Enforcer Implementation Guide for Symantec™ Network Access Control
Symantec Network Access Control Enforcer Implementation Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version 11.00.05.00.00

Legal Notice

Copyright © 2009 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, Bloodhound, Confidence Online, Digital Immune System, LiveUpdate, Norton, Sygate, and TruScan are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party ("Third Party Programs"). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Please see the Third Party Legal Notice Appendix to this Documentation or TPIP ReadMe File accompanying this Symantec product for more information on the Third Party Programs.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.
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 maintenance 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 Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers automatic software upgrade protection
- Global support that is available 24 hours a day, 7 days a week
- Advanced features, including Account Management Services

For information about Symantec's Maintenance Programs, you can visit our Web site at the following URL:

www.symantec.com/techsupp/

Contacting Technical Support

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

www.symantec.com/techsupp/

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/techsupp/

Customer service
Customer service information is available at the following URL:
www.symantec.com/techsupp/
Customer Service is available to assist with the following types of issues:
  - Questions regarding product licensing or serialization
  - Product registration updates, such as address or name changes
  - General product information (features, language availability, local dealers)
  - Latest information about product updates and upgrades
  - Information about upgrade assurance and maintenance contracts
  - Information about the Symantec Buying Programs
  - Advice about Symantec's technical support options
  - Nontechnical presales questions
  - Issues that are related to CD-ROMs or manuals
Maintenance agreement resources

If you want to contact Symantec regarding an existing maintenance agreement, please contact the maintenance agreement administration team for your region as follows:

<table>
<thead>
<tr>
<th>Region</th>
<th>Contact Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asia-Pacific and Japan</td>
<td><a href="mailto:customercare_apac@symantec.com">customercare_apac@symantec.com</a></td>
</tr>
<tr>
<td>Europe, Middle-East, and Africa</td>
<td><a href="mailto:semea@symantec.com">semea@symantec.com</a></td>
</tr>
<tr>
<td>North America and Latin America</td>
<td><a href="mailto:supportsolutions@symantec.com">supportsolutions@symantec.com</a></td>
</tr>
</tbody>
</table>

Additional enterprise services

Symantec offers a comprehensive set of services that allow you to maximize your investment in Symantec products and to develop your knowledge, expertise, and global insight, which enable you to manage your business risks proactively.

Enterprise services that are available include the following:

- **Symantec Early Warning Solutions**
  These solutions provide early warning of cyber attacks, comprehensive threat analysis, and countermeasures to prevent attacks before they occur.

- **Managed Security Services**
  These services remove the burden of managing and monitoring security devices and events, ensuring rapid response to real threats.

- **Consulting Services**
  Symantec Consulting Services provide on-site technical expertise from Symantec and its trusted partners. Symantec Consulting Services offer a variety of prepackaged and customizable options that include assessment, design, implementation, monitoring, and management capabilities. Each is focused on establishing and maintaining the integrity and availability of your IT resources.

- **Educational Services**
  Educational Services provide a full array of technical training, security education, security certification, and awareness communication programs.

To access more information about Enterprise services, please visit our Web site at the following URL:

[www.symantec.com](http://www.symantec.com)

Select your country or language from the site index.
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About two Gateway Enforcer appliances in a series</td>
<td>45</td>
</tr>
<tr>
<td>Protection of VPN access through a Gateway Enforcer appliance</td>
<td>46</td>
</tr>
<tr>
<td>Protection of wireless access points through a Gateway Enforcer appliance</td>
<td>46</td>
</tr>
<tr>
<td>Protection of servers through a Gateway Enforcer appliance</td>
<td>46</td>
</tr>
<tr>
<td>Protection of non-Windows servers and clients through a Gateway Enforcer appliance</td>
<td>47</td>
</tr>
<tr>
<td>Requirements for allowing non-Windows clients without authentication</td>
<td>48</td>
</tr>
<tr>
<td>Failover planning for Gateway Enforcer appliances</td>
<td>49</td>
</tr>
<tr>
<td>How failover works with Gateway Enforcer appliances in the network</td>
<td>49</td>
</tr>
<tr>
<td>Where to place Gateway Enforcer appliances for failover in a network</td>
<td>50</td>
</tr>
<tr>
<td>Setting up Gateway Enforcer appliances for failover</td>
<td>50</td>
</tr>
<tr>
<td>Installation planning for a DHCP Enforcer appliance</td>
<td>52</td>
</tr>
<tr>
<td>Where to place DHCP Enforcer appliances in a network</td>
<td>52</td>
</tr>
<tr>
<td>DHCP Enforcer appliance IP addresses</td>
<td>54</td>
</tr>
<tr>
<td>Protection of non-Windows clients with DHCP enforcement</td>
<td>55</td>
</tr>
<tr>
<td>About the DHCP server</td>
<td>56</td>
</tr>
<tr>
<td>Failover planning for DHCP Enforcer appliances</td>
<td>57</td>
</tr>
<tr>
<td>How failover works with DHCP Enforcer appliances in the network</td>
<td>57</td>
</tr>
<tr>
<td>Where to place DHCP Enforcer appliances for failover in a network</td>
<td>58</td>
</tr>
<tr>
<td>Setting up DHCP Enforcer appliances for failover</td>
<td>59</td>
</tr>
<tr>
<td>Installation planning for a LAN Enforcer appliance</td>
<td>61</td>
</tr>
<tr>
<td>Where to place LAN Enforcer appliances</td>
<td>61</td>
</tr>
<tr>
<td>Failover planning for LAN Enforcer appliances</td>
<td>64</td>
</tr>
<tr>
<td>Where to place LAN Enforcer appliances for failover in a network</td>
<td>64</td>
</tr>
</tbody>
</table>

**Chapter 3**

Upgrading and migrating Enforcer appliance images

- About upgrading and migrating Enforcer appliance images to version 11.0.3000
- Determining the current version of an Enforcer appliance image
Chapter 7 Configuring the Symantec DHCP Enforcer appliance on the Symantec Endpoint Protection Manager Console

About configuring the Symantec DHCP Enforcer appliance on the Symantec Endpoint Protection Manager Console .............................................................. 121

Changing DHCP Enforcer appliance configuration settings on a management server .............................................................. 122

Using general settings ........................................................................ 124

Adding or editing the name of an Enforcer group with a DHCP Enforcer ....................................................................... 124

Adding or editing the description of an Enforcer group with a DHCP Enforcer ....................................................................... 124

Adding or editing the IP address or host name of a DHCP Enforcer ....................................................................... 125

Adding or editing the description of a DHCP Enforcer ................. 125

Connecting the DHCP Enforcer to a Symantec Endpoint Protection Manager ........................................................ 125

Using authentication settings ........................................................................ 127

About using authentication settings ......................................... 127

About Authentication sessions ................................................ 129

Specifying the maximum number of challenge packets during an authentication session ................................................ 130

Specifying the frequency of challenge packets to be sent to clients ........................................................................ 131

Allowing all clients with continued logging of non-authenticated clients ........................................................................ 132

Allowing non-Windows clients to connect to a network without authentication .............................................................. 133

Having the DHCP Enforcer check the Policy Serial Number on a client .............................................................. 134

Sending a message from a DHCP Enforcer appliance to a client about non-compliance ................................................ 135

Using DHCP servers settings ........................................................ 136

About using DHCP servers settings .......................................... 136
Combining a normal and a quarantine DHCP server on one computer ................................................................. 137
Enabling separate normal and quarantine DHCP servers ................. 137
Adding a normal DHCP server ............................................. 138
Adding a quarantine DHCP server .......................................... 139
Using advanced DHCP Enforcer appliance settings ...................... 140
Setting up an automatic quarantine for a client that fails authentication ....................................................... 141
Specifying a DHCP Enforcer appliance's wait period before it grants a client access to the network ...................... 141
Enabling servers, clients, and devices to connect to the network as trusted hosts without authentication ............. 142
Preventing DNS spoofing .................................................... 143
Allowing a legacy client to connect to the network with a DHCP Enforcer appliance ........................................... 144
Enabling local authentication on the DHCP Enforcer appliance ................................................................. 144

Chapter 8 Configuring the Symantec LAN Enforcer appliance on the Symantec Endpoint Protection Manager Console ................................................................. 147

About configuring the Symantec LAN Enforcer on the Symantec Endpoint Protection Manager appliance console ............................... 148
About configuring RADIUS servers on a LAN Enforcer appliance ........................................................................ 148
About configuring 802.1x wireless access points on a LAN Enforcer appliance ...................................................... 149
Changing LAN Enforcer configuration settings on a Symantec Endpoint Protection Manager Console ................................. 150
Using general settings ........................................................................ 152
Adding or editing the name of a LAN Enforcer appliance group with a LAN Enforcer ...................................................... 153
Specifying a listening port that is used for communication between a VLAN switch and a LAN Enforcer ......................... 153
Adding or editing the description of an Enforcer group with a LAN Enforcer ................................................................. 154
Adding or editing the IP address or host name of a LAN Enforcer ........................................................................... 154
Connecting the LAN Enforcer to a Symantec Endpoint Protection Manager ........................................................................ 155
Using RADIUS server group settings .............................................. 156
Chapter 9 Setting up temporary connections for Symantec Network Access Control On-Demand clients

About setting up temporary connections for Symantec Network Access Control On-Demand Clients .............................................................. 193
Before you configure Symantec Network Access Control On-Demand clients on the console of a Gateway or DHCP Enforcer ................................................................................. 194
Enabling Symantec Network Access Control On-Demand clients to temporarily connect to a network ................................................. 197
Setting up authentication on the Gateway or DHCP Enforcer console for Symantec Network Access Control On-Demand clients ............ 199
Setting up authentication with a local on-board database ................ 199
Setting up authentication with a Microsoft Windows 2003 Server Active Directory .............................................................................. 200
Setting up the On-Demand Client on Windows for authentication with the dot1x protocol ................................................................. 201
Chapter 10 Enforcer appliance command-line interface .......................... 207

About the Enforcer appliance CLI command hierarchy ...................... 207
CLI command hierarchy ..................................................................... 208
Moving up and down the command hierarchy .................................. 211
Enforcer appliance CLI keystroke shortcuts ..................................... 211
Getting help with CLI commands .................................................... 213

Chapter 11 Enforcer appliance command-line interface reference .............. 215

Command conventions ..................................................................... 215
Enforcer appliance CLI in alphabetical reference .............................. 216
Top-level commands ..................................................................... 233
  Clear .................................................................................. 233
  Date .................................................................................. 233
  Exit ................................................................................... 233
  Help ................................................................................... 234
  Hostname ........................................................................... 235
  Password ............................................................................ 235
  Ping ................................................................................... 235
  Reboot ............................................................................... 236
  Shutdown ............................................................................ 236
  Show .................................................................................. 236
  Start .................................................................................. 238
  Stop ................................................................................... 238
  Traceroute .......................................................................... 238
  Update ................................................................................ 238
Capture commands ......................................................................... 239
  Capture Compress ................................................................ 239
  Capture Filter ....................................................................... 239
  Capture Show ........................................................................ 240
  Capture Start ........................................................................ 241
  Capture Upload ..................................................................... 242
  Capture Verbose ................................................................... 242
Configure commands ....................................................................... 243
  Configure advanced commands .............................................. 243
  Configure DNS ....................................................................... 249
On-Demand mac-compliance commands .............................................. 289

Chapter 12 Troubleshooting an Enforcer appliance ............................ 293

About troubleshooting an Enforcer appliance ...................................... 293
General troubleshooting topics and known issues ............................... 294
About debug information transfer over the network ............................. 294

Chapter 13 Frequently asked questions about the Gateway, DHCP, or LAN Enforcer appliances ............................................. 297

Enforcement questions ....................................................................... 297
Which antivirus software provides support for host integrity? .............. 297
Can Host Integrity policies be set at the group level or the global level? ................................................................. 299
Can you create a custom host integrity message? .............................. 299
What happens if Enforcer appliances cannot communicate with Symantec Endpoint Protection Managers? ..................... 299
Is a RADIUS server required when a LAN Enforcer appliance runs in transparent mode? ........................................ 300
How does enforcement manage computers without clients? ............. 300

Section 2 Installing the Symantec NAC Integrated Enforcer for Microsoft DHCP Servers ........................................................................ 303

Chapter 14 Introducing the Symantec NAC Integrated Enforcer for Microsoft DHCP Servers ....................................................... 305

About the Symantec NAC Integrated Enforcer for Microsoft DHCP Servers ............................................................................. 305
How an Integrated Enforcer for Microsoft DHCP Servers works ........ 306
How to get started with the installation of an Integrated Enforcer for Microsoft DHCP Servers ....................................................... 307
Where to find more information about related documentation for an Integrated Enforcer for Microsoft DHCP Servers .................... 308
<table>
<thead>
<tr>
<th>Chapter 15</th>
<th>Planning for the installation of the Symantec NAC Integrated Enforcer for Microsoft DHCP Servers</th>
<th>311</th>
</tr>
</thead>
<tbody>
<tr>
<td>About planning for the installation of an Integrated Enforcer for Microsoft DHCP Servers</td>
<td>311</td>
<td></td>
</tr>
<tr>
<td>Required components for an Integrated Enforcer for Microsoft DHCP Servers</td>
<td>312</td>
<td></td>
</tr>
<tr>
<td>Hardware requirements for an Integrated Enforcer for Microsoft DHCP Servers</td>
<td>312</td>
<td></td>
</tr>
<tr>
<td>Operating system requirements for an Integrated Enforcer for Microsoft DHCP Servers</td>
<td>313</td>
<td></td>
</tr>
<tr>
<td>Planning for the placement of an Integrated Enforcer for Microsoft DHCP Servers</td>
<td>313</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 16</th>
<th>Installing the Symantec NAC Integrated Enforcer for Microsoft DHCP Servers</th>
<th>315</th>
</tr>
</thead>
<tbody>
<tr>
<td>Before you install the Integrated Enforcer for Microsoft DHCP Servers</td>
<td>315</td>
<td></td>
</tr>
<tr>
<td>Installing an Integrated Enforcer for Microsoft DHCP Servers</td>
<td>316</td>
<td></td>
</tr>
<tr>
<td>Upgrading the integrated Enforcer for Microsoft DHCP Servers</td>
<td>319</td>
<td></td>
</tr>
</tbody>
</table>

| Section 3 | Installing the Symantec NAC Integrated Enforcer for Alcatel-Lucent VitalQIP DHCP Servers (Integrated Lucent Enforcer) | 321 |

<table>
<thead>
<tr>
<th>Chapter 17</th>
<th>Introducing the Symantec NAC Integrated Lucent Enforcer</th>
<th>323</th>
</tr>
</thead>
<tbody>
<tr>
<td>About the Integrated Enforcer for Alcatel-Lucent VitalQIP DHCP Servers (Integrated Lucent Enforcer)</td>
<td>323</td>
<td></td>
</tr>
<tr>
<td>What you can do with the Integrated Lucent Enforcer</td>
<td>324</td>
<td></td>
</tr>
<tr>
<td>How the Integrated Lucent Enforcer works</td>
<td>324</td>
<td></td>
</tr>
<tr>
<td>Where to find more information about related documentation for an Integrated Lucent Enforcer</td>
<td>326</td>
<td></td>
</tr>
</tbody>
</table>
Chapter 18  Planning for the installation of the Symantec NAC Integrated Lucent Enforcer ........................................ 329

About planning for the installation of an Integrated Lucent Enforcer ................................................................. 329
Required components for an Integrated Lucent Enforcer .............................................................. 330
Planning for the placement of an Integrated Lucent Enforcer .......................................................... 331
Hardware requirements for an Integrated Lucent Enforcer .......................................................... 333
Operating system requirements for an Integrated Lucent Enforcer ......................................................... 333

Chapter 19  Installing the Symantec NAC Integrated Lucent Enforcer ........................................................... 335

Before you install the Integrated Lucent Enforcer ............................................................. 335
Installing an Integrated Lucent Enforcer .............................................................................. 336
Uninstalling an Integrated Lucent Enforcer ...................................................................... 338
Stopping and starting the Lucent VitalQIP Enterprise DHCP Server .......................................... 339

Section 4  Configuring Symantec NAC Integrated Enforcers on the Enforcer console ............. 341

Chapter 20  Configuring the Symantec NAC Integrated Enforcers on the Enforcer console ............ 343

About configuring the Symantec NAC Integrated Enforcer on an Enforcer console ......................... 344
Establishing or changing communication between a Symantec NAC Integrated Enforcer and Symantec Endpoint Protection Manager servers .............................................................. 344
Configuring automatic quarantine ...................................................................................... 347
Configuring Symantec NAC Integrated Enforcer basic settings .................................................. 349
Adding or editing the name of an Enforcer group for Symantec NAC Integrated Enforcer .................. 349
Adding or editing the description of an Enforcer group with a Symantec NAC Integrated Enforcer .................. 350
Adding or editing the IP address or host name of a Symantec NAC Integrated Enforcer .................. 350
Adding or editing the description of a Symantec NAC Integrated Enforcer .................. 350
Connecting the Symantec NAC Integrated Enforcer to a Symantec Endpoint Protection Manager ........ 351
Editing a Symantec Endpoint Protection Manager connection ............ 352
Configuring a trusted vendor list .................................................... 353
Viewing Enforcer logs on an Enforcer console ................................. 353
Configuring logs for the Symantec NAC Integrated Enforcer .......... 354
Configuring Symantec NAC Integrated Enforcer authentication
settings .................................................................................................. 354
About using authentication settings ......................................... 355
About authentication sessions ...................................................... 356
Specifying the maximum number of challenge packets during
an authentication session .............................................................. 358
Specifying the frequency of challenge packets to be sent to
clients .................................................................................................. 358
Allowing all clients with continued logging of non-authenticated
clients .................................................................................................. 359
Allowing non-Windows clients to connect to a network without
authentication .................................................................................. 360
Having the Symantec NAC Integrated Enforcer check the Policy
Serial Number on a client ................................................................. 361
Sending a message from a Symantec NAC Integrated Enforcer
to a client about non-compliance .................................................. 362
Establishing communication between a Symantec NAC Integrated
Enforcer and a Network Access Control Scanner on an Enforcer
console .............................................................................................. 362
Configuring Symantec NAC Integrated Enforcer advanced
settings .................................................................................................. 363
Enabling servers, clients, and devices to connect to the network
as trusted hosts without authentication ........................................ 364
Enabling local authentication on the Integrated Enforcer .......... 365
Stopping and starting communication services between an Integrated
Enforcer and a management server ............................................... 365
Disconnecting an Integrated Lucent Enforcer from a management
server on an Enforcer console .......................................................... 367
Configuring a secure subnet mask .................................................... 368
Section 5  Installing and configuring the Symantec NAC Integrated Enforcer for Microsoft Network Access Protection ........................................ 369

Chapter 21  Introducing the Symantec NAC Integrated Enforcer for Microsoft Network Access Protection .............. 371

   About the Integrated Enforcer for Microsoft Network Access Protection ........................................................................... 371

Chapter 22  Planning for the installation of the Symantec NAC Integrated Enforcer for Microsoft Network Access Protection .......................................................... 373

   About planning for the installation of the Symantec Integrated NAP Enforcer ............................................................................ 373

   Required components for an Symantec Integrated NAP Enforcer ................................................................................................. 374

   Hardware requirements for a Symantec Integrated NAP Enforcer ................................................................................................. 374

   Operating system requirements for a Symantec Integrated NAP Enforcer ............................................................................. 375

   Operating system requirements for a Symantec Network Access Control client ................................................................. 376

Chapter 23  Installing the Symantec NAC Integrated Enforcer for Microsoft Network Access Protection ............ 377

   Before you install the Symantec Integrated NAP Enforcer ................................................................................................. 377

   Installing the Symantec Integrated NAP Enforcer ................................................................................................. 378

Chapter 24  Configuring the Symantec NAC Integrated Enforcer for Microsoft Network Access Protection on an Enforcer console ......................................................... 381

   About configuring a Symantec Integrated NAP Enforcer on an Enforcer console ................................................................. 382

   Connecting a Symantec Integrated NAP Enforcer to a management server on an Enforcer console ........................................... 382

   Encrypting communication between a Symantec Integrated NAP Enforcer and a management server .................................. 384
Section 7 Working with enforcer reports and logs ........................................ 405

Chapter 27 Managing Enforcer reports and logs ........................................ 407
About Enforcer reports .............................................................................. 407
About Enforcer logs ................................................................................ 408
About the Enforcer Server log ............................................................... 408
About the Enforcer Client log ................................................................. 409
About the Gateway Enforcer Traffic log ................................................ 410
Configuring Enforcer log settings ............................................................ 411
Disabling Enforcer logging on the Symantec Endpoint Protection Manager Console ............................................................... 411
Enabling the sending of Enforcer logs from an Enforcer to the Symantec Endpoint Protection Manager ...................................................... 412
Setting up the size and age of Enforcer logs .......................................... 412
Filtering the Traffic logs for an Enforcer .................................................. 413

Index ........................................................................................................ 415
Installing and configuring the Symantec Network Access Control Enforcer appliances

- Chapter 1. Introducing the Enforcer appliance
- Chapter 2. Planning for the Enforcer appliance installation
- Chapter 3. Upgrading and migrating Enforcer appliance images
- Chapter 4. Installing the Enforcer appliance for the first time
- Chapter 5. Performing basic tasks on the console of an Enforcer appliance
- Chapter 6. Configuring the Symantec Gateway Enforcer appliance on the Symantec Endpoint Protection Manager Console
- Chapter 7. Configuring the Symantec DHCP Enforcer appliance on the Symantec Endpoint Protection Manager Console
- Chapter 8. Configuring the Symantec LAN Enforcer appliance on the Symantec Endpoint Protection Manager Console
- Chapter 9. Setting up temporary connections for Symantec Network Access Control On-Demand clients
■ Chapter 10. Enforcer appliance command-line interface
■ Chapter 11. Enforcer appliance command-line interface reference
■ Chapter 12. Troubleshooting an Enforcer appliance
■ Chapter 13. Frequently asked questions about the Gateway, DHCP, or LAN
   Enforcer appliances
Introducing the Enforcer appliance

This chapter includes the following topics:

- About the Symantec Enforcer appliances
- Types of enforcement
- What you can do with Symantec Network Access Control Enforcer appliances
- About Host Integrity policies and the Enforcer appliance
- How the Gateway Enforcer appliance works
- How the DHCP Enforcer appliance works
- How the LAN Enforcer appliance works
- Support for third-party enforcement solutions
- Where to find more information about the Symantec Enforcer appliances

About the Symantec Enforcer appliances

Symantec Enforcers are the optional network components that work with the Symantec Endpoint Protection Manager.

The following Linux-based Symantec Enforcer appliances work with managed clients, such as Symantec Endpoint Protection clients, and Symantec Network Access Control clients to protect the enterprise network:

- Symantec Network Access Control Gateway Enforcer appliance
- Symantec Network Access Control DHCP Enforcer appliance
Symantec Network Access Control LAN Enforcer appliance

All Windows-based Symantec Enforcers work with managed clients, such as the Symantec Endpoint Protection client and the Symantec Network Access Control client to protect the enterprise network.

**Note:** The Symantec Network Access Control Integrated Enforcer for Microsoft Network Access Protection does not work with guest clients, such as the Symantec Network Access Control On-Demand clients on the Windows and Macintosh platforms.

