes, you can specify an action to occur at a longer interval such as a day. In this case, the stored time value is removed. You could set the script to run as follows:

  - When the client receives a new profile
  - When the user manually runs a Host Integrity check

**To write a custom requirement to set the timestamp of a file**

1 In the console, open a Host Integrity policy.

2 On the **Host Integrity policy** page, click **Requirements > Add**.

3 In the **Add Requirement** dialog box, click either the **Windows** or **Mac** client platform.
4 In the **Select requirement** drop-down list, select **Custom requirement**, and then click **OK**.

   See “**Writing a customized requirement script**” on page 143.

5 In the **Custom Requirement** dialog box, under **Customized Requirement Script**, select the node where you want to add the function.

6 Click **Add**, and then click **Function**.

7 Click **Utility: Set Timestamp**.

8 Type a name up to 255 characters long for the registry setting that stores the date and the time information.

   For example, enter **Date and time of last file update**:

   **To compare the current time to the stored time value**

   1 Write a custom requirement script.

      See “**Writing a customized requirement script**” on page 143.

   2 In the **Custom Requirement** dialog box, under **Customized Requirement Script**, select the node where you want to add the condition.

   3 Click **Add**, and then click **IF..THEN**.

   4 Click **Utility: Check Timestamp**.

   5 Type the name you entered for the saved time registry setting.

   6 Specify an amount of time in minutes, hours, days, or weeks.

      If the specified amount of time has passed, or if the value of the registry setting is empty, the **Set Timestamp** function returns a value of True.

---

**Writing a custom requirement to increment a registry DWORD value**

For a custom requirement, you can increment the Windows registry DWORD value. The **Increment registry DWORD** value function creates the key if it does not exist.

**To write a custom requirement to increment the registry DWORD value**

1 In the console, add a Host Integrity policy with a custom requirement script.

   See “**Writing a customized requirement script**” on page 143.

2 In the **Custom Requirement** dialog box, under **Customized Requirement Script**, select the node where you want to add the function.

3 Click **Add**, and then click **Function**.

4 Click **Registry: Increment registry DWORD value**.

5 Enter the registry key to check in the **Registry key** field.
6 Enter a value name to be checked in the Value name field.
7 Click OK.

Creating a test Host Integrity policy with a custom requirement script

The policy that you create for this test is for demonstration purposes only. The policy detects the existence of an operating system and, when detected, generates a fail event. Normally, you would generate fail events for other reasons.

Complete the following tasks:

- Add a Host Integrity policy with a custom requirement script that checks for the operating system on the client computer.
  See “To create a test Host Integrity policy with a custom requirement script” on page 149.
- Test the Host Integrity policy you have created.
  See “To test the Host Integrity policy on the client computer” on page 150.

Note: If you installed both Symantec Network Access Control and Symantec Endpoint Protection, you can create a Firewall policy for the client computers that fail Host Integrity. If you run Symantec Enforcer with Symantec Network Access Control, you can isolate the clients that fail Host Integrity to specific network segments. This isolation prevents client authentication and domain access.

To create a test Host Integrity policy with a custom requirement script

1 In the console, open a Host Integrity policy.
2 On the Host Integrity policy page, click Requirements > Add.
3 In the Add Requirement dialog box, click either Windows or Mac.
4 In the Select requirement drop-down list, click Custom requirement, and then click OK.
5 In the Name box, type a name for the custom requirement.
6 In the Custom Requirement dialog box, under Customized Requirement Script, right-click Insert statements below, and then click Add > IF..THEN.
7 In the right pane, in the Select a condition drop-down list, click Utility: Operating System is.
8 Under Operating system, check one or more operating systems that your client computers run and that you can test.
9 Under Customized Requirement Script, right-click THEN //Insert statements here, and then click Add > Function > Utility: Show message dialog.

10 In the Caption of the message box field, type a name to appear in the message title.

11 In the Text of the message box field, type the text that you want the message to display.

12 In the left pane, under Customized Requirement Script, click Pass.

13 In the right pane, under As the result of the requirement, return, check Fail, and then click OK.

14 Click OK.

15 In the Host Integrity Policies dialog box, in the left panel, click Assign the policy.

16 In the Assign Host Integrity Policy dialog box, select the groups to which you want to assign the policy, and click Assign.

In the Assign Host Integrity Policy dialog box, click Yes to assign the Host Integrity policy changes.

Note: One Host Integrity policy can be assigned to multiple groups, while a single group can only have a single Host Integrity policy. You can replace an existing policy with a different policy.

To test the Host Integrity policy on the client computer

1 In the console, click Clients > Clients.

2 Under Clients, click and highlight the group that contains the client computers to which you applied the Host Integrity policy.

3 Under Tasks, click Run a command on the group > Update Content, and then click OK.

4 Log on to the computer that runs the client and note the message box that appears.

Because the rule triggered the fail test, the message box appears. After testing, disable or delete the test policy.

See “Writing a customized requirement script” on page 143.

See “Writing a custom requirement to increment a registry DWORD value” on page 148.

See “Writing a custom requirement to run a script on the client” on page 146.
Managing policies

This chapter includes the following topics:

- Performing the tasks that are common to all policies
- About shared and non-shared policies
- Adding a policy
- Editing a policy
- Copying and pasting a policy on the Policies page
- Copying and pasting a policy on the Clients page
- Assigning a policy to a group
- Replacing a policy
- Exporting and importing individual policies
- Converting a shared policy to a non-shared policy
- Withdrawing a policy from a group
- How the client computers get policy updates
- Configuring push mode or pull mode to update client policies and content
- Using the policy serial number to check client-server communication
- Manually updating policies on the client

Performing the tasks that are common to all policies

Your security policies define how the protection technologies protect your computers from known and unknown threats.
You can manage your Symantec Endpoint Protection security policies in many ways. For example, you can create copies of the security policies and then customize the copies for your specific needs. You can lock and unlock certain settings so that users cannot change them on the client computer.

Table 11-1 describes many of the policy tasks that you can perform.

Table 11-1: Tasks common to all policies

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add a policy</td>
<td>If you do not want to use one of the default policies, you can add a new policy. You can add shared policies or non-shared policies. Note: If you add or edit shared policies in the Policies page, you must also assign the policies to a group or location. Otherwise those policies are not effective. See “About shared and non-shared policies” on page 154. See “Adding a policy” on page 155.</td>
</tr>
<tr>
<td>Edit a policy</td>
<td>If you want to change the settings in an existing policy, you can edit it. You can increase or decrease the protection on your computers by modifying its security policies. You do not have to reassign a modified policy unless you change the group assignment. See “Editing a policy” on page 156.</td>
</tr>
<tr>
<td>Assign a policy</td>
<td>To put a policy into use, you must assign it to one or more groups or locations. See “Assigning a policy to a group” on page 158.</td>
</tr>
<tr>
<td>Test a policy</td>
<td>Symantec recommends that you always test a new policy before you use it in a production environment.</td>
</tr>
<tr>
<td>Update the policies on clients</td>
<td>Based on the available bandwidth, you can configure a client to use push mode or pull mode as its policy update method. See “How the client computers get policy updates” on page 164. See “Configuring push mode or pull mode to update client policies and content” on page 165.</td>
</tr>
<tr>
<td>Replace a policy</td>
<td>You can replace a shared policy with another shared policy. You can replace the shared policy in either all locations or for one location. See “Replacing a policy” on page 159.</td>
</tr>
</tbody>
</table>
### Table 11-1  Tasks common to all policies (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copy and paste a policy</td>
<td>Instead of adding a new policy, you may want to copy an existing policy to use as the basis for the new policy.</td>
</tr>
<tr>
<td></td>
<td>You can copy and paste policies on either the Policies page or the Policies tab on the Clients page.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> You can also copy all the policies in a group and paste them into another group, from the Policies tab on the Clients page.</td>
</tr>
<tr>
<td></td>
<td>See “Copying and pasting a policy on the Clients page” on page 157.</td>
</tr>
<tr>
<td></td>
<td>See “Copying and pasting a policy on the Policies page” on page 157.</td>
</tr>
<tr>
<td>Convert a shared policy to a non-shared policy</td>
<td>You can copy the content of a shared policy and create a non-shared policy from that content.</td>
</tr>
<tr>
<td></td>
<td>See “About shared and non-shared policies” on page 154.</td>
</tr>
<tr>
<td></td>
<td>A copy enables you to change the content of a shared policy in one location and not in all other locations. The copy overrides the existing non-shared policy.</td>
</tr>
<tr>
<td></td>
<td>You can convert a shared policy to a non-shared policy if the policy no longer applies to all the groups or all the locations. When you finish the conversion, the converted policy with its new name appears under Location-specific Policies and Settings.</td>
</tr>
<tr>
<td></td>
<td>See “Converting a shared policy to a non-shared policy ” on page 162.</td>
</tr>
<tr>
<td>Export and import a policy</td>
<td>You can export an existing policy if you want to use it at a different site or management server. You can then import the policy and apply it to a group or to a specific location.</td>
</tr>
<tr>
<td></td>
<td>See “Exporting and importing individual policies” on page 161.</td>
</tr>
<tr>
<td>Withdraw a policy</td>
<td>If you delete a policy, Symantec Endpoint Protection Manager removes the policy from the database. If you do not want to delete a policy, but you no longer want to use it, you can withdraw the policy instead.</td>
</tr>
<tr>
<td></td>
<td>You can withdraw any type of policy except a Virus and Spyware Protection policy and a LiveUpdate Settings policy.</td>
</tr>
<tr>
<td></td>
<td>See “Withdrawing a policy from a group” on page 163.</td>
</tr>
</tbody>
</table>
Table 11-1  Tasks common to all policies (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete a policy</td>
<td>If a policy is assigned to one or more groups and locations, you cannot delete it until you have unassigned it from all the groups and locations. You can also replace the policy with another policy</td>
</tr>
<tr>
<td>Check that the client has the latest policy</td>
<td>You can check whether the client has the latest policy. If not, you can manually update the policy on the client.</td>
</tr>
<tr>
<td></td>
<td>See “How the client computers get policy updates” on page 164.</td>
</tr>
<tr>
<td></td>
<td>See “Using the policy serial number to check client-server communication” on page 167.</td>
</tr>
<tr>
<td></td>
<td>See “Manually updating policies on the client” on page 167.</td>
</tr>
</tbody>
</table>

About shared and non-shared policies

Policies are either shared or non-shared. A policy is shared if you apply it to more than one group or location. If you create shared policies, you can easily edit and replace a policy in all groups and locations that use it. You can apply shared policies at the My Company group level or a lower group level and subgroups can inherit policies. You can have multiple shared policies.

If you need a specialized policy for a particular group or location, you create a policy that is unique. You assign this unique, non-shared policy to one specific group or location. You can only have one policy of each policy type per location.

For example, here are some possible scenarios:

- A group of users in Finance needs to connect to an enterprise network by using different locations when at the office and for home. You may need to apply a different Firewall policy with its own set of rules and settings to each location for that one group.

- You have remote users who typically use DSL and ISDN, for which they may need a VPN connection. You have other remote users who want to dial up when they connect to the enterprise network. However, the sales and marketing groups also want to use wireless connections. Each of these groups may need its own Firewall policy for the locations from which they connect to the enterprise network.

- You want to implement a restrictive policy regarding the installation of non-certified applications on most employee workstations to protect the enterprise network from attacks. Your IT group may require access to additional applications. Therefore, the IT group may need a less restrictive security policy than typical employees. In this case, you can create a different Firewall policy for the IT group.
You typically add any policy that groups and locations share in the **Policies** page on the **Policies** tab. However, you add any policy that is not shared between groups and that applies only to a specific location in the **Clients** page. If you decide to add a policy in the **Clients** page, you can add a new policy by using any of the following methods:

- Add a new policy.
  
  See “Adding a policy” on page 155.

- Copy an existing policy to base the new policy on.
  
  See “Copying and pasting a policy on the Policies page” on page 157.

- Import a policy that was previously exported from another site.
  
  See “Exporting and importing individual policies” on page 161.

See “Performing the tasks that are common to all policies” on page 151.

See “Converting a shared policy to a non-shared policy ” on page 162.

## Adding a policy

Symantec Endpoint Protection Manager comes with a default policy for each type of protection. If you need to customize a policy, you add one and edit it. You can create multiple versions of each type of policy.

Symantec recommends that you test all new policies before you use them in a production environment.

**To add a new policy**

1. In the console, click **Policies**.

2. On the **Policies** page, select a policy type, and then click the link to add a new policy.

3. Modify the policy settings to increase or decrease protection.

4. Click **OK** to save the policy.

5. Optionally assign the new policy to a group.

You can assign a new policy to a group during or after policy creation. The new policy replaces the currently assigned policy of the same protection type.

See “Assigning a policy to a group” on page 158.

See “Performing the tasks that are common to all policies” on page 151.
Editing a policy

You can edit shared and non-shared policies on the Policies tab on the Clients page as well as on the Policies page.

Locations as well as groups can share the same policy. You must assign a shared policy after you edit it.

See “Performing the tasks that are common to all policies” on page 151.

To edit a policy in the Policies page

1. In the console, click Policies.
2. On the Policies page, under Policies, click the policy type.
3. In the policy type Policies pane, click the specific policy that you want to edit.
4. Under Tasks, click Edit the Policy.
5. In the policy type Policy Overview pane, edit the name and description of the policy, if necessary.
6. To edit the policy, click any of the policy type Policy pages for the policies.

To edit a policy in the Clients page

1. In the console, click Clients.
2. On the Clients page, under Clients, select the group for which you want to edit a policy.
3. On the Policies tab, uncheck Inherit policies and settings from parent group "group name".
   You must disable inheritance for this group. If you do not uncheck inheritance, you cannot edit a policy.
4. Under Location-specific Policies and Settings, scroll to find the name of the location whose policy you want to edit.
5. Locate the specific policy for the location that you want to edit.
6. To the right of the selected policy, click Tasks, and then click Edit Policy.
7. Do one of the following tasks:
   - To edit a non-shared policy, go to step 8.
   - To edit a shared policy, in the Edit Policy dialog box, click Edit Shared to edit the policy in all locations.
8. You can click a link for the type of policy that you want to edit.
Copying and pasting a policy on the Policies page

You can copy and paste a policy on the Policies page. For example, you may want to edit the policy settings slightly to apply to another group.

To copy a policy in the Policies page

1. In the console, click Policies.
2. On the Policies page, under Policies, click the type of policy that you want to copy.
3. In the policy type Policies pane, click the specific policy that you want to copy.
4. On the Policies page, under Tasks, click Copy the Policy.
5. In the Copy Policy dialog box, check Do not show this message again if you no longer want to be notified about this process.

To redisplay the Do not show this message again check box, click Admin > Administrators, select your administrator account, and click Reset Copy Policy Reminder.

6. Click OK.

To paste a policy in the Policies page

1. In the console, click Policies.
2. On the Policies page, under Policies, click the type of policy that you want to paste.
3. In the policy type Policies pane, click the specific policy that you want to paste.
4. On the Policies page, under Tasks, click Paste a Policy.

See “Copying and pasting a policy on the Clients page” on page 157.

Copying and pasting a policy on the Clients page

You can copy and paste a policy instead of having to add a new policy. You can copy a shared or a non-shared policy on the Clients page.

See “Performing the tasks that are common to all policies” on page 151.

To copy a policy in the Clients page

1. In the console, click Clients.
2. On the Clients page, under Clients, select the group for which you want to copy a policy.
3 On the **Policies** tab, under **Location-specific Policies and Settings**, scroll to find the name of the location from which you want to copy a policy.

4 Locate the specific policy for the location that you want to copy.

5 To the right of the policy, click **Tasks**, and then click **Copy**.

6 Click **OK**.

**To paste a policy on the Clients page**

1 In the console, click **Clients**.

2 On the **Clients** page, under **Clients**, select the group for which you want to paste a policy.

3 On the **Policies** tab, uncheck **Inherit policies and settings from parent group "group name"**.

   You must disable inheritance for this group. If you do not uncheck inheritance, you cannot paste a policy.

4 Under **Location-specific Policies and Settings**, scroll to find the name of the location whose policy you want to paste.

5 Locate the specific policy for the location that you want to paste.

6 To the right of the policy, click **Tasks**, and then click **Paste**.

7 When you are prompted to overwrite the existing policy, click **Yes**.

---

**Assigning a policy to a group**

You assign a policy to a client computer through a group. Every group has exactly one policy of each protection type that is assigned to it at all times. Typically, you create separate groups for clients that run different platforms. If you put clients that run different platforms into the same group, be aware that each client platform ignores any settings that do not apply to it.

Unassigned policies are not downloaded to the client computers in groups and locations. If you do not assign the policy when you add the policy, you can assign it to groups and locations later. You can also reassign a policy to a different group or location.

Policies are assigned to computer groups as follows:

- At initial installation, the Symantec default security policies are assigned to the **My Company** parent group.

- The security policies in the **My Company** parent group are automatically assigned to each newly created child group. Newly created child groups inherit from **My Company** by default.
New groups always inherit from their immediate parent group. If you create a hierarchy of child groups, each one inherits from its immediate parent, not from the top-level parent.

- You replace a policy in a group by assigning another policy of the same type. You can replace a policy that is assigned to the My Company parent group or to any child group.

The user interface in the Assign policy dialog box conveys the following additional information:

- A folder icon indicates a group.
- A round icon indicates a location.
- On a group icon, a check mark in a green circle indicates that this policy is assigned to all of the locations in the group.
- On a location icon, a check mark in a green circle indicates that this policy is assigned to this location.
- Text that is grayed out means that the group or location inherits its policy from its parent group.

See “Performing the tasks that are common to all policies” on page 151.

To assign a policy to a group

1. In the console, click Policies.
2. On the Policies page, select a policy, and then click Assign the policy.
3. In the Assign policy dialog box, select the groups, and then click Assign.
4. Click OK to confirm.

Re replacing a policy

You may want to replace one shared policy with another shared policy. You can replace the shared policy in either all locations or for individual locations.

When you replace a policy for all locations, the management server replaces the policy only for the locations that have it. For example, suppose the Sales group uses the Sales policy for three of its four locations. If you replace the Sales policy with the Marketing policy, only those three locations receive the Marketing policy.
You may want a group of clients to use the same settings no matter what location they are in. In this case, you can replace a non-shared policy with a shared policy. You replace a non-shared policy with a shared policy for each location individually.

See “Performing the tasks that are common to all policies” on page 151.

To replace a shared policy for all locations

1. In the console, click **Policies**.
2. On the **Policies** page, under **Policies**, click the type of policy that you want to replace.
3. In the **policy type Policies** pane, click the policy.
4. In the **Policies** page, under **Tasks**, click **Replace the Policy**.
5. In the **Replace policy type Policy** dialog box, in the **New policy type Policy** list box, select the shared policy that replaces the old one.
6. Select the groups and locations for which you want to replace the existing policy.
7. Click **Replace**.
8. When you are prompted to confirm the replacement of the policy for the groups and locations, click **Yes**.

To replace a shared policy or non-shared policy for one location

1. In the console, click **Clients**.
2. In the **Clients** page, under **Clients**, select the group for which you want to replace a policy.
3. On the **Policies** tab, uncheck **Inherit policies and settings from parent group "group name"**.
   
   You must disable inheritance for this group. If you do not uncheck inheritance, you cannot replace a policy.
4. Under **Location-specific Policies and Settings**, scroll to find the location that contains the policy.
5. Next to the policy that you want to replace, click **Tasks**, and then click **Replace Policy**.
6. In the **Replace Policy** dialog box, in the **New policy** list box, select the replacement policy.
7. Click **OK**.
Exporting and importing individual policies

You can export and import policies rather than recreating the policies. All the settings that are associated with the policy are automatically exported.

You may need to export a policy for the following reasons:

- You update the management server from an older release to a newer release. You want to update the new management server with the policies that you previously customized.
- You want to export a policy for use at a different site.

You export and import each policy one at a time. Once you export a file, you import it and apply it to a group or only to a location. You can export a shared or non-shared policy for a specific location in the Clients page.

See “Performing the tasks that are common to all policies” on page 151.

To export a single policy from the Policies page

1. In the console, click Policies.
2. On the Policies page, under Policies, click the type of policy that you want to export.
3. In the policy type Policies pane, click the specific policy that you want to export.
4. In the Policies page, under Tasks, click Export the Policy.
5. In the Export Policy dialog box, locate the folder where you want to export the policy file to, and then click Export.

To export a shared or non-shared policy from the Clients page

1. In the console, click Clients.
2. Under Clients, select the group for which you want to export a policy.
3. On the Policies tab, uncheck Inherit policies and settings from parent group "group name".
   You must disable inheritance for this group. If you do not uncheck inheritance, you cannot export a policy.
4. Under Location-specific Policies and Settings, scroll to find the name of the location whose policy you want to export.
5. Locate the specific policy for the location that you want to export.
6. To the right of the policy, click Tasks, and then click Export Policy.
7 In the Export Policy dialog box, browse to the folder into which you want to export the policy.

8 In the Export Policy dialog box, click Export.

To import a single policy

1 In the console, click Policies.

2 On the Policies page, under Policies, click the type of policy that you want to import.

3 In the policy type Policies pane, click the policy that you want to import.

4 On the Policies page, under Tasks, click Import a policy type Policy.

5 In the Import Policy dialog box, browse to the policy file that you want to import, and then click Import.

Converting a shared policy to a non-shared policy

You can copy the content of a shared policy and create a non-shared policy from that content. A copy enables you to change the content of a shared policy in one location and not in all other locations. The copy overrides the existing shared policy.

When you finish the conversion, the converted policy with its new name appears under Location-specific Policies and Settings.

See “About shared and non-shared policies” on page 154.

See “Copying and pasting a policy on the Policies page” on page 157.

To convert a shared policy to a non-shared policy

1 In the console, click Clients.

2 In the Clients page, under Clients, select the group for which you want to convert a policy.

3 In the pane that is associated with the group that you selected in the previous step, click Policies.

4 On the Policies tab, uncheck Inherit policies and settings from parent group group_name.
   
   You must disable inheritance for this group. If you do not uncheck inheritance, you cannot replace a policy.

5 Under Location-specific Policies and Settings, scroll to find the name of the location and the specific policy that you want to convert.

6 Beside the specific policy, click Tasks, and then click Convert to Non-shared Policy.
7 In the Overview dialog box, edit the name and description of the policy.
8 Modify the other policy settings as desired.
9 Click OK.

See “Performing the tasks that are common to all policies” on page 151.

Withdrawing a policy from a group

You may want to withdraw a policy from a group or a location under certain circumstances.

For example, a specific group may have experienced problems after you introduced a new policy. If you want the policy to remain in the database, you can withdraw the policy instead of deleting it. If you withdraw a policy, it is automatically withdrawn from the groups and locations that you assigned it to. The number of locations that a policy is used for appears on the policy type Policies pane on the Policies page.

Note: You must withdraw a policy or replace a policy from all groups and locations before you can delete it.

You can withdraw all policies in the Policies page from a location or group except for the following policies:

- Virus and Spyware Protection
- LiveUpdate Settings

You can only replace them with another Virus and Spyware Protection policy or LiveUpdate policy.

See “Replacing a policy” on page 159.

To withdraw a shared policy in the Policies page

1 In the console, click Policies.
2 On the Policies page, under Policies, click the type of policy that you want to withdraw.
3 In the policy type Policies pane, click the specific policy that you want to withdraw.
4 On the Policies page, under Tasks, click Withdraw the Policy.
5 In the Withdraw Policy dialog box, check the groups and locations from which you want to withdraw the policy.
6. Click **Withdraw**.
7. When you are prompted to confirm the withdrawal of the policy from the groups and locations, click **Yes**.

**To withdraw a shared or non-shared policy in the Clients page**

1. In the console, click **Clients**.
2. On the **Clients** page, under **Clients**, select the group for which you want to withdraw a policy.
3. On the **Policies** tab, uncheck **Inherit policies and settings from parent group "group name"**.
   
   You must disable inheritance for this group. If you do not uncheck inheritance, you cannot withdraw a policy.
4. Under **Location-specific Policies and Settings**, scroll to find the name of the location for which you want to withdraw a policy.
5. Locate the policy for the location that you want to withdraw.
6. Click **Tasks**, and then click **Withdraw Policy**.
7. In the **Withdraw Policy** dialog box, click **Yes**.

See “Performing the tasks that are common to all policies” on page 151.

### How the client computers get policy updates

When you configure policies on the management server, you need to have the updated policies downloaded to the client computers. In the console, you can configure client computers to use either of the following update methods:

- **Pull mode**: The client computer connects to the management server periodically, depending on the frequency of the heartbeat setting. The client computer checks the status of the management server when the client connects.

- **Push mode**: The client computer establishes a constant HTTP connection to the management server. Whenever a change occurs in the management server status, it notifies the client computer immediately.

In either mode, the client computer takes the corresponding action, based on the change in the status of the management server. Because it requires a constant connection, push mode requires a large amount of network bandwidth. Client computers that are configured to use pull mode require less bandwidth.

See “Configuring push mode or pull mode to update client policies and content” on page 165.
The heartbeat protocol defines the frequency at which client computers upload data such as log entries and download policies. The first heartbeat occurs immediately after the client starts. The next heartbeat occurs at the heartbeat frequency that you set.

The heartbeat frequency is a key factor in the number of clients that each Symantec Endpoint Protection Manager can support. If you set a heartbeat frequency to 30 minutes or less, it limits the total number of clients that Symantec Endpoint Protection Manager can support. For deployments of 1,000 clients or more, Symantec recommends that you set the heartbeat frequency to the maximum length of time possible. Symantec recommends that you use the longest interval that still meets your company’s security requirements. For example, if you want to update policies and gather logs on a daily basis, then you might set the heartbeat frequency to 24 hours. Consult Symantec Professional Services and Symantec Enterprise Support to assess the proper configuration, hardware, and network architecture necessary for your network environment.

**Note:** You can also update polices manually on a client computer.

See “Using the policy serial number to check client-server communication” on page 167.

**Configuring push mode or pull mode to update client policies and content**

You can specify whether Symantec Endpoint Protection Manager pushes the policy down to the clients or that the clients pull the policy from Symantec Endpoint Protection Manager. The default setting is push mode. If you select pull mode, then by default, clients connect to the management server every 5 minutes, but you can change this default heartbeat interval.

See “How the client computers get policy updates” on page 164.

See “Performing the tasks that are common to all policies” on page 151.

You can set the mode for a group or for a location.

**Note:** If you installed Symantec Endpoint Protection Manager on a Windows XP server, note that Windows XP supports a limited number of concurrent users if the clients are in push mode. It is a best practice to use pull mode when you deploy policies to up to 100 clients.
To configure push mode or pull mode for a group

1. In the console, click Clients.
2. Under Clients, select the group for which you want to specify whether to push or pull policies.
3. Click Policies.
4. Uncheck Inherit policies and setting from the parent group "group name".
5. Under Location-independent Policies and Settings pane, under Settings, click Communications Settings.
6. In the Communications Settings for group name dialog box, under Download, verify that Download policies and content from the management server is checked.
7. Do one of the following tasks:
   - Click Push mode.
   - Click Pull mode and under Heartbeat Interval, set the number of minutes or hours.
8. Click OK.

To specify push mode or pull mode for a location

1. In the console, click Clients.
2. Under Clients, select the group for which you want to specify whether to push or pull policies.
3. Click Policies.
4. Uncheck Inherit policies and setting from the parent group "group name".
5. Under Location-specific Policies and Settings, under Location-specific Policies for the location you want to modify, expand Location-specific Settings.
6. Under Location-specific Settings, to the right of Communications Settings, click Tasks and uncheck Use Group Communications Settings.
7. To the right of Communications Settings, click Local - Push or (Local - Pull).
8. Do one of the following tasks:
   - Click Push mode.
   - Click Pull mode and under Heartbeat Interval, set the number of minutes or hours.
9. Click OK.
Using the policy serial number to check client-server communication

To check whether the server and client communicate, check the policy serial number on the console and on the client. If the client communicates with the management server and receives regular policy updates, the serial numbers should match.

If the policy serial numbers do not match, you can try to manually update the policies on the client computer and check the troubleshooting logs.

To view the policy serial number in the console

1. In the console, click Clients.
2. Under Clients, select the relevant group.
   
The policy serial number and policy date appear in the upper right corner of the program window.

   Note: The policy serial number and the policy date also appear at the bottom of the details list on the Details tab.

To view the policy serial number on the client computer

- On the client computer, in the client, click Help > Troubleshooting.

  On the Management tab, look at the policy serial number.

  The serial number should match the serial number on the console for the group that the client computer is in.

See “Performing the tasks that are common to all policies” on page 151.

Manually updating policies on the client

You can manually update the policies on the client computer if you do not think you have the latest policy on the client. If the client does not receive the update, there might be a communication problem.

Check the policy serial number to check whether your managed client computers can communicate with the management server.
You can only manually update the policy on the client computer.

See “Using the policy serial number to check client-server communication” on page 167.

**To manually update policies on the client**

1. On the client computer, click **Help > Troubleshooting**.
2. In the **Troubleshooting** dialog box, in the left column, click **Management**.
3. On the **Management** panel, under **Policy Profile**, click **Update**.

See “Performing the tasks that are common to all policies” on page 151.
Section 4

Installing the Enforcers

- Chapter 12. Installing Enforcer appliances
- Chapter 13. Installation planning for the Gateway Enforcer appliance
- Chapter 14. Installation planning for the LAN Enforcer appliance
- Chapter 15. Upgrading and reimaging all types of Enforcer appliance images
- Chapter 16. Installing the Symantec Network Access Control Integrated Enforcer for Microsoft DHCP Servers
- Chapter 17. Installing the Symantec Integrated Enforcer for Microsoft Network Access Protection
Installing Enforcer appliances

This chapter includes the following topics:

- About the Symantec Network Access Control Enforcer appliances
- What you can do with Symantec Enforcer appliances
- About installing an Enforcer appliance
- Installing an Enforcer appliance
- About the Enforcer appliance indicators and controls
- Setting up an Enforcer appliance
- Logging on to an Enforcer appliance
- Configuring an Enforcer appliance

About the Symantec Network Access Control Enforcer appliances

Symantec Enforcer appliances are the optional network components that work with the Symantec Network Access Control clients.

Symantec Network Access Control comes with the following Linux-based Enforcer images, which you install on the Symantec Enforcer appliances:

- Symantec Network Access Control Gateway Enforcer appliance image
- Symantec Network Access Control LAN Enforcer appliance image
Additionally, all Windows-based Symantec Enforcers work with managed clients to protect your network. These clients include the Symantec Endpoint Protection client and the Symantec Network Access Control client.

See “Installing an Enforcer appliance” on page 173.

See “Installation planning for a Gateway Enforcer appliance” on page 178.

What you can do with Symantec Enforcer appliances

The Enforcer appliance is installed at network endpoints for external clients or internal clients.

For example, you can install an Enforcer appliance between the network and a VPN server. You can also set up enforcement on the client computers that connect to the network with an 802.1x-aware switch or a wireless access point.

An Enforcer appliance performs host authentication rather than user-level authentication. It ensures that the client computers that try to connect to an enterprise network comply with the security policy of that enterprise. You can configure specific security policies on the Symantec Endpoint Protection Manager.

If the client does not comply with the security policies, the Enforcer appliance can take the following actions:

■ Block access to the network.
■ Allow access to limited resources only.
■ Allow access when the client is non-compliant, and log that action.

The Enforcer appliance can redirect the client to a quarantine area with a remediation server. The client can then obtain the required software, applications, signature files, or patches from the remediation server.

For example, part of a network may already be configured for the clients that connect to the local area network (LAN) through 802.1x-aware switches. If that is the case, you can use a LAN Enforcer appliance for these clients.

You can also use a LAN Enforcer appliance for the clients that connect through a wireless access point that is 802.1x-enabled.

See “How the LAN Enforcer appliance works” on page 256.

See “Planning for the installation of a LAN Enforcer appliance” on page 191.

If you have employees who work remotely and connect through a VPN, you can use the Gateway Enforcer appliance for those clients.

You can also use the Gateway Enforcer appliance if a wireless access point is not 802.1x-enabled.
About installing an Enforcer appliance

You select the type of Enforcer appliance that you want to use during the installation process. Before you start to install any of the Enforcer appliances:

- Familiarize yourself with the locations of the components in your network.
- Locate the Symantec Network Access Control Enforcer installation Disc 2. This disc contains the software for all the types of Symantec Network Access Control Enforcer appliances.
- Identify the host name that you want to assign to the Enforcer appliance. The default host name is Enforcer. You may want to change this name to make it easier to identify each Enforcer appliance in a network.
- Identify the IP addresses of the network interface cards (NICs) on the Enforcer appliance.
- Identify the IP address, host name, or domain ID of the Domain Name Server (DNS), if applicable. Only DNS servers can resolve host names. If you want the Enforcer appliance to connect to a Symantec Endpoint Protection Manager by using a host name, it needs to connect to a DNS server.
You can configure the IP address of the DNS server during the installation. However, you can use the configure DNS command to change the IP address of a DNS server from the Enforcer console with the Configure DNS command. See “Installing an Enforcer appliance” on page 173.

Installing an Enforcer appliance

Table 12-1 lists the steps to install all types of Enforcer appliances.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Learn where to place Enforcers in your network.</td>
<td>Enforcers need to be placed in specific locations on your network to ensure that all endpoints comply with your security policy. See “Installation planning for a Gateway Enforcer appliance” on page 178. See “Where to place LAN Enforcer appliances” on page 192.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Set up the appliance.</td>
<td>Connect the Enforcer appliance to your network. See “About installing an Enforcer appliance” on page 172. See “About the Enforcer appliance indicators and controls” on page 173. See “Setting up an Enforcer appliance” on page 174.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Configure the appliance.</td>
<td>Log on and configure the Enforcer appliance from the Enforcer command line. See “Logging on to an Enforcer appliance” on page 175. See “Configuring an Enforcer appliance” on page 176.</td>
</tr>
</tbody>
</table>

About the Enforcer appliance indicators and controls

The Enforcer appliance is installed on a 1U rack-mountable chassis with support for static rails.

You can use the provided serial port and the serial cable to connect to another system that is hooked up to a monitor and keyboard. Alternatively, you can connect a monitor or keyboard directly. If you connect by using the serial port, the default baud rate that is set on the Enforcer is 9600 bps. You must configure the connection on the other system to match. Connecting by the serial port is the preferred method. It lets you transfer files, such as debugging information, to the connected computer for troubleshooting.

See “Installing an Enforcer appliance” on page 173.
Setting up an Enforcer appliance

Set up the Enforcer appliance hardware by connecting it to your network, switching it on, and logging on at the command line.

See “Installing an Enforcer appliance” on page 173.

See “About the Enforcer appliance indicators and controls” on page 173.

To set up an Enforcer appliance

1. Unpack the Enforcer appliance.
2. Mount the Enforcer appliance in a rack or place it on a level surface.
   See the rack mounting instructions that are included with the Enforcer appliance.
3. Plug it into an electrical outlet.
4. Connect the Enforcer appliance by using one of the following methods:
   - Connect another computer to the Enforcer appliance by using a serial port. Use a null modem cable with a DB9 connector (female). You must use terminal software, such as HyperTerminal, CRT, or NetTerm, to access the Enforcer console. Set your terminal software to 9600 bps, data bits 8, no parity, 1 stop bit, no flow control.
   - Connect a keyboard and VGA monitor directly to the Enforcer appliance.
5. Connect the Ethernet cables to the network interface ports as follows:
   - **Gateway Enforcer appliance**
     Connect two Ethernet cables. One cable connects to the eth0 port (internal NIC). The other cable connects to the eth1 port (external NIC) on the rear of the Enforcer appliance.
     The internal NIC connects to the protected network and the Symantec Endpoint Protection Manager. The external NIC connects to the endpoints.
   - **LAN Enforcer appliance**
     Connect one Ethernet cable to the eth0 port on the rear of the Enforcer appliance. This cable connects to the internal network. The internal network connects to an 802.1x-enabled switch and to any additional 802.1x-enabled switches in your network.
6. Switch on the power.
   The Enforcer appliance starts.
Logging on to an Enforcer appliance

When you turn on or restart the Enforcer appliance, the logon prompt for the Enforcer appliance console appears:

Enforcer Login

The following levels of access are available:

- **Superuser**: Access to all commands
- **Normal**: Access only to the `clear`, `exit`, `help`, and `show` commands for each level of the command hierarchy

__________

**Note**: The Enforcer appliance automatically logs users off after 90 seconds of inactivity.

See “Setting up an Enforcer appliance” on page 174.

To log on to an Enforcer appliance with access to all commands

1. On the command line, log on to an Enforcer appliance with access to all commands by typing the following command:
   
   `root`

2. Type the password that you created during the initial installation.
   
   The default password is `symantec`.
   
   The console command prompt for root is `Enforcer#`

To log on to an Enforcer appliance with limited access to commands

1. If you want to log on to an Enforcer appliance with limited access to commands, type the following command on the command line:
   
   `admin`

2. Type the password on the command line.
   
   The default password is `symantec`.
   
   The console command prompt for admin is `Enforcer$`

See “Configuring an Enforcer appliance” on page 176.
Configuring an Enforcer appliance

After you log on to the Enforcer appliance, you can configure the appliance from the Enforcer command-line interface.

To configure an Enforcer appliance

1. Specify the type of Enforcer appliance as follows, responding to the prompts from the Enforcer:

   1. Select Enforcer mode

      Where:

      G       Gateway Enforcer appliance
      L       LAN Enforcer appliance

2. Change the host name of the Enforcer appliance, or press Enter to leave the host name of the Enforcer appliance unchanged.

   The default host name of the Enforcer appliance is Enforcer. The name of the Enforcer appliance automatically registers on the Symantec Endpoint Protection Manager during the next heartbeat.

   At the prompt, type the following command if you want to change the host name of the Enforcer appliance:

   2. Set the host name

   Note:

   1) Input new hostname or press "Enter" for no change. [Enforcer]:

      hostname hostname

      where hostname is the new host name for the Enforcer appliance.

      Be sure to register the host name of the Enforcer appliance on the Domain Name Server itself.

3. Type the following command to confirm the new host name of the Enforcer appliance:

      show hostname

4. Type the IP address of the DNS server and press Enter.
5 Type the new root password at the prompt by first typing the following command:

```
password
Old password: new password
```

You must change the root password that you used to log on to the Enforcer appliance. Remote access is not enabled until you change the password. The new password must be at least nine characters long, and contain one lowercase letter, one uppercase letter, one digit, and one symbol.

6 Type the new admin password.

7 Set the time zone by following these prompts.

Set the time zone
Current time zone is [+0000]. Change it? [Y/n]
If you click 'Y', follow the steps below:
1) Select a continent or ocean
2) Select a country
3) Select one of the time zone regions
4) Set the date and time
Enable the NTP feature [Y/n]
Set the NTP server:
Note: We set up the NTP server as an IP address

8 Set the date and time.

9 Configure the network settings and complete the installation, following the Enforcer prompts.

Enter network settings

Configure eth0:
Note: Input new settings.
IP address []:
Subnet mask []:
Set Gateway? [Y/n]
   Gateway IP[]:

Apply all settings [Y/N]:

See “Logging on to an Enforcer appliance” on page 175.

See “About the Enforcer appliance CLI command hierarchy” on page 372.
Installation planning for the Gateway Enforcer appliance

This chapter includes the following topics:

- Installation planning for a Gateway Enforcer appliance
- Gateway Enforcer appliance NIC settings
- Failover planning for Gateway Enforcer appliances
- Fail-open and fail-closed planning for a Gateway Enforcer appliance

Installation planning for a Gateway Enforcer appliance

A Gateway Enforcer appliance is generally used inline as a secure policy-enforcing bridge to protect a corporate network from external intruders. Before you install a Gateway Enforcer appliance, you need to think about locating it appropriately on the network. Gateway Enforcer appliances can be placed throughout the enterprise to ensure that all endpoints comply with the security policy.

Another use of the Gateway Enforcer appliance is hosting On-Demand Clients for guest-users. These clients are provided with temporary access to the Enforcer, have their security credentials verified, and are then permitted onto the network.

See "How the On-Demand Client works" on page 351.

The Gateway Enforcer in this case is not passing packets through, but rather serving as a host. This capability is not often used, and is thus done from the command line of the Enforcer.

configure > advanced > guest-enf enable

See “About the Enforcer appliance CLI command hierarchy” on page 372.
Note: If you are upgrading from Symantec Sygate Endpoint Protection 5.1 clients, you must upgrade Symantec Endpoint Protection Manager first, then your Enforcers, then your clients, moving them to version 12.1 first. Once you have Symantec Endpoint Protection Manager and your Enforcers at version 11.0, you must check **Allow Legacy Clients** on the Enforcer menu, if you have clients older than 11.0, before you take the final step. Then finish the upgrade to the current release.

Gateway Enforcer appliances typically are in use in the following network locations:

- **VPN**
- **Wireless access point (WAP)**
- **Dial-up (Remote access server [RAS])**
- **Ethernet (local area network [LAN]) segments**

Several types of planning information can help you implement Gateway Enforcer appliances in a network.

General placement:

- See “Where to place a Gateway Enforcer appliance” on page 179.
- See “Guidelines for IP addresses on a Gateway Enforcer appliance” on page 182.
- See “About two Gateway Enforcer appliances in a series” on page 182.

Specific areas of the network:

- See “Protection of VPN access through a Gateway Enforcer appliance” on page 183.
- See “Protection of wireless access points through a Gateway Enforcer appliance” on page 183.
- See “Protection of servers through a Gateway Enforcer appliance” on page 183.
- See “Protection of non-Windows servers and clients through a Gateway Enforcer appliance” on page 184.
- See “Requirements for allowing non-Windows clients without authentication” on page 185.

Where to place a Gateway Enforcer appliance

You can place Gateway Enforcers at locations where all traffic must pass through a Gateway Enforcer before a client can do the following actions:

- Connect to a corporate network.
- Reach the secured areas of a network.
See “Guidelines for IP addresses on a Gateway Enforcer appliance” on page 182.