Installation, configuration, and administration instructions are included in the documentation for the following Windows-based Enforcers:

- Symantec Network Access Control Integrated Enforcer for Microsoft DHCP servers
  See “About the Symantec NAC Integrated Enforcer for Microsoft DHCP Servers” on page 305.

- Symantec Network Access Control Integrated Enforcer for Microsoft Network Access Protection

- Symantec Network Access Control Integrated DHCP Enforcer for Alcatel-Lucent VitalQIP DHCP servers

**Types of enforcement**

Table 1-1 lists the optional Enforcer appliances and Windows-based Enforcers.
<table>
<thead>
<tr>
<th>Type of Enforcer appliance</th>
<th>Description</th>
</tr>
</thead>
</table>
| Symantec Gateway Enforcer appliance | Provides the enforcement at access points for the external computers that connect remotely through one of the following methods:  
  - Virtual private network (VPN)  
  - Wireless LAN  
  - Remote Access Server (RAS)  
  
  You can also set up the Gateway Enforcer appliance to restrict access to certain servers by allowing only specified IP addresses. The Symantec Gateway Enforcer is supported on an Enforcer appliance.  
  
  See “How the Gateway Enforcer appliance works” on page 32.  
  See “Installation planning for a Gateway Enforcer appliance” on page 42. |
| Symantec LAN Enforcer appliance | Provides the enforcement for the clients that connect to the network through a switch or a wireless access point that supports 802.1x authentication. The LAN Enforcer appliance acts as a Remote Authentication Dial-In User Service (RADIUS) proxy. It can work with or without a RADIUS server that provides user-level authentication. The Symantec LAN Enforcer is supported on an Enforcer appliance.  
  
  See “How the LAN Enforcer appliance works” on page 35.  
  See “Installation planning for a LAN Enforcer appliance” on page 61. |
| Symantec DHCP Enforcer appliance | Provides the enforcement for the clients that gain access to the network. Clients receive a dynamic IP address through a Dynamic Host Configuration Protocol (DHCP) server. The Symantec DHCP Enforcer is supported on an Enforcer appliance.  
  
  See “How the DHCP Enforcer appliance works” on page 33.  
  See “Installation planning for a DHCP Enforcer appliance” on page 52. |
Table 1-1 Types of enforcement (continued)

<table>
<thead>
<tr>
<th>Type of Enforcer appliance</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symantec Integrated Enforcer for Microsoft DHCP Servers</td>
<td>Provides the enforcement for the clients that gain access to the network. Clients receive a dynamic IP address through a Dynamic Host Configuration Protocol (DHCP) server. The Symantec Integrated DHCP Enforcer is supported on the Windows platform. The Symantec Integrated Enforcer for Microsoft DHCP Servers is not supported on an Enforcer appliance. See “How an Integrated Enforcer for Microsoft DHCP Servers works” on page 306. See “Planning for the placement of an Integrated Enforcer for Microsoft DHCP Servers” on page 313.</td>
</tr>
<tr>
<td>Symantec Integrated Enforcer for Microsoft Network Access Protection</td>
<td>Provides the enforcement for the clients that gain access to the network. Clients receive a dynamic IP address or pass 802.1x authentication through a Dynamic Host Configuration Protocol (DHCP) server. The Symantec Integrated NAP Enforcer is supported on the Windows Server 2008 platform. The Symantec Integrated Enforcer for Microsoft Network Access Protection is not supported on an Enforcer appliance.</td>
</tr>
<tr>
<td>Symantec Integrated Enforcer for Alcatel-Lucent VitalQIP DHCP Servers</td>
<td>Provides the enforcement for the clients that gain access to the network. Clients receive a dynamic IP address or pass 802.1x authentication through a Dynamic Host Configuration Protocol (DHCP) server. The Symantec Integrated DHCP Enforcer is supported on the Windows platform. The Symantec Integrated DHCP Enforcer for Alcatel-Lucent VitalQIP DHCP Servers is not supported on an Enforcer appliance.</td>
</tr>
</tbody>
</table>

What you can do with Symantec Network Access Control Enforcer appliances

The optional 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 or in front of a DHCP server. You can also set it up for 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 policies of that enterprise. You can configure a company’s 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 its access to the network.
- Allow access to limited resources only.

The optional 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 35.

See “Installation planning for a LAN Enforcer appliance” on page 61.

You may have other parts of the network that are not set up for 802.1x support. You can use a DHCP Enforcer appliance to manage enforcement for these clients.

See “How the DHCP Enforcer appliance works” on page 33.

See “Installation planning for a DHCP Enforcer appliance” on page 52.

If you have employees who work remotely and connect through a VPN or dial-up, 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.

See “How the Gateway Enforcer appliance works” on page 32.

See “Installation planning for a Gateway Enforcer appliance” on page 42.

If high availability is required, you can install two or more Gateway Enforcer, DHCP, or LAN Enforcer appliances at the same location to provide failover.

See “Failover planning for Gateway Enforcer appliances” on page 49.

See “Failover planning for DHCP Enforcer appliances” on page 57.

See “Failover planning for LAN Enforcer appliances” on page 64.

If you want to implement high availability for LAN Enforcer appliances, you must install multiple LAN Enforcer appliances and the 802.1x-aware switch. High availability is accomplished through the addition of the 802.1x-aware switch. If
you only install multiple LAN Enforcer appliances without an 802.1x-aware switch, then high availability fails. You can configure an 802.1x-aware switch for high availability.

For information about the configuration of an 802.1x-aware switch for high availability, see the accompanying documentation for the 802.1x-aware switch.

In some network configurations, a client may connect to a network through more than one Enforcer appliance. After the first Enforcer appliance provides authentication to the client, all the remaining Enforcer appliances must authenticate the client before the client can connect to the network.

### About Host Integrity policies and the Enforcer appliance

The security policies that all Enforcer appliances check on client computers are called Host Integrity policies. You create and manage Host Integrity policies on the console of a Symantec Endpoint Protection Manager.

Host Integrity policies specify the software that is required to run on a client. For example, you can specify that the following security software that is located on a client computer must comply with certain requirements:

- Antivirus software
- Antispyware software
- Firewall software
- Patches
- Service packs

If the predefined requirements do not meet your needs, you can also customize the requirements.

See the Administration Guide for Symantec Endpoint Protection and Symantec Network Access Control for more information about how configure and customize Host Integrity policies.

You can configure clients to run Host Integrity checks at various times. When a client tries to connect to the network, it runs a Host Integrity check. It then sends the results to an Enforcer appliance.

Typically the Enforcer appliance is set up to verify that the client passes the Host Integrity check before it grants network access to the client. If the client passes the Host Integrity check, it is in compliance with the Host Integrity policy at your company. However, each type of Enforcer appliance defines the network access criteria differently.
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 that controls how it 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 unique identifier (UID). The Enforcer appliance sends the UID to the management server and receives an accept response or a reject response.

If an Enforcer appliance is configured to authenticate the UID, 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, such as the client identifier or client profile, 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.

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 unique identifier (UID), which the Enforcer passes on to the Manager 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 notifies the client to update its profile.

After the DHCP Enforcer or Gateway Enforcer appliance allows the client to connect to a network, it continues to communicate with the client at a regular predefined interval. 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, 802.1 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.

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 company's network.

A Gateway Enforcer appliance uses the following processes to authenticate a client:

1. When a client tries to access the network, the Gateway Enforcer appliance first checks whether the client runs the Symantec Endpoint Protection client or the Symantec Network Access Control client. If the client runs any of the client software, the Gateway Enforcer appliance begins the host authentication process.
2. The client that runs on a user's computer performs a Host Integrity check. It then passes the results to the Gateway Enforcer appliance with its identification information and information about the status of its security policy.
3. The Gateway Enforcer appliance verifies with the Symantec Endpoint Protection Manager that the client is a legitimate client and that its security policy is up to date.
4. The Gateway Enforcer appliance verifies that the client has passed the Host Integrity check and therefore complies with the security policies.
5. If all processes pass, the Gateway Enforcer appliance allows the client to connect 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 the network to allow the use of network resources for remediation.

To set up the Gateway Enforcer appliance authentication, you can configure which client IP addresses to check. You can specify the trusted external IP addresses that the Gateway Enforcer appliance allows without authentication. For remediation, you can configure the Gateway Enforcer appliance to allow clients access to trusted internal IP addresses. For example, you can allow clients to have access to an update server or a file server that contains antivirus DAT files.

For clients without the Symantec client software, you can redirect client HTTP requests to a Web server. For example, you can provide additional instructions on where to obtain remediation software or allow a client to download client software.

You can also configure the Gateway Enforcer appliance to allow non-Windows clients to access the network. 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.

How the DHCP Enforcer appliance works

A DHCP Enforcer appliance is used inline as a secure policy-enforcing bridge to protect an internal network. The clients that try to connect to the network send a DHCP request for a dynamic IP address. The switch or the router that acts as a DHCP relay client routes the DHCP request to the DHCP Enforcer appliance. The DHCP Enforcer appliance is configured inline in front of the DHCP server. Before it forwards the DHCP request to the DHCP server, the Enforcer appliance verifies that clients comply with security policies.

If a client complies with security policies, the DHCP Enforcer appliance sends the client request for an IP address to the normal DHCP Server. If the agent does not comply with the security policies, the Enforcer connects it to the quarantine DHCP server. The quarantine server assigns the client to a quarantine network configuration.

You can install one DHCP server on one computer and configure it to provide both a normal and a quarantine network configuration. To complete the DHCP Enforcer appliance solution, the administrator needs to set up a remediation server. The remediation server restricts the access of the quarantined clients so that such clients can interact only with the remediation server. If high availability is
required, then you can install two or more DHCP Enforcers appliances to provide failover capabilities.

The DHCP Enforcer enforces security policies on the clients that try to access a DHCP server. It does not block the DHCP request if the client fails authentication. The DHCP Enforcer appliance forwards the DHCP request to a quarantine DHCP server for a short-term, restricted-range network configuration.

When the client first sends the DHCP request, the DHCP Enforcer appliance forwards it to the quarantine DHCP server for a temporary IP address with a short lease time. The DHCP Enforcer appliance can then begin its authentication process with the client.

The DHCP Enforcer appliance authenticates clients by using the following methods:

- When a client tries to access the enterprise network, the Enforcer appliance first checks whether the client computer runs the Symantec Network Access Control client software. If the client computer runs the Symantec Network Access Control client software, the Enforcer appliance begins the process for host authentication.

- The Symantec client software that runs on the client computer performs a Host Integrity check. The client then passes the results to the Enforcer appliance, along with its identification information and information about the status of its security policy.

- The DHCP Enforcer appliance verifies with the Symantec Endpoint Protection Manager that the client is a legitimate client and that its security policy is up to date.

- The DHCP Enforcer appliance verifies that the client has passed the Host Integrity check and therefore complies with the security policies.

- If all steps are passed, the DHCP Enforcer appliance ensures that the quarantine IP address is released. The DHCP Enforcer appliance then routes the client DHCP request to the normal DHCP server. The client then receives a normal IP address and network configuration.

If the client does not meet the security requirements, the DHCP Enforcer appliance ensures that the DHCP request is renewed with the quarantine DHCP server. The client receives a quarantine network configuration, which must be set up to allow access to a remediation server.

The DHCP Enforcer appliance can be configured to allow non-Windows clients to have access to the normal DHCP server.
How the LAN Enforcer appliance works

The LAN Enforcer appliance acts as a Remote Authentication Dial-In User Service (RADIUS) proxy.

You can use the LAN Enforcer appliance with a RADIUS server to do the following actions:

■ Perform traditional 802.1x/EAP user authentication.
   You deny network access to rogue computers. Any users that try to connect to the network must authenticate through RADIUS first.

■ Verify that client computers comply with the security policies set on the management server (host authentication).
   You can enforce security policies, such as ensuring that the computer has the correct antivirus software, patches, or other software. You can validate that the client computer runs the Symantec client and that it passed the Host Integrity check.

In the networks that do not use a RADIUS server, the LAN Enforcer appliance performs host authentication only.

A LAN Enforcer appliance communicates with a switch or wireless access point that supports EAP/802.1x authentication. The switch or wireless access point is often configured into two or more virtual local area networks (VLANs). Symantec clients on client computers pass the EAP information or Host Integrity information to the switch by using the EAPOL (EAP over LANs) protocol. The switch forwards the information to the LAN Enforcer appliance for authentication.

You can configure the LAN Enforcer appliance with a set of possible responses to an authentication failure. The responses depend on the type of authentication failure: host authentication or EAP user authentication.

If you use a switch or wireless access point, you can set up the LAN Enforcer appliance to direct an authenticated client to different VLANs. The switch or wireless access point must provide dynamic VLAN switching capability. The VLANs might include a remediation VLAN.

If you use the LAN Enforcer with a RADIUS server, you can configure multiple RADIUS server connections for the Enforcer. If a RADIUS server connection is down, the LAN Enforcer appliance can switch to a different one. In addition, multiple LAN Enforcer appliances can be set up to connect to the switch. If one LAN Enforcer appliance fails to respond, a different LAN appliance Enforcer can handle the authentication.
How LAN Enforcer basic configuration works

If you are familiar with 802.1x authentication, you can view details about the clients that try to access the network by using the basic configuration. You can use this information for troubleshooting network connections.

Basic configuration of 802.1x LAN Enforcement works as follows:

- A supplicant (for example, a client computer) tries to access the network through an authenticator (for example, an 802.1x switch).
- The switch sees the computer and requests identification.
- The 802.1x supplicant on the computer prompts the user for a user name and password, and responds with its identification.
- The switch forwards this information to the LAN Enforcer, which then forwards it to the RADIUS server.
- The RADIUS server generates an EAP challenge by selecting an EAP type that is based on its configuration.
- The LAN Enforcer receives this challenge, adds a Host Integrity challenge, and forwards it to the switch.
- The switch forwards the EAP and Host Integrity challenges to the client.
- The client receives the challenges and sends a response.
- The switch receives the response and forwards it to the LAN Enforcer.
- The LAN Enforcer examines the Host Integrity check result and client status information and forwards it to the RADIUS server.
- The RADIUS Server performs EAP authentication and sends the result back to the LAN Enforcer.
- The LAN Enforcer receives the authentication results and forwards the result and action to take.
- The switch selects the appropriate action and allows normal network access, blocking access, or permitting access to an alternate VLAN depending on the results.

How LAN Enforcer transparent mode works

LAN Enforcer transparent mode works in the following ways:

- A supplicant (for example, a client computer) tries to access the network through an authenticator (for example, an 802.1x switch).
- The authenticator sees the computer and sends an EAP authentication packet (EAP traffic only allowed).
The client that acts as an EAP supplicant sees the authentication packet and responds with Host Integrity authentication.

The switch sends Host Integrity authentication results to the LAN Enforcer appliance that runs as a RADIUS Proxy server.

LAN Enforcer appliance replies to the switch with information about the VLAN assignments that is based on authentication results.

About 802.1x authentication

IEEE 802.1X-2001 is a standard that defines access control for wireless and wired LANs. The standard provides a framework for authenticating and controlling user traffic on a protected network. The standard specifies the use of the Extensible Authentication Protocol (EAP), which uses a centralized authentication server, such as Remote Authentication Dial-In User Service (RADIUS).

The server authenticates each user that tries to access the network. The 802.1x standard includes the specifications for EAP-over-LAN (EAPOL). EAPOL is used for encapsulating EAP messages in link layer frames (for example, Ethernet) and also provides control functions.

The 802.1x architecture includes the following key components:

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authenticator</td>
<td>The entity that brokers the authentication, such as an 802.1x-compliant LAN switch or wireless access point</td>
</tr>
<tr>
<td>Authentication Server</td>
<td>The entity that provides the actual authentication by validating the credentials that are supplied in response to the challenge, such as a RADIUS server</td>
</tr>
<tr>
<td>Supplicant</td>
<td>The entity that seeks network access and tries to successfully authenticate, such as a computer</td>
</tr>
</tbody>
</table>

When a supplicant device is connected to a network switch authenticator with 802.1x enabled, the following process occurs:

- The switch issues an EAP Identity Request.
- The EAP supplicant software responds with an EAP Identity Response, which is forwarded to the authentication server (for example, RADIUS) by the switch.
- The authentication server issues an EAP Challenge, which is forwarded to the supplicant by the switch.
- The user enters authentication credentials (user name and password, token, and so forth).
The supplicant sends an EAP Challenge Response, including the user-supplied credentials, to the switch, which forwards it to the authentication server.

The authentication server validates the credentials and replies with an EAP or User Authentication result, which indicates the success or failure of the authentication.

If authentication succeeds, the switch permits access for normal traffic. If authentication fails, client device access is blocked. The supplicant is notified of the result in either case.

Only EAP traffic is permitted during the authentication process.

For details on EAP, refer to the IETF’s RFC 2284 at the following URL:

http://www.ietf.org/rfc/rfc2284.txt

For additional details on IEEE Standard 802.1x, refer to the text of the standard at the following URL:


Support for third-party enforcement solutions

Symantec provides the enforcement solutions for the following third-party vendors:

- Universal Enforcement API
  Symantec has developed the Universal Enforcement API to allow other vendors with related technology to integrate their solutions with the Symantec software.

- Cisco Network Admissions Control
  Symantec clients can support the Cisco Network Admissions Control enforcement solution.

Where to find more information about the Symantec Enforcer appliances

Table 1-2 lists the various sources that provide information about related the tasks that you may need to perform before or after an Enforcer has been installed.
Table 1-2 Symantec Enforcer documentation

<table>
<thead>
<tr>
<th>Enforcer document</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Installation Guide for Symantec Endpoint Protection and Symantec Network Access Control</em></td>
<td>Describes how to install the Symantec Endpoint Protection Manager, Symantec Endpoint Protection client, and Symantec Network Access Control clients. It also explains how to configure the embedded and Microsoft SQL database, and to set up replication.</td>
</tr>
<tr>
<td><em>Administration Guide for Symantec Endpoint Protection and Symantec Network Access Control</em></td>
<td>Describes how to configure and administer the Symantec Endpoint Protection Manager, the Symantec Endpoint Protection clients, and the Symantec Network Access Control clients. It also describes how to set up the Host Integrity policies that an Enforcer uses to implement compliance on client computers.</td>
</tr>
<tr>
<td><em>Client Guide for Symantec Endpoint Protection and Symantec Network Access Control</em></td>
<td>Describes how to use the Symantec Endpoint Protection clients and the Symantec Network Access Control clients.</td>
</tr>
<tr>
<td><em>Enforcer Implementation Guide for Symantec Network Access Control</em></td>
<td>Describes how to install and administer all types of Symantec Network Access Control appliances and integrated enforcers. Also explains how to use the on-demand clients for Macintosh and Linux.</td>
</tr>
<tr>
<td>Online Help</td>
<td>Explains how to use the Symantec Endpoint Protection Manager, the Symantec Endpoint Protection client, the Symantec Network Access Control clients. Also explains the use of each of the Integrated Enforcers.</td>
</tr>
<tr>
<td>Online Help for the On-Demand clients</td>
<td>Explains how to use the Macintosh and Linux on-demand clients.</td>
</tr>
<tr>
<td>Enforcer Command-Line Interface Help</td>
<td>Provides help when you type the ? key on the command line interface (CLI) command line.</td>
</tr>
<tr>
<td>readme.txt file</td>
<td>Includes the latest information about critical Enforcer-related the defects that may also affect the Symantec Endpoint Protection Manager.</td>
</tr>
</tbody>
</table>
Introducing the Enforcer appliance
Where to find more information about the Symantec Enforcer appliances
Planning for the Enforcer appliance installation

This chapter includes the following topics:

- Installation planning for Enforcer appliances
- Installation planning for a Gateway Enforcer appliance
- Failover planning for Gateway Enforcer appliances
- Installation planning for a DHCP Enforcer appliance
- Failover planning for DHCP Enforcer appliances
- Installation planning for a LAN Enforcer appliance
- Failover planning for LAN Enforcer appliances

Installation planning for Enforcer appliances

You must plan where to integrate the following Linux-based Symantec Network Access Control Enforcer appliances in a network:

- Symantec Network Access Control Gateway Enforcer appliance
  See “Installation planning for a Gateway Enforcer appliance” on page 42.
- Symantec Network Access Control DHCP Enforcer appliance
  See “Installation planning for a DHCP Enforcer appliance” on page 52.
- Symantec Network Access Control LAN Enforcer appliance
  See “Installation planning for a LAN Enforcer appliance” on page 61.
- Symantec Network Access Control Integrated DHCP Enforcer for Microsoft DHCP Servers
See “About planning for the installation of an Integrated Enforcer for Microsoft DHCP Servers” on page 311.

- Symantec Network Access Control Integrated DHCP Enforcer for Microsoft Network Access Protection Servers
  See “About planning for the installation of the Symantec Integrated NAP Enforcer” on page 373.

- Symantec Network Access Control Integrated DHCP Enforcer for Alcatel-Lucent VitalQIP DHCP Servers
  See “About planning for the installation of an Integrated Lucent Enforcer” on page 329.

**Installation planning for a Gateway Enforcer appliance**

Several types of planning information can help you implement Gateway Enforcer appliances in a network.

You can place the Gateway Enforcer appliance to help protect the following areas in a network:

- General placement
  See “Where to place a Gateway Enforcer appliance” on page 42.

- See “Guidelines for IP addresses on a Gateway Enforcer appliance” on page 45.

- See “About two Gateway Enforcer appliances in a series” on page 45.

- See “Protection of VPN access through a Gateway Enforcer appliance” on page 46.

- See “Protection of wireless access points through a Gateway Enforcer appliance” on page 46.

- See “Protection of servers through a Gateway Enforcer appliance” on page 46.

- See “Protection of non-Windows servers and clients through a Gateway Enforcer appliance” on page 47.

- See “Requirements for allowing non-Windows clients without authentication” on page 48.

**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 45.

You typically can place Gateway Enforcer appliances at the following locations:

<table>
<thead>
<tr>
<th>Location</th>
<th>Placement</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN</td>
<td>Between virtual private network (VPN) concentrators and the corporate network</td>
</tr>
<tr>
<td>Wireless Access Point (WAP)</td>
<td>Between a wireless access point and the corporate network</td>
</tr>
<tr>
<td>Servers</td>
<td>In front of corporate servers</td>
</tr>
</tbody>
</table>

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.

You can place Gateway Enforcer appliances next to a wireless access point (WAP) or a virtual private network (VPN). In a corporate network you can also safeguard servers that contain sensitive information. Gateway Enforcer appliances must use two network interface cards (NICs).

**Figure 2-1** provides an example of where you can place Gateway Enforcer appliances in the overall network configuration.
Figure 2-1 Placement of Gateway Enforcer appliances

Another location where a Gateway Enforcer appliance protects a network is at a remote access server (RAS). Clients can dial 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

You 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 if the clients can get 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 will generate a bogus external NIC address, based on the internal NIC address. You do not need to configure this again if you install another Gateway Enforcer.

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 five-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 the *Administration Guide for Symantec Endpoint Protection and Symantec Network Access Control* for information about trusted internal IP addresses.
Protection of VPN access through a Gateway Enforcer appliance

The protection of VPN access is the first and most common reason for which Gateway Enforcer appliance is used. 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.

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 the 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.

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.
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 about 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 47.
- Implement support without a Gateway Enforcer appliance.
  See “Implementation of non-Windows without a Gateway Enforcer appliance” on page 47.

Implementation of non-Windows support through a Gateway Enforcer appliance

You can implement support for non-Windows clients by configuring the Gateway Enforcer 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.

Implementation of non-Windows 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.
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 non-Windows clients” on page 48.

When a client tries to access the corporate 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 does not run 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.

For the Gateway Enforcer appliance to correctly detect that an operating system is a Windows operating system, the following requirements must be met on the Windows client:

■ 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.

Requirements for non-Windows clients

The Gateway Enforcer appliance must meet the following requirements before it allows a Macintosh client to connect to a network:

■ Windows Sharing must be on.
  This default setting is enabled.
Macintosh built-in firewall must be off.
This setting is the default.
The Gateway Enforcer has the following requirement to allow a Linux client:
- The Linux system must run the Samba service.

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 fail. 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.

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.

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 2-2 shows how to set up two Gateway Enforcer appliances for failover to protect network access at a VPN concentrator.
Planning for the Enforcer appliance installation

Failover planning for Gateway Enforcer appliances

Figure 2-2  Placement of two Gateway Enforcer appliances

Remote clients

VPN

Outside company

Internet

Inside company

Corporate firewall

VPN

Server

Internal clients

External NIC

Gateway Enforcer 1

Internal NIC

Hub/VLAN

Protected servers

Symantec Endpoint Protection Manager

Internal clients

Corporate Backbone

Gateway Enforcer 2

External NIC

Rent

35

51
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 49.

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 50.

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 45.

Installation planning for a DHCP Enforcer appliance

Several types of planning information can help you implement DHCP Enforcer appliances in a network.

You can place the DHCP Enforcer appliance to help protect the following areas in a network:

- See “Where to place DHCP Enforcer appliances in a network” on page 52.
- See “DHCP Enforcer appliance IP addresses” on page 54.
- See “Protection of non-Windows clients with DHCP enforcement” on page 55.
- See “About the DHCP server” on page 56.

Where to place DHCP Enforcer appliances in a network

If you want to ensure that the DHCP Enforcer appliance can intercept all DHCP messages between DHCP clients and DHCP servers, you must install the DHCP Enforcer as an inline device. The DHCP Enforcer must be installed between the clients and the DHCP Server.

The internal NIC of the DHCP Enforcer appliance connects to the DHCP servers. The external NIC of the DHCP Enforcer connects to the clients through a router or switch, which acts as a DHCP relay agent. The Symantec Endpoint Protection Manager also connects to the DHCP Enforcer appliance’s external NIC.
You can configure one DHCP Enforcer appliance to communicate with multiple DHCP servers. For example, you can have multiple DHCP servers on the same subnet for failover purposes. If you have DHCP servers in different locations on the network, each one requires a separate DHCP Enforcer appliance.

For each of your DHCP server locations, you configure a normal DHCP server and a quarantine DHCP server. You can configure the Enforcer to recognize multiple quarantine DHCP servers, as well as multiple normal DHCP servers.

**Note:** You can install one DHCP server on one computer and configure it to provide both a normal and quarantine network configuration.

You also must set up a remediation server so that the clients that receive quarantine configurations can connect with the remediation server. Optionally, the Symantec Endpoint Protection Manager can run on the same computer as the remediation server. Neither the Symantec Endpoint Protection Manager nor the remediation server requires any direct connection with the DHCP Enforcer appliance or the DHCP servers.

If the client meets security requirements, the DHCP Enforcer appliance acts as a DHCP relay agent. The DHCP Enforcer appliance connects the client to the normal DHCP server and the client receives a regular network configuration. If the client does not meet the security requirements, the DHCP Enforcer appliance connects it to a quarantine DHCP server. The client then receives a quarantine network configuration.

**Figure 2-3** shows an example of the various components that are required for a DHCP Enforcer appliance and where they are placed.

**Note:** Although the illustration shows a quarantine DHCP server on a separate computer, only one computer is required. If you use only one computer, you must configure the DHCP server to provide two different network configurations. One of the network configurations must be a quarantine network configuration.
DHCP Enforcer appliance IP addresses

When you set up an IP address for a DHCP Enforcer appliance, you must follow certain guidelines.

You follow these guidelines when you set up the internal NIC for a DHCP Enforcer appliance:

- The DHCP Enforcer appliance's internal IP address must be in the same subnet as the DHCP servers.
Clients must be able to communicate with the DHCP Enforcer appliance’s internal IP address.

If you use multiple DHCP Enforcers in a failover configuration, the IP address of the internal NIC on each DHCP Enforcer appliance must be different.

If you use multiple DHCP Enforcer appliances in a failover configuration, clients must be able to communicate with the internal IP address of both the active and standby DHCP Enforcer appliances.

You follow these guidelines when you set up the external NIC for a DHCP Enforcer appliance:

- The DHCP Enforcer appliance’s external IP address must be able to communicate with the Symantec Endpoint Protection Manager. It must be in the same subnet as the IP range of the internal NIC. In this case, the Symantec Endpoint Protection Manager is located on one side of a switch while the DHCP Enforcer appliance is located on the other side of a switch.

- If you use multiple DHCP Enforcer appliances in a failover configuration, the IP address of the external NIC on each DHCP Enforcer appliance must be different.

Protection of non-Windows clients with DHCP enforcement

You can install the Symantec Endpoint Protection software or the Symantec Network Access Control software on the clients that run the Microsoft Windows operating system. The DHCP Enforcer cannot authenticate clients without the Symantec Endpoint Protection software. If an organization includes clients with operating systems on which the software is not supported, such as Linux or Solaris, your planning must include how to handle these clients.

If you can implement support for non-Windows clients, you can configure the DHCP Enforcer appliance to allow all non-Windows clients to connect to the network. When the DHCP Enforcer appliance is configured in this way, the DHCP Enforcer appliance performs operating system detection to identify the clients that run non-Windows operating systems.

As an alternate method, you can configure a DHCP Enforcer to allow specific MAC addresses to access the corporate network. When a client with a trusted MAC address tries to connect to the network, the DHCP Enforcer forwards the client’s DHCP request to the normal DHCP server without authentication.
About the DHCP server

You can set up a separate quarantine DHCP server on a separate computer. You can also configure the same DHCP server to provide both normal and quarantine network configurations.

The quarantine network configuration must provide access to the following components:

- Remediation server
- Symantec Endpoint Protection Manager
- DHCP server
- DHCP Enforcer appliance

If you use multiple DHCP Enforcer appliances for failover, the quarantine network configuration must provide access to those components.

The quarantine IP address is used during DHCP Enforcer authentication as follows:

- The DHCP Enforcer appliance initially gets a temporary quarantine IP address for the client to carry out the authentication with a client.
  If the authentication is successful, the DHCP Enforcer appliance sends a notification message to the client prompting it to perform an IP release and an IP renew immediately.
  You can assign a short lease time to the quarantine configuration. Symantec recommends two minutes.

- If you support two DHCP servers, you can set up a range of IP addresses that is separate from the range of the normal network IP addresses. You can then use any IP addresses from the separate IP address range for the quarantine of unauthorized clients. However, the range of IP addresses that is used for quarantine must be located in the same subnet as the normal network IP addresses. You can assign some restricted IP addresses that the quarantine DHCP server can use. You can also use an ACL-enabled router or switch to prevent these restricted IP addresses from accessing the regular network resources.

- If you use one DHCP server, you must configure a user class called SYGATE_ENF that is used for the quarantine configuration. Some of the configuration steps are performed on the DHCP server. Other configuration tasks are performed on the Enforcer console after you complete the installation.

Normal and quarantine DHCP server on one DHCP server

You can use the same server for both the normal DHCP server and the quarantine DHCP server. It is recommended that you use two servers.
If you want to use one DHCP server as both the normal and quarantine DHCP server, you must configure consider the following guidelines:

- Microsoft DHCP servers do not support multiple subnets. If you use Microsoft DHCP servers, you may require two DHCP servers.
- If you want to use only one Microsoft DHCP server, all computers must use the same IP address subnet.
- If you are in an environment that uses two different subnets, you must make sure that the routers can manage two subnets on a single router interface. For example, Cisco routers have a feature called IP secondary. See the router documentation for more information.

**Failover planning for DHCP Enforcer appliances**

An enterprise can configure two DHCP Enforcer appliances in a network to continue operations in case one of the DHCP Enforcer appliances fails. If a DHCP Enforcer appliance fails in a network that is not configured for failover, then network access at that location is automatically blocked. If a DHCP Enforcer appliance fails in a network that does not provide for failover, then users can no longer connect to the network. This problem continues to occur until the problem with the DHCP Enforcer appliance is corrected.

For a DHCP Enforcer appliance, failover is implemented through the DHCP Enforcer appliance itself instead of third-party switches. If the hardware configuration is set up correctly, the Symantec Endpoint Protection Manager automatically synchronizes the settings for the failover DHCP Enforcer appliances.

**How failover works with DHCP Enforcer appliances in the network**

The DHCP Enforcer appliance that is operational is called the active DHCP Enforcer appliance. The backup DHCP Enforcer appliance is called the standby DHCP Enforcer appliance. The active DHCP Enforcer appliance is also referred to as the primary DHCP Enforcer appliance. If the active DHCP Enforcer appliance fails, the standby DHCP Enforcer appliance takes over the enforcement tasks.

The sequence in which the two DHCP Enforcer appliances are started is as follows:

- When the first DHCP Enforcer appliance is started, it runs in standby mode while it queries the network to determine whether another DHCP Enforcer appliance runs. It sends out three queries to search for another DHCP Enforcer. Therefore it can take a few minutes to change its status to Online.
- If it does not detect another DHCP Enforcer appliance, it becomes the active DHCP Enforcer appliance.
While the active DHCP Enforcer appliance runs, it broadcasts failover packets on both the internal and the external networks. It continues to broadcast the failover packets.

The second DHCP Enforcer appliance is then started. It runs in standby mode while it queries the network to determine whether another DHCP Enforcer appliance is running.

The second DHCP Enforcer appliance detects the active DHCP Enforcer appliance that is running and therefore remains in standby mode.

If the active DHCP Enforcer appliance fails, it stops to broadcast failover packets. The standby DHCP Enforcer appliance no longer detects an active DHCP Enforcer appliance. It now becomes the active DHCP Enforcer appliance that handles network connections and security at this location.

If you start the other DHCP Enforcer appliance, it remains the standby DHCP Enforcer appliance because it detects that another DHCP Enforcer appliance is running.

### Where to place DHCP Enforcer appliances for failover in a network with only one or multiple VLANs

You set up a DHCP Enforcer appliance for failover by their 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.

DHCP Enforcer appliance for failover must be set up on the same network segment. A router or gateway cannot be installed between the two DHCP 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.

Configuring DHCP Enforcer appliances for failover at a wireless AP, dial-up RAS, or other access points is similar. The external NICS of both DHCP Enforcer appliances connect to the external network through a wireless AP or RAS server. The internal NICS connect to the internal network or the area that is protected.

*Figure 2-4* shows how to set up two DHCP Enforcer appliances for failover to protect network access at a VPN concentrator.
Setting up DHCP Enforcer appliances for failover

You should familiarize yourself with the concepts that are involved in DHCP Enforcer appliance failover before you set up standby DHCP Enforcer appliances.

See “How failover works with DHCP Enforcer appliances in the network” on page 57.
To set up DHCP Enforcer appliances for failover

1. Place the computers in the network.
   
   See “Where to place DHCP Enforcer appliances for failover in a network with only one or multiple VLANs” on page 58.

2. Set up the external and internal NICs.
   
   The external NICs on multiple DHCP Enforcer appliances must each have a different IP address. The internal NICs on multiple DHCP Enforcer appliances must each have a different IP address.
   
   See “DHCP Enforcer appliance IP addresses” on page 54.

3. Install and start the primary DHCP Enforcer appliance.
   
   If the primary DHCP Enforcer appliance does not locate another DHCP Enforcer, it takes the role of the active DHCP Enforcer appliance.

4. Install and start the standby DHCP Enforcer appliance.

5. Connect the standby DHCP Enforcer appliance to the same Symantec Endpoint Protection Manager as the active DHCP Enforcer appliance.
   
   If both DHCP Enforcer appliances have run for the same amount of time, then the one with the lower IP address becomes the primary DHCP Enforcer appliance.

   Failover is enabled by default on the Symantec Endpoint Protection Manager. The Symantec Endpoint Protection Manager automatically assigns the standby DHCP Enforcer appliance to the same Enforcer group. Therefore the settings of the primary and standby DHCP Enforcer appliances are synchronized.

   The following failover settings are enabled by default:

   ■ The default setting for the failover UDP port is 39999.
     
     A failover DHCP Enforcer appliance uses this port to communicate with each other.

   ■ The default setting for the failover sensitivity level is High (fewer than five seconds).
     
     The failover sensitivity level determines how quickly the standby DHCP Enforcer appliance becomes the primary DHCP Enforcer appliance. The failover only occurs if the standby DHCP Enforcer appliance detects that the primary DHCP Enforcer appliance is no longer active.
Installation planning for a LAN Enforcer appliance

Several types of planning information can help you implement LAN Enforcer appliances in a network.

See “Where to place LAN Enforcer appliances” on page 61.

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.

Figure 2-5 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 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:

- **Basic configuration**
  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 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 basic configuration.

- **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 basic configuration.

- **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 basic configuration 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

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, you must specify the same group Enforcer name on the Enforcer console.

If you use a RADIUS server in your network, you can 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.

Where to place LAN Enforcer appliances for failover in a network

Figure 2-6 describes how to provide failover for LAN Enforcer appliances.
Planning for the Enforcer appliance installation

Failover planning for LAN Enforcer appliances

Figure 2-6 Placement of two LAN Enforcer appliances

- Clients
- Remediation server
- Remediation VLAN
- 802.1x-aware LAN switch with dot1x-enabled ports for internal clients
- Corporate Backbone
- Failover RADIUS server
- RADIUS server
- LAN Enforcer appliance (RADIUS proxy)
- Symantec Endpoint Protection Manager
- Protected servers
Planning for the Enforcer appliance installation

Failover planning for LAN Enforcer appliances
Upgrading and migrating Enforcer appliance images

This chapter includes the following topics:

- About upgrading and migrating Enforcer appliance images to version 11.0.3000
- Determining the current version of an Enforcer appliance image
- Upgrading the Enforcer appliance image from 11.0 or 11.0.2000 to 11.0.3000
- Migrating the Enforcer appliance image from 5.1.x to 11.0.3000
- Reimaging an Enforcer appliance image

About upgrading and migrating Enforcer appliance images to version 11.0.3000

You may want to determine the version of the Enforcer appliance software before you plan to update, migrate, or reimagine any of the Enforcer appliance software.

See “Determining the current version of an Enforcer appliance image” on page 68.

You may need to upgrade the image of an Enforcer appliance to version 11.0.3000 if you want to connect to a Symantec Endpoint Protection Manager version 11.0.3. The upgrade enables you to take advantage of the new features that the Symantec Network Access Control Enforcer appliance version 11.0.3000 provides.

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 from 11.0 or 11.0.2000 to 11.0.3000” on page 68.
Migrate from the 5.1.x Enforcer appliance image to the 11.0.2000 Enforcer appliance image.
See “Migrating the Enforcer appliance image from 5.1.x to 11.0.3000” on page 69.

Install a different Enforcer appliance image over a previous Enforcer appliance image.
See “Reimaging an Enforcer appliance image” on page 70.
The Symantec Network Access Control Enforcer appliance version 11.0.3 works with the following versions of the Symantec Endpoint Protection Manager:

- Version 11.0.2
- Version 11.0.3

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. The latest version 11.0.3000. If you have a version that precedes 11.0.3000, you should try to upgrade or migrate.

For example, if you determine the version of a DHCP Enforcer appliance image, then the output may appear as follows:

Symantec Network Access Control Enforcer 6100 Series - v11.0.1
build XXXX, 2007-11-29,19:09
DHCP Enforcer mode

To determine the current version of an Enforcer appliance image

- Type the following command on the command-line interface of an Enforcer appliance: show version

Upgrading the Enforcer appliance image from 11.0 or 11.0.2000 to 11.0.3000

You can use the following method to update an Enforcer appliance image from version 11.0 or 11.0.2000 to version 11.0.3000.
To upgrade the Enforcer appliance image from 11.0 or 11.0.2000 to 11.0.3000

1. Insert the CD in the CDROM drive of the Enforcer appliance.
2. Type the following command on the console of an Enforcer appliance:
   
   Enforcer# update

Migrating the Enforcer appliance image from 5.1.x to 11.0.3000

You can use any of the following methods to update an Enforcer appliance image from version 5.1.x to version 11.0.3000:

- Migrate the Enforcer appliance image from 5.1.x to 11.0.3000 with a USB (Universal Serial Bus) disk.
- Migrate the Enforcer appliance image from 5.1.x to 11.0.3000 from a TFTP server.

To migrate the Enforcer appliance image from 5.1.x to 11.0.3 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 update the Enforcer appliance:
   
   Enforcer# update
   
   See “Update” on page 238.

To migrate the Enforcer appliance image from 5.1.x to 11.0.3000 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
   
   See “Update” on page 238.
3. Select Y when you are prompted to launch the new image.
4. Select 1 to restart the Enforcer appliance after applying the new image.

It is not recommended that you launch the new image without restarting the Enforcer appliance.
5 Log on to the Enforcer appliance.
6 See “Logging on to an Enforcer appliance” on page 82.

Reimaging an Enforcer appliance image

The Enforcer appliance comes with reimaging software for all Enforcer appliances: Gateway, LAN, and DHCP. 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 CD, 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.

See “Installation planning for Enforcer appliances” on page 41.

To reimage an Enforcer appliance

1 Insert the CD in the CD-ROM drive of 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 CD.
   If you miss the Setup menu, the Enforcer appliance restarts from the disk rather than the CD. To reimage, you must restart from the CD.
4 Install and configure the Enforcer appliance.
   See “Installing an Enforcer appliance” on page 75.
Installing the Enforcer appliance for the first time

This chapter includes the following topics:

- Before you install the Enforcer appliance
- Installing an Enforcer appliance

Before you install the Enforcer appliance

The Enforcer appliance is a hardware device that enforces network access control to clients that try to connect to the network. If clients are in compliance with security policies, they are permitted to access resources on the network.

The type of Enforcer appliance that you can implement depends on the type of Symantec Network Access Control product that you purchased.

See your license agreement for more information.

You can deploy the Enforcer appliance that works with the Symantec Endpoint Protection Manager and clients.

The Enforcer includes the following types:

- Gateway Enforcer appliance
- DHCP Enforcer appliance
- LAN Enforcer appliance

About the Gateway Enforcer appliance installation

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.

You can use Gateway Enforcer appliances to protect servers within the company. They can ensure that only the trusted or the authenticated clients can access the servers.

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

See “Where to place a Gateway Enforcer appliance” on page 42.

About the DHCP Enforcer appliance installation

A DHCP Enforcer is used inline as a secure policy-enforcing bridge to protect an internal network.

Clients that try to connect to the network send a DHCP request for a dynamic IP address. The switch or router (that acts as a DHCP relay client) routes the DHCP request. The DHCP request is sent to the DHCP Enforcer appliance, which is configured inline in front of the DHCP server. Before the DHCP Enforcer appliance forwards the DHCP request to the DHCP server, the DHCP Enforcer appliance verifies that clients comply with security policies.

If a client complies with security policies, the DHCP Enforcer sends the client request for an IP address to the normal DHCP server.

If the client does not comply with the security policies, the DHCP Enforcer appliance connects it to the quarantine DHCP server. The quarantine DHCP server assigns the client a quarantine network configuration.

To complete the DHCP Enforcer configuration, you must set up a remediation server and restrict the access of the quarantined clients. Restricted clients can interact only with the remediation server.

If high availability is required, you can install two or more DHCP Enforcer appliances to provide failover capabilities.

See “Where to place DHCP Enforcer appliances in a network” on page 52.
About the LAN Enforcer appliance installation

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, as appropriate, based on the results of the Host Integrity check.

If you have Symantec Endpoint Protection, 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.

See “Where to place LAN Enforcer appliances” on page 61.

About the Enforcer appliance indicators and controls

The Enforcer appliance is installed on a 1U rack-mountable chassis with support for static rails.

Figure 4-1 shows the controls, indicators, and connectors that are located behind the optional bezel on the front panel.

**Figure 4-1** Enforcer appliance front panel

1. CD-ROM drive
2. Power switch
3. Reset icon
4. USB ports
Figure 4-2 shows the back panel of the system.

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. 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.

Table 4-1 lists the hardware specifications for the Enforcer appliance.
Table 4-1  Hardware specifications

<table>
<thead>
<tr>
<th>Part</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base unit</td>
<td>521, 2.8-GHz/1 MB cache, Pentium 4 800-MHz front side bus</td>
</tr>
<tr>
<td>Memory</td>
<td>1 GB DDR2, 533-MHz, 2x512 single-ranked DIMMs</td>
</tr>
<tr>
<td>Hard drive</td>
<td>160 GB, SATA, 1-inch, 7200-RPM hard drive</td>
</tr>
<tr>
<td>Network adapters</td>
<td>Single network adapter with two ports (eth0 is internal NIC and eth1 is external NIC by default). Failopen model has four ports, two of which are not used.</td>
</tr>
<tr>
<td>CD-ROM drive</td>
<td>24X, CD, 650 MB, internal</td>
</tr>
</tbody>
</table>

Gateway Enforcer appliance or DHCP Enforcer appliance NIC settings

The network interface cards (NICs) on a Gateway Enforcer appliance or a DHCP Enforcer appliance is configured by default as follows:

eth0  Internal NIC
      If you use the Gateway Enforcer appliance, the internal NIC must connect to the Symantec Endpoint Protection Manager.

eth1  External NIC
      If you use the DHCP Enforcer appliance, the external 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.

See “Configure interface-role” on page 251.

For the DHCP Enforcer, use this command with the manager option, to specify the NIC that is used to connect to the Symantec Endpoint Protection Manager.

The following example shows the syntax:

configure interface-role manager eth1

See “Installing an Enforcer appliance” on page 75.

Installing an Enforcer appliance

Before you start to install any of the Enforcer appliances, you should have familiarized yourself with the locations of the components in your network.
The Symantec Network Access Control Enforcer appliance comes with an installation CD called CD2 that contains software for the following components:

- Gateway Enforcer appliance
- LAN Enforcer appliance
- DHCP Enforcer appliance

You select the type of Enforcer appliance that you want to choose during the installation process.

During the installation of an Enforcer appliance, you must have handy the following information:

- 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.

- IP addresses of the network interface cards (NICs) on the Enforcer appliance

- IP address, host name, or domain ID of the domain name server (DNS) if applicable
  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. Only DNS servers can resolve host names. 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.
  See “Configure DNS” on page 249.

Installation of the Enforcer appliance involves the following tasks:

- Setup of an Enforcer appliance
- Configuration of an Enforcer appliance

**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 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. Connecting through the Serial Console is the preferred method because it allows for file transfers from the Enforcer appliance.

- 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.