You typically can place Gateway Enforcer appliances at the following locations:

VPN
   Between virtual private network (VPN) concentrators and the corporate network

Wireless Access Point (WAP)
   Between a wireless access point and the corporate network

Servers
   In front of corporate servers

Larger organizations may require a Gateway Enforcer appliance to protect every network entry point. Gateway Enforcers are typically located in different subnets. In most cases, you can integrate Gateway Enforcer appliances into a corporate network without having to make hardware configuration changes.

Gateway Enforcer appliances must use two network interface cards (NICs).

Figure 13-1 shows how to place Gateway Enforcer appliances in the overall network configuration.
Another location where a Gateway Enforcer appliance protects a network is at a Remote Access Server (RAS). Clients can dial up to connect to a corporate network.
RAS dial-up clients are configured similarly to wireless and VPN clients. The external NIC connects to the RAS server and the internal NIC connects to the network.

Guidelines for IP addresses on a Gateway Enforcer appliance

Follow these guidelines when you set up the internal NIC address for a Gateway Enforcer appliance:

- A Gateway Enforcer appliance’s internal NIC must be able to communicate with a Symantec Endpoint Protection Manager. By default, the internal NIC must face a Symantec Endpoint Protection Manager.

- Clients must be able to communicate with the Gateway Enforcer appliance’s internal IP address. The VPN server or wireless AP can be in a different subnet. This works if the clients can be routed to the same subnet as the Gateway Enforcer appliance’s internal IP address.

- For the Gateway Enforcer appliance that protects internal servers, the internal NIC connects to the VLAN that in turn connects to the servers.

- If you use multiple Gateway Enforcer appliances in a failover configuration, the IP address of the internal NIC on each Gateway Enforcer appliance must have its own IP address.

The Gateway Enforcer generates a bogus external NIC address, based on the internal NIC address. You do not need to configure this address again if you install another Gateway Enforcer.

See “Setting up an Enforcer appliance” on page 174.

About two Gateway Enforcer appliances in a series

If a network supports two Gateway Enforcer appliances in a series so that a client connects to the network through more than one Gateway Enforcer appliance, you must specify the Enforcer appliance that is closest to the Symantec Endpoint Protection Manager as a trusted internal IP address of the other Gateway Enforcer appliance. Otherwise a 5-minute delay can occur before the client can connect to the network.

This delay can occur when the client runs a Host Integrity check that fails. As part of Host Integrity remediation, the client downloads the required software updates. Then the client runs the Host Integrity check again. At that point the Host Integrity check passes, but network access is delayed.

See “Adding a trusted internal IP address for clients on a management server” on page 245.
Protection of VPN access through a Gateway Enforcer appliance

The protection of VPN access is the first and the most common reason to use a Gateway Enforcer appliance. You can place Gateway Enforcer appliances at VPN entry points to secure access to a corporate network. The Gateway Enforcer appliance is placed between the VPN server and the corporate network. It allows access only to authorized users and prevents access by anyone else.

See “Where to place a Gateway Enforcer appliance” on page 179.
See “Setting up an Enforcer appliance” on page 174.

Protection of wireless access points through a Gateway Enforcer appliance

Enforcer appliances protect the corporate network at wireless access points (WAP). The Gateway Enforcer appliance ensures that anyone who connects to the network by using wireless technology runs the client and meets Host Integrity and other security requirements.

After these conditions are met, the client is granted access to the network. The Gateway Enforcer appliance is placed between the WAP and the corporate network. The external NIC points toward the WAP and the internal NIC points toward the corporate network.

See “Where to place a Gateway Enforcer appliance” on page 179.
See “Setting up an Enforcer appliance” on page 174.

Protection of servers through a Gateway Enforcer appliance

Gateway Enforcer appliances can protect the corporate servers that hold sensitive information in the corporate network. An organization may place important data on the servers that may be located in a locked computer room. Only system administrators may have access to the locked computer room.

The Gateway Enforcer appliance acts like an additional lock on the door. It does so by allowing only the users that meet its criteria to access the protected servers. Servers locate the internal NIC in this setup. However, users who try to gain access must pass through the external NIC.

To safeguard these servers, you can limit access only to clients with designated IP addresses and you can set up strict Host Integrity rules. For example, you can configure a Gateway Enforcer appliance to protect servers in a network. A Gateway Enforcer appliance can be located between clients on a corporate LAN and the servers that it safeguards. The external NIC points to the corporate LAN inside the
company and the internal NIC points toward the protected servers. This configuration prevents unauthorized users or clients from gaining access to the servers.

See “Where to place a Gateway Enforcer appliance” on page 179.
See “Setting up an Enforcer appliance” on page 174.

Protection of non-Windows servers and clients through a Gateway Enforcer appliance

You can install the servers and the clients on an operating system other than Microsoft Windows. However, the Gateway Enforcer appliance cannot authenticate any servers and clients that do not run on a computer that does not support Microsoft Windows.

If an organization includes servers and clients with operating systems on which the client software is not installed, you must decide which of the following methods to use:

■ Implement support through a Gateway Enforcer appliance.

■ See “Implementation of non-Windows support through a Gateway Enforcer appliance” on page 184.

■ Implement support without a Gateway Enforcer appliance.

See “Implementation of support for non-Windows clients without a Gateway Enforcer appliance” on page 184.

Implementation of non-Windows support through a Gateway Enforcer appliance

You can implement support for non-Windows clients by configuring the Gateway Enforce appliance to allow all non-Windows clients to access the network. If you configure the Gateway Enforcer appliance in this way, it performs operating system detection to identify the clients that run non-Windows operating systems.

See “Where to place a Gateway Enforcer appliance” on page 179.
See “Setting up an Enforcer appliance” on page 174.

Implementation of support for non-Windows clients without a Gateway Enforcer appliance

You can implement support for non-Windows clients by allowing non-Windows clients to access the network through a separate access point.

You can connect the following clients that support non-Windows operating systems through a separate VPN server:
One VPN Server can support the clients that have the client software installed on them. The Windows-based client computers can connect to the corporate network through a Gateway Enforcer appliance.

Another VPN server can support the clients that run non-Windows operating systems. The non-Windows-based client computer can then connect to the corporate network without a Gateway Enforcer appliance.

See “Where to place a Gateway Enforcer appliance” on page 179.

See “Setting up an Enforcer appliance” on page 174.

Requirements for allowing non-Windows clients without authentication

You can configure the Gateway Enforcer appliance to allow non-Windows clients without authentication.

See “Requirements for Mac and Linux clients” on page 186.

When a client tries to access the network through a Gateway Enforcer appliance, the Enforcer appliance first checks whether the client software has been installed on the client computer. If the client software is not running and if the option to allow non-Windows clients is set, the Gateway Enforcer appliance checks the operating system.

It checks the operating system by sending packets of information to probe the client to detect the type of operating system that it currently runs. If the client runs a non-Windows operating system, the client is allowed regular network access.

Requirements for Windows clients

When a Gateway Enforcer appliance is configured to allow non-Windows clients to connect to a network, it first tries to determine a client’s operating system. If the operating system is a Windows-based operating system, the Gateway Enforcer appliance authenticates the client. Otherwise, the Gateway Enforcer appliance allows the client to connect to the network without authentication.

The Gateway Enforcer appliance correctly detects the Windows operating system if the Windows client meets the following requirements:

- The Client for Microsoft Networks option must be installed and enabled on the client.
  See the Windows documentation.
- The UDP port 137 must be open on the client. It must be accessible by the Gateway Enforcer.

If a Windows client fails to meet these requirements, the Gateway Enforcer appliance may interpret the Windows client to be a non-Windows client. Therefore the Gateway
Enforcer appliance can allow the non-Windows client to connect to the network without authentication.
See “Allowing non-Windows clients to connect to a network without authentication” on page 235.

Requirements for Mac and Linux clients
The Gateway Enforcer appliance must meet the following requirements before it allows a Mac client to connect to a network:

- Windows Sharing must be on.
  This default setting is enabled.
- Mac built-in firewall must be off.
  This setting is the default.

The Gateway Enforcer has the following requirement to allow a Linux client to access the network:

- The Linux system must run the Samba service.

See “Allowing non-Windows clients to connect to a network without authentication” on page 235.

Gateway Enforcer appliance NIC settings
The network interface cards (NICs) on a Gateway Enforcer appliance are configured by default so that eth0 is used for the internal NIC. The internal NIC must connect to the Symantec Endpoint Protection Manager.

You can use the configure interface-role command if you need to change which NIC is external and which is internal.

**Note:** If you use the Gateway Enforcer to download On-Demand Clients and you have enabled 801.Q trunking on the switch, check the NIC connection speed. To successfully download the On-Demand Client, both NICs must connect to the switch with the same connection speed.

See “About the Enforcer appliance CLI command hierarchy” on page 372.

Failover planning for Gateway Enforcer appliances
An enterprise can support two Gateway Enforcer appliances that are configured to continue operations when one of the Gateway Enforcer appliances fails. If a Gateway
Enforcer appliance fails in a network that is not configured for failover, then network access at that location is automatically blocked. If a Gateway Enforcer appliance fails in a network that does not provide for failover, the clients can no longer connect to the network. The clients continue to be blocked from connecting to the network until the problem with the Gateway Enforcer appliance is corrected.

For a Gateway Enforcer appliance, failover is implemented through the Gateway Enforcer appliance itself instead of third-party switches. If the configuration is set up correctly, the Symantec Endpoint Protection Manager automatically synchronizes the settings for the failover Gateway Enforcer appliances.

Note: Failover capabilities are not possible if your Enforcers are set in fail-open mode. Choose to have failover capabilities or fail-open. The choices are mutually exclusive.

See “Setting up Gateway Enforcer appliances for failover” on page 190.
See "Fail-open and fail-closed planning for a Gateway Enforcer appliance" on page 190.

How failover works with Gateway Enforcer appliances in the network

The Gateway Enforcer appliance that is operational is called the active Gateway Enforcer appliance. The backup Gateway Enforcer appliance is called the standby Gateway Enforcer appliance. The active Gateway Enforcer appliance is also referred to as the primary Gateway Enforcer appliance. If the active Gateway Enforcer appliance fails, the standby Gateway Enforcer appliance takes over the enforcement tasks.

The sequence in which the two Gateway Enforcer appliances are started is as follows:

- When the first Gateway Enforcer appliance is started, it runs in standby mode. While in standby mode, it queries the network to determine whether another Gateway Enforcer appliance runs. It sends out three queries to search for another Gateway Enforcer. Therefore it can take a few minutes to change its status to Online.

- If the first Gateway Enforcer appliance does not detect another Gateway Enforcer appliance, the first Gateway Enforcer appliance becomes the active Gateway Enforcer appliance.

- While the active Gateway Enforcer appliance runs, it broadcasts failover packets on both the internal and the external networks. It continues to broadcast the failover packets.
As soon as the second Gateway Enforcer appliance is started, it runs in standby mode. It queries the network to determine whether another Gateway Enforcer appliance runs.

The second Gateway Enforcer appliance then detects the active Gateway Enforcer appliance that is running and therefore remains in standby mode.

If the active Gateway Enforcer appliance fails, it stops to broadcast failover packets. The standby Gateway Enforcer appliance no longer detects an active Gateway Enforcer appliance. Therefore it now becomes the active Gateway Enforcer appliance that handles network connections and security at this location.

If you start the other Gateway Enforcer appliance, it remains the standby Gateway Enforcer appliance because it detects that another Gateway Enforcer appliance is active.

See “Setting up Gateway Enforcer appliances for failover” on page 190.

Where to place Gateway Enforcer appliances for failover in a network with one or more VLANs

You set up a Gateway Enforcer appliance for failover by its physical location and by the configuration that you perform on the Symantec Endpoint Protection Manager. If you use a hub that supports multiple VLANs, you can use only one VLAN unless you integrate an 802.1Q-aware switch instead of a hub.

The Gateway Enforcer appliance for failover must be set up on the same network segment. A router or gateway cannot be installed between the two Gateway Enforcer appliances. A router or gateway does not forward the failover packet. The internal NICs must both connect to the internal network through the same switch or hub. The external NICs must both connect to the external VPN server or access point through the same switch or hub.

You use similar processes to configure Gateway Enforcer appliances for failover at a wireless AP, dial-up RAS, or other access points. The external NICs of both Gateway Enforcer appliances connect to the external network through a wireless AP or RAS server. The internal NICs connect to the internal network or area that is protected.

Figure 13-2 shows how to set up two Gateway Enforcer appliances for failover to protect network access at a VPN concentrator.
Figure 13-2  Placement of two Gateway Enforcer appliances

See “Setting up Gateway Enforcer appliances for failover” on page 190.
Setting up Gateway Enforcer appliances for failover

You should familiarize yourself with the concepts that are involved in Gateway Enforcer appliance failover before you set up standby Enforcers.

See "How failover works with Gateway Enforcer appliances in the network" on page 187.

To set up Gateway Enforcer appliances for failover

1. Place the computers in the network.
   
   See "Where to place Gateway Enforcer appliances for failover in a network with one or more VLANs" on page 188.

2. Set up the internal NICs.
   
   The internal NICs on multiple Gateway Enforcer appliances must each have a different IP address.
   
   See "Guidelines for IP addresses on a Gateway Enforcer appliance" on page 182.

Fail-open and fail-closed planning for a Gateway Enforcer appliance

Fail-open is available for Gateway Enforcer appliance models with a fail-open NIC. Fail-open is an alternative to failover that provides network availability when the Enforcer service is not available.

---

**Note:** Beginning with Symantec Network Access Control version 11.0 RU6 MP1, Enforcers will ship with a Silcom NIC card that is in configured in fail-open mode. To configure the Enforcer to be in fail-closed mode, issue the following CLI command:

```
configure interface failopen disable
```

---

**Note:** Failover capabilities are not possible if your Enforcers are set in fail-open mode. Choose to have failover capabilities or fail-open. The choices are mutually exclusive.

See "Installing an Enforcer appliance" on page 173.

See "Failover planning for Gateway Enforcer appliances" on page 186.
Installation planning for the LAN Enforcer appliance

This chapter includes the following topics:

- Planning for the installation of a LAN Enforcer appliance
- Failover planning for LAN Enforcer appliances and RADIUS servers

Planning for the installation of a LAN Enforcer appliance

The LAN Enforcer appliance can perform host authentication and act as a pseudo-RADIUS server (even without a RADIUS server). The Enforcement client acts as an 802.1x supplicant. It responds to the switch’s Extensible Authentication Protocol (EAP) challenge with the Host Integrity status and policy number information. The RADIUS server IP address is set to 0 in this case, and no traditional EAP user authentication takes place. The LAN Enforcer appliance checks Host Integrity. It can allow, block, or dynamically assign a VLAN, based on the results of the Host Integrity check.

Another configuration is also available. You can use a LAN Enforcer appliance with a RADIUS server to enforce 802.1x EAP authentication internally in a corporate network. If a LAN Enforcer appliance is used in this configuration, you need to position it so that it can communicate with the RADIUS server.

If your switch supports dynamic VLAN switching, additional VLANs can be configured on the switch and accessed through the LAN Enforcer appliance. The switch can dynamically put the client into a VLAN that is based on the reply from the LAN Enforcer appliance. You may want to add VLANs for quarantine and remediation.
Several types of planning information can help you implement LAN Enforcer appliances in a network.

**Note:** If you are upgrading from Symantec Sygate Endpoint Protection 5.1 clients, you must upgrade Symantec Endpoint Protection Manager first, then your Enforcers, then your clients, moving them to version 11.0 first. Once you have Symantec Endpoint Protection Manager and your Enforcers at version 11.0, you must check **Allow Legacy Clients** on the Enforcer menu before you take the final step. Then finish the upgrade to the current release.

See “Where to place LAN Enforcer appliances” on page 192.

### Where to place LAN Enforcer appliances

A LAN Enforcer appliance acts as a RADIUS proxy. Administrators typically use a LAN Enforcer appliance with a RADIUS server to enforce 802.1x Extensible Authentication Protocol (EAP) authentication in a corporate network. If you use a LAN Enforcer appliance in this configuration, the LAN Enforcer appliance must be able to communicate with the RADIUS server.

For example, you can connect a LAN Enforcer appliance to an 802.1x-aware LAN switch on an internal VLAN with a Symantec Endpoint Protection Manager, RADIUS server, and clients. A computer that does not have the client software cannot connect to the network. However, the client is directed to a remediation server from which it can obtain the software that it needs to become compliant.

See “Setting up an Enforcer appliance” on page 174.

**Figure 14-1** shows an example of where you can place a LAN Enforcer appliance in the overall internal network configuration.
If a switch supports dynamic VLAN switching, additional VLANs can be configured on the 802.1x-aware switch and accessed through the LAN Enforcer appliance. The 802.1x-aware switch can dynamically put the client into a VLAN after it receives a reply from the RADIUS server. Some 802.1x-aware switches also include a default VLAN or guest VLAN feature. If a client has no 802.1x supplicant, the 802.1x-aware switch can put the client into a default VLAN.
You can install the LAN Enforcer appliance so that you can enable EAP authentication throughout the network with the equipment that is already deployed. LAN Enforcer appliances can work with existing RADIUS servers, 802.1x supplicants, and 802.1x-aware switches. They perform the computer level authentication. It makes sure that the client complies with security policies.

For example, it checks that antivirus software has been updated with the latest signature file updates and the required software patches. The 802.1x supplicant and the RADIUS server perform the user-level authentication. It authenticates the clients who try to connect to the network are the ones who they claim to be.

Alternatively, a LAN Enforcer appliance can also work in transparent mode, removing the need for a RADIUS server. In transparent mode, the client passes Host Integrity information to the 802.1x-aware switch in response to the EAP challenge. The switch then forwards that information to the LAN Enforcer. A LAN Enforcer appliance then sends authentication results back to the 802.1x-aware switch. The information that the LAN Enforcer appliance sends is based on the Host Integrity validation results. Therefore the LAN Enforcer appliance requires no communication with a RADIUS server.

The following configurations are available for a LAN Enforcer appliance:

- **Full 802.1x mode**
  This configuration requires a RADIUS server and third-party 802.1x supplicants. Both traditional EAP user authentication and Symantec Host Integrity validation are performed.

- **Transparent mode**
  This configuration does not require a RADIUS server or the use of a third-party 802.1x supplicants. Only Host Integrity validation is performed.

You can consider the following issues:

- **Do you have clients such as printers and IP phones that do not have 802.1x supplicants running on them?**
  Consider using MAB authentication.

- **Do you have clients such as printers and IP phones that have custom 802.1x supplicants running on them?**
  Consider configuring the ignore Symantec NAC Client checking.

- **Do you plan to have an 802.1x supplicant installed on every computer?**
  If you plan to have an 802.1x supplicant installed on every computer, you can use the Full 802.1x mode.

- **Do you want to perform a user level authentication in addition to the Host Integrity check?**
  If you want to perform a user level authentication in addition to the Host Integrity check, you must use the Full 802.1x mode.
Do you plan to use a RADIUS server in a network configuration?
If you plan to use a RADIUS server in a network configuration, you can use either the Full 802.1x mode or transparent mode. If you do not plan to use a RADIUS server in a network configuration, you must use the transparent mode.

Failover planning for LAN Enforcer appliances and RADIUS servers

If you have installed two LAN Enforcer appliances in a network, failover is handled through the 802.1x-aware switch. An 802.1x-aware switch can support multiple LAN Enforcer appliances. You can easily synchronize the settings of LAN Enforcer appliances on the Symantec Endpoint Protection Manager through the use of synchronization settings.

If you want to synchronize the settings of one LAN Enforcer appliance with another LAN Enforcer appliance, specify the same group Enforcer name on the Enforcer console.

If you use a RADIUS server in your network, provide for RADIUS server failover by configuring the LAN Enforcer appliance to connect to multiple RADIUS servers. If all the RADIUS servers that are configured for that LAN Enforcer appliance become disabled, the switch assumes that the LAN Enforcer appliance is disabled. Therefore, the 802.1x-aware switch connects to a different LAN Enforcer appliance that provides additional failover support.

See “Configuring an Enforcer appliance” on page 176.

Where to place RADIUS servers for failover in a network

Figure 14-2 describes how to provide failover for LAN Enforcer appliances.
Figure 14-2 Placement of two RADIUS servers

Installation planning for the LAN Enforcer appliance
Failover planning for LAN Enforcer appliances and RADIUS servers
See “Failover planning for LAN Enforcer appliances and RADIUS servers” on page 195.
Upgrading and reimaging all types of Enforcer appliance images

This chapter includes the following topics:

- About upgrading and reimaging Enforcer appliance images
- Enforcer hardware compatibility matrix
- Determining the current version of an Enforcer appliance image
- Upgrading the Enforcer appliance image
- Reimaging an Enforcer appliance image

About upgrading and reimaging Enforcer appliance images

Determine the version of your Enforcer appliance software before you plan to upgrade or reimage any of the Enforcer appliance software.

See “Determining the current version of an Enforcer appliance image” on page 199.

You may need to upgrade the image of an Enforcer appliance to the current version if you want to connect to the most current version of Symantec Endpoint Protection Manager. The upgrade enables you to take advantage of the new features that the Symantec Network Access Control Enforcer appliance provides. The Enforcer appliances work with Symantec Endpoint Protection Manager 11.0 and all subsequent versions and release updates.
You can select any of the following methods to upgrade the Enforcer appliance image:

- Upgrade the current Enforcer appliance image.
  See “Upgrading the Enforcer appliance image” on page 200.
- Install a different Enforcer appliance image over a previous Enforcer appliance image.
  See “Reimaging an Enforcer appliance image” on page 200.

Enforcer hardware compatibility matrix

Enforcer hardware compatibility matrix lists Symantec Network Access Control appliance image releases and their level of testing and support for Dell Enforcer appliance hardware models.

<table>
<thead>
<tr>
<th>Image version</th>
<th>Dell PE 850</th>
<th>Dell PE 860</th>
<th>Dell R200</th>
<th>Dell R210</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image version 12.1.x</td>
<td>Not supported</td>
<td>Partially tested and fully supported</td>
<td>Fully tested and fully supported</td>
<td>Fully tested and fully supported</td>
</tr>
<tr>
<td>Image version 11.0.6100 and above (RU6 MP1 and above)</td>
<td>Partially tested and fully supported</td>
<td>Partially tested and fully supported</td>
<td>Fully tested and fully supported</td>
<td>Fully tested and fully supported</td>
</tr>
<tr>
<td>Image version 11.0.6</td>
<td>Fully tested and fully supported</td>
<td>Fully tested and fully supported</td>
<td>Fully tested and fully supported</td>
<td>Not supported</td>
</tr>
<tr>
<td>Image versions 11.0.2, 11.0.3, 11.0.4, and 11.0.5</td>
<td>Fully tested and fully supported</td>
<td>Fully tested and fully supported</td>
<td>Fully tested and fully supported</td>
<td>Not supported</td>
</tr>
<tr>
<td>Image version 11.0.0, 11.0.1</td>
<td>Fully tested and fully supported</td>
<td>Fully tested and fully supported</td>
<td>Not supported</td>
<td>Not supported</td>
</tr>
</tbody>
</table>

Determining the current version of an Enforcer appliance image

You should determine the current version of the image that is supported on the Enforcer appliance. You should try to upgrade if you do not have the latest version.

To check the current version of an Enforcer appliance image, type the following command on the command-line interface of an Enforcer appliance: `show version`

See “About the Enforcer appliance CLI command hierarchy” on page 372.
Upgrading the Enforcer appliance image

You can use any of the following methods to upgrade an Enforcer appliance image to the latest image:

- Upgrade the Enforcer appliance image from 5.1.x to the current version with a USB (Universal Serial Bus) disk.
- Upgrade the Enforcer appliance image from 5.1.x to the current version from a TFTP server.

To upgrade the Enforcer appliance image from 5.1.x with a USB disk
1 Copy the two update files, initrd-Enforcer.img.gpg and package list, to a USB disk.
2 Type the following command to automatically upgrade the Enforcer appliance:
   Enforcer# update

To upgrade the Enforcer appliance image from 5.1.x with a TFTP server
1 Upload the two update files, initrd-Enforcer.img.gpg and package list to a Trivial File Transfer Protocol (TFTP) server to which an Enforcer appliance can connect.
2 Run the following command on the console of the Enforcer appliance:
   Enforcer: # update tftp://IP address of TFTP server
3 Select Y when you are prompted to launch the new image.
4 Select 1 to restart the Enforcer appliance after you apply a new image.
   Do not launch the new image without restarting the Enforcer appliance.
5 Log on to the Enforcer appliance.
   See “Logging on to an Enforcer appliance” on page 175.

See “About the Enforcer appliance CLI command hierarchy” on page 372.

Reimaging an Enforcer appliance image

The Enforcer appliance comes with reimaging software for all Enforcer appliances: Gateway and LAN. The reimaging software includes the hardened Linux operating system and the Enforcer appliance software for replacement of an Enforcer appliance image.

When you start the installation from the product installation file, the reimaging process erases the existing configuration on the Enforcer appliance. New files are
installed over all existing files. Any configuration that was previously set on the Enforcer appliance is lost.

You can install a different type of Enforcer appliance image if you want to change the type that you use. If you change the type of Enforcer appliance image, it may involve the relocation of an Enforcer appliance in the corporate network.

When you reimage an Enforcer, you should also discard all group information related to that Enforcer that was stored in Symantec Endpoint Protection Manager. You are starting from the beginning with the new type of Enforcer. The Enforcer discards all previous Symantec Endpoint Protection Manager group information completely. You must create a new share key, and Symantec Endpoint Protection Manager group information should be re-configured manually as needed to ensure proper coordination.

To reimage an Enforcer appliance

1. Download the installation file to the Enforcer appliance.

2. On the command line, type the following command:
   
   Enforcer:# reboot
   
   This command restarts the Enforcer appliance.

3. In the Setup menu, select Setup Symantec Enforcer from the product installation file.
   
   If you do not use the Setup menu, the Enforcer appliance restarts from the hard disc instead of the product installation file. To reimage, you must restart from the installation file.

4. Install and configure the Enforcer appliance.
   
   See “About installing an Enforcer appliance” on page 172.
Installing the Symantec Network Access Control Integrated Enforcer for Microsoft DHCP Servers

This chapter includes the following topics:

- **Process for installing the Symantec Network Access Control Integrated Enforcer for Microsoft DHCP Server**
- **How to get started with the installation of an Integrated Enforcer for Microsoft DHCP servers**
- **System requirements for an Integrated Enforcer for Microsoft DHCP Servers**
- **Components for an Integrated Enforcer for Microsoft DHCP servers**
- **Placement requirements for an Integrated Enforcer for Microsoft DHCP Servers**
- **Installing an Integrated Enforcer for Microsoft DHCP Servers**

**Process for installing the Symantec Network Access Control Integrated Enforcer for Microsoft DHCP Server**

*Table 16-1* lists the steps to install the Symantec Network Access Control Integrated Enforcer for Microsoft DHCP servers.
Table 16-1  Installation summary for the Symantec Network Access Control Integrated Enforcer for Microsoft DHCP server

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Read the system requirements and the installation requirements.</td>
<td>Identifies the hardware, software, and Symantec Network Access Control components you need to obtain to run the Enforcer and helps you plan for its placement on your network.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “System requirements for an Integrated Enforcer for Microsoft DHCP Servers” on page 205.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Components for an Integrated Enforcer for Microsoft DHCP servers” on page 206.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Install the Symantec Endpoint Protection Manager.</td>
<td>Installs the application that you use to support the Enforcer on your network.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Install the Symantec Network Access Control Integrated Enforcer for Microsoft DHCP server.</td>
<td>Installs the Symantec Network Access Control Integrated Enforcer for Microsoft DHCP server components.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Installing an Integrated Enforcer for Microsoft DHCP Servers” on page 208.</td>
</tr>
</tbody>
</table>

How to get started with the installation of an Integrated Enforcer for Microsoft DHCP servers

The documentation describes how to install, configure, and use the Integrated Enforcer for Microsoft DHCP Servers. Perform the following tasks to get started:
## Table 16-2  Process for installing an Integrated Enforcer for Microsoft DHCP servers

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 1| Locate the Symantec Network Access Control installation components. | Describes the components that are needed for the installation of an Integrated Enforcer for Microsoft DHCP servers.  
See “Components for an Integrated Enforcer for Microsoft DHCP servers” on page 206.                                                                 |
| Step 2| Obtain the required hardware.                                | Lists the hardware requirements for an Integrated Enforcer for Microsoft DHCP servers.  
See “System requirements for an Integrated Enforcer for Microsoft DHCP Servers” on page 205.                                                          |
| Step 3| Obtain the required operating system.                        | Lists the operating system requirements that for an Integrated Enforcer for Microsoft DHCP servers.                                                                                                        |
| Step 4| Place the Integrated Enforcer for Microsoft DHCP servers on your network. | Explains where to place an Integrated Enforcer for Microsoft DHCP servers in a network.  
See “Placement requirements for an Integrated Enforcer for Microsoft DHCP Servers” on page 206.                                                  |
| Step 5| Install an Integrated Enforcer for Microsoft DHCP server    | Explains how to install an Integrated Enforcer for Microsoft DHCP servers.  
See “Installing an Integrated Enforcer for Microsoft DHCP Servers” on page 208.                                                                         |
| Step 6| Configure the Integrated Enforcer for Microsoft DHCP servers | Explains how to configure the connections and settings of an Integrated Enforcer for Microsoft DHCP servers on an Enforcer console.  
See “About configuring Integrated Enforcers on an Enforcer console” on page 307.                                                                         |
System requirements for an Integrated Enforcer for Microsoft DHCP Servers

Table 16-3 summarizes the minimum requirements for the computers on which you install the Integrated Enforcer for Microsoft DHCP Servers.

Table 16-3 Integrated Enforcer for Microsoft DHCP Servers system requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware</td>
<td>For installations of up to 10,000 users, use the following recommended requirements:</td>
</tr>
<tr>
<td></td>
<td>■ Pentium III 750 MHz</td>
</tr>
<tr>
<td></td>
<td>■ 256 MB of memory</td>
</tr>
<tr>
<td></td>
<td>■ 120 MB of disk space</td>
</tr>
<tr>
<td></td>
<td>■ Fast Ethernet network adapters</td>
</tr>
<tr>
<td></td>
<td>■ One network interface card (NIC) with TCP/IP installed</td>
</tr>
<tr>
<td></td>
<td>For installations of 10,000 users or greater, use the following recommended requirements:</td>
</tr>
<tr>
<td></td>
<td>■ Pentium 4 2.4 GHz</td>
</tr>
<tr>
<td></td>
<td>■ 512 MB of memory</td>
</tr>
<tr>
<td></td>
<td>■ 512 MB of disk space</td>
</tr>
<tr>
<td></td>
<td>■ 1-GB network adapters</td>
</tr>
<tr>
<td></td>
<td>■ 800 x 600 resolution monitor with 256 colors (minimum)</td>
</tr>
<tr>
<td></td>
<td>■ One network interface card (NIC) with TCP/IP installed</td>
</tr>
<tr>
<td>Operating system</td>
<td>The Integrated Enforcer requires that the Microsoft DHCP server and the following 32-bit and 64-bit operating systems are installed:</td>
</tr>
<tr>
<td></td>
<td>■ Windows Server 2003 Service Pack</td>
</tr>
<tr>
<td></td>
<td>■ Windows Server 2003 Service Pack 1</td>
</tr>
<tr>
<td></td>
<td>■ Windows Server 2003 x64</td>
</tr>
<tr>
<td></td>
<td>■ Windows Server 2008</td>
</tr>
<tr>
<td></td>
<td>■ Windows Server 2008 x64</td>
</tr>
<tr>
<td></td>
<td>■ Windows Server 2008 R2</td>
</tr>
<tr>
<td></td>
<td>■ Windows Server 2012</td>
</tr>
<tr>
<td></td>
<td>■ Windows Server 2012 R2</td>
</tr>
</tbody>
</table>
Components for an Integrated Enforcer for Microsoft DHCP servers

The Integrated Enforcer for Microsoft DHCP servers works with the Microsoft DHCP server, Symantec Endpoint Protection Manager, and the Symantec Network Access Control client. It verifies that the clients that try to connect to the network comply with configured security policies.

Table 16-4 shows the components that are required for using the Integrated Enforcer for Microsoft DHCP servers:

Table 16-4 Components for Symantec Network Access Control Integrated Enforcer for Microsoft DHCP servers

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symantec Endpoint Protection Manager</td>
<td>Creates the security policies in a centralized location and assigns them to clients.</td>
</tr>
<tr>
<td>Symantec Network Access Control client</td>
<td>Protects the end users by enforcing the security policies that the Integrated Enforcer for Microsoft DHCP servers provides.</td>
</tr>
<tr>
<td>Microsoft DHCP server</td>
<td>Provides DHCP addresses to clients.</td>
</tr>
<tr>
<td>Integrated Enforcer for Microsoft DHCP servers (installed on the same computer as the DHCP service)</td>
<td>Authenticaates the clients and enforces the security policies.</td>
</tr>
</tbody>
</table>

Placement requirements for an Integrated Enforcer for Microsoft DHCP Servers

Figure 16-1 illustrates how to place the Integrated Enforcer for Microsoft DHCP Servers, the Microsoft DHCP Server, and the Symantec Endpoint Protection Manager, as well as internal or remote clients in a network.
Figure 16-1 Placement of Symantec Network Access Control Integrated Enforcer for Microsoft DHCP Servers

Symantec Endpoint Protection Manager

Clients

Relay Agent

Protected Servers

Corporate Backbone

Hub/Switch

DHCP Server with Integrated Enforcer
Installing an Integrated Enforcer for Microsoft DHCP Servers

You must install an Integrated Enforcer for Microsoft DHCP servers on the same computer on which you have already installed the following:

- A Microsoft Windows server operating system
- The DHCP service

You must log in as an administrator or as a user in the administrators group.

---

**Note:** After installing the Microsoft DHCP server, you must configure the Integrated Enforcer for Microsoft DHCP servers. The Integrated Enforcer for Microsoft DHCP servers can then connect to the Symantec Endpoint Protection Manager.

---

**To install the Integrated Enforcer for Microsoft DHCP Servers with a Wizard**

1. From the product installation files, double-click one of the following, based on whether the operating system is 32-bit or 64-bit:
   - `IntegratedEnforcerInstaller86.exe` (32-bit)
   - `IntegratedEnforcerInstaller64.exe` (64-bit)

   You must exit the installation and install the DHCP server if you see the following message:

   You must have the DHCP server on this machine to install this product. To install the DHCP server, in the Control Panel, use the Add/Remove Windows Components Wizard.

   If the DHCP server is already installed, the **Welcome to Symantec Integrated Enforcer Installation Wizard** appears.

2. In the **Welcome** panel, click **Next**.

3. In the **License Agreement** panel, click **I accept the license agreement**.

4. Click **Next**.

5. In the **Destination Folder** panel, perform one of the following tasks:

   - If you want to accept the default destination folder, click **Next**.
   - Click **Browse**, locate and select a destination folder, click **OK**, and click **Next**.
6 If the **Role Selection** panel appears, select **DHCP Enforcement for Microsoft DHCP Server** and click **Next**.

The **Role Selection** panel only appears if more than one type of Symantec Network Access Control Integrated Enforcer can be installed based on the services running on the server.

7 In the **Ready to Install the Application** panel, click **Next**.

8 When you are prompted to restart the DHCP server, perform one of the following tasks:

- To restart the DHCP server immediately, click **Yes**.
- To restart the DHCP server manually later, click **No**.

  If you restart the DHCP server later, you must stop and then start it.

You must restart the DHCP server or the Symantec Integrated Enforcer does not function.

See “**Stopping and starting the Microsoft DHCP Server manually**” on page 211.

9 Click **Finish**.

If you need to reinstall the Integrated Enforcer, you must first uninstall it.

See “**Uninstalling the Symantec Network Access Control Integrated Enforcer for Microsoft DHCP servers**” on page 210.

To install the Integrated Enforcer for Microsoft DHCP Servers from the command line

1 To begin the command-line installation, open a DOS command prompt.

  The command-line installation process uses only default settings.

2 At the command line, specify the directory in which the Integrated Enforcer Installer is located.

  The install location defaults to one of the following:

  - C:\Program Files\Symantec\Symantec Endpoint Protection\Integrated Enforcer for 32-bit operating systems
  - C:\Program Files (x86)\Symantec\Symantec Endpoint Protection\Integrated Enforcer for 64-bit operating systems

3 Type `IntegratedEnforcerInstaller86.exe /qr` (for 32-bit operating systems)

  or `IntegratedEnforcerInstaller64.exe /qr` (for 64-bit operating systems) at the command line and type: **Enter**.
Uninstalling the Symantec Network Access Control Integrated Enforcer for Microsoft DHCP servers

You can uninstall the Symantec Network Access Control Integrated Enforcer for Microsoft DHCP servers from the Windows taskbar or the command line.

To uninstall the Integrated Enforcer for Microsoft DHCP Servers

1. On the Windows taskbar, click **Start > Control Panel > Add or Remove Programs**.
2. Click **Symantec NAC Integrated Enforcer**, and then click **Remove**.
3. When asked whether you want to remove the software, click **Yes**.
4. When asked whether you want to restart the DHCP server, do one of the following tasks:
   - To restart the DHCP server immediately, click **Yes**.
   - To restart the DHCP server manually later (the default), click **No**.
     If you restart the DHCP server later, you must stop and then start it.
     You must restart the DHCP server to completely uninstall the Symantec Integrated Enforcer.

To uninstall the Integrated Enforcer for Microsoft DHCP Servers from the command line

1. Open a DOS command prompt.
2. At the command prompt, type:
   
   `misexec.exe /qn /X <filename>`
   The filename should be under Program Files\Common Files\Wise Installation Wizard.

Upgrading the Integrated Enforcer for Microsoft DHCP Servers

The following steps detail how to upgrade to a Symantec Network Access Control Integrated Enforcer for Microsoft DHCP Servers:

Table 16-5  Upgrade steps for the Integrated Enforcer for Microsoft DHCP Servers

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Uninstall the old version.</td>
<td>Uninstall the existing version of the Integrated Enforcer. See “Uninstalling the Symantec Network Access Control Integrated Enforcer for Microsoft DHCP servers” on page 210.</td>
</tr>
</tbody>
</table>
Table 16-5  Upgrade steps for the Integrated Enforcer for Microsoft DHCP Servers (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Install the new version.</td>
<td>Install the new version of the Integrated Enforcer.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Installing an Integrated Enforcer for Microsoft DHCP Servers” on page 208.</td>
</tr>
</tbody>
</table>

**Note:** Migration is not supported. You must uninstall the old version and install the new one.

**Stopping and starting the Microsoft DHCP Server manually**

Stop the Microsoft DHCP Server manually before upgrading to a new version of the Integrated Enforcer for Microsoft DHCP Servers. You then restart it after you complete the upgrade.

**To stop and start the Microsoft DHCP Server manually**

1. On the Windows taskbar, click **Start > Control Panel > Administrative Tools > Services**.
2. Right-click **DHCP Server** and click **Stop**.
3. Click **Start**.
Installing the Symantec Integrated Enforcer for Microsoft Network Access Protection

This chapter includes the following topics:

- Before you install the Symantec Integrated Enforcer for Microsoft Network Access Protection
- Process for installing the Symantec Network Access Control Integrated Enforcer for Microsoft Network Access Protection
- System requirements for an Integrated Enforcer for Microsoft Network Access Protection
- Components of a Symantec Integrated Enforcer for Microsoft Network Access Protection
- Installing the Integrated Enforcer for Microsoft Network Access Protection

Before you install the Symantec Integrated Enforcer for Microsoft Network Access Protection

Before you install the Symantec Integrated Enforcer for Microsoft Network Access Protection, you must have completed the following installation and configuration tasks:

- Installation of Symantec Endpoint Protection Manager
Note: You install Symantec Endpoint Protection Manager before you install the Symantec Integrated Enforcer for Network Access Protection. Symantec Endpoint Protection Manager must be installed before the Symantec Integrated Enforcer for Microsoft Network Access Protection can work properly.

See “Installing Symantec Endpoint Protection Manager” on page 51.

- Verification of hardware and software requirements for the computer on which you plan to install the following components:
  - DHCP server service
  - Network Access Protection Server service
  - Domain controller
  - Symantec Integrated Enforcer for Microsoft Network Access Protection


Process for installing the Symantec Network Access Control Integrated Enforcer for Microsoft Network Access Protection

Table 17-1 lists the steps to install the Symantec Network Access Control Integrated Enforcer for Microsoft Network Access Protection.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 1 | Read the system requirements and the installation requirements. | Identifies the hardware, software, and Symantec Network Access Control components you need to obtain to run the Enforcer and plan its placement on your network.  
See “System requirements for an Integrated Enforcer for Microsoft Network Access Protection” on page 214.  
Table 17-1 Installation summary for the Symantec Network Access Control Integrated Enforcer for Microsoft Network Access Protection (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Install the Symantec Endpoint Protection Manager.</td>
<td>Installs the application that you use to support the Enforcer on your network. See “Installing Symantec Endpoint Protection Manager” on page 51.</td>
</tr>
</tbody>
</table>

System requirements for an Integrated Enforcer for Microsoft Network Access Protection

Table 17-2 summarizes the minimum requirements for the computers on which you install the Integrated Enforcer for Microsoft Network Access Protection.
## Table 17-2 Integrated Enforcer for Microsoft Network Access Protection system requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirement</th>
</tr>
</thead>
</table>
| Hardware   | Note: The type of NAP enforcement you plan to use affect your hardware choices. The following are guidelines. For installations of up to 10,000 users, use the following recommended requirements:  
- Pentium III 750 MHz  
- 256 MB of memory  
- 120 MB of disk space  
- Fast Ethernet network adapters  
- One network interface card (NIC) with TCP/IP installed  
For installations of 10,000 users or greater, use the following recommended requirements:  
- Pentium 4 2.4 GHz  
- 512 MB of memory  
- 512 MB of disk space  
- 1-GB network adapters  
- 800 x 600 resolution monitor with 256 colors (minimum)  
- One network interface card (NIC) with TCP/IP installed |
Table 17-2 Integrated Enforcer for Microsoft Network Access Protection system requirements (continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating system</td>
<td>Ensure that the following operating system and services are installed:</td>
</tr>
<tr>
<td></td>
<td>■ Windows Server 2008 Standard Edition</td>
</tr>
<tr>
<td></td>
<td>■ Windows 2008 R2</td>
</tr>
<tr>
<td></td>
<td>■ You can select one of the following configurations:</td>
</tr>
<tr>
<td></td>
<td>■ Windows Server 2008 DHCP service if you plan to use DHCP enforcement. The Windows Server 2008 DHCP service should be located on the same computer as the Windows Server 2008 Network Policy Server.</td>
</tr>
<tr>
<td></td>
<td>■ Windows DHCP service if you plan to use 802.1x enforcement. The Windows DHCP service can be located on the same computer as the Windows Server 2008 Network Policy Server. You can also configure the DHCP service on a separate computer that you have configured as a Windows 2008 DHCP server or a Windows 2003 DHCP server.</td>
</tr>
<tr>
<td></td>
<td>■ Windows Server 2008 Network Policy Server (NPS) service</td>
</tr>
</tbody>
</table>

Components of a Symantec Integrated Enforcer for Microsoft Network Access Protection

The Symantec Integrated Enforcer for Microsoft Network Access Protection works with the Microsoft DHCP Server, Symantec Endpoint Protection Manager, and the Symantec Network Access Control client with Network Access Protection enabled. The Symantec Integrated Enforcer for Microsoft Network Access Protection verifies that the clients comply with configured security policies before any clients can connect to a network.

The following required components must be installed before you can use the Symantec Integrated Enforcer for Network Access Protection:

Symantec Endpoint Protection Manager  Required to create security policies in a centralized location and assign them to clients.
Installing the Symantec Integrated Enforcer for Microsoft Network Access Protection

You must install the Integrated Enforcer for Microsoft Network Access Protection on the same computer on which the Microsoft Network Policy Server is installed. You must log in as an administrator or a user in the administrators group.

**Note:** After you complete the installation of the Symantec Integrated NAP Enforcer, you must connect to Symantec Endpoint Protection Manager.

To install the Integrated Enforcer for Microsoft Network Access Protection with the Installation Wizard

1. From the product installation files, double-click one of the following, based on whether the operating system is 32-bit or 64-bit:
   - **IntegratedEnforcerInstaller86.exe** (32-bit)
   - **IntegratedEnforcerInstaller64.exe** (64-bit)

   You must exit the installation and install the NPS server if the NPS server is not already installed.

   If the NAP Server service is already installed, the **Welcome to Symantec Integrated NAP Enforcer Installation Wizard** appears.

2. In the **Welcome** panel, click **Next**.
3 In the License Agreement panel, click I accept the license agreement, and then click Next.

4 In the Destination Folder panel, perform one of the following tasks:
   - If you want to accept the default destination folder, click Next.
     The install location defaults to one of the following:
     - C:\Program Files\Symantec\Symantec Endpoint Protection\Integrated Enforcer for 32-bit operating systems
     - C:\Program Files (x86)\Symantec\Symantec Endpoint Protection\Integrated Enforcer for 64-bit operating systems
   - Click Browse to locate and select a destination folder, click OK, and click Next.

5 If the Role Selection panel appears, select NAP Enforcement and click Next.
   The Role Selection panel appears if more than one type of Symantec NAC Integrated Enforcer can be installed based on the services running on the server.

6 In the Ready to Install the Application panel, click Next.
   If you need to modify any of the previous settings, click Back.

7 Click Finish.
   If you need to reinstall the Symantec Integrated NAP Enforcer, you must first uninstall it.

8 Click Start > Programs > Symantec Endpoint Protection Manager > Symantec NAC Integrated Enforcer to launch the program.

Uninstalling the Integrated Enforcer for Microsoft Network Access Protection

You can uninstall the Integrated Enforcer for Microsoft Network Access Protection from the Windows taskbar or the command line.

To uninstall the Integrated Enforcer for Microsoft Network Access Protection
1 On the Windows taskbar, click Start > Control Panel > Add or Remove Programs.
2 Click Symantec NAC Integrated Enforcer, and then click Remove.
3 To respond the prompt about whether you want to remove the software, click Yes.

4 To respond the prompt about whether you want to restart the NPS server, do one of the following:
   - To restart the NPS server immediately, click Yes.
   - To restart the NPS service manually later (the default), click No.
     If you restart the NPS service later, you must stop and then start it.
     You must restart the NPS service to completely uninstall the Symantec Integrated Enforcer.

To uninstall the Integrated Enforcer for Microsoft Network Access Protection from the command line

1 Open a DOS command window.

2 At the command prompt, type one of:
   - `MsiExec.exe /qn/X{A145EB45-0852-4E18-A9DC-9983A6AF2329}` for x86
   - `MsiExec.exe /qn/X{977BF644-A8FF-484f-8AF7-C1AF40F38DEA}` for x64

3 Restart the NPS server.

**Stopping and starting the Network Access Protection server manually**

Stop the Network Access Protection (NAP) server manually before upgrading to a new version of the Integrated Enforcer for Microsoft Network Access Control. You then restart it after you complete the upgrade.

To stop and start the NAP server manually

1 On the Windows taskbar, click **Start > Control Panel > Administrative Tools > Services**.

2 Click **NAP Server**.

3 Right-click, and then click **Stop**.

4 Click **Start**.
Configuring the Enforcers

- Chapter 18. Configuring the Gateway Enforcer appliance from the Symantec Endpoint Protection Manager
- Chapter 19. Configuring the LAN Enforcer appliance on the Symantec Endpoint Protection Manager
- Chapter 20. Configuring the Integrated Enforcers on the Enforcer console
- Chapter 21. Configuring the Integrated Enforcer for Microsoft DHCP Server on the Symantec Endpoint Protection Manager
- Chapter 22. Configuring the Integrated Enforcer for Microsoft Network Access Protection on an Enforcer console
- Chapter 23. Configuring the Integrated Enforcer for Microsoft Network Access Protection on the Symantec Endpoint Protection Manager
- Chapter 24. Configuring the Symantec Network Access Control On-Demand Clients
- Chapter 25. Performing basic tasks on the console of all types of Enforcer appliances
- Chapter 26. Managing Enforcers on the Symantec Endpoint Protection Manager
- Chapter 27. Troubleshooting the Enforcer appliance
Configuring the Gateway Enforcer appliance from the Symantec Endpoint Protection Manager

This chapter includes the following topics:

- How the Gateway Enforcer appliance works
- About configuring the Symantec Gateway Enforcer appliance on the Symantec Endpoint Protection Manager Console
- Changing Gateway Enforcer appliance configuration settings in Symantec Endpoint Protection Manager
- About authentication settings on a Gateway appliance
- Authentication range settings
- About advanced Gateway Enforcer appliance settings

How the Gateway Enforcer appliance works

Gateway Enforcer appliances perform one-way checking. They check the clients that try to connect through the Gateway Enforcer appliance’s external NIC to the organization’s network.

A Gateway Enforcer appliance uses the following processes to check client computers and determine if they can access the protected network:
The Gateway Enforcer appliance checks for client information and verifies that the client has passed the Host Integrity check. See “How the Enforcers work with Host Integrity policies” on page 132.

If the client satisfies the requirements for access, the Gateway Enforcer appliance connects it to the network.

If a client does not satisfy the requirements for access, you can set up the Gateway Enforcer appliance to perform the following actions:

- Monitor and log certain events.
- Block users if the Host Integrity check failed.
- Display a pop-up message on the client.
- Provide the client with limited access to a quarantine section of the network to allow the use of network resources for remediation. To provide limited access, you redirect client HTTP requests to a web server with remediation information. For example, this web server can include instructions on where to obtain remediation software. Or, it can allow the client to download the Symantec Network Access Control client software.
- Allow the client to access the network even though it has failed the Host Integrity check.

The Gateway Enforcer appliance has the following optional configuration capabilities:

- Allow the client computers with trusted IP addresses to access the network immediately.
  You can configure which client IP addresses to check and which IP addresses are trusted. Clients with trusted IP addresses are granted access without additional authentication.
- Allow the computers that do not run Windows to access the network. In this case, the Gateway Enforcer appliance functions as a bridge instead of a router. As soon as a client is authenticated, the Gateway Enforcer appliance forwards packets to allow the client to have access to the network.

See “About the Symantec Network Access Control Enforcer appliances” on page 170.

See “What you can do with Symantec Enforcer appliances” on page 171.

See “About installing an Enforcer appliance” on page 172.
About configuring the Symantec Gateway Enforcer appliance on the Symantec Endpoint Protection Manager Console

You can add or edit the configuration settings for the Gateway Enforcer appliance in the Symantec Endpoint Protection Manager Console.

Before you can proceed, you must complete the following tasks:

- Install the software for the Symantec Endpoint Protection Manager on a computer.
  See “Installing Symantec Endpoint Protection Manager” on page 51.
  The computer on which the Symantec Endpoint Protection Manager software is installed is also referred to as the management server.

- Connect the Symantec Gateway Enforcer appliance to the network.
  See “Setting up an Enforcer appliance” on page 174.

- Configure the Symantec Gateway Enforcer appliance on the local Gateway Enforcer console during the installation.
  See “Configuring an Enforcer appliance” on page 176.

After you finish these tasks, you can specify additional configuration settings for the Gateway Enforcer appliance on a management server.

When you install a Gateway Enforcer appliance, a number of default settings and ports are automatically set up. The default settings for the Gateway Enforcer appliance on the Symantec Endpoint Protection Manager allow all clients to connect to the network if the client passes the Host Integrity check. The Gateway Enforcer appliance acts as a bridge. Therefore you can complete the process of setting up the Gateway Enforcer appliance and deploying clients without blocking access to the network.

However, you need to change the default settings on Symantec Endpoint Protection Manager to limit which clients are allowed access without authentication. Optionally, there are other Enforcer default settings for the Gateway Enforcer appliance that you may want to customize before you start enforcement.

Changing Gateway Enforcer appliance configuration settings in Symantec Endpoint Protection Manager

You can change the Gateway Enforcer appliance configuration settings on a management server. The configuration settings are automatically downloaded from
the management server to the Gateway Enforcer appliance during the next heartbeat.

To change Gateway Enforcer appliance configuration settings in Symantec Endpoint Protection Manager

1. In the Symantec Endpoint Protection Manager Console, click Admin.
2. In the Admin page, click Servers.
3. In Servers, select the group of Enforcers of which the Gateway Enforcer appliance is a member.

   The Enforcer group must include the Gateway Enforcer appliance for which the configuration settings must be changed.

4. Select the Gateway Enforcer appliance for which the configuration settings must be changed.
5 Under **Tasks**, click **Edit Group Properties**.

6 In the **Settings** dialog box, change any of the configuration settings.

The **Gateway Enforcer Settings** dialog box provides the following categories of configuration settings:

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>Settings for the Enforcer group description and management server list.</td>
</tr>
<tr>
<td>Authentication</td>
<td>Settings for a variety of parameters that affect the client authentication process. If a matching address is still not found, the Gateway Enforcer appliance begins the authentication session and sends the challenge packet. See “About authentication settings on a Gateway appliance” on page 226.</td>
</tr>
<tr>
<td>Auth Range</td>
<td>Settings that specify an individual IP address for a client or IP address ranges for clients who need to be authenticated. You can also specify an individual IP address or IP address ranges for the clients that are allowed to connect to a network without authentication. See “Authentication range settings” on page 239.</td>
</tr>
<tr>
<td>Advanced</td>
<td>Settings for authentication timeout parameters and Gateway Enforcer appliance message timeouts. Settings for MAC addresses for the trusted hosts that the Gateway Enforcer appliance allows to connect without authentication (optional). See “About advanced Gateway Enforcer appliance settings” on page 249.</td>
</tr>
<tr>
<td>Log Settings</td>
<td>Settings for enabling logging of Server logs, Client Activity logs, and specifying log file parameters. See “About Enforcer reports and logs” on page 380. See “Configuring Enforcer log settings” on page 381.</td>
</tr>
</tbody>
</table>
About authentication settings on a Gateway appliance

You can specify a number of authentication settings for a Gateway Enforcer appliance authentication session. When you apply these changes, they are automatically sent to the selected Gateway Enforcer appliance during the next heartbeat.

See “Authentication settings on a Gateway appliance” on page 226.

Authentication settings on a Gateway appliance

You may want to implement a number of authentication settings to further secure the network.

Table 18-1 provides more information about the options on the Authentication tab.

Table 18-1  Authentication configuration settings for a Gateway Enforcer appliance

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Maximum number of packets per authentication session | The maximum number of challenge packets that the Gateway Enforcer appliance sends in each authentication session.  
The default number is 10 packets. The range is 2 through 100 packets.  
See “Specifying the maximum number of challenge packets during an authentication session” on page 231. |
| Time between packets in authentication session (seconds) | The time in seconds between each challenge packet that the Enforcer sends.  
The default value is 3 seconds. The range is 3 through 10.  
See “Specifying the frequency of challenge packets to be sent to clients” on page 231. |
| Time rejected client will be blocked (seconds) | The amount of time in seconds for which a client is blocked after it fails authentication.  
The default setting is 30 seconds. The range is 10 through 300 seconds.  
See “Specifying the time period for which a client is blocked after it fails authentication” on page 232. |
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time authenticated client will be allowed (seconds)</td>
<td>The amount of time in seconds for which a client is allowed to retain its network connection without reauthentication. The default setting is 30 seconds. The range is 10 through 300 seconds. See “Specifying the time period for which a client is allowed to retain its network connection without reauthentication” on page 233.</td>
</tr>
<tr>
<td>Allow all clients, but continue to log which clients are not authenticated</td>
<td>If this option is enabled, the Gateway Enforcer appliance authenticates all users by checking that they are running a client. The Gateway Enforcer appliance also checks if the client passed the Host Integrity check. If the client passes the Host Integrity check, the Gateway Enforcer appliance then logs the results. It then forwards the Gateway request to receive a normal rather than a quarantine network configuration, whether the checks pass or fail. The default setting is not enabled. See “Allowing all clients with continued logging of non-authenticated clients” on page 234.</td>
</tr>
<tr>
<td>Allow all clients with non-Windows operating systems</td>
<td>If this option is enabled, the Gateway Enforcer checks for the operating system of the client. The Gateway Enforcer appliance then allows all clients that do not run the Windows operating systems to receive a normal network configuration without being authenticated. If this option is not enabled, the clients receive a quarantine network configuration. The default setting is not enabled. See “Allowing non-Windows clients to connect to a network without authentication” on page 235.</td>
</tr>
</tbody>
</table>
Table 18-1  Authentication configuration settings for a Gateway Enforcer appliance (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Check the Policy Serial Number on Client before allowing Client into network | If this option is enabled, the Gateway Enforcer appliance verifies that the client has received the latest security policies from the management server. If the policy serial number is not the latest, the Gateway Enforcer notifies the client to update its security policy. The client then forwards the Gateway request to receive a quarantine network configuration.  
 If this option is not enabled and if the Host Integrity check succeeds, the Gateway Enforcer appliance forwards the Gateway request to receive a normal network configuration. The Gateway Enforcer forwards the request even if the client does not have the latest security policy.  
 The default setting is not enabled.  
 See "Checking the policy serial number on a client" on page 235.                                                                                                                                                                                                                  |
| Enable pop-up message on client if Client is not running               | If this option is enabled, a message appears to users on Windows computers that try to connect to an enterprise network without running a client. The default message is set to display only one time. The message tells the users that they are blocked from accessing the network because a client is not running and tells them to install it. To edit the message or to change how often it is displayed, you can click Message. The maximum message length is 128 characters.  
 The default setting is enabled.  
 **Note:** Popup messages do not appear on Mac clients.  
 See "Sending a message from a Gateway Enforcer appliance to a client about non-compliance" on page 237.                                                                                                                                                                          |
| Enable HTTP redirect on client if Client is not running                | If this option is enabled, the Gateway Enforcer can redirect clients to a remediation Web site.  
 If this option is enabled, the Gateway Enforcer appliance redirects HTTP requests to an internal Web server if the client does not run.  
 This option cannot be enabled without having specified a URL.  
 The default setting is enabled, with the value http://localhost.  
 See "Redirecting HTTP requests to a Web page" on page 238.                                                                                                                                                                                                                                           |
Table 18-1 Authentication configuration settings for a Gateway Enforcer appliance (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP redirect URL</td>
<td>You can specify a URL of up to 255 characters when you redirect clients to a remediation Web site. The default setting for the redirect URL is <a href="http://localhost">http://localhost</a>. See “Redirecting HTTP requests to a Web page” on page 238.</td>
</tr>
<tr>
<td>HTTP redirect port</td>
<td>You can specify a port number other than 80 when you redirect clients to a remediation Web site. The default setting for the Web server is port 80. See “Redirecting HTTP requests to a Web page” on page 238.</td>
</tr>
</tbody>
</table>

About authentication sessions on a Gateway Enforcer appliance

When a client tries to access the internal network, the Gateway Enforcer establishes an authentication session with it. An authentication session is a set of challenge packets that are sent from a Gateway Enforcer appliance to a client.

During an authentication session, the Gateway Enforcer appliance sends a challenge packet to the client at a specified frequency. The default setting is every three seconds. It keeps sending packets until it receives a response from the client, or until it has sent out the maximum number of packets specified. The default number is 10 packages.

If the client responds and passes authentication, the Gateway Enforcer appliance allows it access to the internal network for a specified number of seconds. The default is 30 seconds. The Gateway Enforcer appliance starts a new authentication session during which the client must respond to retain the connection to the internal network. The Gateway Enforcer appliance disconnects the clients that do not respond or are rejected because they fail authentication.

If the client does not respond or fails authentication, the Gateway Enforcer appliance blocks it for a specified number of seconds. The default is 30 seconds. If another client tries to log on using that same IP address, it has to be reauthenticated.

You can configure the authentication session for each Gateway Enforcer appliance on the management server.

See “Changing Gateway Enforcer appliance configuration settings in Symantec Endpoint Protection Manager” on page 223.

See “Authentication settings on a Gateway appliance” on page 226.
About client authentication on a Gateway Enforcer appliance

The Gateway Enforcer appliance authenticates remote clients before it allows access to the network. Client authentication in the Gateway Enforcer performs the following functions:

- Determines whether to authenticate the client or allow it without authentication
  You can specify individual clients or ranges of IP addresses to trust or to authenticate on the Auth Range tab.

- Carries out the authentication session
  You configure the settings for the authentication session on the Authentication tab.

Each Gateway Enforcer maintains the following lists of trusted IP addresses that are allowed to connect to the network through the Gateway Enforcer:

- A static list
  The trusted external IP addresses that are configured for the Enforcer on the Auth Range tab.

- A dynamic list
  The additional trusted IP addresses that are added and dropped as clients are authenticated, allowed to connect to the network, and finally disconnected.

When traffic arrives from a new client, the Gateway Enforcer appliance determines whether this client is included in the list of trusted client IP addresses. If the client has a trusted IP address, it is allowed on the network with no further authentication.

If the client lacks a trusted IP address, the Gateway Enforcer appliance checks if the trusted IP address is within the client IP address range for the clients that should be authenticated. If the client's IP address is within the client IP address range, the Gateway Enforcer appliance begins an authentication session.

During the authentication session, the client sends its unique ID number, the results of the Host Integrity check, and its policy serial number. The policy serial number identifies if the client security policies are up to date.

The Gateway Enforcer appliance checks the results. It can optionally check the policy serial number. If the results are valid, the Gateway Enforcer appliance gives the client an authenticated status and allows network access to the client. If the results are not valid, the Gateway Enforcer appliance blocks the client from connecting to the network.

When a client is authenticated, that client's IP address is added to the dynamic list with a timer. The default timer interval is 30 seconds. After the timer interval has elapsed, the Gateway Enforcer appliance begins a new authentication session with the client. If the client does not respond or fails authentication, the client’s IP address is deleted from the list. The IP address is also blocked for a specified interval. The
default setting is 30 seconds. When another client tries to log on by using that same IP address, the client has to be reauthenticated.

See “Authentication settings on a Gateway appliance” on page 226.

Specifying the maximum number of challenge packets during an authentication session

During the authentication session, the Gateway Enforcer appliance sends a challenge packet to the client at a specified frequency.

The Gateway Enforcer appliance continues to send packets until the following conditions are met:

- The Gateway Enforcer appliance receives a response from the client.
- The Gateway Enforcer appliance has sent the specified maximum number of packets.

The default setting is 10 packets for the maximum number of challenge packets for an authentication session. The range is from 2 through 100 packets.

See “About authentication settings on a Gateway appliance” on page 226.

To specify the maximum number of challenge packets during an authentication session

1. In Symantec Endpoint Protection Manager, click Admin.
2. Click Servers.
3. Select and expand the group of Enforcers.
   The Enforcer group must include the Gateway Enforcer appliance for which you want to specify the maximum number of challenge packets during an authentication session.
5. In the Gateway Settings dialog box, on the Authentication tab, under Authentication Parameters type the maximum number of challenge packets that you want to allow during an authentication session in the Maximum number of packets per authentication session field.
   The default setting is 10 seconds. The range is from 2 through 100 packets.
6. Click OK.

Specifying the frequency of challenge packets to be sent to clients

During the authentication session, the Gateway Enforcer appliance sends a challenge packet to the client at a specified frequency.
The Gateway Enforcer appliance continues to send packets until the following conditions are met:

- The Gateway Enforcer appliance receives a response from the client.
- The Gateway Enforcer appliance has sent the specified maximum number of packets.

The default setting is every 3 seconds. The range is 3 through 10 seconds.

See “About authentication settings on a Gateway appliance” on page 226.

To specify the frequency of challenge packets to be sent to clients

1. In the Symantec Endpoint Protection Manager Console, click **Admin**.
2. Click **Servers**.
3. Select and expand the group of Enforcers.
   The Enforcer group must include the Gateway Enforcer appliance for which you want to specify the frequency of challenge packets to be sent to clients.
4. Under **Tasks**, click **Edit Group Parameters**.
5. In the **Settings** dialog box, on the Authentication tab, under Authentication Parameters, type the maximum number of challenge packets that you want the Gateway Enforcer appliance to keep sending to a client during an authentication session in the **Time between packets in authentication session** field.
   The default setting is 3 seconds. The range is from 3 through 10 seconds.
6. In the **Settings** dialog box, on the Authentication tab, click **OK**.

Specifying the time period for which a client is blocked after it fails authentication

You can specify the amount of time for which a client is blocked after it fails authentication.

The default setting is 30 seconds. The range is 10 through 300 seconds.

See “About authentication settings on a Gateway appliance” on page 226.

To specify the time period for which a client is blocked after it fails authentication

1. In the Symantec Endpoint Protection Manager Console, click **Admin**.
2. Click **Servers**.
3 Select and expand the group of Enforcers.
   The Enforcer group must include the Gateway Enforcer appliance for which you want to specify the amount of time that a client is blocked after it fails authentication.

4 Under Tasks, click Edit Group Properties.

5 In the Settings dialog box, on the Authentication tab, under Authentication Parameters, type the number of seconds for the amount of time for which a client is blocked after it fails authentication in the Time rejected client will be blocked (seconds) field.

6 Click OK.

Specifying the time period for which a client is allowed to retain its network connection without reauthentication

You can specify the amount of time in seconds for which a client is allowed to retain its network connection without reauthentication.

The default setting is 30 seconds. The range is 10 through 300 seconds.

See “About authentication settings on a Gateway appliance” on page 226.

To specify the time period for which a client is allowed to retain its network connection without reauthentication

1 In the Symantec Endpoint Protection Manager Console, click Admin.

2 Click Servers.

3 Under Servers, select and expand the group of Enforcers.
   The Enforcer group must include the Gateway Enforcer appliance for which you want to specify the amount of time that a client is blocked after it fails authentication.

4 Under Tasks, click Edit Group Properties.

5 In the Settings dialog box, on the Authentication tab, under Authentication Parameters, type the number of seconds for which a client is allowed to retain its network connection without reauthentication in the Time authenticated client will be allowed (seconds) field.
   The default setting is 30 seconds. The range is 10 through 300 seconds.

6 Click OK.
Allowing all clients with continued logging of non-authenticated clients

It can take some time to deploy all the client software. You may want to configure the Gateway Enforcer appliance to allow all clients to connect to the network until you have finished distributing the client package to all users. A Gateway Enforcer appliance blocks all clients that do not run the Symantec Endpoint Protection Windows client. This means that the Gateway Enforcer appliance blocks all non-Windows clients. However, you have the option of allowing all non-Windows clients to connect to the network.

If a client is not authenticated with this setting, the Gateway Enforcer appliance detects the operating system type. Therefore Windows clients are blocked and non-Windows clients are permitted to access the network.

The default setting is not enabled.

Use the following guidelines when you apply the configuration settings:

- This setting should be a temporary measure because it makes the network less secure.
- While this setting is in effect, you can review Enforcer logs. You can learn about the types of clients that try to connect to the network at that location. For example, you can review the Client Activity Log to see if any of the clients do not have the Symantec Endpoint Protection client software installed. You can then make sure that the client software is installed on those clients before you disable this option.

See “About authentication settings on a Gateway appliance” on page 226.

To allow all clients with continued logging of non-authenticated clients

1. In the Symantec Endpoint Protection Manager Console, click Admin.
2. Click Servers.
3. Select and expand the group of Enforcers.
   - The Enforcer group must include the Gateway Enforcer appliance for which you want to allow all clients while continuing the logging of non-authenticated clients.
5. In the Settings dialog box, on the Authentication tab, check Allow all clients, but continue to log which clients are not authenticated.
   - The default setting is not enabled.
6. In the Settings dialog box, on the Authentications tab, click OK.
Allowing non-Windows clients to connect to a network without authentication

The Gateway Enforcer appliance cannot authenticate a client that is running a non-Windows operating system. Therefore non-Windows clients cannot connect to the network unless you specifically allow them to connect to the network without authentication.

The default setting is not enabled.

You can use one of the following methods to enable the clients that support a non-Windows platform to connect to the network:

- Specify each non-Windows client as a trusted host.
- Allow all clients with non-Windows operating systems.

The Gateway Enforcer appliance detects the operating system of the client and authenticates Windows clients. However, it does not allow non-Windows clients to connect to the Gateway Enforcer appliance without authentication.

If you need to have non-Windows clients connect to the network, then you must configure additional settings on the Symantec Endpoint Protection Manager Console.

See “Requirements for allowing non-Windows clients without authentication” on page 185.

See “About authentication settings on a Gateway appliance” on page 226.

To allow non-Windows clients to connect to a network without authentication

1. In the Symantec Endpoint Protection Manager Console, click **Admin**.
2. In the **Admin** page, click **Servers**.
3. Under **Servers**, select and expand the group of Enforcers.
   - The Enforcer group must include the Gateway Enforcer appliance for which you want to allow all non-Windows clients to connect to a network.
4. Under **Tasks**, click **Edit Group Properties**.
5. In the **Settings** dialog box, on the **Authentication** tab, check **Allow all clients with non-Windows operating systems**.
   - The default setting is not enabled.
6. Click **OK**.

Checking the policy serial number on a client

The Symantec Endpoint Protection Manager updates a client’s policy serial number every time that the client’s security policy changes. When a client connects to the
Symantec Endpoint Protection Manager, it receives the latest security policies and the latest policy serial number.

When a client tries to connect to the network through the Gateway Enforcer appliance:

- Retrieves the policy serial number from the Symantec Endpoint Protection Manager.
- Compares the policy serial number with the one that it receives from the client.
- If the policy serial numbers match, the Gateway Enforcer appliance has validated that the client is running an up-to-date security policy.

The default value for this setting is not enabled.

The following guidelines apply:

- If the **Check the Policy Serial Number on Client before allowing Client into network** option is checked, a client must have the latest security policy before it can connect to the network through the Gateway Enforcer appliance. If the client does not have the latest security policy, the client is notified to download the latest policy. The Gateway Enforcer appliance then forwards its Gateway request to receive a quarantine network configuration.

- If the **Check the Policy Serial Number on Client before allowing Client into network** option is not checked and the Host Integrity check is successful, a client can connect to the network. The client can connect through the Gateway Enforcer appliance even if its security policy is not up-to-date.

See “About authentication settings on a Gateway appliance” on page 226.

**To have the Gateway Enforcer appliance check the policy serial number on a client**

1. In the Symantec Endpoint Protection Manager Console, click **Admin**.
2. In the **Admin** page, click **Servers**.
3. Select and expand the group of Gateway Enforcer appliances.
   - The Enforcer group must include the Gateway Enforcer appliance that checks the Policy Serial Number on a client.
4. In the **Settings** dialog box, on the **Authentication** tab, check **Check the Policy Serial Number on the Client before allowing a Client into the network**.
5. Click **OK**.
Sending a message from a Gateway Enforcer appliance to a client about non-compliance

You can send a Windows pop-up message to inform a user that they cannot connect to the network. The message typically tells the user that a client cannot connect to the network because it does not run the Symantec Network Access Control client.

Most administrators type a brief statement of the need to run the Symantec Endpoint Protection client or the Symantec Network Access Control client. The message may include information about a download site where users can download the required client software. You can also provide a contact telephone number and other relevant information.

This setting is enabled by default. It applies only to clients that do not run the Symantec Endpoint Protection client or the Symantec Network Access Control client.

As soon as you complete this task, the pop-up message appears on the client if the Windows Messenger service is running on the client.

---

**Note:** Popup messages do not appear on Mac clients.

See “About authentication settings on a Gateway appliance” on page 226.

To send a message from a Gateway Enforcer appliance to a client about non-compliance

1. In the Symantec Endpoint Protection Manager Console, click **Admin**.
2. Click **Servers**.
3. Select and expand the group of Enforcers.
4. Under **Tasks**, click **Edit Group Properties**.
5. In the **Settings** dialog box, on the **Authentication** tab, check **Enable pop-up message on Windows client if Client is not running**.
6. Click **Message**.
7. In the **Pop-up Message Settings** dialog box, select how often you want the message to appear on a client from the **Following message will pop up** list.

You can select any of the following time periods:

- **Once**
  
  The default value is Once.

- **Every 30 seconds**

- **Every minute**
Every 2 minutes
Every 5 minutes
Every 10 minutes

8 Type the message that you want to appear in the text box.
The maximum number of characters is 125. This number includes spaces and punctuation.
The default message is:
You are blocked from accessing the network because you do not have the Symantec Client running. You will need to install it.

9 Click OK.

10 In the Settings dialog box, on the Authentication tab, click OK.

Redirecting HTTP requests to a Web page

The Gateway Enforcer appliance has an option to redirect HTTP requests to an internal Web server if the client tries to access an internal Web site through a browser and a client is not running on the client. If you do not specify a URL, the Gateway Enforcer appliance pop-up message appears as the HTML body for the first HTML page. You may want to connect users to a Web page that you set up. Clients can download Remediation software from this Web site. The Gateway Enforcer appliance can redirect the HTTP GET request to a URL that you specify. This setting is enabled by default.

For example, you can redirect a request to a Web server from which the client can download the client software, patches, or up to date versions of applications.

See “About authentication settings on a Gateway appliance” on page 226.

To redirect HTTP requests to a Web page

1 In the Symantec Endpoint Protection Manager Console, click Admin.

2 Click Servers.

3 Select and expand the group of Gateway Enforcer appliances.

4 Under Tasks, click Edit Group Properties.

5 In the Gateway Settings dialog box, on the Authentication tab, check Enable HTTP redirect on client if the client is not running.
6 Type the URL in the HTTP redirect URL field.

The host of the redirect URL must either be the Symantec Endpoint Protection Manager or an IP address that is listed as part of the internal trusted IP address range.

The URL can have as many as 255 characters.

If you want to specify a name of a Web server, you must also enable Allow all DNS request packets on the Advanced tab.

If you leave the URL field empty and then click OK, the following message appears:

The HTTP redirect URL must be a valid URL.

This also uses the Gateway Enforcer pop-up message as the HTML body for the first HTML page it sends back to the client.

7 In the Gateway Settings dialog box, on the Authentication tab, click OK.

Authentication range settings

You can configure the following settings:

- Client IP addresses that the Gateway Enforcer appliance authenticate
  See “Adding client IP address ranges to the list of addresses that require authentication” on page 243.

- External IP addresses that the Gateway Enforcer appliance does not authenticate
  See “Specifying trusted external IP addresses” on page 246.

- Internal IP address to which the Gateway Enforcer allows access
  See “Adding a trusted internal IP address for clients on a management server” on page 245.

After you apply the settings, the changes are sent to the selected Gateway Enforcer appliance during the next heartbeat. Keep in mind the following information:

- The option to Only authenticate clients with these IP addresses is not selected by default. If you leave this option selected and do not specify any IP addresses to authenticate, the Gateway Enforcer appliance acts as a network bridge and allows all clients access.

- For Trusted External IP address range addresses, you should add the IP address of the corporate VPN server, as well as any other IP addresses that are allowed to have access to the corporate network without running a client. You may also want to include the devices that normally have access to the network and are running an operating system other than Windows.
For **Trusted Internal IP address range addresses**, you may need to specify addresses, such as an update server, a file server containing antivirus signature files, a server that is used for remediation, or a DNS or WINS server that is required to resolve domain or host names.

If you specify that the Gateway Enforcer appliance verifies that the client profile is up-to-date, clients may need to connect to the Symantec Endpoint Protection Manager to download the latest security policies. If you use this option when you refer to the Symantec Endpoint Protection Manager by DNS or host name, you must add the DNS or WINS server’s IP address to the trusted internal IP list.

**Client IP address ranges compared to trusted external IP addresses**

The Client IP address range is similar to what is called a blacklist. You can specify the client IP addresses that tell the Gateway Enforcer appliance to only check specific IP addresses to see if they are running the client and meet required security policies. If a client is not on the Client IP list, then it functions as if it had been assigned a trusted IP address.

In contrast to the Client IP address range, trusted external IP addresses are similar to what is called a white list. If you check **Assigning trusted external IP addresses**, the Gateway Enforcer appliance validates the client that tries to connect from the external side except clients with trusted external IP addresses. This process is the opposite of Client IP address range, which tells the Gateway Enforcer appliance to only validate the clients in the Client IP address range.

See “Adding client IP address ranges to the list of addresses that require authentication” on page 243.

**When to use client IP address ranges**

Client IP address range allows administrators to specify a range of IP addresses that represent the computers the Gateway Enforcer appliance must authenticate. Computers with addresses outside the Client IP address range are allowed to pass through the Gateway Enforcer appliance without requiring the client software or other authentication.

The reasons for using Client IP address ranges include:

- Allowing network access to external Web sites
- Authenticating a subset of clients

See “Adding client IP address ranges to the list of addresses that require authentication” on page 243.
Allowing network access to external Web sites

One reason for using Client IP address ranges is to allow network access to external Web sites from within your internal network. If an organization has computers on the corporate network that go out through the Gateway Enforcer appliance to access Web sites on the Internet, such as Symantec or Yahoo, the internal clients can query the Internet. However, the Gateway Enforcer appliance tries to authenticate the Web sites trying to respond to the client request.

Therefore internal clients connecting to the Internet through the Gateway Enforcer appliance are unable to access the Internet unless you configure the Client IP address range.

The Client IP address range may be all the IP addresses a VPN server would assign to any client.

For example, an internal client can access the Internet if Client IP address range is configured. When an internal user contacts a Web site, the site can respond to the client because its IP address is outside the client IP address range. Therefore the internal user does not need to be authenticated.

See “Adding client IP address ranges to the list of addresses that require authentication” on page 243.

Authentication of a subset of clients

You may want to use client IP addresses to have a Gateway Enforcer appliance authenticate a limited subset of clients at a company.

You can have the Gateway Enforcer appliance check only those clients that connect through one subnet if you have already installed the clients on all of the computers. Other clients accessing the corporate network at that location are allowed to pass through without authentication. As the client is installed on other clients, you can add their addresses to the Client IP address range or use a different authentication strategy.

See “Adding client IP address ranges to the list of addresses that require authentication” on page 243.

About trusted IP addresses

You work with the following types of trusted IP addresses on a Gateway Enforcer:

- Trusted external IP addresses
  A trusted external IP address is the IP address of an external computer that is allowed to access the corporate network without running the client.
  See “Specifying trusted external IP addresses” on page 246.
Trusted internal IP addresses
A trusted internal IP address is the IP address of a computer within the corporate network that any client can access from the outside.
See “Adding a trusted internal IP address for clients on a management server” on page 245.

You can add trusted IP addresses of both types on the Symantec Endpoint Protection Manager Console. Traffic to the console is always allowed from the Gateway Enforcer appliance.

Trusted external IP addresses
One of the primary duties of a Gateway Enforcer appliance is to check that all computers that try to access the network are running the client. Some computers may not be running the Windows operating system or may not be running the client.
For example, VPN and wireless servers do not typically run the client. In addition, a network setup may include the devices that normally access the network and run an operating system other than Windows. If these computers need to bypass a Gateway Enforcer appliance, you need to make sure that the Gateway Enforcer appliance knows about them. You can accomplish this objective by creating a range of trusted external IP addresses. In addition, you must also assign an IP address from that IP address range to a client.
See “Specifying trusted external IP addresses” on page 246.

Trusted internal IP addresses
A trusted internal IP address represents the IP address of a computer inside the corporate network that external clients can access from the outside. You can make certain internal IP addresses into trusted internal IP addresses.
When you specify trusted internal IP addresses, clients can get to that IP address from outside the corporate network whether or not:
- The client software has been installed on the client computer
- The client complies with a security policy

Trusted internal IP addresses are the internal IP addresses that you want users outside the company to be able to access.
Examples of the internal addresses that you may want to specify as trusted IP addresses are as follows:
- An update server
- A file server that contains antivirus signature files
- A server that is used for remediation
A DNS server or a WINS server that is required to resolve domain or host names.

When a client tries to access the internal network and does not get authenticated by the Gateway Enforcer appliance, the client can be placed in quarantine when:

- The client is not running the client software on the client computer
- The Host Integrity check failed
- The client does not have an up-to-date policy

The client is still allowed to access certain IP addresses; these are the trusted internal IP addresses.

For example, the concept of trusted internal IP addresses may have an external client that needs to access the corporate network to get the client or other needed software. The Gateway Enforcer appliance allows the external client to get to a computer that is on the list of trusted internal IP addresses.

See “Adding a trusted internal IP address for clients on a management server” on page 245.

Adding client IP address ranges to the list of addresses that require authentication

You can specify those clients with IP addresses to which the Gateway Enforcer appliance authenticates.

You want to be aware of the following issues:

- You must check the Enable option that is located next to the IP address or range if you want that address to be authenticated. If you want to temporarily disable authentication of an address or range, uncheck Enable.
- If you type an invalid IP address, you receive an error message when you try to add it to the Client IP list.

See “When to use client IP address ranges” on page 240.

To restrict a client's network access despite authentication

1. In Symantec Endpoint Protection Manager, click Admin.
2. Click Servers.
3. Select and expand the Gateway Enforcer appliance groups.
5 In the **Gateway Settings** dialog box, on the **Auth Range** tab, in the **Authenticate Client IP address range** area, check **Only authenticate clients with these IP addresses**.

If you do not check this option, any IP addresses listed are ignored. Therefore all clients who try to connect to the network are authenticated. If you check this option, the Gateway Enforcer appliance authenticates only the clients with the IP addresses that are added to the list.

6 Click **Add**.

7 In the **Add Single IP Address** dialog box, select **from Single IP address to IP address range or Subnet**.

The fields change to enable you to enter the appropriate information.

8 Select whether to add:
   - A single IP address
   - An IP address range
   - An IP address plus subnet mask

9 Type either a single IP address, a start address and an end address of a range, or an IP address plus subnet mask.

10 Click **OK**.

   The address information you typed is added to the Client IP address range table, with the **Enable** option selected.

11 Continue to click **Add** and specify any other IP addresses or ranges of addresses that you want the Gateway Enforcer to authenticate.

12 Click **OK**.

**Editing client IP address ranges on the list of addresses that require authentication**

You may need to edit client IP address ranges that you want to be authenticated.

See “**When to use client IP address ranges**” on page 240.

**To edit client IP address ranges on the list of addresses that require authentication**

1 In Symantec Endpoint Protection Manager, click **Admin**.

2 Click **Servers**.

3 Select and expand the group of Enforcers.

4 Select the group of Enforcers for which you want to edit client IP address ranges on the list of addresses that require authentication.
5 Under Tasks, click Edit Group Properties.

6 In the Gateway Settings dialog box, on the Auth Range tab, in the Client IP address range area, click anywhere in the column of IP addresses and click Edit all.

7 Click OK.

8 In the Gateway Settings dialog box, click OK.

Removing client IP address ranges from the list of addresses that require authentication

You may need to remove client IP address ranges.

See “When to use client IP address ranges” on page 240.

To remove client IP address ranges from the list of addresses that require authentication

1 In Symantec Endpoint Protection Manager, click Admin.

2 Click Servers.

3 Select and expand the group of Enforcers.

4 Select the group of Gateway Enforcer appliances for which you want to edit client IP address ranges on the list of addresses that require authentication.

5 Under Tasks, click Edit Group Properties.

6 In the Gateway Settings dialog box, on the Auth Range tab, in the Client IP address range area, click the row containing the IP address that you want to remove.

7 Click Remove.

8 Click OK.

Adding a trusted internal IP address for clients on a management server

The Trusted Internal IP table has a list of internal IP addresses that external clients are allowed to communicate with, regardless of whether a client currently runs or has passed the Host Integrity check.