   **DHCP 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 DHCP server; the external NIC connects to the endpoints and the Symantec Endpoint Protection Manager.

   **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.

7. Press **Enter** twice.

8. At the logon prompt, log in as follows:
   - Console Login: root
   - Password: symantec

   The Enforcer appliance automatically logs users off after 90 seconds of inactivity.
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
      D       DHCP 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 or 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

      See “Hostname” on page 235.

      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: symantec

New 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 9 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]:
About the Enforcer appliance lock

The Enforcer appliance comes with a separate bezel that can be attached to the front panel. It includes a key. Therefore, you can lock the Enforcer appliance for additional security. The use of the bezel is optional. It is recommended for highest security. You must place the key in a secure location.
Performing basic tasks on the console of an Enforcer appliance

This chapter includes the following topics:

■ About performing basic tasks on the console of an Enforcer appliance
■ Logging on to an Enforcer appliance
■ 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
■ Enforcer reports and debug logs

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 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 83.

Although you typically administer an Enforcer appliance on the console of the Symantec Endpoint Protection Manager after you complete the initial installation and configuration of an Enforcer appliance, you may still need to perform many of the administrative tasks on the console of an Enforcer appliance. 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 any number of parameters.

See “About the Enforcer appliance CLI command hierarchy” on page 207.

## 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.
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$

Configuring a connection between an Enforcer appliance and a Symantec Endpoint Protection Manager

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 external NICs on the Enforcer appliance.

See “Installing an Enforcer appliance” on page 75.

If you want to establish communication between an Enforcer appliance and the Symantec Endpoint Protection Manager on an Enforcer console, you need to have the following information on hand:

- 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 to which you want to assign the Enforcer appliance on the console of an Enforcer appliance, the
Enforcer group name is automatically registered 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 80.

- 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

   ```
   spm ip ipaddress group Enforcer group name http port number key encrypted password
   ```

   See “Configure SPM” on page 253.

   You can use the following example as a guideline:

   ```
   spm ip 192.168.0.64 group CorpAppliance http 80 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 80 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 85.

4  Configure, deploy, and install or download client software if you have not already done so.

See the Installation Guide for Symantec Endpoint Protection and Symantec Network Access Control for more information about configuration, deployment, and installation of a Symantec Endpoint Protection or a Symantec Network Access Control client, also known as a managed client.

If you want guests—also known as unmanaged client computers—to be able to automatically download Symantec Network Access Control On-Demand Clients on Windows and Macintosh platforms, you need to configure a Gateway or a DHCP Enforcer to manage the automatic downloading process.

See “Enabling Symantec Network Access Control On-Demand clients to temporarily connect to a network ” on page 197.

**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 82.

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 80:

```
Enforcer#: show status
Enforcer Status: ONLINE(ACTIVE)
Policy Manager Connected: YES
Policy Manager: 192.168.0.1 HTTP 80
Packets Received: 3659
Packets Transmitted: 3615
Packet Receive Failed: 0
Packet Transfer Failed: 0
Enforcer Health: EXCELLENT
Enforcer Uptime: 10 days 01:10:55
```

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

Enforcer reports and debug logs

You can view the Enforcer reports and the debug logs on the Symantec Endpoint
Protection Manager Console as well as on the Enforcer console.

See “About Enforcer reports” on page 407.
See “About Enforcer logs” on page 408.
Configuring the Symantec Gateway Enforcer appliance on the Symantec Endpoint Protection Manager Console

This chapter includes the following topics:

- About configuring the Symantec Gateway Enforcer appliance on the Symantec Endpoint Protection Manager Console
- Changing Gateway Enforcer appliance configuration settings on a management server
- Using general settings
- Using authentication settings
- Authentication range settings
- Using advanced Gateway Enforcer appliance settings
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 the *Installation Guide for Symantec Endpoint Protection and Symantec Network Access Control*.
  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 “To set up an Enforcer appliance” on page 76.

- Configure the Symantec Gateway Enforcer appliance on the local Gateway Enforcer console during the installation.
  See “To configure an Enforcer appliance” on page 78.

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 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 the Protection Manager in order 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 start enforcement.

Changing Gateway Enforcer appliance configuration settings on a management server

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 the Symantec Endpoint Protection Manager Console

1. In the Symantec Endpoint Protection Manager Console, click **Admin**.
2. In the Admin page, click **Servers**.
3. In the Admin page, under View 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. In the Admin page, under View Servers, select the Gateway Enforcer appliance for which the configuration settings must be changed.
5 In the Admin page, 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></td>
<td>See “Using general settings” on page 91.</td>
</tr>
<tr>
<td>Authentication</td>
<td>Settings for a variety of parameters that affect the client authentication process.</td>
</tr>
<tr>
<td></td>
<td>If a matching address is still not found, the Gateway Enforcer appliance begins the authentication session and sends the challenge packet.</td>
</tr>
<tr>
<td></td>
<td>See “Using authentication settings” on page 94.</td>
</tr>
<tr>
<td>Auth Range</td>
<td>Settings that specify an individual IP address for a client or IP ranges for clients who need to be authenticated. You can also specify an individual IP address or IP ranges for the clients that are allowed to connect to a network without authentication.</td>
</tr>
<tr>
<td></td>
<td>See “Authentication range settings” on page 107.</td>
</tr>
<tr>
<td>Advanced</td>
<td>Settings for authentication timeout parameters and Gateway Enforcer appliance message timeouts.</td>
</tr>
<tr>
<td></td>
<td>Settings for MAC addresses for the trusted hosts that the Gateway Enforcer appliance allows to connect without authentication (optional).</td>
</tr>
<tr>
<td></td>
<td>Settings for DNS Spoofing and Local Authentication.</td>
</tr>
<tr>
<td></td>
<td>Settings for protocols to be allowed without blocking clients.</td>
</tr>
<tr>
<td>Log Settings</td>
<td>Settings for enabling logging of Server logs, Client Activity logs, and specifying log file parameters.</td>
</tr>
<tr>
<td></td>
<td>See “About Enforcer reports” on page 407.</td>
</tr>
<tr>
<td></td>
<td>See “About Enforcer logs” on page 408.</td>
</tr>
<tr>
<td></td>
<td>See “Configuring Enforcer log settings” on page 411.</td>
</tr>
</tbody>
</table>
Using general settings

You can add or edit the description of a Gateway Enforcer appliance or a Gateway Enforcer appliance group in the Symantec Endpoint Protection Manager Console.

See “Adding or editing the description of a Gateway Enforcer appliance group” on page 91.

See “Adding or editing the description of a Gateway Enforcer appliance” on page 92.

You cannot add or edit the name of a Gateway Enforcer appliance group in the Symantec Endpoint Protection Manager Console. You cannot add or edit the IP address or host name of a Gateway Enforcer appliance in the Symantec Endpoint Protection Manager Console. Instead, you must perform these tasks on the Enforcer console.

You can add or edit the IP address or host name of a Gateway Enforcer appliance in a management server list.

See “Adding or editing the IP address or host name of a Gateway Enforcer appliance” on page 92.

You can also add or edit the IP address or host name of a Symantec Endpoint Protection Manager in a management server list.

See “Establishing communication between a Gateway Enforcer appliance and a Symantec Endpoint Protection Manager through a management server list” on page 93.

Adding or editing the description of a Gateway Enforcer appliance group

You can add or edit the description of an Enforcer group of which a Symantec Gateway Enforcer appliance is a member. You can perform this task on the Symantec Endpoint Protection Manager Console instead of the Enforcer console.

To add or edit the description of a Gateway Enforcer appliance group

1 In the Symantec Endpoint Protection Manager Console, click Admin.
2 In the Admin page, click Servers.
3 In the Admin page, under View Servers, select and expand the Gateway Enforcer appliance group whose description you want to add or edit.
4 In the Admin page, under Tasks, click Edit Group Properties.
Adding or editing the description of a Gateway Enforcer appliance

Adding or editing the IP address or host name of a Gateway Enforcer appliance
Establishing communication between a Gateway Enforcer appliance and a Symantec Endpoint Protection Manager through a management server list

Gateway Enforcer appliances must be able to connect to servers on which the Symantec Endpoint Protection Manager is installed. The Symantec Endpoint Protection Manager includes a file that helps manage the traffic between clients, Symantec Endpoint Protection Managers, and optional Enforcers such as a Gateway Enforcer appliance.

This file is called a management server list. The management server list specifies to which Symantec Endpoint Protection Manager server a Gateway Enforcer connects. It also specifies to which Symantec Endpoint Protection server a Gateway 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 Symantec Endpoint Protection Managers 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 Gateway Enforcer appliances can connect after the initial installation. You may want to create a custom management server list before you deploy any Gateway Enforcer appliances. If you create a custom management server list, you can specify the priority in which a Gateway Enforcer appliance can connect to management servers.

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 Gateway Enforcer appliance to connect. If there is only one management server at a site, then you can select the default management server list.

See the Administration Guide for Symantec Endpoint Protection and Symantec Network Access Control for more information on how to customize management server lists.

To establish communication between a Gateway Enforcer between a Symantec Endpoint Protection Manager

1. In the Symantec Endpoint Protection Manager Console, click Admin.
2. In the Admin page, click Servers.
3. In the Admin page, under View Servers, select and expand the group of Enforcers.

The Enforcer group must include the Gateway Enforcer appliance for which you want to change the IP address or host name in a management server list.
Using authentication settings

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.

About using authentication settings

You may want to implement a number of authentication settings to further secure the network.

Table 6-1 provides more information about the options on the Authentication tab.

Table 6-1 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 99. |
### Table 6-1: Authentication configuration settings for a Gateway Enforcer appliance (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time between packets in authentication session (seconds)</td>
<td>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 100.</td>
</tr>
<tr>
<td>Time rejected client will be blocked (seconds)</td>
<td>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 101.</td>
</tr>
<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 101.</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 102.</td>
</tr>
</tbody>
</table>
Table 6-1  Authentication configuration settings for a Gateway Enforcer appliance (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Allow all clients with non-Windows operating systems | 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 103. |
| 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 is successful, 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 “Having the Gateway Enforcer appliance check the policy serial number on a client” on page 104. |
| 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.  
See “Sending a message from a Gateway Enforcer appliance to a client about non-compliance” on page 105. |
Table 6-1 Authentication configuration settings for a Gateway Enforcer appliance (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 106. |
| HTTP redirect URL                                 | 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 http://localhost.  
See “Redirecting HTTP requests to a Web page” on page 106. |
| HTTP redirect port                                | 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 106. |

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.
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.

About client authentication on a Gateway Enforcer appliance

The Gateway Enforcer appliance authenticates remote clients before allowing 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 does not have a trusted IP address, the Gateway Enforcer appliance then checks to see if the trusted IP address is within the client IP range for the clients that should be authenticated. If the client’s IP address is within the client IP 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.

**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.

**To specify the maximum number of challenge packets during an authentication session**

1. In the Symantec Endpoint Protection Manager Console, click **Admin**.
2. In the Admin page, click **Servers**.
3. In the Admin page, under View Servers, 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.
4. In the Admin page, under Tasks, click **Edit Group Properties**.
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 In the Gateway 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 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.

To specify the frequency of challenge packets to be sent to clients

1 In the Symantec Endpoint Protection Manager Console, click Admin.

2 In the Admin page, click Servers.

3 In the Admin page, under View Servers, 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 In the Admin page, under Tasks, click Edit Group Properties.

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.

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. In the Admin page, click **Servers**.
3. In the Admin page, under View 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. In the Admin page, 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.
   
   The default setting is 30 seconds. The range is 10 through 300 seconds.
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.

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. In the Admin page, click **Servers**.
3 In the Admin page, under View 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 In the Admin page, 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 client. Because the client does not run on non-Windows operating systems such as Linux or Solaris, the Gateway Enforcer appliance blocks these clients. 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 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 the Symantec Endpoint Protection Manager Console, click **Admin**.

2 In the Admin page, click **Servers**.
3 In the Admin page, under View Servers, 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.

4 In the Admin page, under Tasks, click Edit Group Properties.

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 Authentication 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 48.

### 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 In the Admin page, under View 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 In the Admin page, 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**.

### Having the Gateway Enforcer appliance check 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, the Gateway Enforcer appliance retrieves the Policy Serial Number from the Symantec Endpoint Protection Manager. The Gateway Enforcer appliance then 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.
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. In the Admin page, under View Servers, 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 an end user that they cannot connect to the network. The message typically tells the end 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 end 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 provided the Windows Messenger service is running on the client.

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. In the Admin page, click **Servers**.

3. In the Admin page, under View Servers, select and expand the group of Enforcers.

4. In the Admin page, under Tasks, click **Edit Group Properties**.

5. In the Settings dialog box, on the Authentication tab, check **Enable pop-up message on 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.
To redirect HTTP requests to a Web page

1. In the Symantec Endpoint Protection Manager Console, click **Admin**.
2. In the Admin page, click **Servers**.
3. In the Admin page, under View Servers, select and expand the group of Gateway Enforcer appliances.
4. In the Admin page, under Tasks, click **Edit Group Properties**.
5. In the Gateway Settings dialog box, on the Authentication tab, check **Check 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 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.

   It also uses the Gateway Enforcer pop-up message as the HTML body for the first HTML page sent 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
- External IP addresses that the Gateway Enforcer appliance does not authenticate
- Internal IP address to which the Gateway Enforcer allows access

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 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 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 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 ranges compared to trusted external IP addresses**

The Client IP Range is similar to what is called a Black List. 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 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 Range, which tells the Gateway Enforcer appliance to only validate the clients in the Client IP Range.

**When to use client IP ranges**

Client IP 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 range are allowed to pass through the Gateway Enforcer appliance without requiring the client software or other authentication.

The reasons for using Client IP Ranges include:

- Allowing network access to external Web sites
- Authenticating a subset of clients
Allow network access to external Web sites

One reason for using Client IP 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 Range.

The Client IP 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 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 range. Therefore the internal user does not need to be authenticated.

Authentication of a subset of clients

You may want the Gateway Enforcer appliance to authenticate a limited subset of clients. This is especially useful when clients are deployed over a long period of time.

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 requiring authentication. As the client is installed on other clients, you can add their addresses to the Client IP Range or use a different authentication strategy.

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.

- **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.
You can add trusted IP addresses of both type by on the Symantec Endpoint Protection Manager Console. Traffic to the Symantec Endpoint Protection Manager 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, such as certain servers, 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.

**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 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 or 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 under the following circumstances:
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 software that it needs. The Gateway Enforcer appliance allows the external client to get to a computer that is on the list of trusted internal IP addresses.

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 will authenticate.

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.

To restrict a client’s network access despite authentication

1 In the Symantec Endpoint Protection Manager Console, click Admin.
2 In the Admin page, click Servers.
3 In the Admin page, under View Servers, select and expand the Gateway Enforcer appliance groups.
4 In the Admin page, under Tasks, click Edit Group Properties.
5 In the Gateway Settings dialog box, on the Auth Range tab, in the Authenticate Client IP 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 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 range
   ■ An IP address plus subnet mask

9 Type either a single IP address, a start and 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 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.

To edit client IP address ranges on the list of addresses that require authentication

1 In the Symantec Endpoint Protection Manager Console, click Admin.

2 In the Admin page, click Servers.

3 In the Admin page, under View Servers, 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 In the Admin page, under Tasks, click Edit Group Properties.

6 In the Gateway Settings dialog box, on the Auth Range tab, in the Client IP 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.

**To remove client IP address ranges from the list of addresses that require authentication**

1. In the Symantec Endpoint Protection Manager Console, click **Admin**.
2. In the Admin page, click **Servers**.
3. In the Admin page, under View Servers, 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. In the Admin page, under Tasks, click **Edit Group Properties**.
6. In the Gateway Settings dialog box, on the Auth Range tab, in the Client IP 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 the Symantec Endpoint Protection Manager needs to be specified as a trusted internal IP address of the other Gateway Enforcer appliance. If a client first fails a Host Integrity check and then passes it, you may have up to a five-minute delay before a client can connect to the network.

**To add a trusted internal IP address for clients on a management server**

1. In the Symantec Endpoint Protection Manager Console, click **Admin**.
2. In the Admin page, click **Servers**.
3. In the Admin page, under View Servers, 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 In the Admin page, under Tasks, click Edit Group Properties.

6 In the Gateway Settings dialog box, on the Auth Range tab, in the Trusted IP Range area, select Trusted Internal IP 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.

To specify trusted external IP addresses

1 In the Symantec Endpoint Protection Manager Console, click Admin.

2 In the Admin page, click Servers.

3 In the Admin page, under View Servers, select and expand the group of Enforcers.

4 Select the group of Enforcers for which you want to specify trusted external IP addresses.

5 In the Admin page, under Tasks, click Edit Group Properties.

6 In the Gateway Settings dialog box, on the Auth Range tab, in the Trusted IP Range area, select Trusted External IP 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.

**To edit a trusted internal or external IP address**

1  In the Symantec Endpoint Protection Manager Console, click **Admin**.

2  In the Admin page, click **Servers**.

3  In the Admin page, under View Servers, 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  In the Admin page, under Tasks, click **Edit Group Properties**.

6  In the Gateway Settings dialog box, on the Auth Range tab, in the Trusted IP Range area, select Trusted External IP Range or Trusted External IP Range from the drop-down list.

   The addresses for the selected type appear in the table.

7  In the **Trusted IP Range** table, click anywhere in the column of IP addresses and click **Edit all**.

8  In the IP Address Editor dialog box, locate any addresses you want to change and edit them.

9  Click **OK**.

10  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, you can remove the IP address from the Trusted Internal IP Address table.

**To remove a trusted internal IP or trusted external IP address**

1  In the Symantec Endpoint Protection Manager Console, click **Admin**.

2  In the Admin page, click **Servers**.
3 In the Admin page, under View Servers, 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 In the Admin page, under Tasks, click **Edit Group Properties**.

6 In the Gateway Settings dialog box, on the Auth Range tab, in the Trusted IP Range area, select Trusted External IP Range or Trusted External IP 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 range checking order

If both Client IP 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 Range is enabled, the Gateway Enforcer appliance checks the Client IP Range table for an address matching the source IP of the client.
- If the Client IP Range does not include an IP address for that client, the Gateway Enforcer appliance allows the client without authentication.
- If the Client IP Range does include an IP address for that client, the Gateway Enforcer appliance next checks the Trusted External IP Range for a matching address.
- If an address matching the client is found in the Trusted External IP Range, the Gateway Enforcer appliance allows the client.
- If no matching address is found in the Trusted External IP Range, the Gateway Enforcer appliance then checks the destination address against the Trusted Internal IP Range list and the list of Symantec Endpoint Protection Managers. If a matching address is still not located, the Gateway Enforcer appliance begins the authentication session and sends the challenge packet.

### Using 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 117.

- Allowing legacy clients

See “Allowing a legacy client to connect to the network with a Gateway Enforcer appliance” on page 118.

- Enabling local authentication

See “Enabling local authentication on a Gateway Enforcer appliance” on page 119.

When you apply the settings, the changes that have 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.

**To specify packet types and protocols**

1. In the Symantec Endpoint Protection Manager Console, click **Admin**.
2. In the Admin page, click **Servers**.
3. In the Admin page, under View Servers, 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. In the Admin page, 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 the 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.

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.

To allow a legacy client to connect to the network with a Gateway Enforcer appliance
1 In the Symantec Endpoint Protection Manager Console, click Admin.
2 In the Admin page, click Servers.
3 In the Admin page, under View Servers, select and expand the group of Gateway Enforcers appliances.
4 In the Admin page, under Tasks, click Edit Group Properties.
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.

To enable local authentication on a Gateway Enforcer appliance

1. In the Symantec Endpoint Protection Manager Console, click Admin.
2. In the Admin page, click Servers.
3. In the Admin page, under View Servers, select and expand the group of Gateway Enforcers appliances.
4. In the Admin page, under Tasks, click Edit Group Properties.
5. In the Settings dialog box, on the Advanced tab, check Enable Local Authentication.
6. Click OK.
Configuring the Symantec Gateway Enforcer appliance on the Symantec Endpoint Protection Manager Console

Using advanced Gateway Enforcer appliance settings
Configuring the Symantec DHCP Enforcer appliance on the Symantec Endpoint Protection Manager Console

This chapter includes the following topics:

- About configuring the Symantec DHCP Enforcer appliance on the Symantec Endpoint Protection Manager Console
- Changing DHCP Enforcer appliance configuration settings on a management server
- Using general settings
- Using authentication settings
- Using DHCP servers settings
- Using advanced DHCP Enforcer appliance settings
About configuring the Symantec DHCP Enforcer appliance on the Symantec Endpoint Protection Manager Console

You can add or edit the configuration settings for the DHCP 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 the *Installation Guide for Symantec Endpoint Protection and Symantec Network Access Control*.
  The computer on which the Symantec Endpoint Protection Manager software is installed is also referred to as the management server.

- Connect the Symantec DHCP Enforcer appliance to the network.
  See “To set up an Enforcer appliance” on page 76.

- Configure the Symantec DHCP Enforcer appliance on the Enforcer console during the installation.
  See “To configure an Enforcer appliance” on page 78.

After you finish these tasks, you can specify additional configuration settings for the DHCP Enforcer appliance on a management server.

Changing DHCP Enforcer appliance configuration settings on a management server

You can change the DHCP Enforcer appliance configuration settings on a management server. The configuration settings are automatically downloaded from the management server to the DHCP Enforcer appliance during the next heartbeat.

To change DHCP Enforcer appliance configuration settings on a management server

1. In the Symantec Endpoint Protection Manager Console, click **Admin**.
2. In the Admin page, click **Servers**.
3. In the Admin page, under View Servers, select the DHCP Enforcer appliance group of which the DHCP Enforcer appliance is a member.

   The DHCP Enforcer appliance group must include the DHCP Enforcer appliances whose configuration settings need to be changed.
4 In the Admin page, under View Servers, select the DHCP Enforcer appliance whose configuration settings need to be changed.

5 In the Admin page, under Tasks, click **Edit Group Properties**.

6 In the Settings dialog box, change any of the configuration settings.

The DHCP Enforcer Settings dialog box provides the following categories of configuration settings:

<table>
<thead>
<tr>
<th>Category</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>Settings for the description of the DHCP Enforcer appliance group and management server list. See “Using general settings” on page 124.</td>
</tr>
<tr>
<td>Authentication</td>
<td>Settings for a variety of parameters that affect the client authentication process. See “Using authentication settings” on page 127.</td>
</tr>
<tr>
<td>DHCP Servers</td>
<td>Settings that specify the IP address, port number, and priority for normal and quarantine DHCP servers. This information is required. You must configure information about the DHCP server before you can begin enforcement. See “Using DHCP servers settings” on page 136.</td>
</tr>
<tr>
<td>Advanced</td>
<td>Settings for authentication timeout parameters and DHCP message timeouts. Settings for MAC addresses for the trusted hosts that the DHCP Enforcer appliance allows to connect without authentication (optional). Settings for DNS Spoofing, and Local Authentication. See “Using advanced DHCP Enforcer appliance settings” on page 140.</td>
</tr>
</tbody>
</table>
Using general settings

You can add or edit the description of a DHCP Enforcer or a DHCP Enforcer group in the Symantec Endpoint Protection Manager Console.

See “Adding or editing the name of an Enforcer group with a DHCP Enforcer” on page 124.

See “Adding or editing the description of an Enforcer group with a DHCP Enforcer” on page 124.

However, you cannot add or edit the name of a DHCP Enforcer group in the Symantec Endpoint Protection Manager Console. You cannot add or edit the IP address or host name of a DHCP Enforcer in the Symantec Endpoint Protection Manager Console. Instead, you must perform these tasks on the Enforcer console.

See “Adding or editing the IP address or host name of a DHCP Enforcer” on page 125.

You can also add or edit the IP address or host name of a Symantec Endpoint Protection Manager in a management server list.

See “Connecting the DHCP Enforcer to a Symantec Endpoint Protection Manager” on page 125.

Adding or editing the name of an Enforcer group with a DHCP Enforcer

You can add or edit the name of an Enforcer group of which a DHCP Enforcer appliance 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 the Enforcer Implementation Guide for Symantec Network Access Control for information on how to add or edit the name of an Enforcer group.

All Enforcers in a group share the same configuration settings.

Adding or editing the description of an Enforcer group with a DHCP Enforcer

You can add or edit the description of an Enforcer group of which a Symantec DHCP Enforcer appliance is a member. You can perform this task on the Symantec Endpoint Protection Manager Console instead of the DHCP Enforcer console.

To add or edit the description of an Enforcer group with a DHCP Enforcer

1 In the Symantec Endpoint Protection Manager Console, click Admin.
2 In the Admin page, click Servers.
3 In the Admin page, under View Servers, select and expand the Enforcer group whose description you want to add or edit.

4 In the Admin page, under Tasks, click **Edit Group Properties**.

5 In the Settings dialog box, on the Basic Settings tab, add or edit a description for the Enforcer group in the Description field.

6 In the Settings dialog box, click **OK**.

Adding or editing the IP address or host name of a DHCP Enforcer

You can only change the IP address or host name of a DHCP Enforcer on the Enforcer console during the installation. Later, if you want to change the IP address or host name of a DHCP Enforcer, you can do so on the DHCP Enforcer console.

See the *Enforcer Implementation Guide for Symantec Network Access Control* for more information.

Adding or editing the description of a DHCP Enforcer

You can add or edit the description of a DHCP Enforcer. You can perform this task on the Symantec Endpoint Protection Manager Console instead of the DHCP Enforcer console. After you complete this task, the description appears in the Description field of the Management Server pane.

**To add or edit the description of a DHCP Enforcer**

1 In the Symantec Endpoint Protection Manager Console, click **Admin**.

2 In the Admin page, click **Servers**.

3 In the Admin page, under View Servers, select and expand the Enforcer group that includes the DHCP Enforcer whose description you want to add or edit.

4 In the Admin page, under View Servers, select the DHCP Enforcer whose description you want to add or edit.

5 In the Admin page, under Tasks, click **Edit Enforcer Properties**.

6 In the Enforcer Properties dialog box, add or edit a description for the DHCP Enforcer in the Description field.

7 In the Enforcer Properties dialog box, click **OK**.

Connecting the DHCP Enforcer to a Symantec Endpoint Protection Manager

Enforcers must be able to connect to servers on which the Symantec Endpoint Protection Manager is installed. The Symantec Endpoint Protection Manager
includes a file that helps manage the traffic between clients, Symantec Endpoint Protection Managers, and optional Enforcers such as a DHCP Enforcer.

This file is called a management server list. The management server list specifies to which Symantec Endpoint Protection Manager server a DHCP Enforcer connects. It also specifies to which Symantec Endpoint Protection server a DHCP 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 Symantec Endpoint Protection Managers 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 DHCP 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 a DHCP 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 DHCP Enforcer to connect. If there is only one management server at a site, then you can select the default management server list.

See the Administration Guide for Symantec Endpoint Protection and Symantec Network Access Control for more information on how to customize management server lists.

**To connect the DHCP Enforcer to a Symantec Endpoint Protection Manager**

1. In the Symantec Endpoint Protection Manager Console, click **Admin**.
2. In the Admin page, click **Servers**.
3. In the Admin page, under View Servers, select and expand the group of Enforcers.
   
   The Enforcer group must include the DHCP Enforcer for which you want to change the IP address or host name in a management server list.
4. In the Admin page, under Tasks, click **Edit Group Properties**.
5. In the Settings dialog box, on the Basic Settings tab, under Communication, select the management server list that you want this DHCP Enforcer to use.
6. In the Settings dialog box, on the Basic Settings tab, under Communication, click **Preview**.

   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 Settings dialog box, click **OK**.

**Using authentication settings**

You can specify a number of authentication settings for a DHCP Enforcer authentication session. When you apply these changes, they are automatically sent to the selected DHCP 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 7-1 provides more information about the options on the Authentication tab.

**Table 7-1** Authentication configuration settings for a DHCP Enforcer

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum number of packets per authentication session</td>
<td>The maximum number of challenge packets that the DHCP Enforcer sends in each authentication session. The default number is 10.</td>
</tr>
<tr>
<td></td>
<td>See “Specifying the maximum number of challenge packets during an authentication session” on page 130.</td>
</tr>
<tr>
<td>Time between packets in authentication session</td>
<td>The time (in seconds) between each challenge packet that the Enforcer sends. The default value is 3.</td>
</tr>
<tr>
<td></td>
<td>See “Specifying the frequency of challenge packets to be sent to clients” on page 131.</td>
</tr>
<tr>
<td>Allow all clients, but continue to log which clients are not authenticated</td>
<td>If this option is enabled, the Enforcer authenticates all users by checking that they are running a client. The DHCP Enforcer also checks if the client passed the Host Integrity check. If the client passes the Host Integrity check, the DHCP Enforcer then logs the results. It then forwards the DHCP 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 132.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Allow all clients with non-Windows operating systems</td>
<td>If this option is enabled, the DHCP Enforcer checks for the operating system of the client. The DHCP 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 133.</td>
</tr>
<tr>
<td>Check Policy Serial Number on Client before allowing Client into network</td>
<td>If this option is enabled, the DHCP 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 DHCP Enforcer notifies the client to update its security policy. The client then forwards the DHCP request to receive a quarantine network configuration. If this option is not enabled and the Host Integrity check is successful, the DHCP Enforcer forwards the DHCP request to receive a normal network configuration. The DHCP Enforcer forwards the DHCP request even if the client does not have the latest security policy. The default setting is not enabled. See “Having the DHCP Enforcer check the Policy Serial Number on a client” on page 134.</td>
</tr>
<tr>
<td>Enable pop-up message on client if Client is not running</td>
<td>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. See “Sending a message from a DHCP Enforcer appliance to a client about non-compliance” on page 135.</td>
</tr>
</tbody>
</table>
About Authentication sessions

When a client tries to access the internal network, the DHCP Enforcer appliance first detects whether the client is running a client. If it is, the DHCP Enforcer appliance 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 DHCP Enforcer appliance for its authentication process.

The DHCP Enforcer appliance then begins its authentication session with the client. An authentication session is a set of challenge packets that the DHCP Enforcer appliance sends to a client.

During the authentication session, the DHCP Enforcer appliance sends a challenge packet to the client at a specified frequency.

The default setting is every three seconds.

The DHCP Enforcer appliance continues to send packets until one of the following conditions are met:

- The DHCP Enforcer appliance receives a response from the client
- The DHCP Enforcer appliance has sent the maximum number of packets specified.
  
  The default setting is 10.

The frequency (3 seconds) times the number of packets (10) is the value that is used for the DHCP Enforcer appliance's heartbeat. The heartbeat is the interval that the DHCP Enforcer appliance allows the client to remain connected before it starts a new authentication session.

The default setting is 30 seconds.

The client sends information to the DHCP Enforcer appliance that contains the following items:

- Unique identification (UID)
- Its current Profile Serial Number
- The results of the Host Integrity check

The DHCP Enforcer appliance verifies the client UID and the Policy Serial Number with the Symantec Endpoint Protection Manager. If the client is updated with the latest security policies, its Policy Serial Number matches the one that the DHCP Enforcer appliance receives from the management server. The Host Integrity check results show whether or not the client complies with the current security policies.

If the client information passes the authentication requirements, the DHCP Enforcer appliance forwards its DHCP request to the DHCP server. The DHCP
Enforcer appliance expects to receive a normal DHCP network configuration. Otherwise the DHCP Enforcer appliance forwards it to the quarantine DHCP server to receive a quarantine network configuration.

You can install one DHCP server on one computer and configure it to provide both a normal and a quarantine network configuration. See “Installation planning for a DHCP Enforcer appliance” on page 52.

After the heartbeat interval or whenever the client tries to renew its IP address, the DHCP Enforcer appliance starts a new authentication session. The client must respond to retain the connection to the internal network.

The DHCP Enforcer appliance disconnects the clients that do not respond.

For the clients that were previously authenticated but now fail authentication, the DHCP Enforcer appliance sends a message to the DHCP server. The message is a request for the release of the current IP address. The DHCP Enforcer appliance then sends a DHCP message to the client. The client then sends a request for a new IP address and network configuration to the DHCP Enforcer appliance. The DHCP Enforcer forwards this request to the quarantine DHCP server.

Specifying the maximum number of challenge packets during an authentication session

During the authentication session, the DHCP Enforcer appliance sends a challenge packet to the client at a specified frequency.

The DHCP Enforcer appliance continues to send packets until the following conditions are met:

- The DHCP Enforcer appliance receives a response from the client
- The DHCP Enforcer appliance has sent the specified maximum number of packets.

The default setting for the maximum number of challenge packets for an authentication session: 10.

To specify the maximum number of challenge packets during an authentication session

1. In the Symantec Endpoint Protection Manager Console, click Admin.
2. In the Admin page, click Servers.
In the Admin page, under View Servers, select and expand the group of Enforcers. The DHCP Enforcer appliance group must include the DHCP Enforcer for which you want to specify the maximum number of challenge packets during an authentication session.

In the Admin page, under Tasks, click Edit Group Properties.

On the Authentication tab, under Authentication Parameters, type the maximum number of packets to be allowed during an authentication session in the field **Maximum number of packets per authentication session**. The default setting is 10.

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 DHCP Enforcer appliance sends a challenge packet to the client at a specified frequency. The DHCP Enforcer appliance continues to send packets until the following conditions are met:

- The DHCP Enforcer appliance receives a response from the client
- The DHCP Enforcer appliance has sent the specified maximum number of packets.

The default setting is every 3 seconds.

To **specify the frequency of challenge packets to be sent to clients**

1. In the Symantec Endpoint Protection Manager Console, click **Admin**.
2. In the Admin page, click **Servers**.
3. In the Admin page, under View Servers, select and expand the group of Enforcers.

   The DHCP Enforcer appliance group must include the DHCP Enforcer appliance for which you want to specify the frequency of challenge packets to be sent to clients.
4. In the Admin page, under Tasks, click **Edit Group Properties**.
5 On the Authentication tab, under Authentication Parameters, type the maximum number of challenge packets the DHCP Enforcer is to keep sending to a client during an authentication session in the field Time between packets in authentication session.

The default setting is 10.

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 DHCP Enforcer appliance to allow all clients to connect to the network after you distribute the client package to all users. These users all connect to a DHCP server at the location of this DHCP Enforcer appliance.

The DHCP Enforcer appliance still authenticates all users by checking that they are running a client, checking Host Integrity, and logging the results. It forwards the DHCP requests to receive the normal DHCP server network configuration instead of the quarantine network configuration. 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 the Symantec Endpoint Protection Manager Console, click Admin.

2 In the Admin page, click Servers.

3 In the Admin page, under View Servers, select and expand the group of Enforcers.

The Enforcer group must include the DHCP Enforcer for which you want to allow all clients while continuing the logging of non-authenticated clients.

4 In the Admin page, under Tasks, click Edit Group Properties.
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 Click **OK**.

### Allowing non-Windows clients to connect to a network without authentication

The DHCP 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 DHCP 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 normal DHCP server without authentication.

**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 In the Admin page, under View Servers, select and expand the group of Enforcers.

   The DHCP Enforcer appliance group must include the DHCP Enforcer appliance for which you want to allow all non-Windows clients to connect to a network.

4 In the Admin page, 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**.
Having the DHCP Enforcer check 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 DHCP Enforcer appliance, the DHCP Enforcer appliance retrieves the Policy Serial Number from the Symantec Endpoint Protection Manager. The DHCP Enforcer appliance then compares the Policy Serial Number with the one that it receives from the client. If the Policy Serial Numbers match, the DHCP 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 normal DHCP server. If the client does not have the latest security policy, the client is notified to download the latest policy. The DHCP Enforcer appliance 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 DHCP Enforcer 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. In the Admin page, under View Servers, select and expand the group of Enforcers.
   The DHCP Enforcer appliance group must include the DHCP 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 DHCP Enforcer appliance to a client about non-compliance

You can inform the client that cannot connect to the network with a Windows pop-up message. The message typically tells the end user that a client cannot connect to the network. The client cannot connect to the network because it does not run the Symantec Endpoint Protection client or 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 end 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 provided the Windows Messenger service is running on the client.

To send a message from a DHCP Enforcer appliance to a client about non-compliance

1. In the Symantec Endpoint Protection Manager Console, click **Admin**.
2. In the Admin page, click **Servers**.
3. In the Admin page, under View Servers, select and expand the group of Enforcers.
4. In the Admin page, under Tasks, click **Edit Group Properties**.
5. In the Settings dialog box, on the Authentication tab, check **Enable pop-up message on client if Client is not running**.
6. In the Settings dialog box, on the Authentication tab, click **Message**.
7. In the Pop-up Message Settings dialog box, select how often the message is to appear on a client.

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 In the Pop-up Message Settings dialog box, click OK.

10 In the Settings dialog box, on the Authentication tab, click OK.

Using DHCP servers settings

You can specify a number of DHCP server settings. When you apply these changes, they are automatically sent to the selected DHCP Enforcer appliance during the next heartbeat.

About using DHCP servers settings

You can specify up to 256 DHCP servers. If you specify multiple DHCP servers, you can provide failover and load balancing. You can use the DHCP Server Priority setting to have the DHCP Enforcer appliance send DHCP requests to multiple DHCP servers at the same time.

You can also set up normal and quarantine DHCP servers on separate computers or on one computer. If a client is authorized to connect to the network, the normal DHCP server assigns an IP address to the client. If you set up a quarantine DHCP server, an unauthorized client can still connect to the network. However, the unauthorized client can only communicate with limited computers in the network. See “Adding a normal DHCP server” on page 138.

See “Adding a quarantine DHCP server” on page 139.

If you plan to set up a normal and quarantine DHCP server on the same computer, you must check the Enable User Class ID option.

If you check the Enable User Class ID option, the DHCP Enforcer appliance adds a quarantine user class in the DHCP messages. These DHCP messages are forwarded to the DHCP server. The DHCP server then assigns the quarantine configuration to the client that is based on the presence of this user class ID. You
can use one DHCP server that functions as both a normal and as a quarantine DHCP server.

See “Combining a normal and a quarantine DHCP server on one computer” on page 137.

If you uncheck the Enable User Class ID option, you need to set up two separate DHCP servers. One of the DHCP servers functions as a normal DHCP server. The second DHCP server functions as a quarantine DHCP server.

See “Enabling separate normal and quarantine DHCP servers” on page 137.

Combining a normal and a quarantine DHCP server on one computer

The Enable User Class ID option enables you to set up a normal and a quarantine DHCP server on one computer. You therefore need fewer computers to achieve maximum security.

To combine a normal and a quarantine DHCP server on one computer

1. In the Symantec Endpoint Protection Manager Console, click Admin.
2. In the Admin page, click Servers.
3. In the Admin page, under View Servers, select and expand the group of Enforcers.
4. In the Admin page, under Tasks, click Edit Group Properties.
5. In the Settings dialog box, on the DHCP Servers tab, check Enable User Class ID.
6. In the Settings dialog box, on the DHCP Servers tab, click OK.

Enabling separate normal and quarantine DHCP servers

The Enable User Class ID option enables you to set up separate normal DHCP servers as well as quarantine DHCP servers. You therefore can achieve maximum security if the traffic in a network demands it.

To enable separate normal and quarantine DHCP servers

1. In the Symantec Endpoint Protection Manager Console, click Admin.
2. In the Admin page, click Servers.
3. In the Admin page, under View Servers, select and expand the group of Enforcers.
4. In the Admin page, under Tasks, click Edit Group Properties.
In the Settings dialog box, on the DHCP Servers tab, uncheck **Enable User Class ID**.

Click **OK**.

### Adding a normal DHCP server

The information for the normal DHCP server appears as a row in a table in the Settings dialog box.

**To add a normal DHCP server**

1. In the Symantec Endpoint Protection Manager Console, click **Admin**.
2. In the Admin page, click **Servers**.
3. In the Admin page, under View Servers, select and expand the group of Enforcers.
4. In the Admin page, under Tasks, click **Edit Group Properties**.
5. In the Settings dialog box, on the DHCP Servers tab, under Normal DHCP Servers, click **Add**.
6. In the Add DHCP Server dialog box, check **Enable** if not already checked.
7. Type the IP address or host name of the DHCP server in the DHCP server IP text box.
8. Type the port number of the DHCP server in the DHCP server port text box. The default port setting on the DHCP server is 67.
Select the Priority Number for the DHCP server in the DHCP server priority text box.

The default setting for the Priority is 1.

If you use one DHCP server on one computer as both a normal and quarantine DHCP server, add the DHCP server in this dialog box as both a normal and quarantine DHCP server. You fill in the same information in the Add DHCP Server dialog box for both types of DHCP servers.