If you run two Gateway Enforcer appliances in a series so that a client connects through more than one Gateway Enforcer appliance, the Gateway Enforcer appliance closest to Symantec Endpoint Protection Manager needs to be specified as a trusted internal IP address of the other Gateway Enforcer appliances. If a client first fails
a Host Integrity check and then passes it, you may have up to a 5-minute delay before a client can connect to the network.

See “About trusted IP addresses” on page 241.

To add a trusted internal IP address for clients on a management server

1. In Symantec Endpoint Protection Manager, click Admin.
2. In the Admin page, click Servers.
3. Select and expand the group of Enforcers.
4. Select the Gateway Enforcer appliance group for which you want to edit client IP address ranges on the list of addresses that require authentication.
5. Under Tasks, click Edit Group Properties.
6. In the Gateway Settings dialog box, on the Auth Range tab, in the Trusted IP address range area, select Trusted Internal IP address range from the drop-down list.
7. Click Add.
8. In the IP Address Settings dialog box, type an IP address or address range.
9. Click OK
   The IP address is added to the list and a check mark appears in the Enable column.
10. In the Settings dialog box, click OK.

Specifying trusted external IP addresses

If you add trusted external IP addresses, the Gateway Enforcer appliance allows clients at these IP addresses to connect to the network even if they do not run any client software.

Because a client is not installed on VPN servers, you should add the server IP to the trusted IP list if you have a VPN server requiring network access through a Gateway Enforcer.

If you enter an invalid IP address, you receive an error message.

Note: You need to add the corporate VPN server’s internal IP address in the Trusted external IP Addresses field first.

See “About trusted IP addresses” on page 241.
To specify trusted external IP addresses

1. In Symantec Endpoint Protection Manager, click **Admin**.
2. Click **Servers**.
3. Select and expand the group of Enforcers.
4. Select the group of Enforcers for which you want to specify trusted external IP addresses.
5. Under **Tasks**, click **Edit Group Properties**.
6. In the **Gateway Settings** dialog box, on the **Auth Range** tab, in the **Trusted IP address range** area, select **Trusted External IP address range** from the drop-down list.
7. Click **Add**.
8. In the **IP Address Settings** dialog box, type an IP address or address range.
9. Click **OK**.
   The IP address is added to the list and a check mark appears in the **Enable** column.
10. In the **Settings** dialog box, click **OK**.

Editing trusted internal or external IP address

You may need to edit trusted internal as well as external IP addresses.

See “About trusted IP addresses” on page 241.

To edit a trusted internal or external IP address

1. In Symantec Endpoint Protection Manager, click **Admin**.
2. Click **Servers**.
3. Select and expand the group of Enforcers.
4. Select the group of Enforcers for which you want to edit a trusted internal or external IP address.
5. Under **Tasks**, click **Edit Group Properties**.
6. In the **Gateway Settings** dialog box, on the **Auth Range** tab, in the **Trusted IP address range** area, select **Trusted Internal IP address range** or **Trusted External IP address range** from the drop-down list.
   The addresses for the selected type appear in the table.
7. In the **Trusted IP address range** table, click anywhere in the column of IP addresses and click **Edit all**.
In the IP Address Editor dialog box, locate any addresses you want to change and edit them.

Click OK.

In the Settings dialog box, click OK.

Removing a trusted internal or trusted external IP address

If you no longer want to allow external users who are not fully authenticated to have access to a particular internal location, remove the IP address from the Trusted Internal IP Address table.

See “About trusted IP addresses” on page 241.

To remove a trusted internal IP or trusted external IP address

1 In Symantec Endpoint Protection Manager, click Admin.
2 Click Servers.
3 Select and expand the Gateway Enforcer appliance group.
4 Select the group of Gateway Enforcer appliances for which you want to remove a trusted internal IP or trusted external IP address.
5 Under Tasks, click Edit Group Properties.
6 In the Gateway Settings dialog box, on the Auth Range tab, in the Trusted IP address range area, select Trusted Internal IP address range or Trusted External IP address range from the drop-down list.
   The addresses for the selected type appear in the table.
7 In the table, click the row containing the IP address that you want to remove.
8 Click Remove.
9 In the Settings dialog box, click OK.

IP address range checking order

If both Client IP address range and trusted internal IP addresses are in use, the Gateway Enforcer appliance checks client addresses in the following order when a packet is received from a client:

- If the Client IP address range is enabled, the Gateway Enforcer appliance checks the Client IP address range table for an address matching the source IP of the client.
- If the Client IP address range does not include an IP address for that client, the Gateway Enforcer appliance allows the client without authentication.
If the Client IP address range does include an IP address for that client, the Gateway Enforcer appliance next checks the trusted external IP address range for a matching address.

If an address matching the client is found in the trusted external IP address range, the Gateway Enforcer appliance allows the client.

If no matching address is found in the trusted external IP address range, the Gateway Enforcer appliance then checks the destination address against the trusted internal IP address range list and the list of instances of the Symantec Endpoint Protection Manager.

If a matching address is still not located, the Gateway Enforcer appliance begins the authentication session and sends the challenge packet.

See “Specifying trusted external IP addresses” on page 246.

See “Adding client IP address ranges to the list of addresses that require authentication” on page 243.

About advanced Gateway Enforcer appliance settings

You can configure the following advanced Gateway Enforcer appliance configuration settings:

- Allow all DHCP request packets.
- Allow all DNS request packets.
- Allow all ARP request packets.
- Allow other protocols besides IP and ARP.
  You can specify the types of protocols that you want to allow in the Filter field.
  See “Specifying packet types and protocols” on page 250.
- Allow legacy clients
  See “Allowing a legacy client to connect to the network with a Gateway Enforcer appliance” on page 251.
- Enable local authentication
  See “Enabling local authentication on a Gateway Enforcer appliance” on page 251.
- Enable system time updates for Gateway Enforcer appliance clients
  See “Enabling system time updates for the Gateway Enforcer appliance using the Network Time Protocol” on page 252.
- Use the Gateway Enforcer as a Web server
  See “Using the Gateway Enforcer appliance as a Web server” on page 252.
- Use the Gateway Enforcer as a DNS spoofing server
See “Using the Gateway Enforcer as a DNS spoofing server” on page 253.

When you apply the settings, the changes that have been made are sent to the selected Gateway Enforcer appliance during the next heartbeat.

Specifying packet types and protocols

You can specify that the Gateway Enforcer appliance allows certain packet types to pass through without requiring a client to run or require authentication.

See “About advanced Gateway Enforcer appliance settings” on page 249.

To specify packet types and protocols

1. In Symantec Endpoint Protection Manager, click Admin.
2. In the Admin page, click Servers.
3. Select and expand the Gateway Enforcer appliance group.
4. Select the group of Gateway Enforcer appliances for which you want to specify packet types and protocols.
5. Under Tasks, click Edit Group Properties.
6. In the Gateway Settings dialog box, on the Advanced tab, check or uncheck the following packet types or protocols:

   - **Allow all DHCP request packets**
     When enabled, the Gateway Enforcer appliance forwards all DHCP requests from the external network into the internal network. Because disabling this option prevents the client from getting an IP address, and since the client requires an IP address to talk to a Gateway Enforcer appliance, it is recommended that this option remain enabled. The default setting is enabled.

   - **Allow all DNS request packets**
     When enabled, the Enforcer forwards all DNS requests from the external network into the internal network. This option must be enabled if the client is configured to communicate with Symantec Endpoint Protection Manager by name rather than by IP address. This option must also be enabled if you want to use the HTTP redirect requests option on the Authentication tab. The default setting is enabled.

   - **Allow all ARP request packets**
     When this option enabled, the Gateway Enforcer appliance allows all ARP packets from the internal network. Otherwise the Gateway Enforcer appliance treats the packet as a normal IP packet and uses the sender IP as source IP and target IP as destination IP and carries out the authentication process.
The default setting is enabled.

- **Allow other protocols besides IP and ARP**
  When this option is enabled, the Gateway Enforcer appliance forwards all packets with other protocols. Otherwise it drops them.
  The default setting is disabled.
  If you checked *Allow other protocols besides IP and ARP*, you may want to complete the **Filter** field. You can hover over the field to see examples, some of which follow.
  **Examples:** allow 800, 224.12.21,900-90d, 224.21.20-224-12.21.100; block 810,224.12.21.200

7. Click **OK**.

### Allowing a legacy client to connect to the network with a Gateway Enforcer appliance

You can enable a Gateway Enforcer appliance to connect to 5.1.x legacy clients. If your network supports an 11.0.2 Symantec Endpoint Protection Manager, a Symantec Gateway Enforcer appliance, and needs to support 5.1.x legacy clients, you can enable the support of 5.1.x legacy clients on the management server console so that the Symantec Gateway Enforcer appliance does not block them.

See “**About advanced Gateway Enforcer appliance settings**” on page 249.

#### To allow a legacy client to connect to the network with a Gateway Enforcer appliance

1. In Symantec Endpoint Protection Manager, click **Admin**.
2. Click **Servers**.
3. Select and expand the group of Gateway Enforcers appliances.
4. Under **Tasks**, click **Edit Group Properties**.
5. In the Settings dialog box, on the **Advanced** tab, check **Allow legacy clients**.
6. Click **OK**.

### Enabling local authentication on a Gateway Enforcer appliance

With local authentication enabled, the Gateway Enforcer appliance loses its connection with the server on which the Symantec Endpoint Protection Manager is installed. Therefore the Gateway Enforcer appliance authenticates a client locally.

See “**About advanced Gateway Enforcer appliance settings**” on page 249.
To enable local authentication on a Gateway Enforcer appliance

1. In Symantec Endpoint Protection Manager, click Admin.
2. Click Servers.
3. Select and expand the group of Gateway Enforcers appliances.
5. In the Settings dialog box, on the Advanced tab, check Enable Local Authentication.
6. Click OK.

Enabling system time updates for the Gateway Enforcer appliance using the Network Time Protocol

With Network Time Protocol (NTP) enabled, Gateway Enforcer appliance clocks can update to the correct time. This setting is disabled by default, but it can be overridden if it is specified in a group policy.

See “About advanced Gateway Enforcer appliance settings” on page 249.

To enable time updates for Gateway Enforcer appliance from the Symantec Endpoint Protection Manager

1. In Symantec Endpoint Protection Manager, click Admin.
2. In the Admin page, click Servers.
6. Enter the IP address or the fully qualified domain name of the NTP server.
7. Click OK.

From the Enforcer console, you can temporarily change this setting to help troubleshoot time synchronization issues. From the Enforcer console command line, enter Enforcer (configure)# ntp.

Using the Gateway Enforcer appliance as a Web server

You can use the Gateway Enforcer appliance as a Web server which communicates with Symantec Endpoint Protection Manager and serves On-Demand agents. As a Web server, the Enforcer stops forwarding non-Enforcer local traffic from internal and external network but it continues to communicate with the Symantec Endpoint Protection Manager. The ability to act as a Web server is especially useful in 802.1x
environments when you want to deploy the Enforcer on a VLAN and serve On-Demand clients to guest users.

To use the Gateway Enforcer appliance as a Web server, you disable guest enforcement. You can enable guest enforcement when you want to switch back to using the Gateway Enforcer appliance to enforce guest access.

See “About advanced Gateway Enforcer appliance settings” on page 249.

To use the Gateway Enforcer appliance as a Web server

1. Log on to the Gateway Enforcer appliance as a superuser.
2. Type the following command:
   `Enforcer#configure advanced`
3. Type the following command:
   `Enforcer (advanced)#guest-enf disable`

To enable guest enforcement, type the following command:

`Enforcer(advanced)# guest_enf enable`

To check the status of guest enforcement, type the following command:

`Enforcer(advanced)# show status`

Status can be OFFLINE or ONLINE with an ACTIVE, STANDBY, or GUEST ENFORCEMENT status.

Using the Gateway Enforcer as a DNS spoofing server

When guest enforcement is enabled, the Gateway Enforcer provides DNS spoofing functionality. You cannot use this feature unless guest enforcement is enabled.

The enabled mode routes URL requests to the Gateway Enforcer instead of a remediation Web site. To activate this functionality, you must provide an IP address as the answer in a DNS response packet.

To use the Gateway Enforcer as a DNS spoofing server

1. Log on to the Gateway Enforcer appliance as a superuser.
2. Type the following command:
   `Enforcer#configure advanced`
3 Type the following command:

   Enforcer (advanced)# **dns-spoofing enable | use_local_ip | dns_spoofing_ip**

4 You can use the Gateway Enforcer's IP address or set a custom IP address.

   Enforcer (advanced)# **dns-spoofing use-local-ip enable**

   Enforcer (advanced)# **dns-spoofing-ip IP_ADDRESS**

   Where:

   *IP_ADDRESS* is your selected IP address

   To disable DNS spoofing, type the following command:

   Enforcer (advanced)# **dns-spoofing disable**

   To check DNS spoofing status, type the following command:

   Enforcer (advanced)# **show**

   The status shows the DNS spoofing feature as ENABLED or DISABLED.
Configuring the LAN Enforcer appliance on the Symantec Endpoint Protection Manager

This chapter includes the following topics:

- How the LAN Enforcer appliance works
- About configuring the Symantec LAN Enforcer on the Symantec Endpoint Protection Manager Console
- About configuring RADIUS servers on a LAN Enforcer appliance
- About configuring 802.1x wireless access points on a LAN Enforcer appliance
- Changing LAN Enforcer configuration settings in Symantec Endpoint Protection Manager
- Using general settings
- Using RADIUS server group settings
- Using switch settings
- Using advanced LAN Enforcer appliance settings
- Configuring MAC addresses and MAC authentication bypass (MAB) on the LAN Enforcer
- Using 802.1x authentication
How the LAN Enforcer appliance works

The LAN Enforcer appliance gives you the option of 802.1x EAP (Extensible Authentication Protocol) authentication, plus having the client perform a Host Integrity check.

Note: For details on EAP, refer to the IETF’s RFC 2284 at PPP Extensible Authentication Protocol (EAP). For additional details on IEEE Standard 802.1x, refer to the text of the standard at IEEE8021-PAE-MIB Definitions.

You can deploy the LAN Enforcer using one of the following modes:

- **Transparent mode**: Checks if the client is compliant with your Host Integrity policy but does not check the user name and password. Transparent mode does not use a RADIUS server, but requires an 802.1x-capable switch.

- **Full 802.1x mode**: Authenticates the user's credentials (user name and password) in addition to having the client check Host Integrity. Non-compliant clients are routed to a guest VLAN that your organization has set up for client security remediation. Full 802.1x authentication requires a RADIUS server, an 802.1x-capable switch or wireless access point, and supplicant (client) software.

In transparent mode, a LAN Enforcer appliance uses the following methods to process client computer requests to access the network:

- The client computer connects and sends logon, host authentication compliance, and policy data through EAP.

- The switch or wireless access point forwards the client computer data to the LAN Enforcer appliance.

- The LAN Enforcer appliance verifies that the client has passed a Host Integrity check.
  
  See “How the Enforcers work with Host Integrity policies” on page 132.

- If the client passes the Host Integrity check, the Enforcer opens a part of the switch and allows full network access.

- If the client fails the Host Integrity check, the Enforcer assigns the client to a quarantine VLAN where it can access remediation resources.

In full 802.1x mode, a LAN Enforcer appliance does the following to process client computer requests to access the network:

- The client computer connects and sends logon, host authentication compliance, and policy data through EAP.

- The supplicant on the client computer asks the user for their user name and password.
The switch forwards the user name and password to the LAN Enforcer.

The LAN Enforcer forwards the user name and password to the RADIUS server.

The RADIUS server generates an EAP challenge (user name and password).

The LAN Enforcer receives the EAP challenge and adds the Host Integrity check.

The LAN Enforcer verifies that the client has passed the Host Integrity check.

The LAN Enforcer checks the Host Integrity results and forwards them to the RADIUS server.

The RADIUS server performs EAP authentication and sends the result to the LAN Enforcer.

The LAN Enforcer receives the authentication result and forwards it and the action to take to the switch.

If the client passes the EAP and Host Integrity challenges, the switch allows network access.

If the client does not pass the challenges, the switch routes it to an alternate VLAN where it can access remediation resources.

The LAN Enforcer appliance has the following additional optional configuration capabilities. You can:

- Use a switch or wireless access point to direct the client to a remediation VLAN. (Recommended)

- Configure the possible failure responses, depending on whether you use EAP authentication or Host Integrity checking.

- Connect multiple LAN Enforcer appliances to one switch for LAN Enforcer failover.

- Configure multiple RADIUS servers for RADIUS server failover.

See “What you can do with Symantec Enforcer appliances” on page 171.

About configuring the Symantec LAN Enforcer on the Symantec Endpoint Protection Manager Console

You can add or edit the configuration settings for the LAN Enforcer in the Symantec Endpoint Protection Manager console. The Symantec Endpoint Protection Manager is also referred to as the management server.

Before you can proceed, you must complete the following tasks:

- Install the software for the Symantec Endpoint Protection Manager on a computer.
Connect the Symantec LAN Enforcer appliance to the network.
See “Setting up an Enforcer appliance” on page 174.

Configure the Symantec LAN Enforcer appliance on the local LAN Enforcer console during the installation.
See “Changing LAN Enforcer configuration settings in Symantec Endpoint Protection Manager” on page 260.

After you finish these tasks, you can specify all additional configuration settings for the LAN Enforcer appliance on a management server.

About configuring RADIUS servers on a LAN Enforcer appliance

You can modify the LAN Enforcer settings in the Symantec Endpoint Protection Manager console. The Enforcer must be installed and connected to the Symantec Endpoint Protection Manager before you can configure it to enforce Host Integrity policies on the client.

You can configure the following options for the LAN Enforcer:

- Define the Enforcer group description, listen port, and management server list.
- Configure the RADIUS server Group. You configure the host name or IP address, authentication port, timeout, shared secret, and number of retransmits. If you configure multiple servers in the group and one goes down, the LAN Enforcer connects to the next server in the list.
- Configure a switch or group of switches.
- Settings for enabling logging and specifying log file parameters.
- Enable and disable local authentication and legacy clients.
- Configure the LAN Enforcer working as an NTP client.

If a setting refers to an 802.1x-aware switch, the same instructions apply to configuring wireless access points.

See “About configuring 802.1x wireless access points on a LAN Enforcer appliance” on page 259.
About configuring 802.1x wireless access points on a LAN Enforcer appliance

The LAN Enforcer appliance supports a number of wireless protocols, which includes WEP 56, WEP 128, and WPA/WPA2 with 802.1x.

You can configure a LAN Enforcer to protect the wireless access point (AP) as much as it protects a switch if the following conditions are met:

- The network includes a wireless LAN Enforcer appliance with 802.1x.
- Wireless clients run a supplicant that supports one of these protocols.
- The wireless AP supports one of these protocols.

For wireless connections, the authenticator is the logical LAN port on the wireless AP.

You configure a wireless AP for 802.1x and for switches in the same way. You include wireless APs to the LAN Enforcer settings as part of a switch profile. Wherever an instruction or part of the user interface refers to a switch, use the comparable wireless AP terminology. For example, if you are instructed to select a switch model, select the wireless AP model. If the vendor of the wireless AP is listed, select it for the model. If the vendor is not listed, choose Others.

The configuration for wireless AP for 802.1x and for switches include the following differences:

- Only basic configuration is supported.
  The transparent mode is not supported.

- There can also be differences in support for VLANs, depending on the wireless AP.
  Some dynamic VLAN switches may require you to configure the AP with multiple service set identifiers (SSIDs). Each SSID is associated with a VLAN.
  See the documentation that comes with the dynamic VLAN switch.

Based on the wireless AP model that you use, you may want to use one of the following access control options instead of a VLAN:
Access control lists (ACLs)

Some wireless APs support ACLs that enable the network administrator to define policies for network traffic management. You can use the generic option on the LAN Enforcer by selecting the vendor name of the wireless AP. As an alternative, you can select Others for the 802.1x-aware switch model (if it is not listed).

The generic option sends a generic attribute tag with the VLAN ID or name in it to the access point. You can then customize the access point. Now the access point can read the generic attribute tag for the VLAN ID and match it with the WAP’s ACL ID. You can use the Switch Action table as an ACL Action table.

Additional configuration on the wireless AP or AP controller may be required. For example, you may need to map the RADIUS tag that is sent to the wireless AP on the AP controller.

See the wireless AP documentation for details.

MAC level 802.1x

You can plug the wireless AP into a switch that supports MAC level 802.1x. For this implementation, you must disable 802.1x on the wireless AP. You can only use it on the switch. The switch then authenticates the wireless clients by recognizing the new MAC addresses. After it authenticates a MAC address, it puts that MAC address on the specified VLAN instead of the whole port. Every new MAC address has to be authenticated. This option is not as secure. However, this option enables you to use the VLAN switching capability.

See “Changing LAN Enforcer configuration settings in Symantec Endpoint Protection Manager” on page 260.

Changing LAN Enforcer configuration settings in Symantec Endpoint Protection Manager

You can change the LAN Enforcer configuration settings on a management server. The configuration settings are automatically downloaded from the management server to the LAN Enforcer appliance during the next heartbeat.

To change LAN Enforcer configuration settings in Symantec Endpoint Protection Manager

1. In Symantec Endpoint Protection Manager, click Admin.
2. Click Servers.
3 Select the group of Enforcers of which the LAN Enforcer appliance is a member. The Enforcer group must include the LAN Enforcer whose configuration settings need to be changed.

4 Select the LAN Enforcer appliance whose configuration settings need to be changed.

5 Under **Tasks**, click **Edit Group Properties**.

6 In the **Settings** dialog box, change any of the configuration settings.

The **LAN Enforcer Settings** dialog box provides the following categories of configuration settings:

**General**

This tab provides the following LAN Enforcer settings:

- Group name for LAN Enforcer appliances
- Listening port
- Description for the LAN Enforcer appliance group
- Selection of the management server list that the LAN Enforcer uses

See “**Using general settings**” on page 262.

**RADIUS Server Group**

This tab provides the following LAN Enforcer settings:

- Name for the RADIUS Server group
- Host name or IP address for the RADIUS Server
- Port number for the RADIUS Server
- Friendly name for the RADIUS Server

See “**Using RADIUS server group settings**” on page 266.

**Switch**

This tab provides the following LAN Enforcer settings:

- Enable the switch policy
- The name of the switch policy
- The switch model, selected from a list of supported switches
- The shared secret
- The RADIUS server group
- The reauthentication timeout period
- Whether the switch forwards other protocols besides EAP
- Switch Address
- The VLAN on the Switch
- Action

See “**Using switch settings**” on page 273.
Advanced

This tab provides the following advanced LAN Enforcer settings:

- Configure MAC Authentication Bypass (MAB)
- Specify MAC addresses and VLANs
- Allow legacy client
- Enable local authentication
- Configure Network Time Protocol

See “Using advanced LAN Enforcer appliance settings” on page 298.

Log settings

Settings for enabling logging of Server logs, Client Activity logs, and specifying log file parameters.

See “About Enforcer reports and logs” on page 380.

See “Configuring Enforcer log settings” on page 381.

Using general settings

You can add or edit the description of a LAN Enforcer appliance or a LAN Enforcer appliance group in the Symantec Endpoint Protection Manager Console.

See “Adding or editing the description of an Enforcer group with a LAN Enforcer” on page 264.

See “Adding or editing the description of a LAN Enforcer” on page 264.

You must establish a listening port that is used for communication between the VLAN switch and the LAN Enforcer appliance.

See “Specifying a listening port for communication between a VLAN switch and a LAN Enforcer” on page 263.

However, you cannot add or edit the name of a LAN Enforcer appliance group in the Symantec Endpoint Protection Manager Console. You cannot add or edit the IP address or host name of a LAN Enforcer appliance in the Symantec Endpoint Protection Manager Console. Instead, you must perform these tasks on the Enforcer console.

See “Adding or editing the name of a LAN Enforcer appliance group with a LAN Enforcer” on page 263.

However, you can only change the IP address or host name of a LAN Enforcer on the Enforcer console during the installation. If you later want to change the IP address or host name of a LAN Enforcer, you can do so on the LAN Enforcer console.

See “Adding or editing the IP address or host name of a LAN Enforcer” on page 264.
However, you can add or edit the IP address or host name of a Symantec Endpoint Protection Manager in a management server list.

See “Connecting the LAN Enforcer to Symantec Endpoint Protection Manager” on page 265.

Adding or editing the name of a LAN Enforcer appliance group with a LAN Enforcer

You cannot add or edit the name of a LAN Enforcer appliance group of which a LAN Enforcer appliance is a member. You perform these tasks on the Enforcer console during the installation. If you later want to change the name of a LAN Enforcer appliance group, you can do so on the Enforcer console.

All Enforcers in a group share the same configuration settings.

See “Using general settings” on page 262.

Specifying a listening port for communication between a VLAN switch and a LAN Enforcer

When you configure the settings for a LAN Enforcer you specify the following listening ports:

- The listing port that is used for communication between the VLAN switch and the LAN Enforcer.
  The VLAN switch sends the RADIUS packet to the UDP port.

- The listening port that is used for communication between the LAN Enforcer and a RADIUS server.
  You specify this port when you specify a RADIUS server.

If the RADIUS server is installed on the management server, it should not be configured to use port 1812. The RADIUS servers are configured to use port 1812 as the default setting. Because the management server also uses port 1812 to communicate with the LAN Enforcer, there is a conflict.

See “Using general settings” on page 262.

To specify a listening port that is used for communication between a VLAN switch and a LAN Enforcer

1. In the Symantec Endpoint Protection Manager Console, click Admin.
2. Click Servers.
3. Under Servers, select the Enforcer group.
5 In the **LAN Enforcer Settings** dialog box, on the **General** tab, type the number of the UDP port that you want to assign in the **Listen port** field.

The default setting for the port is 1812. The range extends from 1 through 65535.

6 Click **OK**.

**Adding or editing the description of an Enforcer group with a LAN Enforcer**

You can add or edit the description of an Enforcer group of which a Symantec LAN Enforcer appliance is a member. You can perform this task on Symantec Endpoint Protection Manager instead of the LAN Enforcer console.

See “**Using general settings**” on page 262.

**To add or edit the description of an Enforcer group with a LAN Enforcer**

1 In Symantec Endpoint Protection Manager, click **Admin**.

2 Click **Servers**.

3 Select and expand the Enforcer group whose description you want to add or edit.

4 Under **Tasks**, click **Edit Group Properties**.

5 In the **Settings** dialog box, on the **General** tab, add or edit a description for the Enforcer group in the **Description** field.

6 Click **OK**.

**Adding or editing the IP address or host name of a LAN Enforcer**

You can only change the IP address or host name of a LAN Enforcer on the Enforcer console during the installation. If you later want to change the IP address or host name of a LAN Enforcer, you can do so on the LAN Enforcer console.

See “**Using general settings**” on page 262.

**Adding or editing the description of a LAN Enforcer**

You can add or edit the description of a LAN Enforcer. You can perform this task on Symantec Endpoint Protection Manager instead of the LAN Enforcer console.

After you complete this task, the description appears in Description field of the Management Server pane.

See “**Using general settings**” on page 262.
To add or edit the description of a LAN Enforcer

1. In Symantec Endpoint Protection Manager, click **Admin**.
2. Click **Servers**.
3. Select and expand the Enforcer group that includes the LAN Enforcer whose description you want to add or edit.
4. Select the LAN Enforcer whose description you want to add or edit.
5. Under **Tasks**, click **Edit Enforcer Properties**.
6. In the **Enforcer Properties** dialog box, add or edit a description for the LAN Enforcer in the **Description** field.
7. Click **OK**.

Connecting the LAN Enforcer to Symantec Endpoint Protection Manager

Enforcers must be able to connect to servers on which Symantec Endpoint Protection Manager is installed. Symantec Endpoint Protection Manager uses a management server list to help manage the traffic between clients, management servers, and optional Enforcers, such as a LAN Enforcer. The management server list specifies to which Symantec Endpoint Protection Manager a LAN Enforcer connects. It also specifies to which Symantec Endpoint Protection Manager a LAN Enforcer connects in case of a management server's failure.

If an administrator has created multiple management server lists, you can select the specific management server list that includes the IP addresses or host names of those management servers to which you want the LAN Enforcer to connect. If there is only one management server at a site, then you can select the default management server list. You can also select the management server list that you want an Enforcer group to be able to roam among, making choices in the same dialog box.

See “Using general settings” on page 262.

To connect the LAN Enforcer to Symantec Endpoint Protection Manager

1. In Symantec Endpoint Protection Manager, click **Admin**.
2. Click **Servers**.
3. Select and expand the group of Enforcers.

   The Enforcer group must include the LAN Enforcer for which you want to change the management server list.

4. Under **Tasks**, click **Edit Group Properties**.
In the **Settings** dialog box, on the **General** tab, under **Communication**, select the management server list that you want this LAN Enforcer to use.

On the **General** tab, under **Communication**, click **Select**.

You can view the IP addresses and host names of all available management servers, as well as the priorities that have been assigned to them.

In the **Management Server List** dialog box, click **Close**.

Click **OK**.

### Using RADIUS server group settings

You can configure the LAN Enforcer to connect to one or more RADIUS servers. You need to specify RADIUS servers as part of a RADIUS server group. Each group can contain one or more RADIUS servers. The purpose of a RADIUS server group is for RADIUS servers to provide failover. If one RADIUS server in the RADIUS server group becomes unavailable, the LAN Enforcer tries to connect with another RADIUS server that is part of the RADIUS server group.

You can add, edit, and delete the name of a RADIUS server group in the Symantec Endpoint Protection Manager Console.

See “Adding a RADIUS server group name and RADIUS server” on page 266.

See “Editing the name of a RADIUS server group” on page 268.

See “Deleting the name of a RADIUS server group” on page 272.

Add, edit, and delete the name, host name, IP address, authentication port number, and the shared secret of a RADIUS server in the Symantec Endpoint Protection Manager Console.

See “Adding a RADIUS server group name and RADIUS server” on page 266.

See “Editing the friendly name of a RADIUS server” on page 269.

See “Editing the host name or IP address of a RADIUS server” on page 270.

See “Editing the authentication port number of a RADIUS server” on page 270.

See “Editing the shared secret of a RADIUS server” on page 271.

See “Deleting a RADIUS server” on page 273.

### Adding a RADIUS server group name and RADIUS server

You can add a RADIUS server group name and RADIUS server at the same time.

See “Using RADIUS server group settings” on page 266.
To add a RADIUS server group name and RADIUS server

1. In Symantec Endpoint Protection Manager, click **Admin**.
2. Click **Servers**.
3. Select the Enforcer group.
4. Under **Tasks**, click **Edit Group Properties**.
5. In the **LAN Enforcer Settings** dialog box, on the **RADIUS Server Group** tab, click **Add**.
   
   The name of the RADIUS server group and the IP address of an existing RADIUS server appear in the table.

6. In the **Add RADIUS Server Group** dialog box, type the name of the RADIUS server group in the **Group** text box.
   
   The name of the RADIUS server group, the host name or IP address of an existing RADIUS server, and the port number of the RADIUS server appear in the table.

7. Click **Add**.
8 In the **Add RADIUS Server** dialog box, type the following:

- **In the field: Friendly name of RADIUS server**
  - Type a name that easily identifies the name of the RADIUS server when it appears on the list of servers for that group.

- **In the field: Hostname or IP address**
  - Type the hostname or IP address of the RADIUS server.

- **In the field: Authentication port**
  - Type the network port on the RADIUS server where the LAN Enforcer sends the authentication packet from the client.
  - The default setting is 1812.

- **In the field: Switch timeout (in seconds)**
  - Type the switch timeout value. The default is 3 seconds.

- **In the field: Switch retransmits**
  - Type the switch retransmits value. The default is one.

- **In the field: Shared secret**
  - Type the shared secret that is used for encrypted communication between the RADIUS server and the LAN Enforcer. The shared secret between a RADIUS server and a LAN Enforcer can be different from the shared secret between an 802.1x-aware switch and a LAN Enforcer. The shared secret is case sensitive.

- **In the field: Confirm shared secret**
  - Type the shared secret again.

9 Click **OK**.

The name, Hostname or IP address, and port for the RADIUS server you added now appear in the **RADIUS Server Group** list in the **Add RADIUS Server Group** dialog box.

10 In the **Add RADIUS Server Group** dialog box, click **OK**.

11 In the **LAN Enforcer Settings** dialog box, click **OK**.

**Editing the name of a RADIUS server group**

You can change the name of the RADIUS server group at any time if circumstances change.

See “**Using RADIUS server group settings**” on page 266.
To edit the name of a RADIUS server group

1. In Symantec Endpoint Protection Manager, click Admin.
2. Click Servers.
3. Select the Enforcer group of which the LAN Enforcer is a member.
5. In the LAN Enforcer Settings dialog box, on the RADIUS Server Group tab, click the RADIUS server group whose name you want to change.
6. Click Edit.
7. In the Add RADIUS Server dialog box, edit the name of the RADIUS server group in the Group name field.
8. Click OK.
9. In the LAN Enforcer Settings dialog box, on the RADIUS Server Group tab, click OK.

Editing the friendly name of a RADIUS server

You can change the friendly name of the RADIUS server at any time if circumstances change.

See “Using RADIUS server group settings” on page 266.

To edit the friendly name of a RADIUS server

1. In Symantec Endpoint Protection Manager, click Admin.
2. Click Servers.
3. Select the Enforcer group of which the LAN Enforcer is a member.
5. In the LAN Enforcer Settings dialog box, on the RADIUS Server Group tab, click the RADIUS server group that includes the RADIUS server whose friendly name you want to change.
6. Click Edit.
7. In the Add a RADIUS Server dialog box, edit the friendly name of the RADIUS server in the Friendly name of RADIUS server field.
8. Click OK.
9. In the LAN Enforcer Settings dialog box, on the RADIUS Server Group tab, click OK.
Editing the host name or IP address of a RADIUS server

You can change the host name or IP address of the RADIUS server at any time if circumstances change.

See “Using RADIUS server group settings” on page 266.

To edit the host name or IP address of a RADIUS server

1. In Symantec Endpoint Protection Manager, click **Admin**.
2. Click **Servers**.
3. Select the Enforcer group of which the LAN Enforcer is a member.
4. Under **Tasks**, click **Edit Group Properties**.
5. In the **LAN Enforcer Settings** dialog box, on the **RADIUS Server Group** tab, click the RADIUS server group that includes the RADIUS server whose host name or IP address you want to change.
6. Click **Edit**.
7. In the **Add a RADIUS Server** dialog box, edit the host name or IP address of the RADIUS server in the **Hostname or IP Address** field.
8. Click **OK**.
9. In the **LAN Enforcer Settings** dialog box, on the **RADIUS Server Group** tab, click **OK**.

Editing the authentication port number of a RADIUS server

You can change the authentication port number of the RADIUS server at any time if circumstances change.

See “Using RADIUS server group settings” on page 266.

To edit the authentication port number of a RADIUS server

1. In Symantec Endpoint Protection Manager, click **Admin**.
2. Click **Servers**.
3. Select the Enforcer group of which the LAN Enforcer is a member.
4. Under **Tasks**, click **Edit Group Properties**.
5. In the **LAN Enforcer Settings** dialog box, on the **RADIUS Server Group** tab, click the RADIUS server group that includes the RADIUS server whose authentication port number you want to change.
6. Click **Edit**.
7 In the **Add a RADIUS Server** dialog box, edit the authentication port number of the RADIUS server in the **Authentication port** field.

8 Click **OK**.

9 In the **LAN Enforcer Settings** dialog box, on the **RADIUS Server Group** tab, click **OK**.

---

**Editing the shared secret of a RADIUS server**

You can change the shared secret of the RADIUS server at any time if circumstances change.

See “Using RADIUS server group settings” on page 266.

**To edit the shared secret of a RADIUS server**

1 In Symantec Endpoint Protection Manager, click **Admin**.

2 Click **Servers**.

3 Select the Enforcer group of which the LAN Enforcer is a member.

4 Under **Tasks**, click **Edit Group Properties**.

5 In the **LAN Enforcer Settings** dialog box, on the **RADIUS Server Group** tab, click the RADIUS server group that includes the RADIUS server whose shared secret you want to change.

6 In the **LAN Enforcer Settings** dialog box, on the **RADIUS Server Group** tab, click **Edit**.

7 In the **Add a RADIUS Server** dialog box, edit the shared secret of the RADIUS server in the **Shared secret** field.

The shared secret is used for encrypted communication between the RADIUS server and the LAN Enforcer. The shared secret between a RADIUS server and a LAN Enforcer can be different from the shared secret between an 802.1x-aware switch and a LAN Enforcer. The shared secret is case sensitive.

8 Edit the shared secret of the RADIUS server in the **Confirm shared secret** field.

9 Click **OK**.

10 In the **LAN Enforcer Settings** dialog box, on the **RADIUS Server Group** tab, click **OK**.
Enabling support for Windows Network Policy Server (NPS) on the LAN Enforcer

When you use a Microsoft Windows Server as a RADIUS server, it has in the past used Internet authentication server (IAS). With Windows Server 2008, IAS has been replaced with Network Policy Server (NPS). If you are using Server 2008, you must specify that you are using NPS.

Note: Enabling support for Windows NPS requires that clients and LAN Enforcers run Symantec Endpoint Protection version 11.0 RU6 MP2 or higher (including 12.1). If you enable this option on LAN Enforcers with legacy clients, Symantec Network Access Control functionality is not supported.

To enable support for Windows Network Policy Server

1. On the Servers screen, select the LAN Enforcer.
2. Under Tasks, click Edit Group Properties.
3. In the LAN Enforcer Settings dialog box, click the RADIUS Server Group tab.
4. At the bottom of the screen, click to Enable support for Windows Network Policy Server (NPS).

You will see a Warning note that is similar to the Note above. Be certain that your clients and LAN Enforcers are running version 11.0 RU6 MP2 or higher.
5. Click OK to save your configuration.

Deleting the name of a RADIUS server group

You can delete the name of the RADIUS server group at any time if circumstances change.

See “Using RADIUS server group settings” on page 266.

To delete the name of a RADIUS server group

1. In Symantec Endpoint Protection Manager, click Admin.
2. Click Servers.
3. Select the Enforcer group of which the LAN Enforcer is a member.
5. In the LAN Enforcer Settings dialog box, on the RADIUS Server Group tab, click the RADIUS server group whose name you want to delete.
Deleting a RADIUS server

You can delete a RADIUS server at any time if circumstances change.

See “Using RADIUS server group settings” on page 266.

To delete a RADIUS server

1. In Symantec Endpoint Protection Manager, click Admin.
2. Click Servers.
3. Under Servers, select the Enforcer group of which the LAN Enforcer is a member.
5. In the LAN Enforcer Settings dialog box, on the RADIUS Server Group tab, click the RADIUS server group of which the RADIUS server that you want to delete is a member.
6. In the LAN Enforcer Settings dialog box, on the RADIUS Server Group tab, click Edit.
7. In the Add RADIUS Server dialog box, click the RADIUS server that you want to delete.
8. Click Remove.
9. Click OK.
10. In the LAN Enforcer Settings dialog box, on the RADIUS Server Group tab, click OK.

Using switch settings

You configure a switch policy when you specify LAN Enforcer settings for switches. A switch policy is a collection of settings that is applied to a group of switches of the same manufacturer or model. The only information that you need to enter separately for individual switches is the IP address of the switch.

See “Adding an 802.1x switch policy for a LAN Enforcer appliance with a wizard” on page 277.

See “Editing basic information about the switch policy and 802.1x-aware switch” on page 285.
Switch settings

You need to specify the following basic information before LAN Enforcer appliances, management servers, clients, and 802.1x-aware switches all work together:

- A name of your choice for the switch policy
- The switch manufacturer and model
  You select the switch model from a list of supported switches.
- The encrypted password or shared secret
- The RADIUS server group that is used
- The reauthentication timeout period for the 802.1x-aware switch
  The default setting is 30 seconds.
- Whether the switch forwards other protocols besides EAP
  The default setting is to forward other protocols.

See “Adding an 802.1x switch policy for a LAN Enforcer appliance with a wizard” on page 277.

See “Editing basic information about the switch policy and 802.1x-aware switch” on page 285.

You need to specify the following information for the set of 802.1x-aware switches to which the switch policy applies:

- A friendly switch name of your choice
- IP address, IP address range, or subnet

See “Adding an 802.1x switch policy for a LAN Enforcer appliance with a wizard” on page 277.

See “Editing information about the 802.1x-aware switch” on page 290.

You need to specify the following VLAN information:

- VLAN ID
- VLAN name
- Optionally, you can specify the customized RADIUS attributes in hexadecimal format.

See “Adding an 802.1x switch policy for a LAN Enforcer appliance with a wizard” on page 277.

See “Editing VLAN information for the switch policy” on page 291.

If an 802.1x-aware switch supports dynamic VLAN switching, you can specify that the client must connect to a specific VLAN.
You need to specify the actions that the 802.1x-aware switch needs to take when certain criteria are met:

- Host authentication result: Pass, Fail, Unavailable, or Ignore Result
- User authentication result: Pass, Fail, Unavailable, or Ignore Result
- Policy Check result: Pass, Fail, Unavailable, or Ignore Result

See “Adding an 802.1x switch policy for a LAN Enforcer appliance with a wizard” on page 277.

About the support for attributes of switch models

When you configure the LAN Enforcer appliance, you specify the model of the 802.1x-aware switch. Different 802.1x-aware switches look for different attributes to determine which client can access the VLAN. Some switches identify VLANs by VLAN ID and others by VLAN Name. Some devices have limited or no VLAN support.

The LAN Enforcer appliance forwards attributes from the RADIUS server to the switch. If necessary, however, it modifies or appends the VLAN attribute based on the switch type by using supported values. If a conflict exists between the vendor-specific attribute information that the RADIUS server sends and the vendor-specific VLAN attribute information that the LAN Enforcer uses, the LAN Enforcer removes the vendor-specific information that the RADIUS server sends.

The LAN Enforcer then replaces that information with the information that appears in Table 19-1.

If you want to keep the attributes from the RADIUS server, you can select an action called **Open Port**. With this action, the LAN Enforcer forwards all attributes from the RADIUS server to the 802.1x-aware switch without any modifications.

The 802.1x-aware switch model can use VLAN ID or VLAN Name to perform dynamic VLAN assignments. Specify both the VLAN ID and VLAN name when you provide VLAN information for the LAN Enforcer, with the exception of the Aruba switch.

See “Changing LAN Enforcer configuration settings in Symantec Endpoint Protection Manager” on page 260.

**Table 19-1** describes the 802.1x-aware switch models and attributes.
<table>
<thead>
<tr>
<th>Switch model</th>
<th>Attributes added by LAN Enforcer</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Airespace Wireless</td>
<td>The vendor code is 14179. The vendor-assigned attribute number is 5. The attribute format is</td>
<td>VLAN Name is used. Name is case sensitive.</td>
</tr>
<tr>
<td>Controller</td>
<td>“string.”</td>
<td></td>
</tr>
<tr>
<td>Alcatel</td>
<td>Vendor Specific (#26)</td>
<td>VLAN ID is used.</td>
</tr>
<tr>
<td></td>
<td>The vendor ID of Alcatel is 800. All “Vendor Specific” attributes from RADIUS with an ID of</td>
<td></td>
</tr>
<tr>
<td></td>
<td>800 are removed in case of conflict.</td>
<td></td>
</tr>
<tr>
<td>Aruba</td>
<td>Vendor Specific (#14823)</td>
<td>Both VLAN name and VLAN ID can be used. Alternately, you can use only a</td>
</tr>
<tr>
<td></td>
<td>Vendor ID is 14823 for Aruba. The Aruba-User-Role attribute permits you to set up either VLAN</td>
<td>VLAN name or only a VLAN ID. A valid VLAN ID ranges from 1 to 4094.</td>
</tr>
<tr>
<td></td>
<td>IDs or VLAN names.</td>
<td>A VLAN name cannot exceed 64 bytes.</td>
</tr>
<tr>
<td>Cisco Aironet Series</td>
<td>Depends on whether you use SSID access control. RADIUS user attributes used for VLAN-ID</td>
<td>VLAN ID is used.</td>
</tr>
<tr>
<td></td>
<td>assignment:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IETF 64 (Tunnel Type): Set this attribute to “VLAN”</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IETF 65 (Tunnel Medium Type): Set this attribute to “802”</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IETF 81 (Tunnel Private Group ID): Set this attribute to VLAN-ID</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RADIUS user attribute used for SSID access control:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco IOS/PIX RADIUS Attribute, 009\001 cisco-av-pair</td>
<td></td>
</tr>
<tr>
<td>Cisco Catalyst Series</td>
<td>Tunnel Type (#64)</td>
<td>VLAN Name is used. Name is case sensitive.</td>
</tr>
<tr>
<td></td>
<td>Tunnel Medium Type (#65)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Tunnel Private Group ID (#81)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Tunnel Type is set to 13 (VLAN)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Tunnel Medium Type is set to 6 (802 media)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Tunnel Private Group ID is set to VLAN name.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>All attributes with these three types from RADIUS server are removed in case of conflict.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Also, any attribute with type “Vendor Specific” and the vendor ID is 9 (Cisco) are also removed.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 19-1  
Support for attributes of switch models (*continued*)

<table>
<thead>
<tr>
<th>Switch model</th>
<th>Attributes added by LAN Enforcer</th>
<th>Comments</th>
</tr>
</thead>
</table>
| Foundry, HP, Nortel, 3com, Huawei | Tunnel Type (#64)  
Tunnel Medium Type (#65)  
Tunnel Private Group ID (#81)  
Tunnel Type is set to 13 (VLAN)  
Tunnel Medium Type is set to 6 (802 media)  
Tunnel Private Group ID is set to VLAN ID.  
All attributes with these three types from RADIUS server are removed in case of conflict. | VLAN ID is used. |
| Enterasys | Filter ID (#11)  
Filter ID is set to  
Enterasys:  
version=1:  
mgmt=su:  
policy=NAME  
All "Filter ID" attributes from RADIUS Server are removed in case of conflict. | VLAN Name is used and represents “Role name” in the Enterasys switch. The name is case sensitive. |
| Extreme | Vendor Specific (#26)  
Vendor ID is 1916 for Extreme. VLAN Name is added after the Vendor ID. All vendor-specific attributes from RADIUS server with an ID of 1916 are removed in case of conflict. | VLAN Name is used. The name is case sensitive. |

**Adding an 802.1x switch policy for a LAN Enforcer appliance with a wizard**

You can add multiple 802.1x-aware switches for use with a LAN Enforcer appliance as part of a switch policy. You must enter the information that is needed to configure the LAN Enforcer appliance interaction with the switch.

See “Using switch settings” on page 273.
To add an 802.1x switch policy for a LAN Enforcer appliance with a wizard

1. In Symantec Endpoint Protection Manager, click Admin.
2. Click Servers.
3. Select the Enforcer group.
5. In the LAN Enforcer Settings dialog box, on the Switch tab, click Add.
6. In the Welcome to the Switch Policy Configuration Wizard panel of the Switch Policy Configuration Wizard, click Next.
7. In the Basic Information panel of the Switch Policy Configuration Wizard, complete the following tasks:

   Switch policy name  Type a name of your choice that identifies the switch policy. For example, you can use the manufacturer's name and model as the name for the switch policy name.
Switch model

The LAN Enforcer uses the switch model to determine the vendor-specific RADIUS server attribute.

Select one of the following 802.1x-aware models from the list of supported switches:

- Other
  If your model is not listed, select Other to use a generic RADIUS server attribute.
- 3Com
- Alcatel switch
- Cisco Catalyst Series
- Enterasys Matrix Series
- Extreme Summit Series
- Foundry Networks
- HP ProCurve Series
- Nortel BayStack Series
- Cisco Aironet Series
- Aruba Switches
- Airespace Wireless Controller
- Nortel Wireless
- Enterasys wireless controller
- Allied Telesis switches
- HuaWei switches later than Jan. 2009

Note: For the HuaWei switches, if the administrator chooses transparent mode on the switch, the administrator must configure the policy to use transparent mode on the client, rather than letting the user select it.

Shared secret

The shared secret that is used for communication between the 802.1x-aware switch and the LAN Enforcer appliance. The shared secret is case sensitive.

Confirm shared secret

You must type the shared secret again.

RADIUS server group

If you use the LAN Enforcer appliance with a RADIUS server, you must select the RADIUS server group from the available RADIUS server group list.
Typetheamountoftimeinsecondsduringwhichtheclient
mustbereauthenticated.Otherwisetheclientisremoved
fromthelistofconnectedclientsontheLANEnforcer.

Youshouldsetthereauthenticationperiodtobeatleast
doubletheamountoftimeofthereauthenticationintervalon
theswitch.

Forexample,ifthereauthenticationintervalontheswitchis
30seconds,thelANEnforcerapplianceauthentication
periodshouldbeatleast60seconds.OtherwisetheLAN
Enforcerapplianceassumesthattheclientistimedout.
ThereforetheclientdoesnotreleaseandrenewitsIP
address.

The defaultsettingis30seconds.

---

### Reauthentication period (seconds)

<table>
<thead>
<tr>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type the amount of time in seconds during which the client must be reauthenticated. Otherwise the client is removed from the list of connected clients on the LAN Enforcer.</td>
<td></td>
</tr>
</tbody>
</table>

You should set the reauthentication period to be at least double the amount of time of the reauthentication interval on the switch.

For example, if the reauthentication interval on the switch is 30 seconds, the LAN Enforcer appliance reauthentication period should be at least 60 seconds. Otherwise the LAN Enforcer appliance assumes that the client is timed out. Therefore the client does not release and renew its IP address.

The default setting is 30 seconds.

---

### Forward protocols besides EAP

<table>
<thead>
<tr>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>You can select this option to allow the LAN Enforcer appliance to forward the RADIUS packets that contain other authentication protocols besides EAP. Other protocols include Challenge Handshake Authentication Protocol (CHAP) and PAP.</td>
<td></td>
</tr>
</tbody>
</table>

The default setting is enabled.

---

8 In the Basic Information panel of the Switch Policy Configuration Wizard, click Next.

9 In the Switch List panel of the Switch Policy Configuration Wizard, click Add.
Complete the following tasks:

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>In the <strong>Add Single Internal IP address</strong> dialog box, type a friendly name for the switch policy to identify the 802.1x-aware switch into the Name field.</td>
</tr>
<tr>
<td>Single IP Address</td>
<td>In the <strong>Add Single Internal IP Address</strong> dialog box, click <strong>Single IP address</strong>. Then type the IP address of the 802.1x-aware switch in the <strong>IP Address</strong> field.</td>
</tr>
<tr>
<td>IP Address Range</td>
<td>In the <strong>Add Internal IP Address Range</strong> dialog box, click <strong>IP Address Range</strong>. Type the beginning IP address for the 802.1x-aware switch in the <strong>Starting IP Address</strong> field. Type the ending IP address of the IP address range for the 802.1x-aware switch in the <strong>End IP</strong> field.</td>
</tr>
<tr>
<td>Subnet</td>
<td>In the <strong>Add Internal IP Address Subnet</strong> dialog box, click <strong>Subnet</strong>. Type the IP address for the subnet in the <strong>IP address</strong> field and the subnet in the <strong>Subnet Mask</strong> field.</td>
</tr>
</tbody>
</table>

When you specify a switch policy for a LAN Enforcer appliance, you can associate the switch policy with one or more 802.1x-aware switches.

11 In the **Add Internal IP address** dialog box, click **OK**.

12 In the **Switch List** panel of the **Switch Policy Configuration Wizard**, click **Next**.

13 In the **Switch VLAN Configuration** panel of the **Switch Policy Configuration Wizard**, click **Add**.
14 In the **Add VLAN** dialog box, complete the following tasks:

- **VLAN ID**: Type an integer that can range from 1 to 4094 in the VLAN ID field.
  
  The VLAN ID must be the same as the one that is configured on the 802.1x-aware switch except for the Aruba switch.
  
  If you plan to add VLAN information about an Aruba switch, you may want to configure VLAN and role information differently than you have for other 802.1x switches.
  
  See “Configuring VLAN and role information on the 802.1x-aware Aruba switch” on page 293.

- **VLAN Name**: Type a name of the VLAN.
  
  The name for the VLAN can be up to 64 characters. It is case sensitive.
  
  The VLAN name must be the same as the one that is configured on the 802.1x-aware switch except for the Aruba switch.
  
  If you plan to add VLAN information about an Aruba switch, you may want to configure VLAN and role information that is different from other 802.1x switches.
  
  See “Configuring VLAN and role information on the 802.1x-aware Aruba switch” on page 293.

- **Send customized RADIUS attributes to switch**: Check **Send customized RADIUS attributes to switch** if you want the LAN Enforcer to send a customized RADIUS attribute to the 802.1x-aware switch. An attribute can be an access control list (ACL).
  
  See “About the support for attributes of switch models” on page 275.

- **Customized attributes in hex format**: Type the RADIUS attribute in hex format.
  
  The length must be even.

When you specify a switch policy for a LAN Enforcer, you use the **VLAN** tab to add the VLAN information for each VLAN that is configured on the switch. You want the switch policy to be available for use by the LAN Enforcer as an action. The best practice is to specify at least one remediation VLAN.

15 Click **OK**.

16 In the **Switch VLAN Configuration** panel of the **Switch Policy Configuration Wizard**, click **Next**.
17 In the **Switch Action Configuration** panel of the **Switch Policy Configuration Wizard**, click **Add**.

18 In the **Add Switch Action** dialog box, complete the following tasks:

**Host Authentication**
Click any of the following conditions:
- Passed
- Failed
- Unavailable
- Ignore Result

A typical situation in which a Host Integrity check becomes unavailable would be the result of a client not running. If you set Host Authentication to Unavailable, you must also set Policy Check to Unavailable.

**User Authentication**
Click any of the following conditions:
- Passed
  - The client has passed user authentication.
- Failed
  - The client has not passed user authentication.
- Unavailable
  - The user authentication result is always unavailable if user authentication is not performed in transparent mode. If you use the LAN Enforcer in transparent mode, you must create an action for the Unavailable condition.
  - If you use the basic configuration, you may also want to configure an action for the user authentication as an error condition. For example, an 802.1x supplicant uses an incorrect user authentication method or the RADIUS server fails in the middle of the authentication transaction.
  - The user authentication’s Unavailable condition may also occur on some RADIUS servers if the user name does not exist in the RADIUS database. For example, this problem may occur with Microsoft IAS. Therefore you may want to test the condition of a missing user name with your RADIUS server. You may want to see whether it matches the Failed or Unavailable user authentication conditions.
- Ignore Result

A typical situation in which a Host Integrity check becomes unavailable would be the result of a client not running. If you set Policy Check to Unavailable, you must also set Host Authentication to Unavailable.
Policy Check

Click any of the following conditions:

- **Passed**
  The client has passed the Policy Check.

- **Failed**
  The client has not passed the Policy Check.

- **Unavailable**
  The Unavailable result for the policy may occur under the following conditions:
  - If the client has an invalid identifier, then the LAN Enforcer cannot obtain any policy information from the management server. This problem can occur if the management server that deployed the client policy is no longer available.
  - If the client is first exported and installed before it connects to the management server and receives its policy.

Ignore Result

Action

You can select the following actions that the 802.1x-aware switch performs when the conditions are met:

- **Open Port**
  The 802.1x-aware switch allows network access on the default VLAN to which the port is normally assigned. It also allows network access on the VLAN that is specified in an attribute that is sent from the RADIUS server. Therefore the support of users having VLAN access is based on user ID and user role.
  The default action is Open Port.

- **Switch to VLAN-test**
  Allows access to the specified VLAN. The VLANs that are available to select are the ones that you configured previously.

- **Close Port**
  Deny network access on the default or RADIUS-specified VLAN. On some switch models, depending on the switch configuration, the port is assigned to a guest VLAN.

For the Aruba switch, you can restrict access according to a specified role as well as a specified VLAN. The restrictions depend on how you configured the VLAN information for the switch policy.

19 In the Add Switch Action dialog box, click OK.
20 In the **Switch Action Configuration** panel of the **Switch Policy Configuration Wizard**, in the **Switch Action** table, click the switch action policy whose priority you want to change.

The LAN Enforcer checks the authentication results against the entries in the switch action table in the order from top to bottom of the table. After it finds a matching set of conditions, it instructs the 802.1x-aware switch to apply that action. You can change the sequence in which actions are applied by changing the order in which they are listed in the table.

21 Click **Move Up** or **Move Down**.

22 Click **Next**.

23 In the **Complete the Switch Policy Configuration** panel of the **Switch Policy Configuration Wizard**, click **Finish**.

### Editing basic information about the switch policy and 802.1x-aware switch

You can change the following parameters about the switch policy and the 802.1x-aware switch:

- **Switch policy name**
  - See “**Editing the name of a switch policy**” on page 285.

- **Switch model**
  - See “**Selecting a different switch model for the switch policy**” on page 286.

- **Shared secret**
  - See “**Editing an encrypted password or shared secret**” on page 287.

- **RADIUS server group**
  - See “**Selecting a different RADIUS server group**” on page 288.

- **Reauthentication time period**
  - See “**Editing the reauthentication period**” on page 288.

- **Forwarding protocols besides EAP**
  - See “**Enabling protocols other than EAP**” on page 289.

### Editing the name of a switch policy

You can edit the name of the switch policy at any time if circumstances change.

See “**Switch settings**” on page 274.
To edit the name of a switch policy

1. In Symantec Endpoint Protection Manager, click **Admin**.
2. Click **Servers**.
3. Select the Enforcer group.
4. Under **Tasks**, click **Edit Group Properties**.
5. In the **LAN Enforcer Settings** dialog box, on the **Switch** tab in the **Switch Policy** table, click the switch policy that you want to change.
6. Click **Edit**.
7. In the **Edit Switch Policy for name of switch policy** dialog box, on the **Basic Information** tab, edit the name of the switch policy in the **Switch policy name** field.
8. Click **OK**.
9. In the **LAN Enforcer Settings** dialog box, on the **Switch** tab, click **OK**.

Selecting a different switch model for the switch policy

You can select a different switch model for the switch policy at any time if circumstances change.

See “Switch settings” on page 274.

To select a different switch model for the switch policy

1. In Symantec Endpoint Protection Manager, click **Admin**.
2. Click **Servers**.
3. Select the Enforcer group.
4. Under **Tasks**, click **Edit Group Properties**.
5. In the **LAN Enforcer Settings** dialog box, on the **Switch** tab in the **Switch Policy** table, click the switch policy whose switch mode you want to change.
6. Click **Edit**.
7. In the **Edit Switch Policy for name of switch policy** dialog box, on the **Basic Information** tab, select a different switch model from the following Switch model list:
   - Other
     If your model is not listed, select **Other** to use a generic RADIUS server attribute.
   - 3Com
- Alcatel switch
- Cisco Catalyst Series
- Enterasys Matrix Series
- Extreme Summit Series
- Foundry Networks
- HP ProCurve Series
- Nortel BayStack Series
- Cisco Aironet Series
- Aruba Switches
- Airespace Wireless Controller
- Nortel Wireless
- Enterasys wireless controller
- HuaWei switch
  - If the administrator chooses transparent mode on the HuaWei switch, the administrator must configure the policy to use transparent mode on the client, rather than letting the user select it.

8 Click OK.

9 In the LAN Enforcer Settings dialog box, on the Switch tab, click OK.

**Editing an encrypted password or shared secret**

You can edit the shared secret at any time if circumstances change.

See “Switch settings” on page 274.

To edit an encrypted password or shared secret

1 In Symantec Endpoint Protection Manager, click Admin.

2 Click Servers.

3 Select the Enforcer group.

4 Under Tasks, click Edit Group Properties.

5 In the LAN Enforcer Settings dialog box, on the Switch tab in the Switch Policy table, click the switch policy whose shared secret you want to change.

6 Click Edit.

7 In the Edit Switch Policy for name of switch policy dialog box, on the Basic Information tab, edit the name of the shared secret in the Shared secret field.
8. Edit the name of the shared secret in the Confirm shared secret field.
9. Click OK.
10. In the LAN Enforcer Settings dialog box, on the Switch tab, click OK.

Selecting a different RADIUS server group
You can select a different RADIUS server group at any time if circumstances change.
See “Switch settings” on page 274.

To select a different RADIUS server group
1. In Symantec Endpoint Protection Manager, click Admin.
2. Click Servers.
3. Select the Enforcer group.
5. In the LAN Enforcer Settings dialog box, on the Switch tab in the Switch Policy table, click the switch policy whose shared secret you want to change.
6. In the LAN Enforcer Settings dialog box, on the Switch tab in the Switch Policy table, click Edit.
7. In the Edit Switch Policy for name of switch policy dialog box, on the Basic Information tab, select a different RADIUS server group from the RADIUS server group list.
   You must have added more than one RADIUS server group before you can select a different RADIUS server group.
8. Click OK.
9. In the LAN Enforcer Settings dialog box, on the Switch tab, click OK.

Editing the reauthentication period
You can edit the reauthentication period at any time if circumstances change.
You must specify the amount of time in seconds during which the client must be reauthenticated. Otherwise the client is removed from the list of connected clients and disconnected from the network.
You should set the reauthentication period to be at least double the amount of time of the reauthentication interval on the switch.
For example, if the reauthentication interval on the switch is 30 seconds, the LAN Enforcer reauthentication period should be at least 60 seconds. Otherwise the LAN
Enforcer assumes that the client is timed out. Therefore the client does not release and renew its IP address.

The default setting is 30 seconds.

See “Switch settings” on page 274.

To edit the reauthentication period

1. In Symantec Endpoint Protection Manager, click **Admin**.
2. Click **Servers**.
3. Select the Enforcer group.
4. Click **Edit Group Properties**.
5. In the **LAN Enforcer Settings** dialog box, on the **Switch** tab in the **Switch Policy** table, click the switch policy that you want to change.
6. Click **Edit**.
7. In the **Edit Switch Policy for name of switch policy** dialog box, on the **Basic Information** tab, edit the reauthentication period in the Reauthentication period in seconds field.
8. Click **OK**.
9. In the **LAN Enforcer Settings** dialog box, on the **Switch** tab, click **OK**.

**Enabling protocols other than EAP**

You can make the selections that allow the LAN Enforcer to forward the RADIUS packets that contain other authentication protocols besides EAP.

Other protocols include:

- Challenge Handshake Authentication Protocol (CHAP)
- PAP

The default setting is enabled.

See “Switch settings” on page 274.

To enable protocols other than EAP

1. In Symantec Endpoint Protection Manager, click **Admin**.
2. Click **Servers**.
3. Select the Enforcer group.
4. Click **Edit Group Properties**.
5. In the **LAN Enforcer Settings** dialog box, on the **Switch** tab in the **Switch Policy** table, click the switch policy that you want to change.
6 In the **LAN Enforcer Settings** dialog box, on the **Switch** tab in the Switch Policy table, click **Edit**.

7 In the **Edit Switch Policy for name of switch policy** dialog box, on the **Basic Information** tab, check **Enable protocols besides EAP**.

You can have the following protocols forwarded:
- Challenge Handshake Authentication Protocol (CHAP)
- PAP

8 Click **OK**.

9 In the **LAN Enforcer Settings** dialog box, on the **Switch** tab, click **OK**.

**Editing information about the 802.1x-aware switch**

You can change the following parameters about the 802.1x-aware switch:
- Change of IP address, host name, or subnet for an 802.1x-aware switch
  See “**Editing the IP address, host name, or subnet of an 802.1x-aware switch**” on page 290.
- Removal of an 802.1x-aware switch from switch list
  See “**Deleting an 802.1x-aware switch from the switch list**” on page 291.

**Editing the IP address, host name, or subnet of an 802.1x-aware switch**

You can change the IP address, hostname, or subnet of an 802.1x-aware switch at any time if circumstances require it.

See “**About the support for attributes of switch models**” on page 275.

**To edit the IP address, hostname, and subnet of an 802.1x-aware switch**

1 In Symantec Endpoint Protection Manager, click **Admin**.

2 Click **Servers**.

3 Select the Enforcer group.

4 Under **Tasks**, click **Edit Group Properties**.

5 In the **LAN Enforcer Settings** dialog box, on the **Switch** tab in the **Switch Policy** table, click the switch policy that you want to change.

6 Click **Edit**.

7 In the **Edit Switch Policy for name of switch policy** dialog box, on the **Switch Address** tab, check **Edit All**.
In the **Edit IP Addresses** dialog box, add or edit IP addresses, host, names, or subnets for the 802.1x-aware switch.

The format of the text is as follows:

- **Single IP Address**: `name: address`
- **IP address range**: `name: start address-end address`
- **Subnet**: `name: start address/subnet mask`

Click **OK**.

In the **LAN Enforcer Settings** dialog box, on the **Switch** tab, click **OK**.

### Deleting an 802.1x-aware switch from the switch list

You can delete an 802.1x-aware switch from the switch list at any time if circumstances require it.

See “About the support for attributes of switch models” on page 275.

To delete an 802.1x-aware switch

1. In Symantec Endpoint Protection Manager, click **Admin**.
2. Click **Servers**.
3. Select the Enforcer group.
4. Under **Tasks**, click **Edit Group Properties**.
5. In the **LAN Enforcer Settings** dialog box, on the **Switch** tab in the **Switch Policy** table, click the 802.1x-aware switch that you want to delete from the switch list.
6. In the **LAN Enforcer Settings** dialog box, on the **Switch** tab, click **Remove**.
7. Click **OK**.

### Editing VLAN information for the switch policy

You can change the following parameters about VLANs on the 802.1x-aware switch:

- Change the VLAN ID and VLAN name of an 802.1x-aware switch
  See “Editing the VLAN ID and VLAN name of an 802.1x-aware switch” on page 292.

- Configure VLAN and role information on the 802.1x-aware Aruba switch
  See “Configuring VLAN and role information on the 802.1x-aware Aruba switch” on page 293.
Editing the VLAN ID and VLAN name of an 802.1x-aware switch

You can change the VLAN ID and VLAN name of an 802.1x-aware switch at any time if circumstances require it.

Some switches, such as the Cisco switch, have a guest VLAN feature. The guest VLAN is normally used if EAP user authentication fails. If EAP authentication fails, the switch connects the client to the guest VLAN automatically.

If you use the LAN Enforcer for VLAN switching, it is recommended that you do not use the reserved guest VLAN when you set up VLANs and actions on the LAN Enforcer. Otherwise the 802.1x supplicant may respond as if EAP authentication failed.

When setting up VLANs, make sure that all of them can communicate with the management server.

See “Switch settings” on page 274.

To edit the VLAN ID and VLAN name of an 802.1x-aware switch

1. In Symantec Endpoint Protection Manager, click Admin.
2. Click Servers.
3. Select the Enforcer group.
5. In the LAN Enforcer Settings dialog box, on the Switch tab in the Switch Policy table, click the switch policy whose VLAN information you want to change.
6. Click Edit.
7. In the Edit Switch Policy for name of switch policy dialog box, on the Switch Address tab, select the VLAN that you want to edit.
8. On the VLAN tab, check Edit.
9. In the Edit VLAN dialog box, edit the VLAN ID in the VLAN ID field.
10. Edit the VLAN name in the VLAN name field.

If you plan to edit VLAN information about an Aruba switch, you may want to configure VLAN and role information somewhat differently than you have for other 802.1x switches.

See “Configuring VLAN and role information on the 802.1x-aware Aruba switch” on page 293.
11 In the Edit Switch Policy for name of switch policy dialog box, on the VLAN tab, click OK.

12 In the LAN Enforcer Settings dialog box, on the Switch tab, click OK.

Deleting the VLANs on an 802.1x-aware switch

You can delete the VLANs on an 802.1x-aware switch at any time if circumstances require it.

See “Switch settings” on page 274.

To delete the VLANs on an 802.1x-aware switch

1 In Symantec Endpoint Protection Manager, click Admin.
2 Click Servers.
3 Select the Enforcer group.
4 Under Tasks, click Edit Group Properties.
5 In the LAN Enforcer Settings dialog box, on the Switch tab in the Switch Policy table, click the switch policy whose VLAN information you want to delete.
6 Click Edit.
7 In the Edit Switch Policy for name of switch policy dialog box, on the Switch Address tab, select the VLAN that you want to delete.
8 On the VLAN tab, check Remove.
9 Click OK.
10 In the LAN Enforcer Settings dialog box, on the Switch tab, click OK.

Configuring VLAN and role information on the 802.1x-aware Aruba switch

If you use an Aruba switch, you can leave the VLAN ID or the VLAN name field blank. However, for other switches, you must enter information in both fields. For the Aruba switch, you can use these fields to specify either a VLAN or a role or both as follows:

■ To specify a VLAN, enter the VLAN ID in the VLAN ID field.
■ To specify a role, enter the role name in the VLAN name field.

For the Aruba switch you can also use this dialog box to set up separate switch actions for multiple roles on one VLAN or multiple VLANS for one role.

See “Switch settings” on page 274.
To configure VLAN and role information on the 802.1x-aware Aruba switch

1. If you had a VLAN ID 1 with role A and role B, fill in the VLAN ID as 1 and the VLAN name as A. Click OK.

2. Click Add again. In the Add VLAN dialog box, fill in the VLAN ID as 1 and the VLAN name as B and click OK.

Two separate choices become available for configuration on the switch action table.

Editing action information for the switch policy

You can change the following parameters about VLANs on the 802.1x-aware switch:

- Set the order of condition checking
  See “Setting the order of condition checking” on page 295.

- Select a different Host Authentication, User Authentication, or Policy Check condition
  See “Selecting a different Host Authentication, User Authentication, or Policy Check condition” on page 296.

- Select different actions
  See “Selecting different actions” on page 297.

About issues with the switch policy, associated conditions, and actions

When configuring switch policies, note the following:

- The Switch Action table must contain at least one entry.

- If you do not select an action for a particular combination of results, the default action, Open Port, is performed.

- To specify a default action for any possible combination of results, select Ignore Result for all three results.

- When you add the actions to the table, you can edit any cell by clicking on the right corner of a column and row to display a drop-down list.

- Some switches, such as the Cisco switch, have a guest VLAN feature. The guest VLAN is normally intended to be used if user authentication fails. In other words, if user authentication fails, the switch connects the client to the guest VLAN automatically.

If you use the LAN Enforcer for VLAN switching, it is recommended that you do not use the reserved guest VLAN when setting up VLANs and actions on the
LAN Enforcer. Otherwise the 802.1x supplicant may respond as though user authentication failed.

- If you deploy clients and are not ready to implement the full capabilities of the LAN Enforcer, you can specify an action of allowing access to the internal network that is based on the condition Ignore Result for the Host Integrity check and Policy Check. If you want to disregard the user authentication results and allow network access regardless of the results, you can do so with the condition Ignore Result for User Authentication results.

See “Setting the order of condition checking” on page 295.

See “Selecting a different Host Authentication, User Authentication, or Policy Check condition” on page 296.

See “Selecting different actions” on page 297.

### Setting the order of condition checking

You can change a different Host Authentication, User Authentication, or Policy Check condition for a switch policy at any time if circumstances require it.

You can add an entry to the Switch Action table for each of the possible combinations of authentication results.

When you set up the conditions to check for, remember that the only circumstance in which all three results can be Pass or Fail is in the basic configuration. In the basic configuration, the client runs both an 802.1x supplicant that provides information about user authentication and a client that provides information about Host Integrity and the Policy Serial Number.

If you run only an 802.1x supplicant without a client, the results for the Host Integrity check and Policy Check are always unavailable. If you run in transparent mode without a user authentication check, the user authentication result is always Unavailable.

The LAN Enforcer checks the authentication results against the entries in the table in the order from top to bottom of the table. After the LAN Enforcer finds a matching set of conditions, it instructs the 802.1x-aware switch to apply that action. You can change the sequence in which actions are applied by changing the order in which they are listed in the table.

If a LAN Enforcer cannot locate any entry that matches the current condition, a CLOSE PORT action is taken.

See “About issues with the switch policy, associated conditions, and actions” on page 294.
To set the order of condition checking

1. In Symantec Endpoint Protection Manager, click Admin.
2. In the Admin page, click Servers.
3. Select the Enforcer group.
5. In the LAN Enforcer Settings dialog box, on the Switch tab in the Switch Policy table, click the switch policy whose order of conditions checking you want to change.
6. Click Edit.
7. In the Edit Switch Policy for name of switch policy dialog box, on the Action tab, select the switch policy whose order of conditions checking you want to change.
8. Click Move Up or Move Down.
9. Click OK.
10. In the LAN Enforcer Settings dialog box, on the Switch tab, click OK.

Selecting a different Host Authentication, User Authentication, or Policy Check condition

You can select a different Host Authentication, User Authentication, or Policy Check condition for a switch policy at any time if circumstances require it.

See “About issues with the switch policy, associated conditions, and actions” on page 294.

To select a different Host Authentication, User Authentication, or Policy Check condition

1. In Symantec Endpoint Protection Manager, click Admin.
2. Click Servers.
3. Select the Enforcer group.
5. In the LAN Enforcer Settings dialog box, on the Switch tab in the Switch Policy table, click the switch policy whose authentication conditions you want to change.
6. Click Edit.
7 In the Edit Switch Policy for name of switch policy dialog box, on the Action tab, click any of the authentication conditions that you want to change in any of the following columns:

- Host authentication
- User authentication
- Policy check

8 Select any of the following actions that the 802.1x-aware switch needs to take when certain criteria are met:

- Host authentication result: Pass, Fail, Unavailable, or Ignore Result
- User authentication result: Pass, Fail, Unavailable, or Ignore Result
- Policy Check result: Pass, Fail, Unavailable, or Ignore Result

9 Click OK.

10 In the LAN Enforcer Settings dialog box, on the Switch tab, click OK.

Selecting different actions

You can select the different actions that the 802.1x-aware switch can take when certain criteria are met:

See “About issues with the switch policy, associated conditions, and actions” on page 294.

To select a different Host Authentication, User Authentication, or Policy Check condition

1 In Symantec Endpoint Protection Manager, click Admin.

2 Click Servers.

3 Select the Enforcer group.

4 Under Tasks, click Edit Group Properties.

5 In the LAN Enforcer Settings dialog box, on the Switch tab in the Switch Policy table, click the switch policy whose actions you want to change.

6 Click Edit.

7 On the Action tab, click any of the actions that you want to change in the Action column.

8 Select any of the following actions that the 802.1x-aware switch needs to take when certain criteria are met:

- Open Port
The 802.1x-aware switch allows network access on the default VLAN to which the port is normally assigned. It also allows network access on the VLAN that is specified in an attribute that is sent from the RADIUS server. Therefore the support of users having VLAN access is based on user ID and user role.

The default action is Open Port.

- **Switch to VLAN-test**
  Allows access to the specified VLAN. The VLANs that are available to select are the ones that you configured previously.

- **Close Port**
  Deny network access on the default or RADIUS-specified VLAN. On some switch models, depending on the switch configuration, the port is assigned to a guest VLAN.

9 Click **OK**.

10 In the **LAN Enforcer Settings** dialog box, on the **Switch** tab, click **OK**.

### Using advanced LAN Enforcer appliance settings

You can configure the following advanced LAN Enforcer appliance configuration settings:

- **Allow a legacy client.**
  See “Allowing a legacy client to connect to the network with a LAN Enforcer appliance” on page 299.

- **Enable local authentication.**
  See “Enabling local authentication on the LAN Enforcer appliance” on page 299.

- **Add/Edit/Remove/Import/Export MAC address and associated VLAN for MAC Authentication Bypass.**
  See “Configuring MAC addresses and MAC authentication bypass (MAB) on the LAN Enforcer” on page 300.

- **Enabling Network Time Protocol, and the server that provides the service.**

- **Enabling management server health check and interval period.**

Details on implementing each of these settings appear on the context-sensitive help page for LAN Enforcer appliance advanced settings.
Allowing a legacy client to connect to the network with a LAN Enforcer appliance

You can enable a LAN Enforcer appliance to connect to 5.1.x legacy clients. If your network supports an 11.0.2 Symantec Endpoint Protection Manager, a Symantec LAN Enforcer appliance, and needs to support 5.1.x legacy clients, you can enable the support of 5.1.x legacy clients on the management server console so that the Symantec LAN Enforcer appliance does not block them.

See “Using advanced LAN Enforcer appliance settings” on page 298.

To allow a legacy client to connect to the network with a LAN Enforcer appliance

1. In Symantec Endpoint Protection Manager, click Admin.
2. Click Servers.
3. Select and expand the group of LAN Enforcers appliances.
5. In the Settings dialog box, on the Advanced tab, check Allow legacy clients.
6. Click OK.

Enabling local authentication on the LAN Enforcer appliance

If a LAN Enforcer appliance loses its connection with the computer on which the Symantec Endpoint Protection Manager is installed, the LAN Enforcer appliance can authenticate a client locally.

See “Using advanced LAN Enforcer appliance settings” on page 298.

To enable local authentication on the LAN Enforcer appliance

1. In Symantec Endpoint Protection Manager, click Admin.
2. Click Servers.
3. Select and expand the group of LAN Enforcer appliances.
4. Select the LAN Enforcer appliance group for which you want to enable local authentication.
5. Under Tasks, click Edit Group Properties.
6. In the LAN Settings dialog box, on the Advanced tab, check Enable Local Authentication.
7. Click OK.
Enabling system time updates for the Enforcer appliance using the Network Time Protocol

With Network Time Protocol (NTP) enabled, Enforcer appliance clocks can update to the correct time. This setting is disabled by default, but it can be overridden if it is specified in a group policy.

See “Using advanced LAN Enforcer appliance settings” on page 298.

To enable time updates for the LAN Enforcer appliance from the Symantec Endpoint Protection Manager

1. In Symantec Endpoint Protection Manager, click Admin.
2. Click Servers.
3. Under Servers, select and expand the group of LAN Enforcer appliances.
6. Enter the IP address or the fully qualified domain name of the NTP server.
7. Click OK.

From the Enforcer console, you can temporarily change this setting to help troubleshoot time synchronization issues. From the Enforcer console command line, enter

Enforcer (configure) # ntp.

---

**Note:** If you had enabled NTP in an earlier version of Symantec Endpoint Protection, that configuration is lost when you upgrade. You must re-enable NTP.

---

Configuring MAC addresses and MAC authentication bypass (MAB) on the LAN Enforcer

You can change the MAC authentication settings on a management server. The configuration settings are automatically downloaded from the management server to the LAN Enforcer appliance during the next heartbeat.

To configure MAC addresses and MAC authentication bypass on the LAN Enforcer

1. In Symantec Endpoint Protection Manager, click Admin.
2. Click Servers.
3. Under Servers, select and expand the group of Enforcers.
Select the LAN Enforcer.

5. Under Tasks, click Edit Group Properties.

6. Open the Advanced tab.

7. In the dropdown list on the left, select MAC Authentication Bypass, and click Enable.

8. In the Settings dialog box, on the Advanced tab, next to MAC address, click Add.

9. In the Add Trusted Host dialog box, type the MAC address for the client or the trusted host in the Host MAC address field.

   When you specify a MAC address, you can use a wildcard character if you type it for all three fields on the right.

   For example, 11-22-23-*-*-* represents the correct use of the wildcard character. However, 11-22-33-44-*-*-* does not represent the correct use of the wildcard character.

   You can also copy a set of MAC addresses from a text file.

   **Note:** Symantec supports the following format for imports: single MAC address, and MAC address with mask.

To import MAC addresses, click Import. Specify the file in the Import MAC Address From File dialog box.

To export MAC addresses, highlight several MAC addresses, and then click Export. Specify the file in the Export MAC Address To File dialog box.

10. Click OK.

### Using 802.1x authentication

If your corporate network uses a LAN Enforcer for authentication, you must configure the client computer to perform IEEE 802.1x authentication.

The 802.1x authentication process includes the following steps:

- An unauthenticated client or third-party supplicant sends the user information and compliance information to a managed 802.11 network switch.

- The network switch relays the information to the LAN Enforcer appliance. The LAN Enforcer appliance sends the user information to the authentication server for authentication. The RADIUS server is the authentication server.
If the client fails the user-level authentication or is not in compliance with the Host Integrity policy, the Enforcer may block network access. The LAN Enforcer appliance places the non-compliant client computer in network according to the Switch Action table where the computer can be remediated.

After the client remediates the computer and brings it into compliance, the 802.1x protocol reauthenticates the computer and grants the computer access to the network.

To work with the LAN Enforcer appliance, the client can use either a third-party supplicant or a built-in supplicant.

Table 19-2 describes the types of options that you can configure for 802.1x authentication.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Third-party</td>
<td>Uses a third-party 802.1x supplicant.</td>
</tr>
<tr>
<td>supplicant</td>
<td>The LAN Enforcer appliance works with a RADIUS server and third-party 802.1x supplicants to perform user authentication. The 802.1x supplicant prompts users for user information, which the LAN Enforcer passes to the RADIUS server for user-level authentication. The client sends the client profile and the Host Integrity status to the LAN Enforcer appliance so that it authenticates the computer.</td>
</tr>
</tbody>
</table>

**Note:** If you want to use the Symantec Network Access Control client with a third-party supplicant, then you must install the Network Threat Protection module of the Symantec Endpoint Protection client.

To use a third-party 802.1x supplicant, you must:

- Configure the 802.1x switch to use the LAN Enforcer appliance as the RADIUS server so that the switch forwards authentication packets to the LAN Enforcer appliance.
- Add the LAN Enforcer appliance as a client of the RADIUS server so that it accepts requests from the LAN Enforcer appliance.
- In the console, you must specify the RADIUS server information and enable 802.1x authentication for the clients.
Table 19-2 802.1x authentication options *(continued)*

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transparent mode</td>
<td>Uses the client to run as an 802.1x supplicant. You use this method if you do not want to use a RADIUS server to perform user authentication. The LAN Enforcer appliance runs in transparent mode and acts as a pseudo-RADIUS server. Transparent mode means that the supplicant does not prompt users for user information. In transparent mode, the client acts as the 802.1x supplicant. The client responds to the switch’s EAP challenge with the client profile and the Host Integrity status. The switch, in turn, forwards the information to the LAN Enforcer appliance, which acts as a pseudo-RADIUS server. The LAN Enforcer appliance validates the Host Integrity and client profile information from the switch and can allow, block, or dynamically assign a VLAN, as appropriate. <strong>Note:</strong> To use a client as an 802.1x supplicant, you must uninstall or disable third-party 802.1x supplicants on the client computer. In transparent mode, you can leave the RADIUS server information empty on the LAN Enforcer Settings dialog box. The RADIUS server IP address is therefore set to 0 and no traditional EAP user authentication takes place.</td>
</tr>
<tr>
<td>Built-in supplicant</td>
<td>Uses the client computer's built-in 802.1x supplicant. The built-in authentication protocols include Smart Card, PEAP, or TLS. After you enable 802.1x authentication, you or the users must specify which authentication protocol to use.</td>
</tr>
</tbody>
</table>

**Warning:** You must know whether your corporate network uses the RADIUS server as the authentication server. If you configure 802.1x authentication incorrectly, the connection to the network may break.

**Note:** To enable the user to configure 802.1x authentication on the client, you must set the client to client control.

See “How the LAN Enforcer appliance works” on page 256.

To configure the client to use either transparent mode or a built-in supplicant

1. In Symantec Endpoint Protection Manager, click **Clients**.
2. Under **View Clients**, select the group of the clients that you want to perform 802.1x authentication.
3 On the Policies tab, under Settings, click General Settings.

4 On the Security Settings tab, check Enable 802.1x authentication.

5 Check Use the client as an 802.1x supplicant.

6 Do one of the following actions:
   - To select transparent mode, select Use Symantec Transparent Mode.
   - To enable the user to configure a built-in supplicant, select Allows user to select the authentication protocol.
     Users can choose the authentication protocol for their network connection.

7 Click OK.

To configure the client to use a third-party supplicant

1 In the console, click Clients.

2 Under View Clients, select the group of the clients that you want to perform 802.1x authentication.

3 On the Policies tab, under Settings, click General Settings.

4 On the Security Settings tab, check Enable 802.1x authentication.

5 Click OK.

You can configure the client to use the built-in supplicant. You enable the client for both 802.1x authentication and as an 802.1x supplicant.

About reauthentication on the client computer

If the client computer passed the Host Integrity check but the Enforcer blocks the computer, users may need to reauthenticate their computers. Under normal circumstances, users should never need to reauthenticate the computer.

The Enforcer may block the computer when one of the following events has occurred:

   - The client computer failed the user authentication because users typed their user name or their password incorrectly.
   - The client computer is in the wrong VLAN.
   - The client computer does not obtain a network connection. A broken network connection usually happens because the switch between the client computer and the LAN Enforcer did not authenticate the user name and password.
   - Users need to log on to a client computer that authenticated a previous user.
   - The client computer failed the compliance check.
Users can reauthenticate the computer only if you configured the computer with a built-in supplicant. The right-click menu on the notification area icon of the client computer displays a Reauthentication command.

See "Using 802.1x authentication" on page 301.
Configuring the Integrated Enforcers on the Enforcer console

This chapter includes the following topics:

- What you can do with Symantec Integrated Enforcers
- About configuring Integrated Enforcers on an Enforcer console
- Establishing or changing communication between an Integrated Enforcer for Microsoft DHCP servers and a Symantec Endpoint Protection Manager
- Configuring automatic quarantine
- Editing a Symantec Endpoint Protection Manager connection
- Configuring Integrated Enforcer communication settings in Symantec Endpoint Protection Manager
- Configuring a trusted vendor list
- Viewing Enforcer logs on an Enforcer console
- Stopping and starting communication services between an Integrated Enforcer and a management server
- Configuring a secure subnet mask
- Creating DHCP scope exceptions
What you can do with Symantec Integrated Enforcers

The optional Symantec Network Access Control Integrated Enforcers are Enforcers provided as software components. You can configure them to ensure that the clients that connect to the network comply with your organization's configured Host Integrity and other security policies.

- Use the Symantec Network Access Control Integrated Enforcer for DHCP Servers to ensure that a Microsoft DHCP Server's clients comply with Host Integrity and other security policies.
- Use the Symantec Network Access Control Integrated Enforcer for Microsoft Network Access Protection to ensure that clients comply with Microsoft client health policies. You can also use the Symantec Health Agent to check Symantec health policies in addition to Microsoft health policies.

You can perform the following key tasks with the Integrated Enforcers:

- Ensure that client computers that attempt to connect to the network comply with the security policies you set on the Symantec Endpoint Protection Manager.
- Configure a connection to a Symantec Endpoint Protection Manager.
- Start and stop the Enforcer service.
- View the connection status.
- View Security and System logs on the Symantec Endpoint Protection Manager.

See “How an Integrated Enforcer for Microsoft DHCP Servers works” on page 320.

About configuring Integrated Enforcers on an Enforcer console

After you complete the installation of a Symantec Network Access Control Integrated Enforcer, there are two stages of configuration. First, configure the settings on the Integrated Enforcer console. Second, move to the Symantec Endpoint Protection Manager to make any desired changes to the configuration settings for the group that the Integrated Enforcer is part of.

Table 20-1 outlines these tasks.
### Table 20-1  Enforcer console configuration summary

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 1| Establish a connection between the Integrated Enforcer for Microsoft DHCP Servers and a management server. | Use the Integrated Enforcer console to configure the connection between the Integrated Enforcer for Microsoft DHCP Servers and Symantec Endpoint Protection Manager.  
See “Establishing or changing communication between an Integrated Enforcer for Microsoft DHCP servers and a Symantec Endpoint Protection Manager” on page 310. |
<p>| Step 2| Set up the DHCP server with a quarantine configuration.                | Use one of two methods to configure a quarantine user class for remediation.                                                                                                                                  |
|       |                                                                        | See “Configuring automatic quarantine” on page 312.                                                                                                                                                           |
| Step 3| Restart the DHCP service.                                              | Manually stop and start the DHCP service on the DHCP server.                                                                                                                                                  |
|       |                                                                        | See “Stopping and starting the Microsoft DHCP Server manually” on page 211.                                                                                                                                   |
| Step 4| Optionally, change Integrated Enforcer basic settings.                | Add or edit descriptions for an Integrated Enforcer or group of Integrated Enforcers, or for the Integrated Enforcer IP address or host names.                                                               |
|       |                                                                        | See “Configuring Symantec Network Access Control Integrated Enforcer basic settings” on page 322.                                                                                                               |
| Step 5| Connect the Integrated Enforcer to a Symantec Endpoint Protection Manager. | Connect the Integrated Enforcer to a server on which the Symantec Endpoint Protection Manager is installed.                                                                                               |
|       |                                                                        | See “Connecting the Symantec Network Access Control Integrated Enforcer to a Symantec Endpoint Protection Manager” on page 324.                                                                                |</p>
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 6 | As needed, update the connection to the Symantec Endpoint Protection Manager. | Update the connection to the Symantec Endpoint Protection server address and port information as required.  
See “Editing a Symantec Endpoint Protection Manager connection” on page 313.                                                                                       |
| Step 7 | As needed, configure a trusted vendor list.                           | Configure a trusted vendor list for devices on your network such as printers or IP telephones. These are the devices that the Integrated Enforcer does not need to authenticate.  
See “Configuring a trusted vendor list” on page 315.                                                                                                             |
| Step 8 | Optionally, set where you want to view logs.                          | Set up logs for viewing on the Enforcer console or the Symantec Endpoint Protection Manager.  
See “Viewing Enforcer logs on an Enforcer console” on page 315.  
See “Configuring logs for the Symantec Network Access Control Integrated Enforcer” on page 334.                                                                 |
Table 20-1  Enforcer console configuration summary (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 9</td>
<td>Optionally, set authentication settings for your network.</td>
<td>Set up how you want to authenticate clients, servers, and devices.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See &quot;Specifying the maximum number of challenge packets during an authentication session&quot; on page 330.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See &quot;Specifying the frequency of challenge packets to be sent to clients&quot; on page 331.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See &quot;Allowing all clients with continued logging of non-authenticated clients&quot; on page 332.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See &quot;Allowing non-Windows clients to connect to a network without authentication&quot; on page 332.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See &quot;Enabling servers, clients, and devices to connect to the network as trusted hosts without authentication&quot; on page 325.</td>
</tr>
<tr>
<td>Step 10</td>
<td>Optionally, validate that clients are running up-to-date policies.</td>
<td>Validate that clients have the most recent policies by comparing the policy serial number received from the client with the policy serial number in the Symantec Endpoint Protection Manager.</td>
</tr>
</tbody>
</table>

Establishing or changing communication between an Integrated Enforcer for Microsoft DHCP servers and a Symantec Endpoint Protection Manager

You must specify the Symantec Endpoint Protection Manager to which the Integrated Enforcer can connect. After you set up the management server list, you must configure the connection with the encrypted password, group name, and communication protocol. The encrypted password was previously known as a preshared key.

After the Integrated Enforcer connects to a management server, it registers itself automatically.
To establish communication between the Integrated Enforcer console and Symantec Endpoint Protection Manager

1 On the Windows taskbar of the Integrated Enforcer computer, click Start > Programs > Symantec Endpoint Protection > Symantec NAC Integrated Enforcer.

   The Symantec Network Access Control Integrated Enforcer configuration console appears. This main page shows the connection status between the Integrated Enforcer and the Symantec Endpoint Protection Manager. A green light indicates that Integrated Enforcer is actively connected to the management server. A red light indicates that the connection is disconnected.

2 In the left-hand panel, click Symantec Integrated Enforcer > Configure > Management Server.

3 In the Management Server dialog box, type the IP address or name of the Symantec Endpoint Protection Manager in the Server address text field.

   You can type an IP address, host name, or domain name. If you want to use a host name or a domain name, ensure that the name resolves correctly with the Domain Name Server (DNS server).

4 In the Management Server dialog box, edit the port number that the Integrated Enforcer uses to communicate with the Symantec Endpoint Protection Manager.

   The default port number is 8014 for HTTP protocol and 443 for the HTTPS protocol. The HTTPS protocol must be configured identically on the Symantec Endpoint Protection Manager and Integrated Enforcer.

5 In the Encryption password text box, type the password of the Symantec Endpoint Protection Manager for your connection.

   The Symantec Endpoint Protection Manager and Integrated Enforcer must use the same encrypted password for communication.

   To use a hash value instead of the encrypted password, check Use Hash Value. If you enable Use Hash Value, the password must be 32 characters, and must use hexadecimal numbers only.

6 In the Preferred group text box, type a name for the Integrated Enforcer group.

   If you do not specify a group name, the Symantec Endpoint Protection Manager assigns the Symantec Network Access Control Integrated Enforcer to a default Enforcer group with default settings. The default group name is I-DHCP. However, a Symantec Network Access Control Integrated Enforcer for Microsoft NAP Servers and appliance-based enforcers must each be in a separate group.

   You can view the group settings from the Symantec Endpoint Protection Manager console on the Servers page.
To specify the protocol that the Symantec Network Access Control Integrated Enforcer uses to communicate with the Symantec Endpoint Protection Manager, select **HTTP** or **HTTPS**.

You can only use the HTTPS protocol if the Symantec Endpoint Protection Manager is running Secure Sockets Layer (SSL).

If you select HTTPS and want to require verification of the management server’s certificate with a trusted third-party certificate authority, check **Verify certificate when using HTTPS protocol**.

Click **Save**.

After the Integrated Enforcer connects to the Symantec Endpoint Protection Manager, you can change most of the configuration settings on the Symantec Endpoint Protection Manager Console. However, the preshared secret or encrypted password must be the same on the Integrated Enforcer and the Symantec Endpoint Protection Manager in order for them to communicate.

### Configuring automatic quarantine

The clients that try to connect to the network send a DHCP request to the DHCP server.

The Integrated Enforcer appends the quarantine user class to all DHCP messages that come from non-compliant or unknown clients. It also renews the requests from the client to the DHCP server. Clients that are trusted are immediately assigned a normal IP address and are not quarantined. Unknown or untrusted clients are quarantined, authenticated, renewed if authentication succeeds, and then assigned a normal IP address.

Access is based on the Host Integrity policy and group settings that are defined in the Symantec Endpoint Protection Manager.

Enter a list of IP addresses that you want to allow quarantined computers to access, even if authentication fails.

**To configure automatic quarantine for a Symantec Network Access Control Integrated Enforcer**

1. On the Windows taskbar of the Integrated Enforcer computer, click **Start > Programs > Symantec Endpoint Protection > Symantec NAC Integrated Enforcer**.

2. In the left-hand panel, click **Symantec Integrated Enforcer > Configure > Automatic Quarantine Configuration**.

3. In the **Automatic Quarantine Configuration** page of the Integrated Enforcer, click **Add** to begin creating an IP address list.
4 Enter an allowed IP address and click OK to add the IP address to the list.
5 Click Add again to continue adding IP addresses to the list.
6 Modify the IP Address list by clicking Edit, Remove, Remove all, Move Up, or Move down.
7 When all IP Addresses are listed or modified, click OK at the bottom of the page to save your configurations.

Editing a Symantec Endpoint Protection Manager connection

You can update the Symantec Endpoint Protection Manager IP address and port information as required.

To edit a Symantec Endpoint Protection Manager connection
1 On the Windows taskbar of the Enforcer computer, click Start > Programs > Symantec Endpoint Protection > Symantec Integrated Enforcer
2 In the left-hand panel, expand Symantec Integrated Enforcer.
3 Expand Configure.
4 Click Management Servers.
5 In the Management Servers panel, edit the IP address or name of the Symantec Endpoint Protection Manager in the Server address text field.
   You can type an IP address, host name, or domain name. If you want to use a host name or a domain name, the Symantec Network Access Control Integrated Enforcer must connect to a Domain Name Server (DNS) server.
6 Click Save.

Configuring Integrated Enforcer communication settings in Symantec Endpoint Protection Manager

Configuring the Symantec Network Access Control Integrated Enforcer is a two-step process. First, you configure the Integrated Enforcer from the Integrated Enforcer console. Secondly, you complete configuration tasks from the Symantec Endpoint Protection Manager to fully set up communications between the enforcer and the management server. The configuration settings are automatically downloaded from the management server to the Integrated Enforcer during the next heartbeat.

See “About configuring Integrated Enforcers on an Enforcer console” on page 307.
To configure Integrated Enforcer communication settings in Symantec Endpoint Protection Manager

1. In the Symantec Endpoint Protection Manager Console, click **Admin**.
2. Click **Servers**.
3. Under **Servers**, select the group of Enforcers of which the Integrated Enforcer is a member.
4. Select the Integrated Enforcer whose configuration settings need to be changed.
5. Under **Tasks**, click **Edit Group Properties**.
6. In the **Settings** dialog box, change any of the configuration settings.

The Settings dialog box provides the following tabbed categories of configuration settings:

- **General**: Settings for the Enforcer group name, Enforcer group description, and management server list.
  
  See “Configuring Symantec Network Access Control Integrated Enforcer basic settings” on page 322.

- **Authentication**: Settings for a variety of parameters that affect the client authentication process.
  
  See “Configuring Symantec Network Access Control Integrated Enforcer authentication settings” on page 327.

- **Advanced**: Settings for authentication timeout parameters and DHCP message timeouts: these options are displayed but currently unavailable for Symantec Network Access Control Integrated Enforcer configuration.

  Settings for MAC addresses for the trusted hosts that the Integrated Enforcer allows to connect without authentication (optional).

  Settings for Local Authentication.

  See “Configuring Symantec Network Access Control Integrated Enforcer advanced settings” on page 325.

- **Log Settings**: Settings for Server logs, Client Activity logs, and specifying log file parameters.

  See “Configuring logs for the Symantec Network Access Control Integrated Enforcer” on page 334.
Configuring a trusted vendor list

Clients cannot be installed on some network devices such as printers or IP telephones. To allow for those cases, you can configure a trusted vendor list. If the name of the vendor is considered trusted, then the Symantec Network Access Control Integrated Enforcer will not authenticate the device. The devices will obtain normal IP addresses from the DHCP server.

To configure a trusted vendor list


2. In the left-hand panel, click Symantec Integrated Enforcer > Configure > DHCP Trusted Vendors Configuration.

3. To enable the trusted vendor list, check Turn on Trusted Vendors.
   When the Turn on Trusted Vendors box is checked, Host Integrity will not be enforced for DHCP traffic from the selected trusted vendors.

4. Select the vendors you want to establish as trusted vendors.

5. Click Save.

Viewing Enforcer logs on an Enforcer console

The Symantec Network Access Control Integrated Enforcer automatically logs messages in the Enforcer Client log and the Enforcer System log. These Enforcer logs are uploaded to the Symantec Endpoint Protection Manager. The client log provides information about client connections and communication with the Integrated Enforcer. The system log records information that relates to the Integrated Enforcer itself, such as instances of starting and stopping the Enforcer service.

In the Symantec Endpoint Protection Manager, you can enable and disable logging and set log file parameters for the Integrated Enforcer. All logs are enabled and sent to the Symantec Endpoint Protection Manager by default.

To view Enforcer logs on an Enforcer console

1. In the left pane, expand Symantec NAC Integrated Enforcer.

2. Expand View Logs, and click System Log or click Client Log.

3. To view any changes to the log since you last opened the log, click Refresh.

4. Click OK.
Stopping and starting communication services between an Integrated Enforcer and a management server

For troubleshooting purposes, you can stop and start either the Enforcer service or the service (SNACLink.exe) that communicates with the Symantec Endpoint Protection Manager. If you stop the Enforcer service, the Integrated Enforcer removes the compliance information for existing clients. It also stops collecting information for new clients. However, it continues to communicate with a Symantec Endpoint Protection Manager.

If the Symantec Endpoint Protection Manager is unavailable, the Integrated Enforcer still enforces the policy version and GUID for all authenticated clients. The same process is followed if you stop the connection to the Symantec Endpoint Protection Manager.

Stopping the Integrated Enforcer does not stop the DHCP server. If the Integrated Enforcer is stopped, the DHCP server functions as if no Enforcer was ever installed. If the DHCP server becomes unavailable, the Integrated Enforcer stops collecting the compliance status about new clients. However, it continues to communicate with existing clients and continues to log status changes. The DHCP server may become unavailable because of maintenance and other problems.

To stop and start the communication services between an Integrated Enforcer and a management server

1. Start the Symantec Network Access Control Integrated Enforcer.
2. Click Symantec NAC Integrated Enforcer.
3. You can stop or start either the Enforcer service (IntegratedEnf.exe) or the service (SNACLink.exe) that communicates with the Symantec Endpoint Protection Manager.

Perform one or both of the following tasks:

- In the Enforcer service group box, click Stop. This option stops the Enforcer service.
- In the Management server communication service group box, click Stop. This option stops the Enforcer service that connects to the Symantec Endpoint Protection Manager.
If the status is set to Stopped, the service is not running.

4 To restart either service, click Start.

If you turn off or restart the computer to which a Symantec Network Access Control Integrated Enforcer is connected, the Enforcer service restarts automatically when the computer restarts.

If the server communication service is stopped and subsequently restarted, the Symantec Network Access Control Integrated Enforcer tries to connect to a Symantec Endpoint Protection Manager to which it last connected. If that Symantec Endpoint Protection Manager is unavailable, the Integrated Enforcer connects to the first management server that is listed in the management server list.

**Configuring a secure subnet mask**

The Integrated Enforcer Advanced Settings configuration page allows users to configure a secure subnet mask for quarantined clients.

**To configure a secure subnet mask**

1 On the Advanced Settings configuration page, check the option to **Use secure subnet mask** *(255.255.255.255)* for quarantine IP address, or click to clear the configuration. If you clear the configuration, you will use the normal DHCP subnet mask.

2 **Select scopes to be enforced** lists the scopes you can enforce. If there is more than one DHCP scope in the DHCP server, select which scope or scopes to enforce.

3 Click **OK** to save your configuration.

---

**Note:** The secure subnet mask *(255.255.255.255)* option is only available with the Symantec Network Access Control Integrated Enforcer for Microsoft DHCP servers. If it is turned on, the 255.255.255.255 is used for quarantined clients. If it is turned off, the default subnet mask for the current scope will be used.

---

**Creating DHCP scope exceptions**

The Integrated Enforcer Advanced Settings configuration page allows users to manipulate the subnet mask to bypass quarantine. The default configuration at installation is that all DHCP scopes will be enforced for quarantine.
To select subnets for exemption from quarantine

1. On the Advanced Settings configuration page, check the option to Use secure subnet mask (255.255.255.255) for quarantine IP address

2. Under Select scopes to be enforced, click to clear the IP address ranges you want to exempt. IP addresses that belong to the DHCP scopes that are checked will be enforced.

   When a DHCP scope is changed to exempt a scope (by clicking to clear the IP address range), IP addresses that have already been assigned to clients will still be enforced. To clear the enforcement, Release and Renew the IP addresses.

   **Note:** If new scope is created or added after the Enforcer is installed, the new scope will not be enforced until it is selected in the user interface on the Advanced Settings configuration page.

3. When you are satisfied with your settings, click OK to save the configuration.
Configuring the Integrated Enforcer for Microsoft DHCP Server on the Symantec Endpoint Protection Manager

This chapter includes the following topics:

- About the Symantec Network Access Control Integrated Enforcer for Microsoft DHCP Servers
- How an Integrated Enforcer for Microsoft DHCP Servers works
- About configuring the Symantec Network Access Control Integrated Enforcer for Microsoft DHCP Server on the Symantec Endpoint Protection Manager
- Configuring Symantec Network Access Control Integrated Enforcer basic settings
- Configuring Symantec Network Access Control Integrated Enforcer advanced settings
- Configuring Symantec Network Access Control Integrated Enforcer authentication settings
- Configuring logs for the Symantec Network Access Control Integrated Enforcer
About the Symantec Network Access Control Integrated Enforcer for Microsoft DHCP Servers

The Symantec Network Access Control Integrated Enforcer for Microsoft DHCP Servers works in concert with the Microsoft Dynamic Host Configuration Protocol (DHCP) server. It ensures that the clients that try to connect to the network comply with configured security policies.

The Integrated Enforcer for Microsoft DHCP Servers achieves security by intercepting and checking DHCP messages from each client that receives a dynamic IP address through the DHCP server. It then groups non-secure computers into a quarantine class and provides non-secure computers with available, limited resources for each established policy configuration.

How an Integrated Enforcer for Microsoft DHCP Servers works

The Integrated Enforcer for Microsoft DHCP Servers checks for Symantec Endpoint Protection or Symantec Network Access Control client installations on the DHCP clients that the DHCP server manages. It then enforces policies for those clients, as configured on the Symantec Endpoint Protection Manager.

The Integrated Enforcer for Microsoft DHCP Servers also authenticates the client for:

- The existence of an agent.
- A Globally Unique Identifier (GUID).
- Host Integrity compliance.
- The profile version of each configured policy.

The Integrated Enforcer for Microsoft DHCP Servers is a software component that interacts with the Microsoft DHCP Server. Although both must be installed on the same computer, the Integrated Enforcer for Microsoft DHCP Servers is not dependent on the DHCP server. When the Integrated Enforcer for Microsoft DHCP Servers resides on the same computer as the DHCP Server, it eliminates the need for additional hardware.

Note: Stopping the DHCP server does not stop the Integrated Enforcer for Microsoft DHCP Servers. Stopping the Integrated Enforcer for Microsoft DHCP Servers does not stop the DHCP server.
You use the Symantec Endpoint Protection Manager to configure the Host Integrity and other security policies. However, the Integrated Enforcer for Microsoft DHCP Servers enforces those security policies.

The Integrated Enforcer for Microsoft DHCP Servers authenticates the client computers by checking for the responses to the following questions:

- Does the Symantec Endpoint Protection client or the Symantec Network Access Control client run on the client computer?
- Does the Symantec Endpoint Protection client or the Symantec Network Access Control client have the correct Globally Unique Identifier (GUID)?
  Is the GUID a 128-bit hexadecimal number? This number is assigned to a client computer that runs the Symantec Endpoint Protection client or the Symantec Network Access Control client. The management server generates a GUID when the client initially connects.
- Does the client comply with the latest Host Integrity policy that the administrator has set up on the console of the Symantec Endpoint Protection Manager?
- Has the client received the latest security policy?

If the Integrated Enforcer for Microsoft DHCP Servers cannot authenticate the client, it provides access to a quarantined area. The quarantine area provides limited network resources to the client. The quarantine area is configured on the same computer as the Integrated Enforcer for Microsoft DHCP Servers and the Microsoft DHCP server.

You can also set up access to a remediation server. The remediation server provides clients with links to software that enables them to become compliant with your security policies.

See "About the Symantec Network Access Control Integrated Enforcer for Microsoft DHCP Servers" on page 320.

About configuring the Symantec Network Access Control Integrated Enforcer for Microsoft DHCP Server on the Symantec Endpoint Protection Manager

If you want to support the Symantec Integrated Enforcer for Microsoft DHCP Server in a network environment, you must have a DHCP server set up and running. Most of the configuration takes place on the Enforcer console. Once installed, you can configure the following areas from the Symantec Endpoint Protection Manager:

- Configuration, both basic and advanced
Configuring Symantec Network Access Control Integrated Enforcer basic settings

You can add or edit the description of a Symantec Network Access Control Integrated Enforcer or an Integrated Enforcer group in Symantec Endpoint Protection Manager. You can also add or edit them on the Integrated Enforcer console.

See “Adding or editing the description of an Enforcer group with a Symantec Network Access Control Integrated Enforcer” on page 323.

See “Adding or editing the description of a Symantec Network Access Control Integrated Enforcer” on page 323.

However, you cannot add or edit the name of an Integrated Enforcer group in Symantec Endpoint Protection Manager. You cannot add or edit the IP address or host name of an Integrated Enforcer in Symantec Endpoint Protection Manager. Instead, you must perform these tasks on the Enforcer console.

See “Adding or editing the name of an Enforcer group for Symantec Network Access Control Integrated Enforcer” on page 322.

You must connect the Integrated Enforcer to Symantec Endpoint Protection Manager.

See “Connecting the Symantec Network Access Control Integrated Enforcer to a Symantec Endpoint Protection Manager” on page 324.

Adding or editing the name of an Enforcer group for Symantec Network Access Control Integrated Enforcer

You can add or edit the name of an Enforcer group of which an Integrated Enforcer is a member. You perform these tasks on the Enforcer console during the installation.
Later, if you want to change the name of an Enforcer group, you can do so on the Enforcer console.

See “Establishing or changing communication between an Integrated Enforcer for Microsoft DHCP servers and a Symantec Endpoint Protection Manager” on page 310.

All Enforcers in a group share the same configuration settings.

Adding or editing the description of an Enforcer group with a Symantec Network Access Control Integrated Enforcer

You can add or edit the description of an Enforcer group of which a Symantec Network Access Control Integrated Enforcer is a member. You can perform this task on the Symantec Endpoint Protection Manager console instead of the Integrated Enforcer console.

To add or edit the description of an Enforcer group with a Symantec Network Access Control Integrated Enforcer

1. In Symantec Endpoint Protection Manager, click Admin.
2. Click Servers.
3. Under Servers, select and expand the Enforcer group whose name you want to add or edit.
5. In the Settings dialog box, on the General tab, add or edit a description for the Enforcer group in the Description field.
6. Click OK.

Adding or editing the description of a Symantec Network Access Control Integrated Enforcer

You can add or edit the description of a Symantec Network Access Control Integrated Enforcer. You can perform this task on Symantec Endpoint Protection Manager instead of the Integrated Enforcer console. After you complete this task, the description appears in Description field of the Management Server pane.

To add or edit the description of a Symantec Network Access Control Integrated Enforcer

1. In Symantec Endpoint Protection Manager, click Admin.
2. Click Servers.
3. Select and expand the Enforcer group that includes the Integrated Enforcer whose description you want to add or edit.
4 Select the Integrated Enforcer whose description you want to add or edit.
5 Under Tasks, click Edit Enforcer Properties.
6 In the Enforcer Properties dialog box, add or edit a description for the Integrated Enforcer in the Description field.
7 Click OK.

Connecting the Symantec Network Access Control Integrated Enforcer to a Symantec Endpoint Protection Manager

Enforcers must be able to connect to servers on which Symantec Endpoint Protection Manager is installed. The management server includes a file that helps manage the traffic between clients, management servers, and optional Enforcers such as an Integrated Enforcer. This file is called a management server list.

The management server list specifies to which Symantec Endpoint Protection Manager an Integrated Enforcer connects. It also specifies to which Symantec Endpoint Protection Manager an Integrated Enforcer connects in case of a management server's failure.

A default management server list is automatically created for each site during the initial installation. All available management servers at that site are automatically added to the default management server list.

A default management server list includes the management server's IP addresses or host names to which Integrated Enforcers can connect after the initial installation. You may want to create a custom management server list before you deploy any Enforcers. If you create a custom management server list, you can specify the priority in which an Integrated Enforcer can connect to management servers.

You can select the specific management server list that includes the IP addresses or host names of those management servers to which you want the Integrated Enforcer to connect. If there is only one management server at a site, then you can select the default management server list.

To select the management server list for the Symantec Network Access Control Integrated Enforcer

1 In Symantec Endpoint Protection Manager, click Admin.
2 Click Servers.
3 Select and expand the group of Enforcers.
   The Enforcer group must include the Integrated Enforcer for which you want to change the IP address or host name in a management server list.
4 Under Tasks, click Edit Group Properties.
5 In the Settings dialog box, on the General tab, under Communication, select the management server list that you want this Integrated Enforcer to use.

6 On the General tab, under Communication, click Select.

You can view the IP addresses and host names of all available management servers, as well as the priorities that have been assigned to them.

7 In the Management Server List dialog box, click Close.

8 In the General dialog box, click OK.

Configuring Symantec Network Access Control Integrated Enforcer advanced settings

You can configure the following Integrated Enforcer advanced configuration settings:

- Timeout parameters, Authentication timeout, and DHCP message timeout
  Although these options are displayed, they are currently unavailable for Symantec Network Access Control Integrated Enforcer configuration.

- MAC addresses for the trusted hosts that the Integrated Enforcer allows to connect to the normal DHCP server without authentication

- Enabling local authentication

- Symantec Endpoint Protection Manager health check

When you apply any of these configuration settings, the changes are sent to the selected Symantec Network Access Control Integrated Enforcer during the next heartbeat.

See “Enabling servers, clients, and devices to connect to the network as trusted hosts without authentication” on page 325.

See “Enabling local authentication on the Integrated Enforcer” on page 326.

Enabling servers, clients, and devices to connect to the network as trusted hosts without authentication

A trusted host is typically a server that cannot install the client software such as a non-Windows server, or a device, such as a printer. You may also want to identify non-Windows clients as trusted hosts because the Integrated Enforcer is unable to authenticate any clients that do not run the Symantec Endpoint Protection client or the Symantec Network Access Control client.

You can use MAC addresses to designate certain servers, clients, and devices as trusted hosts.
When you designate servers, clients, and devices as trusted hosts, the Integrated Enforcer passes all DHCP messages from the trusted host without authenticating the trusted host.

To enable servers, clients, and devices to connect to the network as trusted hosts without authentication

1. In Symantec Endpoint Protection Manager, click **Admin**.
2. Click **Servers**.
3. Under **Servers**, select and expand the group of Enforcers.
4. Select the Integrated Enforcer that permits servers, clients, and the devices that have been designated as trusted hosts to connect to the network without authentication.
5. Under **Tasks**, click **Edit Group Properties**.
6. In the **Settings** dialog box, on the **Advanced** tab, next to **MAC address**, click **Add**.
7. In the **Add Trusted Host** dialog box, type the MAC address for the client or the trusted host in the Host MAC address field.

When you specify a MAC address, you can use a wildcard character if you type it for all three fields on the right.

For example, 11-22-23-*-*-* represents the correct use of the wildcard character. However, 11-22-33-44-*-* does not represent the correct use of the wildcard character.

You can also copy a set of MAC addresses from a text file.

---

Note: Symantec supports the following format for imports: single MAC address, and MAC address with mask.

---

To import MAC addresses, click **Import**. Specify the file in the **Import MAC Address From File** dialog box.

To export MAC addresses, highlight several MAC addresses, and then click **Export**. Specify the file in the **Export MAC Address To File** dialog box.

8. Click **OK**.

### Enabling local authentication on the Integrated Enforcer

With local authentication enabled, if the Integrated Enforcer loses its connection with the client on which Symantec Endpoint Protection Manager is installed, the
Integrated Enforcer authenticates clients locally. In this case, the Integrated Enforcer considers the client a valid user and only checks the client’s Host Integrity status.

**Note:** If the Integrated Enforcer does not lose its connection with Symantec Endpoint Protection Manager, it always asks the management server to verify the client’s GUID regardless of whether local authentication is enabled or disabled.

To enable local authentication on the Integrated Enforcer

1. In Symantec Endpoint Protection Manager, click **Admin**.
2. Click **Servers**.
3. Under **Servers**, select and expand the group of Integrated Enforcers.
4. Under **Tasks**, click **Edit Group Properties**.
5. In the **Settings** dialog box, on the **Advanced** tab, check **Enable Local Authentication**.
6. Click **OK**.

## Configuring Symantec Network Access Control

### Integrated Enforcer authentication settings

You can specify a number of authentication settings for an Integrated Enforcer authentication session. When you apply these changes, they are automatically sent to the selected Integrated Enforcer during the next heartbeat.

### About using authentication settings

You may want to implement a number of authentication settings to further secure the network.

*Table 21-1* provides more information about the options on the **Authentication** tab.
### Table 21-1  
Authentication configuration settings for a Symantec Network Access Control Integrated Enforcer

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Maximum number of packets per authentication session | The maximum number of challenge packets that the Integrated Enforcer sends in each authentication session.  
The default number is 15.  
See "Specifying the maximum number of challenge packets during an authentication session" on page 330. |
| Time between packets in authentication session   | The time (in seconds) between each challenge packet that the Enforcer sends.  
The default value is 4 seconds.  
See "Specifying the frequency of challenge packets to be sent to clients" on page 331. |
| Allow all clients, but continue to log which clients are not authenticated | If this option is enabled, the Enforcer authenticates all users by checking that they are running a client. It then forwards the request to receive a normal rather than a quarantine network configuration, whether the checks pass or fail.  
The default setting is not enabled.  
See “Allowing all clients with continued logging of non-authenticated clients” on page 332. |
| Allow all clients with non-Windows operating systems | If this option is enabled, the Integrated Enforcer checks for the operating system of the client. The Integrated Enforcer then allows all clients that do not run the Windows operating systems to receive a normal network configuration without being authenticated. If this option is not enabled, the clients receive a quarantine network configuration.  
The default setting is not enabled.  
See "Allowing non-Windows clients to connect to a network without authentication” on page 332. |
Table 21-1  Authentication configuration settings for a Symantec Network Access Control Integrated Enforcer (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check the policy serial number on client before allowing client into network</td>
<td>If this option is enabled, the Integrated Enforcer verifies that the client has received the latest security policies from the management server. If the policy serial number is not the latest, the Integrated Enforcer notifies the client to update its security policy. The client then forwards the request to receive a quarantine network configuration. If this option is not enabled and if the Host Integrity check succeeds, the Integrated Enforcer forwards the Integrated request to receive a normal network configuration. The Integrated Enforcer forwards the Integrated request even if the client does not have the latest security policy. The default setting is not enabled. See “Having the Symantec Network Access Control Integrated Enforcer check the Policy Serial Number on a client” on page 333.</td>
</tr>
</tbody>
</table>

**About authentication sessions**

When a client tries to access the internal network, the Symantec Network Access Control Integrated Enforcer first detects whether the client is running a Symantec Endpoint Protection client. If it is, the Enforcer forwards the client DHCP message to the DHCP server to obtain a quarantine IP address with a short lease time. This process is used internally by the Integrated Enforcer for its authentication process.

The Integrated Enforcer then begins its authentication session with the client. An authentication session is a set of challenge packets that the Integrated Enforcer sends to a client.

During the authentication session, the Enforcer sends a challenge packet to the client at a specified frequency. The default setting is every three seconds.

The Integrated Enforcer continues to send packets until one of the following conditions are met:

- The Integrated Enforcer receives a response from the client
- The Integrated Enforcer has sent the maximum number of packets specified. The default setting is 15.

The frequency (4 seconds) times the number of packets (15) is the value that is used for the Enforcer heartbeat. The heartbeat is the interval that the Integrated
Enforcer allows the client to remain connected before it starts a new authentication session. The default setting is four seconds.

The client sends information to the Integrated Enforcer that contains the following items:

- Globally Unique Identifier (GUID)
- Its current Profile Serial Number
- The results of the Host Integrity check

The Integrated Enforcer verifies the client GUID and the Policy Serial Number with Symantec Endpoint Protection Manager. If the client has been updated with the latest security policies, its Policy Serial Number matches the one that the Integrated Enforcer receives from the management server. The Host Integrity check results show whether or not the client complies with the current security policies.

After the heartbeat interval or whenever the client tries to renew its IP address, the Integrated Enforcer starts a new authentication session. The client must respond to retain the connection to the internal network.

The Integrated Enforcer disconnects the clients that do not respond.

For the clients that were previously authenticated but now fail authentication, the Integrated Enforcer updates its internal status for the client. It then sends a challenge packet to the client requesting that the client renew its IP address. When the client sends the DHCP "renew" request, the Integrated Enforcer assigns a quarantine IP address to the client.

### Specifying the maximum number of challenge packets during an authentication session

During the authentication session, the Integrated Enforcer sends a challenge packet to the client at a specified frequency.

The Integrated Enforcer continues to send packets until the following conditions are met:

- The Integrated Enforcer receives a response from the client
- The Integrated Enforcer has sent the specified maximum number of packets.

The default setting is 15 for the maximum number of challenge packets for an authentication session.
To specify the maximum number of challenge packets during an authentication session

1. In Symantec Endpoint Protection Manager, click **Admin**.
2. Click **Servers**.
3. Select and expand the group of Enforcers.
   The Enforcer group must include the Integrated Enforcer for which you want to specify the maximum number of challenge packets during an authentication session.
4. Under **Tasks**, click **Edit Group Properties**.
5. On the **Authentication** tab, type the maximum number of challenge packets that you want to allow during an authentication session in the **Maximum number of packets per authentication session** field.
6. In the **Settings** dialog box, on the **Authentication** tab, click **OK**.

Specifying the frequency of challenge packets to be sent to clients

During the authentication session, the Integrated Enforcer sends a challenge packet to the client at a specified frequency.

The Integrated Enforcer continues to send packets until the following conditions are met:

- The Integrated Enforcer receives a response from the client
- The Integrated Enforcer has sent the specified maximum number of packets.

The default setting is every 4 seconds.

To specify the frequency of challenge packets to be sent to clients

1. In Symantec Endpoint Protection Manager, click **Admin**.
2. Click **Servers**.
3. Select and expand the group of Enforcers.
   The Enforcer group must include the Integrated Enforcer for which you want to specify the frequency of challenge packets to be sent to clients.
4. Under **Tasks**, click **Edit Group Properties**.
5. On the **Authentication** tab, under **Authentication Parameters**, type the maximum number of challenge packets that you want the Integrated Enforcer to keep sending to a client during an authentication session in the **Time between packets in authentication session** field.
6. In the **Settings** dialog box, on the **Authentication** tab, click **OK**.
Allowing all clients with continued logging of non-authenticated clients

It can take some time to deploy all the client software. You can configure the Integrated Enforcer to allow all clients to connect to the network until you have finished distributing the client package to all users. These users all connect to an DHCP server at the location of this Integrated Enforcer.

The Integrated Enforcer still authenticates all users by checking that they are running a client, checking Host Integrity, and logging the results. This process occurs regardless of whether the Host Integrity checks pass or fail.

The default setting is not enabled.

Use the following guidelines when you apply the configuration settings:

- This setting should be a temporary measure because it makes the network less secure.
- While this setting is in effect, you can review Enforcer logs. You can learn about the types of clients that try to connect to the network at that location. For example, you can review the Client Activity Log to see if any of the clients do not have the client software installed. You can then make sure that the client software is installed on those clients before you disable this option.

To allow all clients with continued logging of non-authenticated clients

1. In Symantec Endpoint Protection Manager, click Admin.
2. Click Servers.
3. Under Servers, select and expand the group of Enforcers.
   - The Enforcer group must include the Integrated Enforcer for which you want to allow all clients while continuing to log non-authenticated clients.
5. In the Settings dialog box, on the Authentication tab, check Allow all clients, but continue to log which clients are not authenticated.
6. In the Settings dialog box, on the Authentication tab, click OK.

Allowing non-Windows clients to connect to a network without authentication

The Integrated Enforcer cannot authenticate a client that supports a non-Windows operating system. Therefore non-Windows clients cannot connect to the network unless you specifically allow them to connect to the network without authentication.

The default setting is not enabled.
You can use one of the following methods to enable the clients that support a non-Windows platform to connect to the network:

- Specify each non-Windows client as a trusted host.
- Allow all clients with non-Windows operating systems.

**To allow non-Windows clients to connect to a network without authentication**

1. In Symantec Endpoint Protection Manager, click **Admin**.
2. Click **Servers**.
3. Select and expand the group of Enforcers.
   The Enforcer group must include the Integrated Enforcer for which you want to allow all non-Windows clients to connect to a network.
4. Under **Tasks**, click **Edit Group Properties**.
5. In the **Settings** dialog box, on the **Authentication** tab, check **Allow all clients with non-Windows operating systems**.
6. Click **OK**.

**Having the Symantec Network Access Control Integrated Enforcer check the Policy Serial Number on a client**

Symantec Endpoint Protection Manager updates a client’s Policy Serial Number every time that the client’s security policy changes. When a client connects to the Symantec Endpoint Protection Manager, it receives the latest security policies and the latest Policy Serial Number.

When a client tries to connect to the network through the Integrated Enforcer, the Integrated Enforcer retrieves the Policy Serial Number from Symantec Endpoint Protection Manager. The Integrated Enforcer then compares the Policy Serial Number with the one that it receives from the client. If the Policy Serial Numbers match, the Integrated Enforcer has validated that the client is running an up-to-date security policy.

The default value for this setting is not enabled.

The following guidelines apply:

- If the **Check the Policy Serial Number on Client before allowing Client into network** option is checked, a client must have the latest security policy before it can connect to the network through the normal DHCP server. If the client does not have the latest security policy, the client is notified to download the latest policy. The Integrated Enforcer then forwards its DHCP request to receive a quarantine network configuration.
If the Check the Policy Serial Number on Client before allowing Client into network option is not checked and the Host Integrity check is successful, a client can connect to the network. The client can connect through the normal DHCP server even if its security policy is not up to date.

To have the Symantec Network Access Control Integrated Enforcer check the Policy Serial Number on a client

1. In Symantec Endpoint Protection Manager, click Admin.
2. In the Admin page, click Servers.
3. Select and expand the group of Enforcers.
   The Enforcer group must include the Integrated Enforcer that checks the Policy Serial Number on a client.
5. In the Settings dialog box, on the Authentication tab, check Check the Policy Serial Number on the Client before allowing a Client into the network.
6. Click OK.

Configuring logs for the Symantec Network Access Control Integrated Enforcer

Logs for a Symantec Network Access Control Integrated Enforcer are stored on the same computer on which you installed the Symantec Network Access Control Integrated Enforcer. Enforcer logs are generated by default.

If you want to view Enforcer logs in Symantec Endpoint Protection Manager, you must enable the sending of logs on the Symantec Endpoint Protection Manager console. If this option is enabled, the logs are sent from the Integrated Enforcer to Symantec Endpoint Protection Manager and stored in a database.

You can modify the log settings for the Integrated Enforcer in Symantec Endpoint Protection Manager. Activities are recorded in the same Enforcer Server log for all Enforcers on a site.

You can configure settings for the following logs that the Integrated Enforcer generates:

- Server log
  The Enforcer Server log provides the information that is related to the functioning of an Enforcer.
- Client Activity log
The Client Activity log provides information about interactions between the Integrated Enforcer and the clients that have tried to connect to the network. It provides information on authentication, failed authentication, and disconnection.
Configuring the Integrated Enforcer for Microsoft Network Access Protection on an Enforcer console

This chapter includes the following topics:

- About the Symantec Network Access Control Integrated Enforcer for Microsoft Network Access Protection
- How an Integrated Enforcer for Microsoft Network Access Protection works with a Microsoft Network Policy Server (NPS)
- About configuring a Symantec Integrated Enforcer for Microsoft Network Access Protection on an Enforcer console
- Connecting a Symantec Integrated Enforcer for Microsoft Network Access Protection to a management server on an Enforcer console
- Encrypting communication between the Symantec Integrated Enforcer for Microsoft Network Access Protection and the management server
- Setting up an Enforcer group name on the Symantec Integrated Enforcer for Microsoft Network Access Protection console
- Setting up an HTTP communication protocol on the Symantec Integrated Enforcer for Microsoft Network Access Protection console
About the Symantec Network Access Control Integrated Enforcer for Microsoft Network Access Protection

The Integrated Enforcer for Microsoft Network Access Protection (NAP) works in concert with the Microsoft Windows Network Policy Server (NPS) on a Microsoft Windows Server 2008 and Windows Server 2008 R2. The Symantec Integrated NAP Enforcer ensures that the clients that try to connect to the network comply with configured security policies.

NAP restricts access to networks by creating a controlled environment. It checks the security posture of a client before the client can connect to the enterprise network. If a client is noncompliant, NAP either corrects the security posture or limits access to endpoints that do not meet a company's security policy.

Network Access Protection is a client "security health policy" creation, enforcement, and remediation technology that is included in the Windows Server 2008 operating system. System administrators can create and automatically enforce security policies. These security health policies may include software requirements, security update requirements, required computer configurations, and other settings. Client computers that are not in compliance with a security health policy can be provided with restricted network access. When their configuration is updated and brought into compliance with a policy, clients have full network access. Depending on how you deploy NAP, noncompliant clients can be automatically updated so that users regain full network access without manually updating or reconfiguring their computers.

Note: Microsoft uses "security health policy" in its documentation for Network Access Protection. Symantec uses "security policy" and "host integrity policy" to mean the same thing.


How an Integrated Enforcer for Microsoft Network Access Protection works with a Microsoft Network Policy Server (NPS)

The Integrated Enforcer for Microsoft Network Access Protection works by letting you extend the capabilities of Microsoft Network Access Protection (NAP), including:
- Checking for adherence to endpoint security policies. Connecting clients can use the same policies or different policies.
- Controlling guest access.
- Authenticating end users.

When you configure a Network Policy Server (NPS) as a NAP policy server, it evaluates statements of health (SoH) sent by NAP-capable clients. If the clients are healthy, they can connect to the network.

You can configure NAP policies on an NPS that allow client computers to update their configuration to become compliant with your organization’s security policy. You configure those policies by following the instructions in the NPS documentation.

See “About the Symantec Network Access Control Integrated Enforcer for Microsoft Network Access Protection” on page 337.

### About configuring a Symantec Integrated Enforcer for Microsoft Network Access Protection on an Enforcer console

After you complete the installation of the Symantec Integrated NAP Enforcer, you must perform the following tasks. Once you complete them, the Symantec Integrated Enforcer for Microsoft Network Access Protection becomes operational.

#### Table 22-1  Enforcer console configuration summary

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Connect the Integrated Enforcer to Symantec Endpoint Protection Manager.</td>
<td>Specify the Symantec Endpoint Protection Manager to which the Symantec Integrated Enforcer for Microsoft Network Access Protection can connect. You include the host name or IP address of Symantec Endpoint Protection Manager in a file that is called a management server list. The Symantec NAC Integrated Enforcer must connect to an IP address or host name of Symantec Endpoint Protection Manager. Otherwise the configuration fails. See “Connecting a Symantec Integrated Enforcer for Microsoft Network Access Protection to a management server on an Enforcer console” on page 339.</td>
</tr>
</tbody>
</table>
### Table 22-1  Enforcer console configuration summary (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Encrypt communication between the Integrated Enforcer and the management server.</td>
<td>Add an encrypted password or a preshared secret that you configured during the installation of Symantec Endpoint Protection Manager. The encrypted password was previously known as a preshared key. See “Encrypting communication between the Symantec Integrated Enforcer for Microsoft Network Access Protection and the management server” on page 341.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Name the Enforcer group.</td>
<td>Set up an Enforcer group name. See “Setting up an Enforcer group name on the Symantec Integrated Enforcer for Microsoft Network Access Protection console” on page 342.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Set up an HTTP or HTTPS communication protocol.</td>
<td>Establish HTTP or HTTPS communication between the Symantec Integrated Enforcer for Microsoft Network Access Protection and Symantec Endpoint Protection Manager. See “Setting up an HTTP communication protocol on the Symantec Integrated Enforcer for Microsoft Network Access Protection console” on page 343.</td>
</tr>
</tbody>
</table>

### Connecting a Symantec Integrated Enforcer for Microsoft Network Access Protection to a management server on an Enforcer console

You need to connect a Symantec Integrated Enforcer for Microsoft Network Access Protection (NAP Enforcer) to a management server on a Network Access Protection Enforcer console.
To establish communication between the Integrated Enforcer console and Symantec Endpoint Protection Manager

1. On the Windows taskbar of the Integrated Enforcer computer, click **Start > Programs > Symantec Endpoint Protection > Symantec NAC Integrated Enforcer**.

   The Symantec Network Access Control Integrated Enforcer configuration console appears. This main page shows the connection status between the Integrated Enforcer and Symantec Endpoint Protection Manager. A green light indicates that Integrated Enforcer is actively connected to the management server. A red light indicates that the connection is disconnected.

2. In the left-hand panel, click **Symantec Integrated Enforcer > Configure > Management Server**.

3. In the **Management Server** dialog box, type the IP address or name of the Symantec Endpoint Protection Manager in the **Server address** text field.

   You can type an IP address, host name, or domain name. If you want to use a host name or a domain name, ensure that the name resolves correctly with the Domain Name Server (DNS server).

4. In the **Management Server** dialog box, edit the port number that the Integrated Enforcer uses to communicate with the Symantec Endpoint Protection Manager.

   The default port number is 8014 for HTTP protocol and 443 for the HTTPS protocol. You can only use the HTTPS protocol if it is configured in the same way on the Symantec Endpoint Protection Manager.

5. In the **Encryption password** text box, type the password of the Symantec Endpoint Protection Manager for your connection.

   Symantec Endpoint Protection Manager and Integrated Enforcer must use the same encrypted password for communication.

   To use a hash value instead of the encrypted password, check **Use Hash Value**. If you enable **Use Hash Value**, the password must be 32 characters, and must use hexadecimal numbers only.

6. In the **Preferred** group text box, type a name for the Integrated Enforcer group.

   If you do not specify a group name, Symantec Endpoint Protection Manager assigns the Symantec Network Access Control Integrated Enforcer to a default Enforcer group with default settings. The default group name is I-DHCP. However, the Symantec Network Access Control Integrated Enforcer for Microsoft NAP Servers and the appliance-based Enforcers must each be in a separate group.

   You can view the group settings from the Symantec Endpoint Protection Manager console on the **Servers** page.
To specify the protocol that the Symantec Network Access Control Integrated Enforcer uses to communicate with Symantec Endpoint Protection Manager, select HTTP or HTTPS.

You can only use the HTTPS protocol if Secure Sockets Layer (SSL) is enabled for Symantec Endpoint Protection Manager.

If you select HTTPS and want to require verification of the management server’s certificate with a trusted third-party certificate authority, check **Verify certificate when using HTTPS protocol**.

Click **Save**.

After the Integrated Enforcer connects to Symantec Endpoint Protection Manager, you can change most of the configuration settings in the Symantec Endpoint Protection Manager console. However, the preshared secret or encrypted password must be the same on the Integrated Enforcer and Symantec Endpoint Protection Manager in order for them to communicate.

### Encrypting communication between the Symantec Integrated Enforcer for Microsoft Network Access Protection and the management server

If you want to add another layer of security, you can secure communication between the Symantec Network Access Control Integrated Enforcer and Symantec Endpoint Protection Manager through encryption. Encrypted communication requires the use of the HTTPS protocol instead of the HTTP protocol. You also need to purchase a third-party certificate from a vendor.

You typically configure an encrypted password during the installation of Symantec Endpoint Protection Manager for the first time. The same password must be configured on the Symantec Integrated NAP Enforcer. If the encrypted passwords do not match, communication between the Symantec Integrated NAP Enforcer and Symantec Endpoint Protection Manager fails.

**To encrypt communication between the Symantec Network Access Control Integrated Enforcer and the management server**

1. On the Windows taskbar of the Enforcer computer, click **Start > Programs > Symantec Endpoint Protection > Symantec Integrated NAP Enforcer**.

2. In the left-hand panel, expand Symantec NAP Enforcer.

3. Expand Configure.

4. Click **Management Servers**.
5 Type the encrypted password in the Encrypted Password text box on the Symantec Integrated NAP Enforcer console.

The Symantec Integrated NAP Enforcer must use the same encrypted password for communication with Symantec Endpoint Protection Manager. The encrypted password is always configured during the installation of Symantec Endpoint Protection Manager.

6 Check Use Hash Value. If Use Hash Value is checked, the encryption password must be 32 characters and must use hexadecimal numbers only.

The letters and numbers of the encrypted password now appear instead of asterisks.

7 Click OK.

Setting up an Enforcer group name on the Symantec Integrated Enforcer for Microsoft Network Access Protection console

You must add a name for the Enforcer group. After the Symantec Network Access Control Integrated Enforcer connects to Symantec Endpoint Protection Manager, it registers the name of the Enforcer group automatically on the management server.

To set up an Enforcer group name on the Symantec Network Access Control Integrated Enforcer console

1 On the Windows taskbar of the Enforcer computer, click Start > Programs > Symantec Endpoint Protection > Symantec Integrated NAP Enforcer.

2 In the left-hand panel, expand Symantec NAP Enforcer.

3 Expand Configure.

4 Click Management Servers.
5 In the right-hand panel, type the name of the Enforcer group in the Preferred group text box on the Symantec Integrated NAP Enforcer console.

If you do not add a name for the Integrated Enforcer group on the Enforcer console: All Integrated Enforcers automatically become part of the Default group on the management server.

If you add the name of the Integrated Enforcer group on the Enforcer console: The name of the Enforcer group is automatically registered on the management server.

6 Click OK.

Setting up an HTTP communication protocol on the Symantec Integrated Enforcer for Microsoft Network Access Protection console

You need to establish a communication protocol between the Symantec Integrated Enforcer for Microsoft Network Access Protection and Symantec Endpoint Protection Manager. Otherwise, the communication between the Symantec Integrated Enforcer for Microsoft Network Access Protection and Symantec Endpoint Protection Manager fails.

You can set up the HTTP or HTTPS protocol. If you select the HTTPS protocol, you need to purchase a certificate from a third-party vendor.

To set up an HTTP communication protocol on the Symantec Integrated Enforcer for Microsoft Network Access Protection

1 On the Windows taskbar of the Enforcer computer, click Start > Programs > Symantec Endpoint Protection > Symantec NAC Integrated Enforcer.

2 In the left-hand panel, expand Symantec NAP Enforcer.

3 Expand Configure.

4 Click Management Servers.

5 In the right-hand panel of the Symantec Integrated NAP Enforcer console, click HTTP.

If you want to set up encrypted communication between the Symantec Integrated NAP Enforcer and Symantec Endpoint Protection Manager, you must use the HTTPS protocol.
6 If you need to verify the certificate because you use the HTTPS protocol, check **Verify certificate when using HTTPS protocol.**

7 Click **OK.**
Configuring the Integrated Enforcer for Microsoft Network Access Protection on the Symantec Endpoint Protection Manager

This chapter includes the following topics:

- About configuring the Symantec Integrated Enforcer for Microsoft Network Access Protection on Symantec Endpoint Protection Manager
- Enabling NAP enforcement for clients
- Verifying that the management server manages the client
- Verifying Security Health Validator policies
- Verifying that clients pass the Host Integrity check
- Configuring logs for the Symantec Integrated Enforcer for Network Access Protection
About configuring the Symantec Integrated Enforcer for Microsoft Network Access Protection on Symantec Endpoint Protection Manager

If you want to support the Symantec Integrated Enforcer for Microsoft Network Access Protection in a network environment, you must enable NAP enforcement on Symantec Endpoint Protection Manager. Otherwise the Enforcer works incorrectly.

You also need to define one or more criteria for the Security Health Validator policy requirements. For example, you can verify whether or not the client's Security Health Validator policy is the latest one that has been installed on a client. If it is not the latest Security Health Validator policy, then the client is blocked and is therefore unable to connect to the network.

Table 23-1 Symantec Endpoint Protection Manager configuration summary

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Enable Network Access Protection enforcement for clients.</td>
<td>Enable Network Access Protection enforcement for clients so that the Integrated Enforcer can run Security Health Validator policies. See &quot;Enabling NAP enforcement for clients&quot; on page 347.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Optionally, verify that Symantec Endpoint Protection Manager manages the Symantec Network Access Control client or the Symantec Endpoint Protection client.</td>
<td>Set up a verification check to ensure that the management server manages the Symantec Network Access Control client or the Symantec Endpoint Protection client. See &quot;Verifying that the management server manages the client&quot; on page 348.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Optionally, verify that the latest Security Health Validator policies are installed.</td>
<td>Verify that the Symantec Network Access Control client and the Symantec Endpoint Protection client have the latest Security Health Validator policies are installed. See &quot;Verifying Security Health Validator policies&quot; on page 348.</td>
</tr>
</tbody>
</table>
### Enabling NAP enforcement for clients

You must enable NAP (Network Access Protection) enforcement for Symantec Endpoint Protection and Symantec Network Access Control clients. If you do not enable NAP enforcement for clients, the Symantec Integrated Enforcer for Microsoft Network Access Protection cannot implement any Security Health Validator policies.

#### To enable NAP enforcement for clients

1. In Symantec Endpoint Protection Manager, click **Clients**.
2. In the **Clients** page, under **View Groups**, select the group for which you want to enable NAP enforcement.
3. On the **Policies** tab, click **General Settings**.
4. In the **Settings** dialog box, click **Security Settings**.
5. On the **Security Settings** tab, in the **Enforce Client** area, check **Enable NAP Enforcement**.
   - The **Enable NAP Enforcement** setting is disabled by default.
6. Click **OK**.

---

**Table 23-1** Symantec Endpoint Protection Manager configuration summary (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 4</td>
<td>Optionally, verify that clients pass the Host Integrity check.</td>
<td>Verify that clients are in compliance with the Host Integrity policy. See “Verifying that clients pass the Host Integrity check” on page 349.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Optionally, configure logs for viewing on Symantec Endpoint Protection Manager.</td>
<td>Enable the sending of log data to Symantec Endpoint Protection Manager. See “Configuring logs for the Symantec Integrated Enforcer for Network Access Protection” on page 349.</td>
</tr>
</tbody>
</table>
Verifying that the management server manages the client

You can set up a verification check to ensure that Symantec Endpoint Protection Manager manages the Symantec Endpoint Protection client or the Symantec Network Access Control client.

To verify that the management server manages the client

1. In Symantec Endpoint Protection Manager, click Admin.
2. Click Servers.
3. Under View, select the Enforcer group for which you want to verify that the management server manages the client.
4. Right-click the Enforcer group and select Edit Properties.
5. In the Client Information area on the NAP Setting tab in the I-DHCP Settings dialog box, check Verify that the management server manages the client.

The Verify that the management server manages the client setting is disabled by default.
6. Click OK.

Verifying Security Health Validator policies

You can make sure that the Symantec Endpoint Protection and Symantec Network Access Control clients have the latest Security Health Validator policies installed.

To verify Security Health Validator policies

1. In Symantec Endpoint Protection Manager, click Admin.
2. Click Servers.
3. Under View, select the group for which you want to set up Security Health Validator policies.
4. Right-click the Enforcer group and select Edit Properties.
5. In the Client Information area on the NAP Setting tab in the I-DHCP Settings dialog box, check Verify that the Security Health Validator policy is current.

The Verify that the Security Health Validator policy is current setting is disabled by default.
6. Click OK.
Verifying that clients pass the Host Integrity check

You can set up a compliance check for clients on Symantec Endpoint Protection Manager.

To verify that clients pass the Host Integrity check

1. In Symantec Endpoint Protection Manager, click **Admin**.

2. Click **Servers**.

3. Under **View**, select the Enforcer group for which you want to verify that the client has passed the Host Integrity check.

4. Right-click the Enforcer group and select **Edit Properties**.

5. In the **Host Integrity Status** area on the **NAP Setting** tab in the **I-DHCP Settings** dialog box, check **Verify that the client passes the Host Integrity check**.

   The **Verify that the client passes the Host Integrity check setting** is disabled by default.

6. Click **OK**.

Configuring logs for the Symantec Integrated Enforcer for Network Access Protection

Logs for the Symantec Integrated Network Access Protection (NAP) Enforcer are stored on the same computer on which you installed the Symantec Integrated NAP Enforcer. Enforcer logs are generated by default.

If you want to view Enforcer logs in the Symantec Endpoint Protection Manager console, you must enable the sending of logs in the Symantec Endpoint Protection Manager console. If this option is enabled, the log are sent from the Symantec Integrated NAP Enforcer to Symantec Endpoint Protection Manager and stored in a database.

You can modify the log settings for the Symantec Integrated NAP Enforcer in the Symantec Endpoint Protection Manager console. Activities are recorded in the same Enforcer Server log for all Enforcers on a site.

You can configure settings for the following logs that the Symantec Integrated NAP Enforcer generates:

- **Server log**
  - The Server log provides the information that is related to the functioning of an Enforcer.
Client Activity log
The Client Activity log provides information about interactions between the Integrated Enforcer and the clients that have tried to connect to the network. It provides information on authentication, failed authentication, and disconnection.
Configuring the Symantec Network Access Control On-Demand Clients

This chapter includes the following topics:

- How the On-Demand Client works
- Before you configure Symantec Network Access Control On-Demand Clients on the console of a Gateway Enforcer
- Setting up guest access challenge using the Symantec Network Access Control DHCP Integrated Enforcer
- Enabling Symantec Network Access Control On-Demand clients to temporarily connect to a network
- Disabling Symantec Network Access Control On-Demand clients
- Setting up authentication on the Gateway Enforcer console for Symantec Network Access Control On-Demand clients
- Editing the banner on the Welcome page

How the On-Demand Client works

The On-Demand Client checks your computer for compliance if you try to connect your computer to a protected network as a guest. If the client computer meets all requirements, a connection between the client computer and Symantec Endpoint Protection Manager is automatically established. If the client meets all security requirements, the client can then access the protected network.
At that point, the security-compliant client computer can perform any task that the administrator has enabled for this group on Symantec Endpoint Protection Manager. If the client computer cannot meet all security requirements, a connection between the client computer and the protected network cannot be automatically established. The user needs to remediate all non-compliant requirements on the client computer by downloading the remediation files as set up by the administrator. Until the remediation is complete, the client cannot access the protected network as a guest.

Your computer must pass or fail a Compliance Status Check when it tries to connect to a company’s protected network. The result of the Compliance Status Check puts your computer into one of the following categories:

- **Allowed**: You can connect to the network. In Allowed mode there is no communication with an Enforcer, or an Enforcer is not installed in the network.
- **Approved**: You are approved to connect to the network by Symantec Network Access Control.
- **Quarantined**: Symantec Network Access Control has placed you in a quarantine area because your client has failed the Host Integrity compliance check or your policy is not the latest one.

  If your computer is quarantined, you may be given the resources to remediate the missing elements to pass the Host Integrity check.

See “Enabling Symantec Network Access Control On-Demand clients to temporarily connect to a network” on page 358.

Before you configure Symantec Network Access Control On-Demand Clients on the console of a Gateway Enforcer

Before you can set up the automatic downloading of the Symantec Network Access Control On-Demand Clients for Windows and Macintosh, you must have already completed the following tasks:

- Installed the Symantec Network Access Control software that is located on the installation file. This software includes the Symantec Endpoint Protection Manager software that you must install.
- Written down the name of the encrypted password that you implemented during the installation of the Network Access Control software.
- Installed and configured a Gateway Enforcer appliance.

When you install and configure an Enforcer appliance for the first time, it assigns a name to the Enforcer group during the installation process. You must plan the assignment of IP addresses, host names, as well as the configuration of the
network interface cards (NICs). If the NICs are incorrectly configured, then the installation fails or behaves in unexpected ways.

The name of the Enforcer group automatically appears on the console of the Symantec Endpoint Protection Manager in the Server pane that is associated with each Enforcer appliance.

You can also set up guest access with the DHCP Integrated Enforcer. See “Setting up guest access challenge using the Symantec Network Access Control DHCP Integrated Enforcer” on page 354.

- Checked the connection status between the Enforcer appliance and the management server on the console of the Enforcer appliance. See “Checking the communication status of an Enforcer appliance on the Enforcer console” on page 371. See “About the Enforcer appliance CLI command hierarchy” on page 372.

- Enabled an HTTP redirect or DNS spoofing on the console of the Symantec Endpoint Protection Manager. The HTTP redirect or DNS spoofing is the IP address of the internal NIC (eth0) that is located on a Gateway Enforcer appliance. See “Redirecting HTTP requests to a Web page” on page 238. For HTTP redirect, you add the URL in the Admin page on the Symantec Endpoint Protection Manager. After you display the Admin page, you must display the Servers pane and select the Enforcer group under View Servers. If you select the Enforcer group of which the Gateway Enforcer is a member, click Edit Group Properties under Tasks. In the Enforcer Settings dialog box, you select the Authentication tab and type the URL in the HTTP redirect URL field.

- You must create the client group as a subgroup of the My Company group with Full Access rights. You add the client group on the Clients page as a subgroup of the My Company group on the Symantec Endpoint Protection Manager. Make sure that you write down the name of the Enforcer client group that manages Symantec Network Access Control On-Demand Clients. If you do not create a separate group, then the Default group on the Symantec Endpoint Protection Manager takes over the management of the Symantec Network Access Control On-Demand Clients.

- Created an optional separate location for an Enforcer client group on the Symantec Endpoint Protection Manager Console. If you do not create a separate location for the group that manages the Symantec Network Access Control On-Demand Clients or guest clients, then the default location is automatically assigned to the guest clients. The best practice is to create a separate location for the Enforcer client group on the Symantec Endpoint Protection Manager Console.
Protection Manager. Another best practice is to use different groups for Windows and Mac clients. Their capabilities differ. For example, Windows On-Demand Clients can be configured to have pop-up messages. Mac On-Demand Clients cannot.

Location criteria help you define the criteria that can identify Symantec Network Access Control On-Demand or guest clients by its IP address, MAC address, host name, or other criteria. The best practice is to create a separate location to which all Symantec Network Access Control On-Demand or guest clients are automatically assigned if they want to connect to a network on a temporary basis without the correct credential.

You can add and assign a location to the Enforcer client group in the Clients page, under Tasks, on the Symantec Endpoint Protection Manager.

- Added and assigned an optional Host Integrity policy to the Enforcer client group and location on the Symantec Endpoint Protection Manager Console.

  It is optional to add and assign a Host Integrity policy to the Enforcer client group and location on the console of a Symantec Endpoint Protection Manager, but the best practice to specify the following criteria:

  - How frequently a host integrity check is run
  - Type of Host Integrity policy that you want to implement

  You can add and assign an optional Host Integrity policy to an Enforcer client group and location in the Policies page, under Tasks, on the Symantec Endpoint Protection Manager.

- Enabled an optional pop-up message for Windows clients. You configure this on the Symantec Endpoint Protection Manager Console.

- Obtain the domain ID number that is located on the Symantec Endpoint Protection Manager Console.

  You should have the domain ID handy because you may need to configure the domain ID on the Gateway or DHCP Enforcer with the on-demand spm-domain command.

  See “Enabling Symantec Network Access Control On-Demand clients to temporarily connect to a network” on page 358.

---

**Setting up guest access challenge using the Symantec Network Access Control DHCP Integrated Enforcer**

Guest Access and the DHCP Integrated Enforcer require a Gateway Enforcer and DNS server, because the DHCP Integrated Enforcer does not support DNS spoofing.

The first step towards enabling this solution is to set up a separate DNS server and Gateway Enforcer in the quarantine network. The guest endpoint receives a
restricted and quarantined IP address with this DNS server. This quarantine DNS server resolves all DNS request to the Gateway Enforcer. The guest endpoint receiving the DNS resolution sends all HTTP request to the Gateway Enforcer. The Gateway Enforcer which then redirects the request to the on-demand Web server for download of the On-Demand Client. Once the download to the endpoint completes, Host Integrity checking runs and the result of this (configurable policy) outcome determines access for the endpoint. If the Host Integrity check passes, the endpoint is granted a normal IP address with the normal DNS server. If Host Integrity fails, the endpoint remains with a quarantined IP address with the quarantined DNS server.

Figure 24-1 Network diagram of DHCP Integrated Enforcer configured to prevent DNS spoofing

To configure the DHCP Integrated Enforcer

1. Configure the DHCP Integrated Enforcer to connect to your Symantec Endpoint Protection Manager.

2. Set up the DHCP Integrated Enforcer to use a secure subnet mask for quarantine IP addresses.

See “Configuring a secure subnet mask” on page 317.
3 Configure the DHCP Integrated Enforcer to add static routes to quarantine IP addresses in the DHCP server. Static routes include DHCP server (192.168.100.1), DNS server (192.168.100.3), SEPM server (192.168.100.2), and Gateway Enforcer internal IP address (192.168.100.4).

4 Verify that static routes are added in the DHCP server. This is configured on the Enforcer console: click **Scope options** and ensure that **033 Static Route Option** is checked for each route.

5 Add a DNS server. Right click on **Scope options**, and then click **Configure options**.

6 On the **Advanced** tab, select **DHCP Standard Options** as the **Vendor class** and **Default User Class** as the **User class**.

7 In the **Available Options** scrolling box, click to select **006 DNS Servers**.

8 In the **IP address** fill-in box, add the normal DNS server IP address (192.168.100.1).

9 Click **Apply**.

10 Add a WINS server, using your usual procedures.

11 Configure quarantine IP address scope settings.

12 Right click on **Scope options**, and then click **Configure options**....

13 On the **Advanced** tab, select **DHCP Standard Options** as the **Vendor class** and **SNAC_QUARANTINE** as the **User class**.

14 In the **Available Options** scrolling box, click to select **006 DNS Servers**.

15 In the **IP address** fill-in box, add the quarantine DNS server IP address (192.168.100.3).

16 Click **Apply**.

17 Add a quarantine WINS server, with the quarantine address of 192.168.100.3.

18 Click **Apply**.

Next you set up the Gateway Enforcer.

**To configure the Gateway Enforcer as a guest appliance**

1 Connect **eth0** to the network and set the IP address to 192.168.100.4.

2 Disconnect **eth1**.

3 Configure settings for configuration of Symantec Endpoint Protection Manager, using the command-line interface on the Gateway Enforcer:

```bash
configure
spm ip 192.168.100.2 key sygate group Gateway
```
4 Ensure that the Enforcer is connected to Symantec Endpoint Protection Manager, by issuing the `show status` command.

5 Enable on-demand, using the command-line interface:

   On-demand
   Spm-domain name <domain name>
   Client-group <client group full path>
   Enable
   Show

Next you set up a quarantine Windows DNS setup for HTTP redirect.

To set up a quarantine Windows DNS HTTP redirect

1 Open the DNS management console on the quarantine DNS server (192.168.100.3).

2 Right click Forward Lookup Zones and select New Zone. The New Zone Wizard appears.

3 In the New Zone Wizard, click Next.

4 Select Primary zone, and click Next.

5 Type a period (.) as the Zone name, and click Next.

6 Select Create a new file with this file name, type root.dns, and click Next.

7 Select Do not allow dynamic updates, and click Next.

8 Click Finish.

Create a new host under the .(root) zone that you just created.

To create a new host in the .(root) zone

1 Right click on the .(root) zone, and then select New Host.

2 Type an asterisk (*) as the Name and the Gateway Enforcer IP address (192.168.100.4) as the IP address for the new host.

3 Click Add Host.

Change the lookup IP address of the DNS server itself.

To change the IP address of the DNS server

1 Double click the DNS server name in the right panel.

2 Change the IP address to the Enforcer IP address (192.168.100.4), and click OK.

Optional: You may want to set up the WINS server to resolve in the same fashion as the DNS server. Computer names are resolved by the WINS server. If the
endpoint is not registered to a domain, it resolves its computer name through WINS server. You may choose to set up a separate WINS server in quarantine to resolve all computer names in the internal network to the Gateway Enforcer eth0 (192.168.100.4).

You should test your configuration.

To test your configuration

1. On the command prompt on the client computer, type
   
   `ipconfig /release`  
   `ipconfig /renew`

   The client should get a quarantine IP address with 255.255.255.255 as the subnet mask, and 192.168.100.3 as the DNS server.

2. Clear the DNS cache. Type `ipconfig /flushdns`.

   
   You should be redirected to the Gateway Enforcer on-demand Web site.

4. Download the On-Demand Client, and pass Host Integrity checks.

5. Your client is issued a normal IP address and 192.168.100.1 as the DNS server.

Enabling Symantec Network Access Control
On-Demand clients to temporarily connect to a network

If you want to enable the automatic downloading of a Symantec Network Access Control On-Demand client on a client computer on the Windows and Macintosh platforms, you must have already completed a number of configuration tasks.

See “Before you configure Symantec Network Access Control On-Demand Clients on the console of a Gateway Enforcer” on page 352.

You need to configure the following commands before you can enable Symantec Network Access Control On-Demand clients to connect to a network:

- Execute the `spm-domain` command.
- Execute the `client-group` command.
- Execute the `enable` command.
- Execute the `authentication enable` command. This command is optional.
To enable Symantec Network Access Control On-Demand clients to temporarily connect to a network

1. Log on to the Gateway Enforcer appliance console as a superuser.
   See “Logging on to an Enforcer appliance” on page 175.

2. On the console of a Gateway Enforcer appliance, type the following command:
   `Enforcer # on-demand`

3. Type the following command:
   `Enforcer (on-demand)# spm-domain`
   where:
   `spm-domain` represents a string that is displayed in the Enforcer automatically.
   See “Before you configure Symantec Network Access Control On-Demand Clients on the console of a Gateway Enforcer” on page 352.

4. Type the following command:
   `Enforcer (on-demand)# client-group "My Company/"name of Enforcer client group"
   where:
   ```
   name of Enforcer client group represents the name of the Enforcer client group that you already set up in the Clients page under View Clients on the console of a Symantec Endpoint Protection Manager. You should have already set up this Enforcer client group as a subgroup to the My Company group with full access rights. If you have not set the Enforcer client group on the console of a Symantec Endpoint Protection Manager, the Enforcer registers to the Default group. The information about the Enforcer client group is automatically sent during the next heartbeat.
   You can now set up authentication for the Symantec Network Access Control On-Demand clients.
   See “Setting up authentication on the Gateway Enforcer console for Symantec Network Access Control On-Demand clients” on page 360.
   ```

5. Type the following command:
   `Enforcer (on-demand)# enable`
   You can also set the duration of time that the On-Demand Client will be "live," using the persistence command.
To make the Symantec Network Access Control On-Demand clients "persistent"

1. Log on to the Gateway Enforcer appliance console as a superuser.
   See “Logging on to an Enforcer appliance” on page 175.

2. On the console of a Gateway Enforcer appliance, type the following command:
   ```
   Enforcer # on-demand
   ```

3. Type the following command:
   ```
   Enforcer (on-demand)# persistence duration days 10
   ```
   where:
   ```
   duration days 10
   ```
   indicates that you want the client to persist for 10 days.

Disabling Symantec Network Access Control On-Demand clients

If you want to stop allowing guest access, you can disable it.

To disable Symantec Network Access Control On-Demand clients for client computers

1. Log on to the Gateway Enforcer appliance console as superuser.
   See “Logging on to an Enforcer appliance” on page 175.

2. On the console of a Gateway Enforcer appliance, type `on-demand`.

3. Type `disable`.

4. Type `exit`.

5. Type `exit` to log off.

Setting up authentication on the Gateway Enforcer console for Symantec Network Access Control On-Demand clients

You can authenticate end users with On-Demand clients by enabling one of the following for authentication.

- The local database of the Gateway Enforcer appliance.
  See “Setting up user authentication with a local database” on page 361.
A Microsoft Windows Server 2003 Active Directory configured to manage the authentication of the end users with the Gateway Enforcer appliance. See “Setting up user authentication with a Microsoft Windows 2003 Server Active Directory” on page 362.

A RADIUS server configured to manage the authentication of the end users with the Gateway Enforcer appliance. See “Setting up user authentication with a RADIUS server” on page 362.

Once you enable authentication, add user names and a password for each authenticated end user.

To run commands for the On-Demand clients, see the Symantec Network Access Control Enforcer Command-line Reference Guide.

Setting up user authentication with a local database

You can configure up to 1,000 users in the local on-board database of the Gateway Enforcer appliance.

To set up authentication with a local database

1. Log on to the Gateway Enforcer appliance console as a superuser. See “Logging on to an Enforcer appliance” on page 175.

2. On a Gateway Enforcer appliance console, type the following command:

   Enforcer # on-demand

3. On a Gateway Enforcer appliance console, type the following command:

   Enforcer (on-demand)# authentication

4. Type the following command:

   Enforcer (authentication)# local-db add user name username password password

5. Type the following command:

   Enforcer (authentication)# local-db enable

6. Type the following command:

   Enforcer (authentication)# enable

For more information on the on-demand authentication local-db commands, see the Symantec Network Access Control Enforcer Command-line Reference Guide.
Setting up user authentication with a Microsoft Windows 2003 Server
Active Directory

The Gateway Enforcer appliance establishes a connection to the Microsoft Windows 2003 Server through the domain name instead of the IP address. Therefore you must have set up a Domain Name Server (DNS) in the network that can resolve the domain name.

To set up authentication with an Active Directory server

1. Log on to the Gateway Enforcer appliance console as a superuser. See “Logging on to an Enforcer appliance” on page 175.
2. On a Gateway Enforcer appliance console, type the following command:
   Enforcer # on-demand
3. Type the following command:
   Enforcer (on-demand)# authentication
4. Type the following command:
   Enforcer (authentication)# ad domain domain name alias name
5. Type the following command:
   Enforcer (authentication)# ad enable
6. Type the following command:
   Enforcer (authentication)# enable

Setting up user authentication with a RADIUS server

You can set up and configure one or more RADIUS servers for authentication. For example, you might want to have multiple RADIUS servers for load balancing.

Note: Note that certificates need to be imported to the Enforcer for PEAP and TLS clients.

To set up the On-Demand client for authentication with a RADIUS server

1. Log on to the Gateway Enforcer appliance console as a superuser. See “Logging on to an Enforcer appliance” on page 175.
2. Type the following command:
   Enforcer# on-demand
3 Type the following command:

```
Enforcer (on-demand)#authentication
```

4 Type the following command:

```
Enforcer (authentication)# radius add name alias name server
RADIUS server address secret shared secret auth_method auth method
```

where:

- *alias_name* represents the name displayed for the RADIUS authentication method listed in **Auth Server** in the logon dialog box.
- *RADIUS server address* represents the RADIUS server and port. Port is an optional number between 1 and 65535. If you do not specify a port number the Enforcer uses a default of port 1812.
- *shared secret* is the shared secret on the RADIUS server.
- *auth method* is PAP, CHAP, MS-CHAP-V1, or MS-CHAP-V2.

5 Type the following command:

```
Enforcer (authentication)# radius enable
```

6 Enforcer (authentication)#enable

In addition to the RADIUS add name and RADIUS enable commands, you can run other RADIUS commands to manage the RADIUS server.

For more information on the on-demand authentication radius server commands, see the **Symantec Network Access Control Enforcer Command-line Reference Guide**.

**Setting up the On-Demand client on Windows for authentication with the dot1x-tls protocol**

The Gateway Enforcer appliance can connect to dot1.x-enabled ports with the tls protocol.

**To set up the On-Demand client on Windows for authentication with the dot1x-tls protocol**

1 On the Enforcer console, type: `Enforcer#on-demand`

2 Type the following command: `Enforcer (on-demand)# dot1x`

3 Type the following command: `Enforcer (dot1x)# protocol tls`

4 Type the following command: `Enforcer (tls)# show protocol`

The protocol must be set to tls. For example, **Active Protocol: TLS**
5 Type the following command: Enforcer (tls)# validate-svr enable

6 Type the following command: Enforcer (cert-svr)# exit

7 Type the following command: Enforcer (tls)# show tls

Make sure that the tls server certificate is enabled. For example:

- TLS Validate Server Certificate: ENABLED
- TLS Certificate Server: ENABLED
- TLS Certificate Server: 127.0.0.1

8 Type the following command: Enforcer (dot1x)# certificate import
tftp 10.34.68.69 password symantec username janedoe user-cert qa.pfx root-cert qa.ce

where:
- 10.34.68.69 is the tftp server from which the Enforcer appliance can import the certificate by tftp.
- symantec is the password of the user certificate
- janedoe is the user name with which you log on the client.
- qa.pfx is the name of the user certificate.
- qa.cer is the name of the root certificate

Setting up the On-Demand client on Windows for authentication with the dot1x-peap protocol

Gateway Enforcer appliance can establish a connection with the peap protocol.

To set up the On-Demand client on Windows for authentication with the peap protocol

1 On the Enforcer console, type: Enforcer#on-demand

2 Type the following command: Enforcer (on-demand)# dot1x

3 Type the following command: Enforcer (dot1x)# protocol peap

4 Type the following command: Enforcer (peap)# show protocol

Make sure that the peap server certificate is enabled; for example:

- PEAP Validate Server Certificate: ENABLED
- PEAP Certificate Server: DISABLED
- PEAP Certificate Server: 127.0.0.1
- PEAP Fast Reconnected: DISABLED
5 If server validation is required, type:

    Enforcer (peap) cert-svr host snac

where snac is the computer that is the CA server for the peap certificate name. Then type:

    Enforcer (peap) exit
    Enforcer (dot1x certificate import tftp 10.34.68.69 root-cert qa.cer

6 If no server validation is required, type:

    Enforcer (peap) validate_svr disable

**Editing the banner on the Welcome page**

You can edit the default banner text on the **Welcome** page of the Symantec Network Access Control On-Demand client.

**To edit the banner on the Welcome page**

1 Log on to the Gateway Enforcer appliance console as a superuser.
   See “Logging on to an Enforcer appliance” on page 175.

2 Type the following command on the console of a Gateway Enforcer appliance:

    Enforcer# on-demand

3 Type the following command:

    Enforcer(on-demand)# banner

    Press Enter.

4 In the pop-up window, type the message that you want users to view on the **Welcome** page of the Symantec Network Access Control On-Demand client. You can type up to 1024 characters.
Performing basic tasks on the console of all types of Enforcer appliances

This chapter includes the following topics:

- About performing basic tasks on the console of an Enforcer appliance
- Communication between an Enforcer appliance and a Symantec Endpoint Protection Manager
- Communication between the Enforcer appliance and clients
- Configuring a connection between an Enforcer appliance and a Symantec Endpoint Protection Manager
- Checking the communication status of an Enforcer appliance on the Enforcer console
- Remote access to an Enforcer appliance
- About the Enforcer appliance CLI command hierarchy

About performing basic tasks on the console of an Enforcer appliance

You must have already configured the following parameters during the installation of the Enforcer appliance:

- Host name of the Enforcer appliance
- Group name of the Enforcer appliance group of which a particular Enforcer appliance is a member
- IP addresses of the internal and the external network interface cards (NICs)
- IP address of the DNS server, if applicable
- IP address of the NTP server, if applicable

However, you must still configure a connection between an Enforcer appliance and a Symantec Endpoint Protection Manager. You execute the `spm` command on the console of the Enforcer appliance to configure this connection. You cannot proceed to use an Enforcer appliance unless you complete this task.

See “Configuring a connection between an Enforcer appliance and a Symantec Endpoint Protection Manager” on page 369.

After initially installing and configuring an Enforcer appliance, you can perform administrative tasks from the Enforcer console or Symantec Endpoint Protection Manager. If you administer multiple Enforcer appliances, it is convenient to administer them all from one centralized location.

All Enforcer appliances also have a command-line interface (CLI) from which you can execute commands to change many parameters.

See “About the Enforcer appliance CLI command hierarchy” on page 372.

**Communication between an Enforcer appliance and a Symantec Endpoint Protection Manager**

The Enforcer appliance stays connected to the Symantec Endpoint Protection Manager. At regular intervals (the heartbeat), the Enforcer appliance retrieves settings from the management server. Those settings control how the Enforcer appliance operates. When you make any changes on the management server that affect the Enforcer appliance, the Enforcer appliance receives the update during the next heartbeat. The Enforcer appliance transmits its status information to the management server. It can log the events that it forwards to the management server. The information then appears in the logs on the management server.

The Symantec Endpoint Protection Manager maintains a list of management servers with replicated database information. It downloads the management server list to connected Enforcers and managed clients and guest clients. If the Enforcer appliance loses communication with one management server, it can connect to another management server that is included in the management server list. If the Enforcer appliance is restarted, it uses the management server list to reestablish a connection to a management server.
When a client tries to connect to the network through the Enforcer appliance, the Enforcer appliance authenticates the client's Globally Unique Identifier (GUID). The Enforcer appliance sends the GUID to the management server and receives an accept response or a reject response.

If an Enforcer appliance is configured to authenticate the GUID, it can retrieve information from the management server. The Enforcer appliance can then determine if the client profile has been updated with the latest security policies. If the client information changes on the management server, the management server can send the information to the Enforcer appliance. The Enforcer appliance can again perform host authentication on the client.

See “Changing Gateway Enforcer appliance configuration settings in Symantec Endpoint Protection Manager” on page 223.

See “Changing LAN Enforcer configuration settings in Symantec Endpoint Protection Manager” on page 260.

Communication between the Enforcer appliance and clients

The communication between the Enforcer appliance and a client begins when the client tries to connect to the network. The Enforcer appliance can detect whether a client is running. If a client is running, the Enforcer begins the authentication process with the client. The client responds by running a Host Integrity check and by sending the results, along with its profile information, to the Enforcer.

The client also sends its Globally Unique Identifier (GUID), which the Enforcer passes on to the management server for authentication. The Enforcer appliance uses the profile information to verify that the client is up to date with the latest security policies. If not, the Enforcer appliance prompts the client to update its profile.

After the Enforcer appliance allows the client to connect, it continues to communicate with the client at regular predefined intervals. This communication enables the Enforcer appliance to continue to authenticate the client. For the LAN Enforcer appliance, the 802.1x switch handles this periodic authentication. For example, the 802.1x switch starts a new authentication session when re-authentication time comes.

The Enforcer appliance needs to run at all times; otherwise the clients that try to connect to the corporate network may be blocked.

See “Creating a test Host Integrity policy with a custom requirement script” on page 149.
You must establish communication between the Enforcer appliance and the Symantec Endpoint Protection Manager on the Enforcer console. You must have also completed the installation of the Enforcer appliance and the configuration of the internal and the external NICs on the Enforcer appliance.

See “About installing an Enforcer appliance” on page 172.

If you want to establish communication between an Enforcer appliance and the Symantec Endpoint Protection Manager on an Enforcer console, you need the following information:

- IP address of the Symantec Endpoint Protection Manager
  Check with the administrator of the server on which the Symantec Endpoint Protection Manager has been installed to obtain the IP address.

- Enforcer group name to which you want to assign the Enforcer appliance
  After you finish configuring the Enforcer group name for the Enforcer appliance, the group name automatically registers on the Symantec Endpoint Protection Manager.

- Port number on the Symantec Endpoint Protection Manager that is used to communicate with the Enforcer appliance.
  The default port number is 8014.

- The encrypted password that was created during the initial installation of the Symantec Endpoint Protection Manager.
To configure a connection between an Enforcer appliance and a Symantec Endpoint Protection Manager

1. At the command line on the console of an Enforcer appliance, type `configure`.
2. Type the following command:
   
   ```
   spm ip ipaddress group Enforcer group name http port number key encrypted password
   ```

   See “configure spm” on page 370.

   You can use the following example as a guideline:

   ```
   spm ip 192.168.0.64 group CorpAppliance http 8014 key symantec
   ```

   This example configures the Enforcer appliance to communicate with the Symantec Endpoint Protection Manager that has an IP address 192.168.0.64 in the CorpAppliance group. It uses HTTP protocol on port 8014 with an encrypted password or preshared secret of `symantec`.

3. Check the communication status of Enforcer appliance and the Symantec Endpoint Protection Manager.

   See “Checking the communication status of an Enforcer appliance on the Enforcer console” on page 371.

4. Configure, deploy, and install or download client software if you have not already done so.

   To allow guests (unmanaged client computers) to automatically download Symantec Network Access Control On-Demand Clients, configure a Gateway Enforcer to manage the automatic downloading process.

   See “Enabling Symantec Network Access Control On-Demand clients to temporarily connect to a network” on page 358.

**configure spm**

The `configure spm` command sets up the connection between the Enforcer and the Symantec Endpoint Protection Manager.

You must type all values if you change any of the values. Any values that you do not specify automatically use default values.

The `configure spm` command uses the following syntax:

```
configure spm {[ip <ipaddress>] | [group <group-name>] | [http <port-number>] | https
```
where:

- **ip** `<ipaddress>`: Enables you to add the IP address of the Symantec Endpoint Protection Manager.
- **del key** `<shared-key>`: Delete the shared secret key.
- **group** `<group-name>`: Enables you to specify a preferred group name for the Enforcer. Symantec recommends that you assign a unique group name to distinguish the Enforcers on the console of the Symantec Endpoint Protection Manager.
- **http** `<port-number>`: Enables you to specify the HTTP protocol and the port number to communicate with the Symantec Endpoint Protection Manager. The default protocol is HTTP. The default port number for the HTTP protocol is 8014.
- **https** `<port-number>`: Enables you to specify the HTTPS protocol and the port number to communicate with the Symantec Endpoint Protection Manager. You should only use this command if the Symantec Endpoint Protection Manager has been set up to use the HTTPS protocol. The default port number for the HTTPS protocol is 443.
- **key** `<key-name>`: Enables you to specify the encrypted password that is required if the Symantec Endpoint Protection Manager has been installed with one.

The following example describes configuring an Enforcer to communicate with the Symantec Endpoint Protection Manager at IP address 192.168.0.64 in an Enforcer group called CorpAppliance. It uses the HTTP protocol on port 8014 with an encrypted password of `security`.

```
configure spm ip 192.168.0.64 group CorpAppliance http 8014 key security
```

### Checking the communication status of an Enforcer appliance on the Enforcer console

You can check the communication status of an Enforcer appliance from the Enforcer console.
To check the communication status of an Enforcer appliance on the Enforcer console

1. Log on to the Enforcer console if you are not already logged on.
   See “Logging on to an Enforcer appliance” on page 175.

2. Type the following command: **show status**

   You can view information about the current connection status.

   The following example indicates that the Enforcer appliance is online and connected to a Symantec Endpoint Protection Manager with an IP address of 192.168.0.1 and communication port 8014:

   ```
   Enforcer#: show status
   Enforcer Status: ONLINE(ACTIVE)
   Policy Manager Connected: YES
   Policy Manager: 192.168.0.1 HTTP 8014
   Packets Received: 3659
   Packets Transmitted: 3615
   Packet Receive Failed: 0
   Packet Transfer Failed: 0
   Enforcer Health: EXCELLENT
   Enforcer Uptime: 10 days 01:10:55
   Policy ID: 24/03/2010 21:31:55
   ```

Remote access to an Enforcer appliance

To securely communicate with the Enforcer for command-line access, use one of the following methods:

- Networked KVM switch or similar device
- SSH client which supports SSH v2 Terminal Console server
- Serial cable

See “Setting up an Enforcer appliance” on page 174.

About the Enforcer appliance CLI command hierarchy

The Enforcer appliance (the Enforcer) uses a command-line interface (CLI) that is organized into the following groups:

- capture
- configure
Performing basic tasks on the console of all types of Enforcer appliances

**About the Enforcer appliance CLI command hierarchy**

- console
- debug
- mab
- monitor
- on-demand
- snmp

For a complete listing of the command-line interface command groups and commands, see the following guide:

*Symantec Network Access Control Enforcer Command-line Reference Guide*

---

**Note:** All material in this guide applies to the Enforcer appliance, not to the software Enforcers.
Managing Enforcers on the Symantec Endpoint Protection Manager

This chapter includes the following topics:

- About managing Enforcers on the management server console
- About managing Enforcers from the Servers page
- About Enforcer groups
- About the Enforcer information that appears on the Enforcer console
- Changing an Enforcer’s name and description
- Deleting an Enforcer or an Enforcer group
- Exporting and importing Enforcer group settings
- Messages for Windows computers that are not running the client (Gateway Enforcer only)
- About Enforcer reports and logs
- Configuring Enforcer log settings

About managing Enforcers on the management server console

The Symantec Enforcer settings on the management server console help you configure the Enforcer, its authentication interactions, and enforcement interactions.
with clients. Before you configure the Enforcer settings on the console, you complete the installation and setup of the Enforcer on the Enforcer appliance or computer.

The Enforcer settings on the Symantec Endpoint Protection Manager console depend on which type of Enforcer appliance you configure: Gateway or LAN. Therefore, the settings for each are covered separately.

You do most Enforcer configuration and administration from the console. Most Enforcer configuration settings can only be changed on the console. However, some Enforcer settings require you to edit an Enforcer file on the Enforcer computer rather than on the console. Almost all settings for Enforcers are set from the Servers page on the console. The LAN Enforcer has a few additional required settings on the Policies page.

See “Configuring an Enforcer appliance” on page 176.

If you administer multiple Enforcers and are responsible for other tasks, it is generally more convenient to administer them all in one centralized location. The console provides this capability. You can log on to a console to display information about all Enforcers.

You must perform a few tasks on the computer on which the Enforcer is installed. The tasks include using the Enforcer local console rather than the management console and hardware maintenance tasks. For example, you troubleshoot an Enforcer and a console connection on the Enforcer itself. To define the problem, you may need to physically check the status of the Enforcer computer hardware or change its network connection.

This chapter does not include information on how to configure the Symantec Enforcement client, which is a separate component from the Enforcer.

### About managing Enforcers from the Servers page

The **Servers** page on the management console lists installed Enforcers, along with connected servers and consoles, in the **View Servers** pane. Each Enforcer is listed under a group name. You edit Enforcer properties at the group level.

See “Changing an Enforcer’s name and description” on page 378.

You need full system administrator privileges to view the **Servers** page.

### About Enforcer groups

Enforcer configuration on the console is done at the Enforcer group level rather than at the individual Enforcer level. Enforcers are listed under a group name on the console Servers page.
Enforcer groups are a way to synchronize Enforcer settings. All Enforcers in a group share the same settings (properties). To update the Enforcer properties, you must select the group name in the **Servers** pane and edit the group properties.

See “Setting up an Enforcer group name on the Symantec Integrated Enforcer for Microsoft Network Access Protection console” on page 342.

**About failover Enforcer groups**

A new Enforcer identifies itself to the console as a standby failover Enforcer. This identification happens if you add a failover Gateway Enforcer that connects by a hub or switch to the same subnet. The console then assigns the new standby failover Enforcer to the same group as the active Enforcer. The assignment occurs whether or not you specified a group name during setup on the local console. This action ensures that the failover Gateway Enforcer has exactly the same settings as the primary Enforcer.

See “Failover planning for Gateway Enforcer appliances” on page 186.

For LAN Enforcers, failover is handled through the switch rather than through the Enforcer so the automatic assignment to the same group does not occur. You can ensure that multiple LAN Enforcers share settings. Specify the same group name in the Enforcer local console on the console **Settings** dialog box.

See “Planning for the installation of a LAN Enforcer appliance” on page 191.

**About changing a group name**

You cannot change an Enforcer group name from the console. However, you can specify a new group name from the Enforcer local console. The Enforcer then moves into the new group. You may need to refresh the console screen to see the change.

**About creating a new Enforcer group**

Usually, you only need to create a new Enforcer group if you add an Enforcer that required different settings from the existing Enforcers.

You can create a new Enforcer group on the Enforcer local console by specifying the new name on the console **Settings** dialog box. The new group has the Enforcer default settings.

You can leave the group name field blank when you connect the new Enforcer from the local console. In that case, the console assigns the Enforcer to a new group. This group takes the name of the Enforcer computer and its default settings.
You can use the same method to move an Enforcer to another group. Specify the desired group name from the Enforcer local console. The Enforcer takes on the settings of the group to which it is moved.

See “Adding or editing the name of a LAN Enforcer appliance group with a LAN Enforcer” on page 263.

See “Adding or editing the name of an Enforcer group for Symantec Network Access Control Integrated Enforcer” on page 322.

### About the Enforcer information that appears on the Enforcer console

You can display information about the Enforcer on the Enforcer console.

You can only change the settings for network interface cards on the Enforcer appliance but not on the management console. If you change the NIC configuration on the Enforcer appliance, the new settings are uploaded to the management console during the next heartbeat.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Same as Hostname field.</td>
</tr>
<tr>
<td>Description</td>
<td>Brief description of the Enforcer. The description is the only information that you can edit on the management console.</td>
</tr>
<tr>
<td>Version</td>
<td>Version of the Enforcer software that runs on the selected Enforcer computer.</td>
</tr>
<tr>
<td>Hostname</td>
<td>Name of the computer on which the Enforcer is installed.</td>
</tr>
<tr>
<td>Operating System</td>
<td>Operating system that is running on the computer on which the selected Enforcer is installed.</td>
</tr>
<tr>
<td>Online Status</td>
<td>Online: The service is running and is the primary active Enforcer. Offline: The service is stopped.</td>
</tr>
<tr>
<td>Failover Status</td>
<td>(Gateway Enforcer only) Whether the Enforcer is active or on standby.</td>
</tr>
<tr>
<td>Internal IP</td>
<td>IP address of the internal network interface card.</td>
</tr>
<tr>
<td>External IP</td>
<td>(Gateway Enforcer only) IP address of the external network interface card.</td>
</tr>
</tbody>
</table>
Table 26-1  Information about the Enforcer appliance on the management console (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal MAC</td>
<td>The MAC address of the internal network interface card.</td>
</tr>
<tr>
<td>External MAC</td>
<td>(Gateway Enforcer only) The MAC address of the external network interface card.</td>
</tr>
<tr>
<td>Internal NIC</td>
<td>Manufacturer and model of the internal network interface card.</td>
</tr>
<tr>
<td>External NIC</td>
<td>(Gateway Enforcer only) Manufacturer and model of the external network interface card.</td>
</tr>
</tbody>
</table>

Changing an Enforcer’s name and description

The Enforcer name is always the host name of the appliance or computer on which it is installed. You can only change the Enforcer name by changing the host name of the computer.

You can change the Enforcer description from the console. For example, you may want to enter a description to identify the Enforcer location.

To change an Enforcer’s description

1. In Symantec Endpoint Protection Manager, on the Admin page, click Servers.
2. Under Servers, click the Enforcer name and then under Tasks, click Edit Enforcer Properties. The Properties dialog box appears. The name field is not editable.
3. Enter the desired text in the Description text box.
4. Click OK.

You can also edit the Enforcer description by right-clicking the name of the Enforcer and selecting Properties.

Deleting an Enforcer or an Enforcer group

You can delete an Enforcer on the management console. When you delete an Enforcer, it frees up a license because the computer being used is no longer running an Enforcer. You cannot delete an Enforcer from the console while the Enforcer is online. You can turn off the Enforcer and then delete it. When you restart the Enforcer computer, the Enforcer reconnects to the console. The Enforcer registers itself again and reappears on the Servers page. To delete an Enforcer permanently from the console, first uninstall the Enforcer from the Enforcer computer.
To delete an Enforcer group after you uninstalled the Enforcer from the Enforcer computer

1. Turn off or uninstall the Enforcer on the Enforcer computer.
2. In Symantec Endpoint Protection Manager, on the Admin page, click Servers.
3. Under Servers, click the Enforcer name, and then under Tasks, click Delete Enforcer. A message box asks you to confirm the deletion.
4. To confirm the deletion, click Yes.

If there are no Enforcers listed in an Enforcer group and you no longer want to use that group, you can delete the Enforcer group. The group must no longer include any names of Enforcers before you can delete it. When you delete an Enforcer group, you delete any customized settings for the group.

To delete an Enforcer group

1. In Symantec Endpoint Protection Manager, click Admin.
   In the Admin page, click Servers.
2. Under Servers, click the Enforcer group name.
3. Click Delete Group.
   A message box asks you to confirm the deletion.
4. To confirm the deletion, click Yes.

Exporting and importing Enforcer group settings

You may want to export or import settings for an Enforcer group. Settings are exported to a file in .xml format. When you import settings, you must import them into an existing Enforcer group, which overwrites the selected group settings.

To export Enforcer group settings

1. In Symantec Endpoint Protection Manager, on the Admin page, click Servers.
2. Under Servers, click the Enforcer group name and then click Export Group Properties.
3. Select a location in which to save the file and specify a file name.
4. Click Save.

To import Enforcer group settings

1. In Symantec Endpoint Protection Manager, on the Admin page, click Servers.
2. Under Servers, click the Enforcer group name whose settings you want to overwrite and then click Import Group Properties.
3 Select the file that you want to import and then click **Open**.
   You are prompted to confirm overwriting the current Enforcer group properties.

4 Click **Yes**.

**Messages for Windows computers that are not running the client (Gateway Enforcer only)**

In some cases, clients try to connect to the enterprise network without running the client. The Gateway Enforcer provides a pop-up message to inform users on Windows computers of the need to install the client software. The message tells the clients that they are blocked from accessing the network because the Symantec client is not running. You can configure the contents of the message on the **Authentication** tab of the Enforcer **Settings** dialog box. Use the Enable pop-up message option on the client if client is not running.

---

**Note:** An alternative to the pop-up message is the HTTP Redirect option. The HTTP Redirect option connects the client to a Web site with remediation instructions or capabilities.

For the Enforcer to cause the client to display a message, UDP ports 137 and 138 must be open to transmit the message.

Windows Messaging, also called Messenger, must be running on Windows NT-based systems (Windows NT 4.0, 2000, XP, and Windows Server 2003) for the computer to display pop-up messages. If the client is running, Windows Messaging is not required for displaying a pop-up message from the client.

**About Enforcer reports and logs**

Enforcer reports and logs let you view Enforcer client activities and how the Enforcers flow through your system. For detailed information about the types reports and logs and how to view them, see Symantec Endpoint Protection Manager Help.

The **Reports** page on the Symantec Endpoint Protection Manager console provides both predefined reports and custom reports. You can view the predefined Quick Reports that contain information about Enforcers on the **Reports** page.

The following Enforcer reports are available:

- The System report that is called **Top Enforcers That Generate Errors** contains information about Enforcers that generated errors and warnings.
The System report that is called **Site Status** contains information about Enforcer system, traffic, and packet log throughput.

The Compliance reports contain information about the compliance status of clients.

Enforcer logs include the data that you can use to monitor and troubleshoot system activity:

The following types of Enforcer logs are available:

- **Enforcer Server log.** This log contains the information that is related to the functioning of an Enforcer.
- **Enforcer Client log.** This log contains information about interactions between an Enforcer and clients trying to connect to the network.
- **Enforcer Traffic log (Gateway Enforcer only).** This log records all traffic that enters through a Gateway Enforcer appliance’s external adapter and leaves through the internal adapter.
- **Enforcer Activity log.** This log contains information about events such as when Enforcers start and when they connect to the Symantec Endpoint Protection Manager.

By default, Enforcer logs are stored on the same computer on which the Enforcer software is installed or on the Enforcer appliance itself. You can have the logs automatically sent from the Enforcer appliance or the computer on which you installed an Integrated Enforcer to the Symantec Endpoint Protection Manager console. However, you must enable the sending of the logs on the Symantec Endpoint Protection Manager console.

The log data is sent from the Enforcer to Symantec Endpoint Protection Manager and stored in the database. You can modify the Enforcer log settings, view Enforcer logs, and generate reports about the Enforcers on the Symantec Endpoint Protection Manager console. Activities are recorded in the same Enforcer Server log for all Enforcers on a site.

For detailed information about the types of reports and logs and how to view them, see Symantec Endpoint Protection Manager Help.

See “Configuring Enforcer log settings” on page 381.

### Configuring Enforcer log settings

You can configure settings for Enforcer logs on the **Enforcer name Settings** dialog box on the **Logging** tab. The changes are sent to the selected Enforcer during the next heartbeat.
To configure Enforcer logs

1. In Symantec Endpoint Protection Manager, click **Admin**.
2. Click **Servers**.
3. Under **Servers**, select the Enforcer group for which you want to change log settings.
4. Under **Tasks**, click **Edit Group Properties**.
5. In the **Enforcer name Settings** dialog box, on the **Logging** tab, change any of the following:

   - **Disable logging on the Symantec Endpoint Protection Manager console**
     - Uncheck **Enable logging** for each log that you want to disable.
   - **Enable the sending of Enforcer logs from an Enforcer to Symantec Endpoint Protection Manager**
     - Check **Send the log to the management server**.
   - **Set up the size and age of logs**
     - In each of the **Maximum log file size** fields, specify that number of kilobytes of data to maintain in each log.
     - In the **Log entry will expire after** field, specify the number of days that the entry remains in the database before it is removed. The range is 1 to 365 days.
   - **Filter the Enforcer traffic log**
     - Select one of the following filter options:
       - **All traffic** to log all traffic including that which is allowed and that which is dropped.
       - **Only blocked traffic** to log only the clients that the Enforcer blocks.
       - **Only allowed traffic** to log only the traffic that the Enforcer allows.

6. Click **OK**.

See “About Enforcer reports and logs” on page 380.

Disabling Enforcer logging on Symantec Endpoint Protection Manager

By default, Enforcer logging is enabled. You can disable it on Symantec Endpoint Protection Manager. If you disable logging, you can enable it from this same location.
To disable Enforcer logging on Symantec Endpoint Protection Manager

1 In Symantec Endpoint Protection Manager, click Admin.
2 Click Servers.
3 Under Servers, select the Enforcer group for which you want to disable Enforcer logging.
4 Under Tasks, click Edit Group Properties.
5 In the Enforcer name Settings dialog box, on the Logging tab, uncheck Enable logging for each log that you want to disable.
6 Click OK.

See “About Enforcer reports and logs” on page 380.

Enabling the sending of Enforcer logs from an Enforcer to Symantec Endpoint Protection Manager

All logs are automatically sent by default from the Enforcer appliance or the computer on which you installed any of the software-based Integrated Enforcer to Symantec Endpoint Protection Manager. As soon as you enable the sending of logs, you can view all Symantec logs in a central location on Symantec Endpoint Protection Manager.

To enable the sending of Enforcer logs from an Enforcer to the Symantec Endpoint Protection Manager

1 In Symantec Endpoint Protection Manager, click Admin.
2 Click Servers.
3 Under Servers, select the Enforcer group for which you want to enable the sending of Enforcer logs from an Enforcer to Symantec Endpoint Protection Manager.
4 Under Tasks, click Edit Group Properties.
5 In the Enforcer name Settings dialog box, on the Logging tab, check Send the log to the management server.

You can enable the sending of each type of log from an Enforcer appliance or a computer on which you installed any of the software-based Integrated Enforcers to Symantec Endpoint Protection Manager.
6 Click OK.

See “About Enforcer reports and logs” on page 380.
Setting up the size and age of Enforcer logs

You can specify the maximum size of Enforcer log files and how many days log entries are stored.

To set up the size and age of Enforcer logs

1. In Symantec Endpoint Protection Manager, click Admin.
2. Click Servers.
3. Under Servers, select the Enforcer group for which you want to set the size and age of Enforcer logs.
5. In the Enforcer name Settings dialog box, on the Logging tab, in each of the Maximum log file size fields, specify the number of KB of data to maintain in each log.
   You can enter a size between 64 KB and 2 GB. The default setting is 512 KB.
6. In the Log entry will expire after field, specify the number of days that the entry remains in the database before it is removed.
   The range is 1 day to 365 days, with a default range of 30 days.
7. Click OK.

See “About Enforcer reports and logs” on page 380.

Filtering the Traffic logs for an Enforcer

If you have many clients that connect through an Enforcer, it may generate a large Traffic log. You can filter the type of data that an Enforcer logs in a Traffic log and thus reduce the average log size. The filter list enables you to filter the traffic that an Enforcer logs before the data is retained.

To filter the Traffic logs for an Enforcer

1. In Symantec Endpoint Protection Manager, click Admin.
2. Click Servers.
3. Under Servers, select the Enforcer group for which you want to filter Traffic logs.
In the Enforcer name **Settings** dialog box, on the **Logging** tab, in the Traffic log filter list, select one of the following filter options:

- **All traffic**: Logs all traffic, including that which is allowed and dropped
- **Only blocked traffic**: Logs only the clients that the Enforcer blocks
- **Only allowed traffic**: Logs only the traffic that the Enforcer allows

6 Click **OK**.

See “About Enforcer reports and logs” on page 380.

**Using the syslog server to monitor an Enforcer**

You can use the syslog facility to log Enforcer messages. You can specify the following aspects:

- IP address of the syslog server
- Level of syslog entry
- Authentication failure threshold
- Alive message interval

To enable logging messages to the syslog for an Enforcer

1 In Symantec Endpoint Protection Manager, click **Admin**.
2 Click **Servers**.
3 Under **Servers**, select the Enforcer group for which you want to enable logging to the syslog.
4 Under **Tasks**, click **Edit Group Properties**.
5 On the **Logging** tab, in the **Syslog** section, select among the following options:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syslog server</td>
<td>Specify the IP address of the syslog server.</td>
</tr>
<tr>
<td>Level</td>
<td>The default level of syslog entry is Information. The levels include: Notice and Information. All logs more serious than the level specified are uploaded to the log server.</td>
</tr>
<tr>
<td>Authentication failure threshold</td>
<td>This parameter is defined in terms of the number of times multiples by the number of seconds. When authentication fails more frequently than specified, the following messages are logged.</td>
</tr>
<tr>
<td>Alive message interval</td>
<td>The Enforcer sends an &quot;alive&quot; message to the syslog server at a specified interval, in seconds. The default value is 1800 seconds.</td>
</tr>
</tbody>
</table>

6 Click **OK**.
Troubleshooting the Enforcer appliance

This chapter includes the following topics:

- Troubleshooting communication problems between an Enforcer appliance and the Symantec Endpoint Protection Manager
- Troubleshooting an Enforcer appliance
- Frequently asked questions for the Enforcer appliances
- Troubleshooting the connection between the Enforcer and the On-Demand Clients

Troubleshooting communication problems between an Enforcer appliance and the Symantec Endpoint Protection Manager

If the Enforcers and the management server do not communicate, look at the following possible reasons and solutions.
Table 27-1 Troubleshooting communication problems between Enforcers and the management server

<table>
<thead>
<tr>
<th>Issue</th>
<th>Solution</th>
</tr>
</thead>
</table>
| Enforcer cannot register with the Symantec Endpoint Protection Manager | ■ Check the management server configuration on Enforcer using the command `configure show spm`. Make sure that you have configured the management server IP address, port number, and pre-shared secret correctly. The default port number is 8014.  
■ If the Enforcer type was re-configured or changed, delete the Enforcer group on the management server or move the Enforcer to a different group. For example, the Enforcer type might have changed from a Gateway Enforcer to a LAN Enforcer.  
■ The management server list for the Enforcer might have a management server that the Enforcer cannot reach or has multiple interfaces of a management server. You might need to add a management server list with only one management server that can connect to the Enforcer. The management server must have one IP address. |
| Delay in connecting to the network through an Enforcer or the Gateway Enforcer appliance blocks clients | If you use a fail-open Enforcer, check the switch configuration. Make sure that PortFast is enabled on both ports to which the Enforcer connects.                                                                                                                                 |
| Client disconnected events in the LAN Enforcer appliance's Client Log | If the clients frequently suspend and do not respond to re-authentication requests (802.1x EAP) from the switch, you may need to decrease the switch-re-authentication timeout.                                                                                               |
| LAN Enforcer appliance does not switch clients to the correct VLAN    | ■ Check that the selected switch model in the configuration matches the switch in use.  
■ Check that the VLAN names exactly match what has been configured on the switch.  
■ Check that the action table’s VLAN assignments are correct for the switch in the management server console.                                                                                                                                                     |

See “Troubleshooting an Enforcer appliance” on page 388.

**Troubleshooting an Enforcer appliance**

Table 27-2 displays the possible problems and solutions you might have with an Enforcer appliance.
Table 27-2  Troubleshooting problems and solutions for an Enforcer appliance

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enforcer root password is shown as invalid when set using the command-line interface</td>
<td>Limit passwords to 128-characters. Use another password of shorter length. See “About the Enforcer appliance CLI command hierarchy” on page 372.</td>
</tr>
<tr>
<td>Changing memory on the R200 causes hardware errors</td>
<td>The errors are due to hard coding of the IRQs. Remove the additional memory or reinstall the Enforcer after the hardware change. Our tests have shown that additional memory does not make an appreciable difference. See “Installing an Enforcer appliance” on page 173.</td>
</tr>
<tr>
<td>Some settings (Debug Level, Capture) return to default when the Enforcer is upgraded</td>
<td>A return to defaults can appear on upgrade, but does not appear thereafter. See “Upgrading the Enforcer appliance image” on page 200.</td>
</tr>
</tbody>
</table>
| Problems appear when you are running SNMP with the Enforcer and HP OpenView | Resolve this problem by configuring HP OpenView:  
  ■ Load the Symantec MIB file by selecting Option > Load/unload MIB  
  ■ Using Option > Event Configuration, choose OnDemandTraps (.1.3.6.1.4.1.393.588), and modify each trap as required. For example on Event Message, choose Log and display in category. Then select a category from the drop-down list. Set the Event Log Message as $1. |

See “Troubleshooting communication problems between an Enforcer appliance and the Symantec Endpoint Protection Manager” on page 387.

Frequently asked questions for the Enforcer appliances

The following issues provide answers about enforcement issues on the Gateway Enforcer appliance, or LAN Enforcer appliance:

■ See “What happens if Enforcer appliances cannot communicate with Symantec Endpoint Protection Manager?” on page 390.

■ See “Is a RADIUS server required when a LAN Enforcer appliance runs in transparent mode?” on page 391.
Which virus protection and antivirus software is managed by Host Integrity?

Host Integrity enables you to add custom requirements to detect and manage virus protection software. In a custom requirement, you can specify virus protection applications and signature file information to check as part of your IF-THEN condition statement. The products that are supported appear in a drop-down list in the custom requirement dialog box.

See “Setting up Host Integrity” on page 133.

What happens if Enforcer appliances cannot communicate with Symantec Endpoint Protection Manager?

If you plan to use Enforcers with Symantec Endpoint Protection, we recommend that you have redundant management servers. If the Symantec Endpoint Protection Manager is unavailable, the Enforcer blocks the traffic from the clients.

Redundant management servers are preferable. The Enforcer sends a UDP packet on port 1812 by using the RADIUS protocol to the Symantec Endpoint Protection Manager to verify the GUID from the clients. If a firewall blocks this port or if a Symantec Endpoint Protection Manager is unavailable, then the clients are blocked.

An option on the Enforcer allows client access to the network when the Symantec Endpoint Protection Manager is unavailable. If this option is enabled and the Symantec Endpoint Protection Manager is unavailable, the GUID check and the profile checks are not performed. Only the Host Integrity check can be performed on the client when the Symantec Endpoint Protection Manager is unavailable.

You can use the advanced local-auth command to enable or disable the Enforcer’s authentication of a client.

See “advanced local-auth” on page 390.

advanced local-auth

The advanced local-auth command enables or disables the Enforcer’s authentication of the client. Use this command for troubleshooting (Gateway Enforcer).

Client authentication is disabled by default.

The advanced local-auth command uses the following syntax:
advanced local-auth {disable | enable}

where:

disable  
Verifies the Agent with the management server. This blocks the Agent if it is unable to connect to a management server.  
The default setting for client authentication is Disable.

enable   
Disables Agent verification and performs Host Integrity validation only.

By default, the Gateway Enforcer verifies the globally unique identifier (GUID) of the client with the Symantec Endpoint Protection Manager. If the Gateway Enforcer is unable to connect with a Symantec Endpoint Protection Manager to verify the GUID, it blocks the client. Although it is not recommended as a troubleshooting step, you can stop the Gateway Enforcer from verifying the GUID.

By default, the Gateway Enforcer verifies the GUID. Instead, the Gateway Enforcer only performs a Host Integrity validation check. Be sure to re-enable this setting if you want the Gateway Enforcer to verify the GUID.

Is a RADIUS server required when a LAN Enforcer appliance runs in transparent mode?

RADIUS server requirements depend on how the switch is configured and what you use the switch to authenticate.

The following are some items to watch out for:

- Switches that use RADIUS servers for more than the authentication of 802.1x users.
  For example, when you log on to the switch, you must type a user name and password. The RADIUS server typically performs authentication for this logon. When the LAN Enforcer appliance is installed, this authentication is sent to the LAN Enforcer appliance. If the authentication is sent to the LAN Enforcer appliance, you must configure the RADIUS server IP address in the LAN Enforcer appliance. You must configure the LAN Enforcer appliance to forward all non-EAP requests directly to the RADIUS server.

- Installation of a 802.1x supplicant on a client system. If an 802.1x supplicant exists on a client system, the LAN Enforcer appliance tries to authenticate with the RADIUS server. 802.1x authentication is enabled by default on Windows XP. If you enable your client to work in transparent mode, it does not automatically disable the built-in 802.1x supplicant. You must make sure that no 802.1x supplicant runs on any of your client computers.
Configuration of the Enforcer to ignore the RADIUS request from any client computer that includes a third-party 802.1x supplicant. You can set up this configuration by using an IP address of 0.0.0.0 for the RADIUS server. You can use this setup if you want to run a LAN Enforcer in transparent mode. Some clients can have an 802.1x supplicant. In this case, you can specify that the LAN Enforcer appliance does not send any traffic to a RADIUS server.

See “Using RADIUS server group settings” on page 266.

How does Host Integrity enforcement manage computers without Symantec clients installed?

Host Integrity can enforce security policies only for the systems that have Symantec clients installed. The security stance of other vendors cannot be enforced. Any enforcement by other vendors can disrupt the network.

The following enforcement methods are available:

Self enforcement

Self enforcement by the Symantec client firewall has no effect on the systems without Symantec clients in the network.

See “How Host Integrity works” on page 131.

Gateway enforcement

In the networks that use gateway enforcement, the systems without clients cannot pass through the gateway. Where you place the Gateway Enforcer in the network is critical; it can block access to critical network resources to which other systems require access.

You can make exceptions for trusted IP addresses so that they can pass through the gateway inbound or outbound without a client. Similarly, the gateway can also exempt non-Microsoft operating systems from enforcement. One network design can be to place non-critical servers on the same side of the gateway. This configuration simplifies the network design without seriously compromising security.

See “How the Gateway Enforcer appliance works” on page 221.
DHCP enforcement restricts the computers that are out of compliance or the systems without clients. It restricts these systems to a separate address space or provides them with a subset of routes on the network. This restriction reduces the network services for these devices. Similar to gateway enforcement, you can make exceptions for trusted MAC addresses and non-Microsoft operating systems.

See “How an Integrated Enforcer for Microsoft DHCP Servers works” on page 320.

LAN enforcement uses the 802.1x protocol to authenticate between the switch and the client systems that connect to the network. To use this method of enforcement, the switch software must support the 802.1x protocol and its configuration must be correct. 802.1x supplicant software is also required if the administrator wants to verify user identity as well has host NAC status. The switch configuration must handle the exceptions for systems without clients, rather than any Symantec configuration.

You have several ways to set up this switch configuration. Methods vary depending on the type of switch and software version it runs. A typical method implements the concept of a guest VLAN. Systems without clients are assigned to a network that has a lower level of network connectivity. Another method involves basing the exceptions on MAC addresses.

You can disable 802.1x on selected ports. However, to disable by selected ports allows anyone to connect by using the port, so it is not recommended. Many vendors have special provisions for the VoIP phones that can automatically move these devices to special voice VLANs.

See “How the LAN Enforcer appliance works” on page 256.

When you use the Universal Enforcement API, the third-party vendor’s implementation of the API handles the exceptions.

See “About the types of enforcement in Symantec Network Access Control” on page 29.
About debug information transfer over the network

When problems occur on the Enforcer appliance, a debug log is created on the Enforcer (kernel.log). If you need to transfer debug information over the network, use one of the following debug commands to transfer the debug logs:

```
debug upload                      To transfer one file to a tftp server
```

File transfer over the network requires a serial connection between a computer and the Enforcer appliance.

The following example represents a file-transfer output that the HyperTerminal performs:

```
<date>  <Time>  <File Name>
2008-08-01 16:32:26  user.log
2008-08-01 16:32:24  kernel.log
2008-08-01 14:30:03  ServerSylink[04-05-2010-14-30-03].xml
2008-08-01 14:29:59  ServerProfile[04-05-2010-14-29-59].xml
Enforcer(debug)# upload tftp 10.1.1.1 filename kernel.log
```

See “About the Enforcer appliance CLI command hierarchy” on page 372.

Troubleshooting the connection between the Enforcer and the On-Demand Clients

There are several areas and known issues that you may check to troubleshoot your connection between the Enforcer and On-Demand clients.

<table>
<thead>
<tr>
<th>Table 27-3 Connection troubleshooting</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Solution</th>
</tr>
</thead>
</table>
| Firewall is blocking the client from working when the user downloads the agent through PPTP VPN, CheckPoint VPN, or Juniper VPN. | Several possible solutions:  
- Change firewall settings to unblock UDP port 39999.  
- Add a static route to the Enforcer's route table. For example:  
  ```
  route add IP netmask NM device eth0
  ```  
  where IP and NM are the IP address and netmask of the client's IP address pool. This pool is configured on the VPN by the administrator. |
| Download times are sometimes long. | The client sometimes sends traffic to VeriSign, making the download speed somewhat long. A workaround is let the admin add the VeriSign to the trusted IP list. |
### Connection troubleshooting (continued)

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Integrity check is sometimes long the first time.</td>
<td>A long Host Integrity check is an issue with DNS resolution, and should not appear after the first Host Integrity check.</td>
</tr>
<tr>
<td>Firewall on the client is blocking the On-Demand client from working when the user does not have Admin rights</td>
<td>Users should change firewall settings to unblock UDP port 39999. Alternatively, set the firewall with the following: <code>cclientctl.exe</code></td>
</tr>
<tr>
<td>Upgrading the Enforcer does not initially contain the manual installation package.</td>
<td>This problem is due to the size of the packages taken together. The workaround is to upgrade the Enforcer and import the Client Manual Install Package on Symantec Endpoint Protection Manager first, and then enable On-Demand functionality on the Enforcer. That adds the manual installation files.</td>
</tr>
<tr>
<td>The redirect URL on the Enforcer will overwrite a previous redirect URL on Symantec Endpoint Protection Manager.</td>
<td>The redirect URL overwrite problem only happens when the On-Demand feature is enabled on the Enforcer. This is expected behavior.</td>
</tr>
<tr>
<td>Vista clients sometimes do not receive an IP address from the DHCP server.</td>
<td>This problem is a timing issue. Change the DHCP timeout setting to 12 seconds or more.</td>
</tr>
<tr>
<td>A normal user cannot install the agent if JRE is not installed.</td>
<td>The workaround is to ensure that JRE is installed. Otherwise only Admin users can install JRE.</td>
</tr>
<tr>
<td>Wireless service is disconnected when the On-Demand client is installed and quits and 802.1x authentication is used.</td>
<td>The user should restart the wireless connection.</td>
</tr>
<tr>
<td>Systems that are running Norton 360 v. 2.x have a problem receiving the client.</td>
<td>To solve this problem, follow the manual download link to download and install and install the client.</td>
</tr>
<tr>
<td>With Firefox, you cannot download the client and NP Plugin with only user rights.</td>
<td>Installation of the NP plugin requires Admin rights.</td>
</tr>
<tr>
<td>Manual installation sometimes fails.</td>
<td>To solve this problem, you may need to install Microsoft patch KB893803. This patch is included with the manual install, and should be installed before the client installation. Admin privileges are required.</td>
</tr>
</tbody>
</table>
Table 27-3  Connection troubleshooting (continued)

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1x authentication fails</td>
<td>The agent needs to install a driver to work. If the user needs 802.1x authentication on Windows Vista, the user needs to open the browser with the &quot;Run as Administrator&quot; method or turn off UAC to make sure that the agent works with Administrator privileges.</td>
</tr>
<tr>
<td>&quot;Old version of ActiveX detected&quot; message appears</td>
<td>You should delete the existing ActiveX by clicking <strong>Tools -&gt; Manage Add-ons -&gt; Enable or Disable Add-ons -&gt; Downloaded ActiveX Controls</strong>, and deleting HodaAgt class.</td>
</tr>
<tr>
<td>Browser notifies the user that it cannot display the webpage, and the client cannot download successfully.</td>
<td>The client may already be running. As a security feature, you cannot download a new client inside of a running client session.</td>
</tr>
<tr>
<td>Firefox browser sometimes cannot download the client.</td>
<td>This problem happens when Firefox runs first. The first few Firefox restarts are required for it to finish its configuration. After that the On-Demand client should download.</td>
</tr>
<tr>
<td>Computers running Mac OS 10.4 sometimes do not authenticate properly due to a changing hostname.</td>
<td>This appears to be a problem with this version of the Mac OS. Version 10.5 and later does not have the problem. The workaround for version 10.4 is to set the hostname in /etc/hostconfig/.</td>
</tr>
<tr>
<td>Custom Host Integrity checks that rely upon the system variable %temp% do not work.</td>
<td>This is because of the transitory nature of %temp%. The workaround is to point to different locations.</td>
</tr>
<tr>
<td>Custom Host Integrity rules that point to Windows registry values do not work properly.</td>
<td>This is because of the transient nature of user sessions.</td>
</tr>
<tr>
<td>Installation of Panda Titanium 2007 or Panda Internet Security 2007 or 2008 software causes a message to appear, &quot;Please wait while Windows configures Symantec Network Access Control.&quot;</td>
<td>Panda deletes a crucial Symantec Network Access Control file. It is automatically reinstalled, and you may safely take no action.</td>
</tr>
<tr>
<td>Mac client transparent mode dot1x authentication sometimes fails</td>
<td>The Mac On-Demand Client is not compatible with PEAP authentication. If your Mac is configured for PEAP authentication, you must disable it in your network connection properties on the Mac. Transparent mode dot1x authentication then works fine.</td>
</tr>
</tbody>
</table>
### Table 27-3  Connection troubleshooting (continued)

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>On Windows Vista, the On-Demand Client fails to authenticate properly when using PEAP and a custom VSA</td>
<td>This problem is specific to using a custom VSA and PEAP authentication on Windows Vista. The workaround is to use a different form of authentication.</td>
</tr>
</tbody>
</table>