You can assign a priority from 0 through 15 to a DHCP server. This setting is used for load balancing. If you configure two DHCP servers with the same priority, the DHCP Enforcer forwards the request to both DHCP servers at the same time. If one DHCP server is busy, the other can respond. If you configure multiple DHCP servers with different priorities, the DHCP Enforcer first forwards DHCP requests to the DHCP server that has the highest priority. The DHCP server then forwards the DHCP requests to the others.

Click OK.

In the Settings dialog box, on the DHCP Servers tab, click OK.

Adding a quarantine DHCP server

The information for the normal DHCP server appears as a row in a table in the Settings dialog box.

To add a quarantine DHCP server

1. In the Symantec Endpoint Protection Manager Console, click Admin.
2. In the Admin page, click Servers.
3. In the Admin page, under View Servers, select and expand the group of Enforcers.
4. In the Admin page, under Tasks, click Edit Group Properties.
5. In the Settings dialog box, on the DHCP Servers tab, under Quarantine DHCP Servers, click Add.
6. In the Add DHCP Server dialog box, check Enable if not already checked.
7. Type the IP address or host name of the DHCP server in the DHCP server IP text box.
8. Type the port number of the DHCP server in the DHCP server port text box. The default port setting on the DHCP server is 67.
9 Select the Priority Number for the DHCP server in the DHCP server priority text box.

The default setting for the Priority is 1.

If you use one DHCP server on one computer as both a normal and quarantine DHCP server, add the DHCP server in this dialog box as both a normal and quarantine DHCP server. You fill in the same information in the Add DHCP Server dialog box for both types of DHCP servers.

You can assign a priority from 0 through 15 to a DHCP server. This setting is used for load balancing. If you configure two DHCP servers with the same priority, the DHCP Enforcer forwards the request to both DHCP servers at the same time. If one DHCP server is busy, the other can respond. If you configure multiple DHCP servers with different priorities, the DHCP Enforcer appliance first forwards the DHCP requests to the DHCP server that has the highest priority and then to the others.

10 Click **OK**.

In the Settings dialog box, on the DHCP Servers tab, click **OK**.

---

Using advanced DHCP Enforcer appliance settings

You can configure the following advanced DHCP Enforcer appliance configuration settings:

- **Authentication timeout**
  
  See “Setting up an automatic quarantine for a client that fails authentication” on page 141.

- **DHCP message timeout**
  
  See “To specify a DHCP Enforcer appliance's wait period before grants a client access to the network” on page 141.

- **MAC addresses for the trusted hosts that the DHCP Enforcer allows to connect to the normal DHCP server without authentication**
  
  See “Enabling servers, clients, and devices to connect to the network as trusted hosts without authentication” on page 142.

- **Enabling DNS spoofing**
  
  See “Preventing DNS spoofing” on page 143.

- **Allowing legacy clients**
  
  See “Allowing a legacy client to connect to the network with a DHCP Enforcer appliance” on page 144.

- **Enabling local authentication**
See “Enabling local authentication on the DHCP Enforcer appliance” on page 144.

When you apply any of these configuration settings, the changes are sent to the selected DHCP Enforcer during the next heartbeat.

Setting up an automatic quarantine for a client that fails authentication

You can specify how long a DHCP Enforcer appliance waits for a response from a client. The response verifies whether or not the Symantec Endpoint Protection client or the Symantec Network Access Control client has been installed. If the DHCP Enforcer appliance considers that the client software has not been installed during the interval that you specify, the client is kept in quarantine.

To set up an automatic quarantine for a client that fails authentication

1. In the Symantec Endpoint Protection Manager Console, click **Admin**.
2. In the Admin page, click **Servers**.
3. In the Admin page, under View Servers, select and expand the group of Enforcers.
4. In the Symantec Endpoint Protection Manager Console, under View Servers, select the DHCP Enforcer appliance for which you want to set the configuration setting.
5. In the Admin page, under Tasks, click **Edit Group Properties**.
6. In the Settings dialog box, on the Advanced tab, under Timeout Parameters, check **Authentication timeout**.
   
   The default setting is three seconds.
7. Click **OK**.

Specifying a DHCP Enforcer appliance's wait period before it grants a client access to the network

You can specify how long a DHCP Enforcer appliance needs to wait for a response after it sends DHCP messages to a client or a DHCP server. If a DHCP Enforcer appliance does not receive a response after a designated interval, it resets its internal status about the client or DHCP server. Therefore the DHCP Enforcer appliance can only receive an initial message.

To specify a DHCP Enforcer appliance's wait period before grants a client access to the network

1. In the Symantec Endpoint Protection Manager Console, click **Admin**.
2. In the Admin page, click **Servers**.
3 In the Admin page, under View Servers, select and expand the group of Enforcers.

4 In the Admin page, under View Servers, select the DHCP Enforcer appliance for which you want to set the configuration setting.

5 In the Admin page, under Tasks, click **Edit Group Properties**.

6 In the Settings dialog box, on the Advanced tab, under Timeout Parameters, check **DHCP message timeout**.

   The default setting is three seconds.

7 Click **OK**.

### 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 DHCP 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 DHCP Enforcer appliance passes all DHCP messages from the trusted host to the normal DHCP server without authenticating the trusted host.

**To enable servers, clients, and devices to connect to the network as trusted hosts without authentication**

1 In the Symantec Endpoint Protection Manager Console, click **Admin**.

2 In the Admin page, click **Servers**.

3 In the Admin page, under View Servers, select and expand the group of Enforcers.

4 In the Admin page, under View Servers, select the DHCP Enforcer appliance that permits servers, clients, and the devices that have been designated as trusted hosts to connect to the network without authentication.

5 In the Admin page, under Tasks, click **Edit Group Properties**.

6 In the Settings dialog box, on the Advanced tab, under Trusted Hosts, 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.

You can also copy MAC addresses from a text file.

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-*66 does not represent the correct use of the wildcard character.

8 Click **OK**.

9 In the Settings dialog box, on the Advanced tab, click **OK**.

The MAC address for the trusted host that you added now appears in the Settings dialog box in the MAC Address area.

10 Click **OK**.

### Preventing DNS spoofing

You can attempt to prevent DNS spoofing. You accomplish this objective by having the DHCP Enforcer appliance modify the relevant DHCP messages that are sent to a client. The DHCP Enforcer appliance replaces the IP address of the DNS server in the DHCP message with the DHCP Enforcer appliance’s external IP address. Therefore the DHCP Enforcer appliance acts as a DNS server to the clients and thus prevents DNS spoofing. This feature must be enabled if you want to deliver Symantec Network Access Control On-Demand clients from a DHCP Enforcer.

**To prevent DNS spoofing**

1 In the Symantec Endpoint Protection Manager Console, click **Admin**.

2 In the Admin page, click **Servers**.

3 In the Admin page, under View Servers, select and expand the group of Enforcers.

4 In the Admin page, under Tasks, click **Edit Group Properties**.
In the Settings dialog box, on the Advanced tab, check **Enable DNS Spoofing.**

Use the Enforcer local IP address as the DNS request reply

The DHCP Enforcer appliance substitutes the officially-requested IP address with its own external IP address. The DHCP Enforcer appliance acts as a domain name server (DNS) when it replies to a DNS query by using the DHCP Enforcer appliance's own IP address.

Use the following IP addresses as DNS request reply

The DHCP Enforcer appliance substitutes the officially requested IP address with any of the IP addresses that you have specified. The DHCP Enforcer appliance acts as a domain name server (DNS) when it replies to a DNS query by using any of the IP addresses that you have specified.

Click **OK.**

### Allowing a legacy client to connect to the network with a DHCP Enforcer appliance

You can enable a DHCP Enforcer appliance to connect to 5.1.x legacy clients. If your network supports an 11.0.2 Symantec Endpoint Protection Manager, a Symantec DHCP 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 DHCP Enforcer appliance does not block them.

**To allow a legacy client to connect to the network with a DHCP Enforcer appliance**

1. In the Symantec Endpoint Protection Manager Console, click **Admin.**
2. In the Admin page, click **Servers.**
3. In the Admin page, under View Servers, select and expand the group of DHCP Enforcers appliances.
4. In the Admin page, 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 the DHCP Enforcer appliance

With local authentication enabled, the DHCP Enforcer appliance loses its connection with the server on which the Symantec Endpoint Protection Manager is installed. Therefore the DHCP Enforcer appliance authenticates a client locally.
To enable local authentication on the DHCP Enforcer appliance

1. In the Symantec Endpoint Protection Manager Console, click Admin.
2. In the Admin page, click Servers.
3. In the Admin page, under View Servers, select and expand the group of DHCP Enforcers appliances.
4. In the Admin page, under Tasks, click Edit Group Properties.
5. In the Settings dialog box, on the Advanced tab, check Enable Local Authentication.
6. Click OK.
Configuring the Symantec DHCP Enforcer appliance on the Symantec Endpoint Protection Manager Console

Using advanced DHCP Enforcer appliance settings
Configuring the Symantec LAN Enforcer appliance on the Symantec Endpoint Protection Manager Console

This chapter includes the following topics:

- About configuring the Symantec LAN Enforcer on the Symantec Endpoint Protection Manager appliance 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 on a Symantec Endpoint Protection Manager Console
- Using general settings
- Using RADIUS server group settings
- Using switch settings
- Using advanced LAN Enforcer appliance settings
- Using 802.1x authentication
About configuring the Symantec LAN Enforcer on the Symantec Endpoint Protection Manager appliance 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.
  See the *Installation Guide for Symantec Endpoint Protection and Symantec Network Access Control*.
  The computer on which the Symantec Endpoint Protection Manager software is installed is also referred to as the management server.

- Connect the Symantec LAN Enforcer appliance to the network.

- Configure the Symantec LAN Enforcer appliance on the local LAN Enforcer console during the installation.

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 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 name and description, listen port, and management server list.

- Configure the RADIUS server or servers. You configure the host name or IP address, authentication port, and shared secret. 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.

Configure clients for 802.1x authentication.

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 149.

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 true:

- Network includes a wireless LAN Enforcer appliance with 802.1x.
- Wireless clients run a supplicant that supports one of these protocols.
- Wireless AP must support 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:
Some wireless APs, such as Aruba, 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 not 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.

Changing LAN Enforcer configuration settings on a Symantec Endpoint Protection Manager Console

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 on a Symantec Endpoint Protection Manager Console

1. In the Symantec Endpoint Protection Manager Console, click Admin.
2. In the Admin page, click Servers.
3. In the Admin page, under View Servers, 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 In the Admin page, under View Servers, select the LAN Enforcer appliance whose configuration settings need to be changed.

5 In the Admin page, 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 152.

- **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 156.

- **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 163.

- **Advanced**
  This tab provides the following advanced LAN Enforcer settings:
  - Enable local authentication
  - Allow legacy client

  See “Using advanced LAN Enforcer appliance settings” on page 188.
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 154.

See “Adding or editing the description of a LAN Enforcer” on page 154.

You must establish a Listen port that is used for communication between the VLAN switch and the LAN Enforcer appliance.

See “Specifying a listening port that is used for communication between a VLAN switch and a LAN Enforcer” on page 153.

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 153.

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 154.

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 a Symantec Endpoint Protection Manager” on page 155.
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.

Specifying a listening port that is used for communication between a VLAN switch and a LAN Enforcer

When you configure the settings for a LAN Enforcer you specify the following Listen ports:

- The Listen 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 Listen 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.

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. In the Admin page, click Servers.
3. In the Admin page, under View Servers, select the Enforcer group.
4. In the Admin page, under View Servers, under Tasks, click Edit Group Properties.
5. In the LAN Enforcer Settings dialog box, on the Basic Settings 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. In the LAN Enforcer Settings dialog box, on the Basic Settings tab, 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 the Symantec Endpoint Protection Manager Console instead of the LAN Enforcer console.

To add or edit the description of an Enforcer group with a LAN Enforcer

1. In the Symantec Endpoint Protection Manager Console, click Admin.
2. In the Admin page, click Servers.
3. In the Admin page, under View Servers, select and expand the Enforcer group whose description you want to add or edit.
4. In the Admin page, under Tasks, click Edit Group Properties.
5. In the Settings dialog box, on the Basic Settings tab, add or edit a description for the Enforcer group in the Description field.
6. In the Settings dialog box, 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 the Installation Guide for Symantec Endpoint Protection and Symantec Network Access Control.

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 the Symantec Endpoint Protection Manager Console instead of the LAN 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 LAN Enforcer

1. In the Symantec Endpoint Protection Manager Console, click Admin.
2. In the Admin page, click Servers.
3. In the Admin page, under View Servers, select and expand the Enforcer group that includes the LAN Enforcer whose description you want to add or edit.
4. In the Admin page, under View Servers, select the LAN Enforcer whose description you want to add or edit.
5 In the Admin page, 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 In the Enforcer Properties dialog box, click **OK**.

### Connecting the LAN Enforcer to a Symantec Endpoint Protection Manager

Enforcers must be able to connect to servers on which the Symantec Endpoint Protection Manager is installed. The Symantec Endpoint Protection Manager includes a file that helps manage the traffic between clients, Symantec Endpoint Protection Managers, and optional Enforcers, such as a LAN Enforcer.

This file is called a management server list. The management server list specifies to which Symantec Endpoint Protection Manager server a LAN Enforcer connects. It also specifies to which Symantec Endpoint Protection server a LAN 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 Symantec Endpoint Protection Managers 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 LAN 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 a LAN Enforcer can connect to management servers.

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.

For more information on how to customize management server lists, see the *Administration Guide for Symantec Endpoint Protection and Symantec Network Access Control*.

#### To connect the LAN Enforcer to a Symantec Endpoint Protection Manager

1 In the Symantec Endpoint Protection Manager Console, click **Admin**.

2 In the Admin page, click **Servers**.
3 In the Admin page, under View Servers, 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 In the Admin page, under Tasks, click Edit Group Properties.

5 In the Settings dialog box, on the Basic Settings tab, under Communication, select the management server list that you want this LAN Enforcer to use.

6 In the Settings dialog box, 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 Settings dialog box, 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 157.

See “Editing the name of a RADIUS server group” on page 158.

See “Deleting the name of a RADIUS server group” on page 162.

You can 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 157.

See “Editing the friendly name of a RADIUS server” on page 159.

See “Editing the host name or IP address of a RADIUS server” on page 160.

See “Editing the authentication port number of a RADIUS server” on page 160.

See “Editing the shared secret of a RADIUS server” on page 161.
Adding a RADIUS server group name and RADIUS server

You can add a RADIUS server group name and RADIUS server at the same time.

**To add a RADIUS server group name and RADIUS server**

1. In the Symantec Endpoint Protection Manager Console, click **Admin**.
2. In the Admin page, click **Servers**.
3. In the Admin page, under View Servers, select the Enforcer group.
4. In the Admin page, under View Servers, 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. In the Add RADIUS Server Group dialog box, 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 UDP 1812.

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 In the Add RADIUS Server dialog box, click OK.
The name, 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.

To edit the name of a RADIUS server group

1 In the Symantec Endpoint Protection Manager Console, click Admin.

2 In the Admin page, click Servers.

3 In the Admin page, under View Servers, select the Enforcer group of which the LAN Enforcer is a member.
4 In the Admin page, under View Servers, 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 whose name you want to change.

6 In the LAN Enforcer Settings dialog box, on the RADIUS Server Group tab, click **Edit**.

7 In the Add RADIUS Server dialog box, edit the name of the RADIUS server group in the Group name field.

8 In the Add RADIUS Server dialog box, 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.

**To edit the friendly name of a RADIUS server**

1 In the Symantec Endpoint Protection Manager Console, click **Admin**.

2 In the Admin page, click **Servers**.

3 In the Admin page, under View Servers, select the Enforcer group of which the LAN Enforcer is a member.

4 In the Admin page, under View Servers, 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 friendly name 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 friendly name of the RADIUS server in the Friendly name of RADIUS server field.

8 In the Add RADIUS Server dialog box, 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.

To edit the host name or IP address of a RADIUS server
1. In the Symantec Endpoint Protection Manager Console, click Admin.
2. In the Admin page, click Servers.
3. In the Admin page, under View Servers, select the Enforcer group of which the LAN Enforcer is a member.
4. In the Admin page, under View Servers, 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. 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 host name or IP address of the RADIUS server in the Hostname or IP Address field.
8. In the Add RADIUS Server dialog box, 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.

To edit the authentication port number of a RADIUS server
1. In the Symantec Endpoint Protection Manager Console, click Admin.
2. In the Admin page, click Servers.
3. In the Admin page, under View Servers, select the Enforcer group of which the LAN Enforcer is a member.
4. In the Admin page, under View Servers, 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 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 authentication port number of the RADIUS server in the Authentication port field.

8 In the Add RADIUS Server dialog box, 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.

**To edit the shared secret of a RADIUS server**

1 In the Symantec Endpoint Protection Manager Console, click **Admin**.

   In the Admin page, click **Servers**.

2 In the Admin page, under View Servers, select the Enforcer group of which the LAN Enforcer is a member.

3 In the Admin page, under View Servers, under Tasks, click **Edit Group Properties**.

4 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.

5 In the LAN Enforcer Settings dialog box, on the RADIUS Server Group tab, click **Edit**.

6 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.

7 In the Add a RADIUS Server dialog box, edit the shared secret of the RADIUS server in the Confirm shared secret field.

8 In the Add RADIUS Server dialog box, click **OK**.

9 In the LAN Enforcer Settings dialog box, on the RADIUS Server Group tab, click **OK**.
Deleting the name of a RADIUS server group

You can delete the name of the RADIUS server group at any time if circumstances change.

**To delete the name of a RADIUS server group**

1. In the Symantec Endpoint Protection Manager Console, click **Admin**.
   
   In the Admin page, click **Servers**.
2. In the Admin page, under View Servers, select the Enforcer group of which the LAN Enforcer is a member.
3. In the Admin page, under View Servers, under Tasks, click **Edit Group Properties**.
4. In the LAN Enforcer Settings dialog box, on the RADIUS Server Group tab, click the RADIUS server group whose name you want to delete.
5. In the LAN Enforcer Settings dialog box, on the RADIUS Server Group tab, click **Remove**.
6. In the LAN Enforcer Settings dialog box, on the RADIUS Server Group tab, click **OK**.

Deleting a RADIUS server

You can delete a RADIUS server at any time if circumstances change.

**To delete a RADIUS server**

1. In the Symantec Endpoint Protection Manager Console, click **Admin**.

   In the Admin page, click **Servers**.
2. In the Admin page, under View Servers, select the Enforcer group of which the LAN Enforcer is a member.
3. In the Admin page, under View Servers, under Tasks, click **Edit Group Properties**.
4. 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.
5. In the LAN Enforcer Settings dialog box, on the RADIUS Server Group tab, click **Edit**.
6. In the Add RADIUS Server dialog box, click the RADIUS server that you want to delete.
7. In the Add RADIUS Server dialog box, click **Remove**.
8 In the Add RADIUS Server dialog box, click OK.
9 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.

About using 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 168.

See “Editing basic information about the switch policy and 802.1x-aware switch” on page 175.

You need to specify the set of 802.1x-aware switches to which the switch policy applies as follows:

- A friendly switch name of your choice
- IP address, IP range, or subnet

See “Adding an 802.1x switch policy for a LAN Enforcer appliance with a wizard” on page 168.

See “Editing information about the 802.1x-aware switch” on page 180.
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 168.

See “Editing VLAN information for the switch policy” on page 182.

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 168.

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 it with the information that appears in the following table.

If you want to keep the attributes from the RADIUS server, you can select action called Open Port. With this action, the LAN Enforcer forwards all attributes from 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. You must specify both the VLAN ID and VLAN name when you provide VLAN information for the LAN Enforcer, with the exception of the Aruba switch.

Table 8-1 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 Controller</td>
<td>The vendor code is 14179. The vendor-assigned attribute number is 5. The attribute format is “string.”</td>
<td>VLAN Name is used. Name is case sensitive.</td>
</tr>
<tr>
<td>Alcatel</td>
<td>Vendor Specific (#26) The vendor ID of Alcatel is 800. All “Vendor Specific” attributes from RADIUS with an ID of 800 are removed in case of conflict.</td>
<td>VLAN ID is used.</td>
</tr>
<tr>
<td>Aruba</td>
<td>Vendor Specific (#14823) Vendor ID is 14823 for Aruba. The Aruba-User-Role attribute permits you to set up either VLAN IDs or VLAN names.</td>
<td>Both VLAN name and VLAN ID can be used. Alternately, you can use only a VLAN name or only a VLAN ID. A valid VLAN ID ranges from 1 to 4094. A VLAN name cannot exceed 64 bytes.</td>
</tr>
</tbody>
</table>
Table 8-1  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>
| Cisco Aironet Series | Depends on whether you use SSID access control.  
RADIUS user attributes used for VLAN-ID assignment:  
IETF 64 (Tunnel Type): Set this attribute to “VLAN”  
IETF 65 (Tunnel Medium Type): Set this attribute to “802”  
IETF 81 (Tunnel Private Group ID): Set this attribute to VLAN-ID  
RADIUS user attribute used for SSID access control:  
Cisco IOS/PIX RADIUS Attribute, 009\001 cisco-av-pair | VLAN ID is used. |
| Cisco Catalyst Series | 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 name.  
All attributes with these 3 types from RADIUS server are removed in case of conflict. Also, any attribute with type “Vendor Specific” and the vendor ID is 9 (Cisco) are also removed. | VLAN Name is used. Name is case sensitive. |
Table 8-1  
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, | 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 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.

To add an 802.1x switch policy for a LAN Enforcer appliance with a wizard

1. In the Symantec Endpoint Protection Manager Console, click **Admin**. In the Admin page, click **Servers**.
2. In the Admin page, under View Servers, select the Enforcer group.
3. In the Admin page, under View Servers, under Tasks, click **Edit Group Properties**.
4. In the LAN Enforcer Settings dialog box, on the Switch tab, click **Add**.
5. In the Welcome to the Switch Policy Configuration Wizard panel of the Switch Policy Configuration Wizard, click **Next**.
6. 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 name and model as the name for the switch policy name.
<table>
<thead>
<tr>
<th>Switch model</th>
<th>The LAN Enforcer uses the switch model to determine the vendor-specific RADIUS server attribute. Select the following 802.1x-aware model from the list of supported switches:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Other</td>
<td>If your model is not listed, select Other to use as a generic RADIUS server attribute.</td>
</tr>
<tr>
<td>3Com</td>
<td></td>
</tr>
<tr>
<td>Alcatel switch</td>
<td></td>
</tr>
<tr>
<td>Cisco Catalyst Series</td>
<td></td>
</tr>
<tr>
<td>Enterasys Matix Series</td>
<td></td>
</tr>
<tr>
<td>Extreme Summit Series</td>
<td></td>
</tr>
<tr>
<td>Foundry Networks</td>
<td></td>
</tr>
<tr>
<td>HP Procurve Series</td>
<td></td>
</tr>
<tr>
<td>Nortel BayStack Series</td>
<td></td>
</tr>
<tr>
<td>Cisco Aironet Series</td>
<td></td>
</tr>
<tr>
<td>Aruba Switches</td>
<td></td>
</tr>
<tr>
<td>Airespace Wireless Controller</td>
<td></td>
</tr>
<tr>
<td>Nortel Wireless</td>
<td></td>
</tr>
<tr>
<td>Enterasys wireless controller</td>
<td></td>
</tr>
<tr>
<td>HuaWei switch</td>
<td></td>
</tr>
<tr>
<td>Note: 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.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Encrypted password or Shared secret</th>
<th>The shared secret that is used for communication between the 802.1x-aware switch and the LAN Enforcer appliance. The encrypted password or shared secret is case sensitive.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confirm encrypted password or shared secret</td>
<td>You must type the encrypted password or shared secret again.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>RADIUS server group</th>
<th>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.</th>
</tr>
</thead>
</table>
Reauthentication period (seconds)  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.

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  You can select 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.

The default setting is enabled.

7 In the Basic Information panel of the Switch Policy Configuration Wizard, click **Next**.

8 In the Switch List panel of the Switch Policy Configuration Wizard, click **Add**.
9 In the Switch List panel of the Switch Policy Configuration Wizard, complete the following tasks:

Name
In the Add Single Internal IP address dialog box, type a friendly name for the switch policy to identify the 802.1x-aware switch into the Name field.

Single IP Address
In the Add Single Internal IP Address dialog box, click Single IP address. Then type the IP address of the 802.1x-aware switch in the IP Address field.

IP Address Range
In the Add Internal IP Address Range dialog box, click IP Address Range. Type the beginning IP address for the 802.1x-aware switch in the Starting IP Address field. Type the ending IP address of the IP range for the 802.1x-aware switch in the End IP field.

Subnet
In the Add Internal IP Address Subnet dialog box, click Subnet. Type the IP address for the subnet in the IP address field and the subnet in the Subnet Mask field.

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.

10 In the Add Internal IP address dialog box, click OK.

11 In the Switch List panel of the Switch Policy Configuration Wizard, click Next.

12 In the Switch VLAN Configuration panel of the Switch Policy Configuration Wizard, click Add.
13 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 183.

- **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 183.

- **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).

- **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. It is recommended that you specify at least one remediation VLAN.

14 In the Add VLAN dialog box, click **OK**.

15 In the Switch VLAN Configuration panel of the Switch Policy Configuration Wizard, click **Next**.
16 In the Switch Action Configuration panel of the Switch Policy Configuration Wizard, click Add.

17 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.
<table>
<thead>
<tr>
<th>Policy Check</th>
<th>Click any of the following conditions:</th>
</tr>
</thead>
<tbody>
<tr>
<td>■ Passed</td>
<td>The client has passed the Policy Check.</td>
</tr>
<tr>
<td>■ Failed</td>
<td>The client has not passed the Policy Check.</td>
</tr>
<tr>
<td>■ Unavailable</td>
<td>The Unavailable result for the policy may occur under the following conditions:</td>
</tr>
<tr>
<td></td>
<td>■ 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.</td>
</tr>
<tr>
<td></td>
<td>■ If the client is first exported and installed before it connects to the management server and receives its policy.</td>
</tr>
<tr>
<td></td>
<td>■ Ignore Result</td>
</tr>
<tr>
<td>Action</td>
<td>You can select the following actions that the 802.1x-aware switch performs when the conditions are met:</td>
</tr>
<tr>
<td></td>
<td>■ Open Port</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>■ Switch to VLAN-test</td>
</tr>
<tr>
<td></td>
<td>Allows access to the specified VLAN. The VLANs that are available to select are the ones that you configured previously.</td>
</tr>
<tr>
<td></td>
<td>■ Close Port</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

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.

18 In the Add Switch Action dialog box, click OK.
19 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.

20 In the Switch Action Configuration panel of the Switch Policy Configuration Wizard, click **Move Up** or **Move Down**.

21 In the Switch Action Configuration panel of the Switch Policy Configuration Wizard, click **Next**.

22 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 175.

- **Switch model**
  See “Selecting a different switch model for the switch policy” on page 176.

- **Shared secret**
  See “Editing an encrypted password or shared secret” on page 177.

- **RADIUS server group**
  See “Selecting a different RADIUS server group” on page 178.

- **Reauthentication time period**
  See “Editing the reauthentication period” on page 179.

- **Forwarding protocols besides EAP**
  See “Enabling protocols other than EAP” on page 179.

**Editing the name of a switch policy**

You can edit the name of the switch policy at any time if circumstances change.
To edit the name of a switch policy
1 In the Symantec Endpoint Protection Manager Console, click Admin. In the Admin page, click Servers.
2 In the Admin page, under View Servers, select the Enforcer group.
3 In the Admin page, under View Servers, under Tasks, click Edit Group Properties.
4 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.
5 In the LAN Enforcer Settings dialog box, on the Switch tab in the Switch Policy table, click Edit.
6 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.
7 In the Edit Switch Policy for name of switch policy dialog box, on the Basic Information tab, click OK.
8 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.
To select a different switch model for the switch policy
1 In the Symantec Endpoint Protection Manager Console, click Admin. In the Admin page, click Servers.
2 In the Admin page, under View Servers, select the Enforcer group.
3 In the Admin page, under View Servers, under Tasks, click Edit Group Properties.
4 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.
5 In the LAN Enforcer Settings dialog box, on the Switch tab in the Switch Policy table, click Edit.
6 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 as a generic RADIUS server attribute.

- 3Com
- Alcatel switch
- Cisco Catalyst Series
- Enterasys Matix 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.

7 In the Edit Switch Policy for name of switch policy dialog box, on the Basic Information tab, click OK.

8 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.

**To edit an encrypted password or shared secret**

1 In the Symantec Endpoint Protection Manager Console, click Admin.
   In the Admin page, click Servers.

2 In the Admin page, under View Servers, select the Enforcer group.

3 In the Admin page, under View Servers, under Tasks, click Edit Group Properties.
4 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.

5 In the LAN Enforcer Settings dialog box, on the Switch tab in the Switch Policy table, click **Edit**.

6 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.

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 Confirm shared secret field.

8 In the Edit Switch Policy for *name of switch policy* dialog box, on the Basic Information tab, click **OK**.

9 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.

**To select a different RADIUS server group**

1 In the Symantec Endpoint Protection Manager Console, click **Admin**.
   In the Admin page, click **Servers**.

2 In the Admin page, under View Servers, select the Enforcer group.

3 In the Admin page, under View Servers, under Tasks, click **Edit Group Properties**.

4 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.

5 In the LAN Enforcer Settings dialog box, on the Switch tab in the Switch Policy table, click **Edit**.

6 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.

7 In the Edit Switch Policy for *name of switch policy* dialog box, on the Basic Information tab, click **OK**.

8 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.

**To edit the reauthentication period**

1. In the Symantec Endpoint Protection Manager Console, click Admin.
   In the Admin page, click Servers.
2. In the Admin page, under View Servers, select the Enforcer group.
3. Click Edit Group Properties.
4. 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.
5. On the Switch tab in the Switch Policy table, click Edit.
6. 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.
7. Click OK.
8. In the LAN Enforcer Settings dialog box, on the Switch tab, click OK.

**Enabling protocols other than EAP**

You can select to 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.
To enable protocols other than EAP
1. In the Symantec Endpoint Protection Manager Console, click Admin.
   In the Admin page, click Servers.
2. In the Admin page, under View Servers, select the Enforcer group.
3. Click Edit Group Properties.
4. 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.
5. In the LAN Enforcer Settings dialog box, on the Switch tab in the Switch Policy table, click Edit.
6. 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
7. Click OK.
8. 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 180.
- Removal of an 802.1x-aware switch from switch list
  See “Deleting an 802.1x-aware switch from the switch list” on page 181.

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.

To edit the IP address, hostname, and subnet of an 802.1x-aware switch
1. In the Symantec Endpoint Protection Manager Console, click Admin.
   In the Admin page, click Servers.
2. In the Admin page, under View Servers, select the Enforcer group.
3 Under Tasks, click **Edit Group Properties**.

4 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.

5 Click **Edit**.

6 In the Edit Switch Policy for *name of switch policy* dialog box, on the Switch Address tab, check **Edit All**.

7 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 Range**: `name: start address-end address`
- **Subnet**: `name: start address/subnet mask`

8 In the Edit Switch Policy for *name of switch policy* dialog box, on the Switch Address tab, click **OK**.

9 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.

**To delete an 802.1x-aware switch**

1 In the Symantec Endpoint Protection Manager Console, click **Admin**.

   In the Admin page, click **Servers**.

2 Under View Servers, select the Enforcer group.

3 Under Tasks, click **Edit Group Properties**.

4 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.

5 In the LAN Enforcer Settings dialog box, on the Switch tab, click **Remove**.

6 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 182.

■ 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 183.

■ Removal of VLANs on an 802.1x-aware switch
  See “Deleting the VLANs on an 802.1x-aware switch” on page 183.

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.

To edit the VLAN ID and VLAN name of an 802.1x-aware switch

1 In the Symantec Endpoint Protection Manager Console, click Admin.

   In the Admin page, click Servers.

2 Under View Servers, select the Enforcer group.

3 Under Tasks, click Edit Group Properties.

4 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.

5 Click Edit.

6 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.
7 On the VLAN tab, check **Edit**.

8 In the Edit VLAN dialog box, edit the VLAN ID in the VLAN ID field.

9 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 183.

10 In the Edit Switch Policy for *name of switch policy* dialog box, on the VLAN tab, click **OK**.

11 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.

**To delete the VLANs on an 802.1x-aware switch**

1 In the Symantec Endpoint Protection Manager Console, click **Admin**.

   In the Admin page, click **Servers**.

2 Under View Servers, select the Enforcer group.

3 Under Tasks, click **Edit Group Properties**.

4 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.

5 Click **Edit**.

6 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.

7 On the VLAN tab, check **Remove**.

8 Click **OK**.

9 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.

**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 185.

- 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 186.

- Select different actions
  See “Selecting different actions” on page 187.

**About issues with the switch policy, associated conditions, and actions**

When configuring switch policies, keep the following issues in mind:

- 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.

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.
To set the order of condition checking

1. In the Symantec Endpoint Protection Manager Console, click Admin.
   In the Admin page, click Servers.
2. Under View Servers, select the Enforcer group.
4. 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.
5. Click Edit.
6. 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.
7. Click Move Up or Move Down.
8. Click OK.
9. 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.

To select a different Host Authentication, User Authentication, or Policy Check condition

1. In the Symantec Endpoint Protection Manager Console, click Admin.
   In the Admin page, click Servers.
2. Under View Servers, select the Enforcer group.
4. 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.
5. Click Edit.
6. 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

7 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

8 Click OK.

9 In the LAN Enforcer Settings dialog box, on the Switch tab, click OK.

Selecting different actions

To select a different Host Authentication, User Authentication, or Policy Check condition

1 In the Symantec Endpoint Protection Manager Console, click Admin.
   In the Admin page, click Servers.

2 Under View Servers, select the Enforcer group.

3 Under Tasks, click Edit Group Properties.

4 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.

5 Click Edit.

6 On the Action tab, click any of the actions that you want to change in the Action column.

7 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.

8 Click OK.

9 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 188.

- Enable local authentication.
  See “Enabling local authentication on the LAN Enforcer appliance” on page 189.

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.

To allow a legacy client to connect to the network with a LAN Enforcer appliance

1 In the Symantec Endpoint Protection Manager Console, click Admin.

2 In the Admin page, click Servers.

3 In the Admin page, under View Servers, select and expand the group of LAN Enforcers appliances.

4 In the Admin page, 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 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.

**To enable local authentication on the LAN Enforcer appliance**

1. In the Symantec Endpoint Protection Manager Console, click **Admin**.
2. In the Admin page, click **Servers**.
3. Under View Servers, 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**.

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 8-2** describes the types of options that you can configure for 802.1x authentication.
Table 8-2 802.1x authentication options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Third-party supplicant| Uses a third-party 802.1x supplicant. 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.  
**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 Network Access Control 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. |
| Transparent mode      | 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.  
**Note:** 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. |
### Table 8-2 802.1x authentication options (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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.

**To configure the client to use either transparent mode or a built-in 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. 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 have 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.
Setting up temporary connections for Symantec Network Access Control On-Demand clients

This chapter includes the following topics:

- About setting up temporary connections for Symantec Network Access Control On-Demand Clients
- Setting up authentication on the Gateway or DHCP Enforcer console for Symantec Network Access Control On-Demand clients
- Editing the banner on the Welcome page
- Troubleshooting the connection between the Enforcer and the On-Demand clients

About setting up temporary connections for Symantec Network Access Control On-Demand Clients

End users often need to temporarily connect to an enterprise network even though their computers do not have the approved software. If an enterprise network includes a Gateway or a DHCP Enforcer appliance, an administrator can configure the appliance to allow noncompliant client computers to temporarily connect to an enterprise network as a guest.
The administrator can configure a Gateway or DHCP Enforcer appliance to automatically download Symantec Network Access Control On-Demand clients on both Windows and Macintosh platforms. As soon as the Symantec Network Access Control On-Demand client is downloaded to a client computer, the client can try to connect to the company's network.

If the client computer meets all requirements, a connection between the client computer and the Symantec Endpoint Protection Manager is automatically established. Therefore the compliant client computer can perform any task that the administrator enabled for this group on the Symantec Endpoint Protection Manager.

If the client computer cannot meet all requirements, a connection between the client computer and the Symantec Endpoint Protection Manager cannot be automatically established. The end user needs to resolve all noncompliant requirements on the client computer.

Before you configure Symantec Network Access Control On-Demand clients on the console of a Gateway or DHCP 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 second CD-ROM called CD2. This software includes the Symantec Endpoint Protection Manager software that you must install. If you accidentally install the Symantec Endpoint Protection software that is located on the first CD-ROM called CD1, the Symantec Endpoint Protection Manager software cannot install all of the required components.
  See the Installation Guide for Symantec Endpoint Protection and Symantec Network Access Control.

- Written down the name of the encrypted password that you implemented during the installation of the Network Access Control software.
  See the Installation Guide for Symantec Endpoint Protection and Symantec Network Access Control.

- Installed and configured a Gateway or DHCP 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.
  See “Before you install the Enforcer appliance” on page 71.
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.

See the *Administration Guide for Symantec Endpoint Protection and Symantec Network Access Control*.

- **Checked the connection status between the Enforcer appliance and the Symantec Endpoint Protection Manager server on the console of the Enforcer appliance.**

  See “Checking the communication status of an Enforcer appliance on the Enforcer console” on page 85.

  See “Show” on page 236.

- **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 (eth1) that is located on a Gateway or DHCP Enforcer appliance.

  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 or DHCP 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.

  For example, you can type http://10.127.33.190 for DNS spoofing. You accomplish this objective by having the DHCP Enforcer appliance modify the relevant DHCP messages that are sent to a client. The DHCP Enforcer appliance replaces the IP address of the DNS server in the DHCP message with the DHCP Enforcer appliance’s external IP address. Therefore the DHCP Enforcer appliance acts as a DNS server to the clients and thus prevents DNS spoofing.

  See the *Administration Guide for Symantec Endpoint Protection and Symantec Network Access Control*.

- **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 right 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.

  See the *Administration Guide for Symantec Endpoint Protection and Symantec Network Access Control*. 
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 or guest clients, then the default location is automatically assigned to the guest clients. It is recommended that you create a separate location for the Enforcer client group on the Symantec Endpoint Protection Manager. 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. It is recommended that you 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. See the Administration Guide for Symantec Endpoint Protection and Symantec Network Access Control.

Added and assigned an optional Host Integrity Policy to the Enforcer client group and location on the Symantec Endpoint Protection Manager Console. Although 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, it is recommended that you 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. See the Administration Guide for Symantec Endpoint Protection and Symantec Network Access Control.

Enabled an optional pop-up message on the Symantec Endpoint Protection Manager Console. See the Administration Guide for Symantec Endpoint Protection and Symantec Network Access Control.

Obtain the domain ID number that is located on the Symantec Endpoint Protection Manager Console. See the Administration Guide for Symantec Endpoint Protection and Symantec Network Access Control. It is recommended that you have the domain ID handy because you may need to configure the domain ID on the Gateway or DCHP Enforcer with the on-demand spm-domain command.
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 or DHCP Enforcer” on page 194.

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.

See “To enable Symantec Network Access Control On-Demand clients to temporarily connect to a network” on page 197.

To enable Symantec Network Access Control On-Demand clients to temporarily connect to a network

1 Log on to the Gateway or DHCP Enforcer appliance console as a superuser. See “Logging on to an Enforcer appliance” on page 82.

2 On the console of a Gateway or DHCP 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 or DHCP Enforcer” on page 194.
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 will register 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 or DHCP Enforcer console for Symantec Network Access Control On-Demand clients” on page 199.

Type the following command:

```
Enforcer (on-demand)# enable
```

**Disabling Symantec Network Access Control On-Demand clients for client computers**

If you want to disable the Symantec Network Access Control On-Demand clients from automatically being downloaded, you can disable this process.

**To disable Symantec Network Access Control On-Demand clients for client computers**

1. Log on to the Gateway or DHCP Enforcer appliance console as superuser. See “Logging on to an Enforcer appliance” on page 82.
2. On the console of a Gateway or DHCP Enforcer appliance, type `on-demand`.
3. Type `disable`.
4. Type `exit`.
5. Type `exit` to log off.
Setting up authentication on the Gateway or DHCP Enforcer console for Symantec Network Access Control On-Demand clients

You can authenticate end users by adding user names and password for each end user in a local database that is on-board of the Gateway and DHCP Enforcer appliance.

See “Setting up authentication with a local on-board database” on page 199.

If you do not want to use the local database that is on-board of the Gateway and DHCP Enforcer appliance, you can configure the Enforcer appliances to use a Microsoft Windows Server 2003 Active Directory to manage the authentication of the end users.


Setting up authentication with a local on-board database

You can configure up to 1000 end users on the on-board database.

See “On-Demand authentication local-db commands” on page 275.

To set up authentication with a local database

1 Log on to the Gateway or DHCP Enforcer appliance console as a superuser.

See “Logging on to an Enforcer appliance” on page 82.

2 On a Gateway or DHCP Enforcer appliance console, type the following command:

   Enforcer # on-demand

3 On a Gateway or DHCP Enforcer appliance console, type the following command:

   Enforcer (on-demand)# authentication

4 Type the following command:

   Enforcer (authentication)# enable
5 Type the following command:

   Enforcer (authentication)# local-db enable

6 Type the following command:

   Enforcer (authentication)# ad domain string
   
   where:

   string represents the domain name of the Microsoft Windows Server 2003 Active Directory. For example, symantec.com.

Setting up authentication with a Microsoft Windows 2003 Server Active Directory

The Gateway and DHCP Enforcer appliances establish 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.

See “On-demand authentication ad commands” on page 272.

To set up authentication with an active directory server

1 Log on to the Gateway or DHCP Enforcer appliance console as a superuser.
   See “Logging on to an Enforcer appliance” on page 82.

2 On a Gateway or DHCP 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)# enable

5 Type the following command:

   Enforcer (authentication)# ad enable

6 Type the following command:

   Enforcer (authentication)# ad domainid

   where:

   domainid represents the domain name of the Microsoft Windows Server 2003 Active Directory. For example, www.symantec.com.
Setting up the On-Demand Client on Windows for authentication with the dot1x protocol

To set up the On-Demand Client on Windows for authentication with the dot1x 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 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 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 Type the following command: `Enforcer (peap) cert-svr host snac`

   where:

   `snac` is the computer that is the CA server for the peap certificate name.

### 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 or DHCP Enforcer appliance console as a superuser.

   See “Logging on to an Enforcer appliance” on page 82.

2 Type the following command on the console of a Gateway or DHCP 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 end users to view on the Welcome page of the Symantec Network Access Control On-demand client. You can type up to 1024 characters.
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 9-1

<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. |
<p>| 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.                          |
| Host Integrity check is sometimes long the first time                  | This is an issue with DNS resolution, and should not appear after the first Host Integrity check.                                                                                                          |
| Firewall on the client is blocking the On-Demand client from working when the user does not have Admin rights | Users should change firewall settings to unblock UDP port 39999. Alternatively, set the firewall to allow <code>cclientctl.exe</code>                                                                                   |
| Upgrading the Enforcer does not initially contain the manual installation package | This 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, then enable On-Demand functionality on the Enforcer. That will add the manual installation files. |
| The redirect URL on the Enforcer will overwrite a previous redirect URL on SEPM | This only happens when the On-Demand feature is enabled on the Enforcer. It is expected behavior.                                                                                                      |
| Vista clients sometimes do not receive an IP address from the DHCP server | This is a timing issue. Change the DHCP timeout setting to 12 seconds or more.                                                                                                                               |</p>
<table>
<thead>
<tr>
<th>Symptom</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>A normal user cannot install the agent if there is no JRE installed.</td>
<td>The workaround is to ensure that JRE is installed. Otherwise only Admin users can install.</td>
</tr>
<tr>
<td>Wireless service is disconnected when the On-Demand client is installed and quit, when 802.1x authentication is used</td>
<td>The user should restart the wireless connection.</td>
</tr>
<tr>
<td>Systems running Norton 360 v. 2.x have a problem receiving the client</td>
<td>Follow the &quot;manual download&quot; link, download and install, and it will work.</td>
</tr>
<tr>
<td>With Firefox, 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>This could need installation of Microsoft patch KB893803. This patch is included with the manual install, and should be installed prior to the client installation. Admin privilege is required.</td>
</tr>
<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 &quot;Run as Administrator&quot; method or turn off UAC to make sure 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 Tools -&gt; Manage Add-ons -&gt; Enable or Disable Add-ons -&gt; Downloaded ActiveX Controls, delete HodaAgt class.</td>
</tr>
<tr>
<td>Browser notifies the user, &quot;can not display webpage,&quot; 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 happens when Firefox is first run. The first one or two Firefox restarts are required for it to finish its configuration. After that the On-Demand client should download.</td>
</tr>
</tbody>
</table>
### Table 9-1 (continued)

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<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 that version of the Mac OS. Version 10.5 does not have the problem. The workaround for version 10.4 is to set the hostname in <code>/etc/hostconfig/</code>.</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 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 SNAC file. It is automatically reinstalled, and you may safely take no action.</td>
</tr>
</tbody>
</table>
Setting up temporary connections for Symantec Network Access Control On-Demand clients

Troubleshooting the connection between the Enforcer and the On-Demand clients
Enforcer appliance command-line interface

This chapter includes the following topics:

- About the Enforcer appliance CLI command hierarchy
- CLI command hierarchy
- Moving up and down the command hierarchy
- Enforcer appliance CLI keystroke shortcuts
- Getting help with CLI commands

About the Enforcer appliance CLI command hierarchy

The Enforcer appliance has a command-line interface (CLI) that is organized into a command hierarchy. The main (top-level commands) include the following command groups that access additional commands:

- capture
- configure
- console
- debug
- mab
- monitor
- on-demand
- snmp
# CLI command hierarchy

Table 10-1 describes the hierarchy for the Enforcer commands.

<table>
<thead>
<tr>
<th>Top-level commands</th>
<th>First sub-level commands</th>
<th>Second sub-level commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>capture</td>
<td>The clear, exit, help, and show commands are only available to the admin logon and root (superuser). You can use the following sub-level commands:</td>
<td>not available</td>
</tr>
<tr>
<td>clear</td>
<td>not available</td>
<td>not available</td>
</tr>
<tr>
<td>configure</td>
<td>The clear, exit, help, and show commands are only available to the admin logon and root (superuser). You can use the following sub-level commands:</td>
<td>Only the advanced command has a set of sub-level commands</td>
</tr>
<tr>
<td>console</td>
<td>baud-rate, clear, exit, help, show, ssh, and sshkey</td>
<td>not available</td>
</tr>
</tbody>
</table>

The clear, exit, help, and show commands are available to the admin logon and root (superuser).
<table>
<thead>
<tr>
<th>Top-level commands</th>
<th>First sub-level commands</th>
<th>Second sub-level commands</th>
</tr>
</thead>
</table>
| date               | ■ date  
                   ■ time  
                   ■ timezone            | not available             |
| debug              | clear, exit, destination, help, level, show, and upload  
                   The clear, exit, help, and show commands are available to the admin logon and root (superuser). | not available             |
| exit               | not available            | not available             |
| help               | not available            | not available             |
| hostname           | not available            | not available             |
| mab                | The clear, exit, help, and show commands are only available to the admin logon and root (superuser).  
                   ■ clear  
                   ■ database  
                   ■ disable  
                   ■ enable  
                   ■ exit  
                   ■ help  
                   ■ ldap  
                   ■ show | not available             |
| monitor            | ■ clear  
                   ■ exit  
                   ■ help  
                   ■ refresh  
                   ■ show | all or IP *ip address*   |
### Table 10-1  Enforcer appliance CLI command hierarchy (continued)

<table>
<thead>
<tr>
<th>Top-level commands</th>
<th>First sub-level commands</th>
<th>Second sub-level commands</th>
</tr>
</thead>
</table>
| on-demand          | The clear, exit, help, and show commands are only available to the admin logon and root (superuser).  
|                    | [ ] authentication  
|                    | [ ] banner  
|                    | [ ] clear  
|                    | [ ] client-group  
|                    | [ ] disable  
|                    | [ ] dot1x  
|                    | [ ] enable  
|                    | [ ] exit  
|                    | [ ] help  
|                    | [ ] mac-compliance  
|                    | [ ] show  
|                    | [ ] spm-domain  
| password           | not available                                                                 | not available                                                                          |
| ping               | not available                                                                 | not available                                                                          |
| reboot             | not available                                                                 | not available                                                                          |
| show               | not available                                                                 | not available                                                                          |
| shutdown           | not available                                                                 | not available                                                                          |
| snmp               | [ ] disable  
|                    | [ ] enable  
|                    | [ ] heartbeat  
|                    | [ ] receiver  
|                    | [ ] show  
|                    | [ ] trap  
|                    | [ ] exit  
|                    | [ ] clear  
|                    | [ ] help  
| start              | not available                                                                 | not available                                                                          |
| stop               | not available                                                                 | not available                                                                          |
| traceroute         | not available                                                                 | not available                                                                          |
Moving up and down the command hierarchy

If you want to access a command that is lower in the hierarchy, you type both the top-level command and lower-level command. If you have several commands that you want to execute in a command group, you can type only the top-level command. You must then press Enter to enter the command group. The same process applies if you want to get a list of commands in a group. You can then type any command available from that group.

For example, the capture group contains a show command that shows the capture configuration settings. If you want to access the show command from the top level, type the following capture command:

```
Enforcer# capture show
```

If you type only the command that gives access to a command group and press Enter, the next prompt shows the command group in parentheses.

For example:

```
Enforcer# capture
```

```
Enforcer(capture)#
```

If you want to move up the hierarchy and access commands outside the group, you must first exit the command group.

```
Enforcer(capture)# exit
```

```
Enforcer#
```

Enforcer appliance CLI keystroke shortcuts

When you use the CLI, you can use keystrokes as shortcuts instead of typing commands or to get help in filling in commands.

*Table 10-2* lists the CLI keyboard shortcuts and help.
## Table 10-2 CLI keyboard shortcuts and help

<table>
<thead>
<tr>
<th>Keys or key combinations</th>
<th>Action</th>
</tr>
</thead>
</table>
| Tab key or ?             | • Lists all available commands or options.  
                          | or  
                          | • Completes the command or option name or lists all possible commands or options that start with the letters that you typed.  
                          | For more information:  
                          | See “Getting help with CLI commands” on page 213. |
| CTRL+D                  | Exits from a command group.   |
| CTRL+C                  | Deletes all characters on the command line.  |
| !                       | Lists the commands in the history buffer.  
                          | Commands that you type are stored in a 16k history ring buffer. The commands are indexed starting with 1. When the buffer overflows, the oldest command is replaced, and the index number changes, so that the oldest command always has index 1.  
                          | The ! command lists all commands in the history buffer. If you type a number following the !, the Enforcer console restores the command that has that number. The command is not executed until you press Enter.  
                          | The following is an example:  
                          | Enforcer# !  
                          | 1. con  
                          | 2. configure  
                          | 3. ping 192.168.0.1  
                          | 4. traceroute 192.168.0.16  
                          | Enforcer# !3  
                          | Enforcer# ping 192.168.0.1  |
| Up-arrow key            | Restores the commands in the history buffer by moving up and down by index. |
| Down-arrow key          | Moves the cursor a character to the left and right. |
| Left-arrow key          | Moves the cursor to the beginning or end of the command line. |
| Right-arrow key         | Deletes a character on the command line that is to the left of the cursor. |
| key Backspace           | Deletes a character on which the cursor resides. |
## Getting help with CLI commands

When you use the CLI, there are several ways to get help on commands and command options.

Table 10-3 shows the ways in which you can get help with CLI commands.

<table>
<thead>
<tr>
<th>What would you like to do?</th>
<th>Action</th>
</tr>
</thead>
</table>
| List all available commands with a short description          | At the command prompt, press Tab or ?  
  
  All commands available at the current hierarchy level are listed.  
  
  Example:  
  
  After you type the configure command and press Enter to access the configure command group, press Tab or ? to display all available configure commands. |
| Display a short description of a specific command             | At the command prompt, type Help followed by the command name. (The command must be available from the current hierarchy level.)          |
| Complete the command name or list all possible commands that start with the letters typed. | Type one or more letters that begin the command name and press Tab or ?  
  
  For example:  
  
  When you type co and then press Tab or ? at the main command prompt, the Enforcer console lists all available commands that begin with co. As shown in the following example, two commands begin with con. Therefore the Enforcer console fills in the letter n.  
  
  Example:  
  
  `Enforcer# co?`  
  
  `configure Configure Enforcer setting`  
  
  `console Console setting`  
  
  `Enforcer# con` |
<table>
<thead>
<tr>
<th>What would you like to do?</th>
<th>Action</th>
</tr>
</thead>
</table>
| Display all the options for a specific command, with a short description of each option. | Type the command and press Tab or ?
For example:
If you are in the configure command group and want to display the options for the interface command, type interface and press Tab or ?
Example:
Enforcer(configure)# interface?
Each interface option is listed with a brief description. |
| Complete the option name or list all available options that start with the letters typed. | After you type the option name, type one or more letters that begin the option name and press Tab or ?
For example:
If you type the capture show command that is followed with the letter f, the Enforcer console lists the two options that begin with the letter f. Because they both begin with the letters fil, the console fills in the il.
For example:
Enforcer# capture show f?
files Display packet capture files
filter Display current packet capture filter
Enforcer# capture show fil |
This chapter includes the following topics:

- Command conventions
- Enforcer appliance CLI in alphabetical reference
- Top-level commands
- Capture commands
- Configure commands
- Console commands
- Debug Commands
- MAB commands
- Monitor commands
- SNMP commands
- On-Demand commands

Command conventions

The following conventions describe the syntax and usage of the Enforcer appliance command-line interface (CLI) commands:
Table 11-1 Conventions for the commands

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>$n$</td>
<td>Variables appear in italics.</td>
</tr>
<tr>
<td></td>
<td>For example, $n$ represents a variable:</td>
</tr>
<tr>
<td>braces {}</td>
<td>If a command has multiple arguments, the multiple arguments are</td>
</tr>
<tr>
<td></td>
<td>enclosed in braces {}.</td>
</tr>
<tr>
<td></td>
<td>The following is an example of multiple arguments where $n$ represents</td>
</tr>
<tr>
<td></td>
<td>a variable:</td>
</tr>
<tr>
<td></td>
<td>{width $n$</td>
</tr>
<tr>
<td>brackets [ ]</td>
<td>Optional arguments are enclosed in brackets []. The following is an</td>
</tr>
<tr>
<td></td>
<td>example of an optional argument:</td>
</tr>
<tr>
<td></td>
<td>[metric]</td>
</tr>
<tr>
<td>pipe symbol</td>
<td>If a command has multiple arguments that exclude each other, a pipe</td>
</tr>
<tr>
<td>symbol</td>
<td>symbol</td>
</tr>
<tr>
<td></td>
<td>The following is an example of multiple arguments that exclude each</td>
</tr>
<tr>
<td></td>
<td>other:</td>
</tr>
<tr>
<td></td>
<td>{width $n$</td>
</tr>
</tbody>
</table>

**Enforcer appliance CLI in alphabetical reference**

The Enforcer appliance commands are organized in a hierarchy with some commands at the top level and others under the following commands: capture, configure, console, debug, mab, monitor, and on-demand. The commands clear, exit, help, and show are available from all levels of the hierarchy. However, they are only listed in the table at the top level. The commands are available when you log on as an administrator. All other commands are available only by logging in as root.

To display a description of all commands available at the current hierarchy level, you can type a question mark (?) or press Tab.

**Table 11-2** gives a brief description of the commands.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>capture</td>
<td>Accesses the packet capture commands.</td>
</tr>
<tr>
<td></td>
<td>See “Capture commands” on page 239.</td>
</tr>
<tr>
<td><strong>Command</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>capture filter</code></td>
<td>Configures the filtSymantec Endpoint Protection Manager to be applied to packet capture. See “Capture Filter” on page 239.</td>
</tr>
<tr>
<td><code>capture show</code></td>
<td>Displays the capture configuration and lists the files that are captured. See “Capture Show” on page 240.</td>
</tr>
<tr>
<td><code>capture start</code></td>
<td>Starts packet capture. See “Capture Start” on page 241.</td>
</tr>
<tr>
<td><code>capture upload</code></td>
<td>Uses tftp protocol to send a file or files. See “Capture Upload” on page 242.</td>
</tr>
<tr>
<td><code>capture verbose</code></td>
<td>Turns on or off the display of packet capture details. See “Capture Verbose” on page 242.</td>
</tr>
<tr>
<td><code>clear</code></td>
<td>Clear the screen. See “Clear” on page 233.</td>
</tr>
<tr>
<td><code>configure</code></td>
<td>Provides access to the Enforcer configure commands. See “Configure commands” on page 243.</td>
</tr>
<tr>
<td><code>configure advanced</code></td>
<td>Accesses the advanced configuration commands. See “Configure advanced commands” on page 243.</td>
</tr>
<tr>
<td><code>configure advanced trunking</code></td>
<td>Enables or disables trunking support (Gateway Enforcer only). See “Configure advanced commands” on page 243.</td>
</tr>
<tr>
<td><code>configure advanced catos</code></td>
<td>Enables or disables Cisco catos support. (LAN Enforcer appliances only) See “Advanced CATOS” on page 243.</td>
</tr>
<tr>
<td><code>configure advanced check-uid</code></td>
<td>Enables or disables UID checking for legacy agents. (Gateway and DHCP Enforcer only) See “Advanced check-uid” on page 243.</td>
</tr>
<tr>
<td><code>configure advanced dns-spoofing</code></td>
<td>Configures a DNS spoofing IP address and enables or disables it on the DHCP Enforcer. Disabling deletes the DNS spoofing IP address and enables it in the DHCP Enforcer. (DHCP Enforcer appliances only) See “Advanced DNS spoofing” on page 244.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>configure advanced failover</td>
<td>Configures Enforcer appliance failover settings. See “Advanced failover” on page 244.</td>
</tr>
<tr>
<td>configure advanced legacy</td>
<td>Allows or blocks legacy agents. See “Advanced legacy” on page 245.</td>
</tr>
<tr>
<td>configure advanced legacy-uid</td>
<td>Specifies legacy UID. (Gateway and DHCP Enforcer appliances only) See “Advanced legacy-uid” on page 246.</td>
</tr>
<tr>
<td>configure advanced local-auth</td>
<td>Enables or disables Enforcer authentication of clients. See “Advanced Radius” on page 246.</td>
</tr>
<tr>
<td>configure advanced re-initialize</td>
<td>Switches to different Enforcer type. This option is not available if you are logged in to SSH session. See “Advanced Re-initialize” on page 247.</td>
</tr>
<tr>
<td>configure advanced radius</td>
<td>Enables or disables Radius accounting proxy support. (LAN Enforcer appliance only) See “Advanced Radius” on page 246.</td>
</tr>
<tr>
<td>configure advanced snacs</td>
<td>Set SNAC scanner IP, port, and pre-share key (Gateway and DHCP Enforcers appliance only). Use this command to re-enable the SNAC scanner if it has been disabled. See “Advanced Symantec Network Access Control Server Scanner” on page 247.</td>
</tr>
<tr>
<td>configure advanced user-class</td>
<td>Enables or disables user class. (DHCP Enforcer appliance only) See “Advanced User-class” on page 248.</td>
</tr>
<tr>
<td>configure dns</td>
<td>Adds or deletes a DNS entry. See “Configure DNS” on page 249.</td>
</tr>
<tr>
<td>configure interface</td>
<td>Configures network interface IP address and net mask. See “Configure Interface” on page 250.</td>
</tr>
<tr>
<td>configure interface-role</td>
<td>Specifies internal and external network interfaces. (Gateway and DHCP Enforcer only) See “Configure interface-role” on page 251.</td>
</tr>
<tr>
<td>configure ntp</td>
<td>Establishes communication between an Enforcer appliance and a Network Time Server with an IP address, domain name, or web address. It also enables or disables synchronization of time between the Network Time Server and the Enforcer appliance. See “Configure NTP” on page 251.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>configure redirect</td>
<td>Specifies HTTP redirect URL when a client is not installed on a computer. See “Configure Redirect” on page 252.</td>
</tr>
<tr>
<td>configure route</td>
<td>Configures route settings. See “Configure Route” on page 252.</td>
</tr>
<tr>
<td>configure show</td>
<td>Displays the current configuration of each command in the configure group. If no argument is specified, all settings appear. See “Configure Show” on page 253.</td>
</tr>
<tr>
<td>configure spm</td>
<td>Configures the connection. If you only modify one of the arguments, you need to modify all of them or the default settings are automatically used for those arguments that you did not modify. See “Configure SPM” on page 253.</td>
</tr>
<tr>
<td>console</td>
<td>Provides access to the console configuration commands. See “Console commands” on page 254.</td>
</tr>
<tr>
<td>console baud-rate</td>
<td>Sets the baud rate. See “Console Baud-rate” on page 254.</td>
</tr>
<tr>
<td>console ssh</td>
<td>Enable or disable SSH remote logon. See “Console SSH” on page 255.</td>
</tr>
<tr>
<td>console sshkey</td>
<td>Sets and deletes the public key for ssh remote logon without a password. See “Console SSHKEY” on page 255.</td>
</tr>
<tr>
<td>console show</td>
<td>Displays the configuration settings for the console of an Enforcer appliance. See “Console Show” on page 255.</td>
</tr>
<tr>
<td>date</td>
<td>Sets the date, time, and time zone. See “Date” on page 233.</td>
</tr>
<tr>
<td>debug</td>
<td>Access the Enforcer appliance debug commands. See “Debug Commands” on page 255.</td>
</tr>
<tr>
<td>debug destination</td>
<td>Sets debug destination (memory, disk, both). See “Debug Destination” on page 256.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>debug level</td>
<td>Sets the debug information level. See “Debug Level” on page 256.</td>
</tr>
<tr>
<td>debug show</td>
<td>Displays the configuration settings for debugging. See “Debug Show” on page 257.</td>
</tr>
<tr>
<td>debug upload</td>
<td>Uses the trusted file transfer protocol (tftp) to send a file or files to another computer. See “Debug Upload” on page 257.</td>
</tr>
<tr>
<td>exit</td>
<td>Logs you off from the console of an Enforcer appliance when the command is used as a top-level command; otherwise the command exits a command group. See “Exit” on page 233.</td>
</tr>
<tr>
<td>help</td>
<td>Displays Help for a command See “Help” on page 234.</td>
</tr>
<tr>
<td>hostname</td>
<td>Specifies the host name of an Enforcer appliance See “Hostname” on page 235.</td>
</tr>
<tr>
<td>mab</td>
<td>Provides access to commands on a LAN Enforcer appliance that enables you to implement MAC Authentication Bypass (MAB) on designated 802.1x-aware switches. You must be logged on to the console of a LAN Enforcer appliance as a superuser before you can execute this command. See “MAB commands” on page 258.</td>
</tr>
<tr>
<td>mab database</td>
<td>Provides access to all commands that add and manage local MAB database entries on a LAN enforcer appliance. You must be logged on to the console of a LAN Enforcer appliance as a superuser before you can execute this command.</td>
</tr>
<tr>
<td>mab database add</td>
<td>Specifies the entries of MAC addresses, MAC address ranges, and MAC address masks of all clients that use MAB. (LAN Enforcer appliance only) You must be logged on to the console of a LAN Enforcer appliance as a superuser before you can execute this command.</td>
</tr>
<tr>
<td>mab database clean</td>
<td>Removes all MAC addresses from the local MAB database on a LAN Enforcer appliance. You must be logged on to the console of a LAN Enforcer appliance as a superuser before you can execute this command.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>mab database download</td>
<td>Enables you to download all MAB entries from a TFTP server to the local MAB database on a LAN Enforcer appliance. You must be logged on to the console of a LAN Enforcer appliance as a superuser before you can execute this command.</td>
</tr>
<tr>
<td>mab database upload</td>
<td>The MAB database upload command enables you to copy all MAB entries from a LAN Enforcer appliance to a location, such as a TFTP server. You must be logged on to the console of a LAN Enforcer appliance as a superuser before you can execute this command.</td>
</tr>
<tr>
<td>mab disable</td>
<td>Disables a LAN Enforcer appliance to implement MAC Authentication Bypass (MAB) on designated 802.1x-aware switches. You must be logged on to the console of a LAN Enforcer appliance as a superuser before you can execute this command. See “MAB disable command” on page 260.</td>
</tr>
<tr>
<td>mab enable</td>
<td>Enables a LAN Enforcer appliance to implement MAC Authentication Bypass (MAB) on designated 802.1x-aware switches. You must be logged on to the console of a LAN Enforcer appliance as a superuser before you can execute this command. See “MAB enable command” on page 261.</td>
</tr>
<tr>
<td>mab ldap</td>
<td>Establishes communication between a LAN Enforcer appliance and a LDAP server. You must be logged on to the console of a LAN Enforcer appliance as a superuser before you can execute this command. See “MAB LDAP commands” on page 261.</td>
</tr>
<tr>
<td>mab ldap disable</td>
<td>Disables MAC Authentication Bypass (MAB) on a LDAP server instead of a LAN Enforcer appliance. You must be logged on to the console of a LAN Enforcer appliance as a superuser before you can execute this command. See “MAB LDAP disable command” on page 261.</td>
</tr>
<tr>
<td>mab ldap enable</td>
<td>Enables MAC Authentication Bypass (MAB) on a LDAP server instead of a LAN Enforcer appliance. You must be logged on to the console of a LAN Enforcer appliance as a superuser before you can execute this command. See “MAB enable command” on page 261.</td>
</tr>
</tbody>
</table>
Table 11-2  Summary of CLI commands (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mab show</td>
<td>Displays configuration information about the LDAP server with which the LAN Enforcer appliance communicates.</td>
</tr>
<tr>
<td></td>
<td>See “MAB show command” on page 264.</td>
</tr>
<tr>
<td>monitor</td>
<td>Provides access to the Enforcer monitor commands.</td>
</tr>
<tr>
<td></td>
<td>You must be logged on to the console of a Gateway or a DHCP Enforcer appliance as a superuser before you can execute this command.</td>
</tr>
<tr>
<td></td>
<td>See “Monitor commands” on page 264.</td>
</tr>
<tr>
<td>monitor refresh</td>
<td>Updates information about a client's IP address, host name, policy ID, and MAC address.</td>
</tr>
<tr>
<td></td>
<td>You must be logged on to the console of a Gateway or a DHCP Enforcer appliance as a superuser before you can execute this command.</td>
</tr>
<tr>
<td></td>
<td>See “Monitor refresh command” on page 265.</td>
</tr>
<tr>
<td>monitor show</td>
<td>Display information about blocked-hosts, connected-guests, and connected-users.</td>
</tr>
<tr>
<td></td>
<td>See “Monitor show command” on page 265.</td>
</tr>
<tr>
<td>monitor show blocked-hosts</td>
<td>Displays information about a blocked host's host name and policy ID.</td>
</tr>
<tr>
<td></td>
<td>You must be logged on to the console of a Gateway or a DHCP Enforcer appliance as a superuser before you can execute this command.</td>
</tr>
<tr>
<td></td>
<td>Displays information about a blocked host's host name, policy ID, and MAC address.</td>
</tr>
<tr>
<td></td>
<td>You must be logged on to the console of a Gateway or a DHCP Enforcer appliance as a superuser before you can execute this command.</td>
</tr>
<tr>
<td></td>
<td>See “Monitor show blocked-hosts command” on page 265.</td>
</tr>
<tr>
<td>monitor show connected-guests</td>
<td>Displays information about a connected guest or On-Demand client's IP address, host name, and policy ID.</td>
</tr>
<tr>
<td></td>
<td>You must be logged on to the console of a Gateway or a DHCP Enforcer appliance as a superuser before you can execute this command.</td>
</tr>
<tr>
<td></td>
<td>Displays information about a connected guest or On-Demand client's IP address, host name, policy ID, and MAC address.</td>
</tr>
<tr>
<td></td>
<td>You must be logged on to the console of a Gateway or a DHCP Enforcer appliance as a superuser before you can execute this command.</td>
</tr>
<tr>
<td></td>
<td>See “Monitor show connected-guests commands” on page 266.</td>
</tr>
</tbody>
</table>
### Table 11-2  Summary of CLI commands (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>monitor show connected-users</td>
<td>Displays information about a connected user or a managed client's IP address, host name, username, and policy ID. A connected user or a managed client supports Symantec Endpoint Protection client software and Symantec Network Access Control client software. You must be logged on to the console of a Gateway or a DHCP Enforcer appliance as a superuser before you can execute this command.</td>
</tr>
<tr>
<td></td>
<td>Displays information about a connected user or a managed client's IP address, host name, policy ID, and MAC address. A connected user or a managed client supports Symantec Endpoint Protection client software and Symantec Network Access Control client software. You must be logged on to the console of a Gateway or a DHCP Enforcer appliance as a superuser before you can execute this command.</td>
</tr>
<tr>
<td></td>
<td>See &quot;Monitor show connected-users command&quot; on page 268.</td>
</tr>
<tr>
<td>on-demand authentication local-db delete</td>
<td>Allows you to remove an existing user account from the local database. Control On-Demand client on a client computer. You must be logged on to the console of a Gateway or a DHCP Enforcer appliance as a superuser before you can execute this command.</td>
</tr>
<tr>
<td>on-demand authentication local-db clear</td>
<td>Allows you to clean up all user accounts from the local database. <strong>Note:</strong> Please keep at least one user account if you use local-db authentication. Control On-Demand client on a client computer. You must be logged on to the console of a Gateway or a DHCP Enforcer appliance as a superuser before you can execute this command.</td>
</tr>
<tr>
<td>on-demand disable</td>
<td>Disables the automatic downloading of Symantec Network Access Control On-Demand or guest clients on the Gateway or DHCP Enforcer console. You must be logged on to the console of a Gateway or a DHCP Enforcer appliance as a superuser before you can execute this command.</td>
</tr>
<tr>
<td></td>
<td>See “Logging on to an Enforcer appliance” on page 82.</td>
</tr>
<tr>
<td></td>
<td>See “Disabling Symantec Network Access Control On-Demand clients for client computers” on page 198.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>on-demand enable</td>
<td>Enables the automatic downloading of Symantec Network Access Control On-Demand or guest clients on the Gateway or DHCP Enforcer console. Otherwise the installation fails. You must be logged on to the console of a Gateway or a DHCP Enforcer appliance as a superuser before you can execute this command. See “Logging on to an Enforcer appliance” on page 82. See “Enabling Symantec Network Access Control On-Demand clients to temporarily connect to a network” on page 197. See “On-Demand authentication local-db commands” on page 275.</td>
</tr>
<tr>
<td>on-demand authentication disable</td>
<td>Enables you to stop the authentication process—the auth-daemon—on the console of a Gateway or DHCP appliance for a Symantec Network Access Control On-Demand client. You must be logged on to the console of a Gateway or a DHCP Enforcer appliance as a superuser before you can execute this command. See “Logging on to an Enforcer appliance” on page 82. You can stop the authentication process—the auth-daemon—on the console of a Gateway or DHCP appliance for a Symantec Network Access Control On-Demand client. The on-demand authentication disable command uses the following syntax: on-demand authentication disable You must be logged on a Gateway or DHCP Enforcer appliance console as a superuser before you can execute this command. See &quot;Logging on to an Enforcer appliance&quot; on page 82. The following example describes how to disable authentication for a Symantec Network Access Control On-Demand client on the console of a Gateway or DHCP Enforcer appliance: Enforcer# on-demand Enforcer (on-demand)# authentication disable on page 274.</td>
</tr>
<tr>
<td>on-demand authentication enable</td>
<td>Enables you to start the authentication process—the auth-daemon—on a Gateway or DHCP appliance console for the Symantec Network Access Control On-Demand client. You must be logged on to the console of a Gateway or a DHCP Enforcer appliance as a superuser before you can execute this command. See “Logging on to an Enforcer appliance” on page 82. See “On-demand authentication enable command” on page 274.</td>
</tr>
<tr>
<td><strong>Command</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>--------</td>
<td>----------------</td>
</tr>
</tbody>
</table>
| **on-demand authentication ad disable** | Disables authentication of the Symantec Network Access Control On-Demand Client computer.  
You must be logged on to the console of a Gateway or a DHCP Enforcer appliance as a superuser before you can execute this command.  
See “Logging on to an Enforcer appliance” on page 82.  
See “On-demand authentication ad disable command” on page 272. |
| **on-demand authentication ad domain** | Configures the communication between an Enforcer appliance and an active directory for the authentication of an On-Demand Client computer.  
You must be logged on to the console of a Gateway or a DHCP Enforcer appliance as a superuser before you can execute this command.  
See “Logging on to an Enforcer appliance” on page 82.  
See “On-demand authentication ad domain command” on page 273. |
| **on-demand authentication ad enable** | Enables authentication of the On-Demand Client computer.  
You must be logged on to the console of a Gateway or a DHCP Enforcer appliance as a superuser before you can execute this command.  
See “Logging on to an Enforcer appliance” on page 82.  
See “On-demand authentication ad enable command” on page 273. |
| **on-demand authentication local-db** | Provides access to the on-demand authentication local-db commands.  
You must be logged on to the console of a Gateway or a DHCP Enforcer appliance as a superuser before you can execute this command.  
See “Logging on to an Enforcer appliance” on page 82.  
See “On-Demand authentication local-db commands” on page 275. |
| **on-demand authentication local-db add** | Enables you to set up the login name and password on a Gateway or DHCP appliance console for an end user who wants to automatically download a Symantec Network Access Control On-Demand client on a client computer.  
You must be logged on to the console of a Gateway or a DHCP Enforcer appliance as a superuser before you can execute this command.  
See “Logging on to an Enforcer appliance” on page 82. |
### Table 11-2 Summary of CLI commands (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>on-demand authentication local-db</td>
<td>Allows you to disable an authentication configuration for an On-Demand Client computer against a local database.</td>
</tr>
<tr>
<td>disable</td>
<td>You must be logged on to the console of a Gateway or a DHCP Enforcer appliance as a superuser before you can execute this command.</td>
</tr>
<tr>
<td></td>
<td>See “Logging on to an Enforcer appliance” on page 82.</td>
</tr>
<tr>
<td>on-demand authentication local-db</td>
<td>Allows you to enable an authentication configuration for an On-Demand Client computer against a local database.</td>
</tr>
<tr>
<td>enable</td>
<td>You must be logged on to the console of a Gateway or a DHCP Enforcer appliance as a superuser before you can execute this command.</td>
</tr>
<tr>
<td></td>
<td>See “Logging on to an Enforcer appliance” on page 82.</td>
</tr>
<tr>
<td>on-demand authentication show</td>
<td>Allows you to display authentication settings for an On-Demand Client computer.</td>
</tr>
<tr>
<td></td>
<td>You must be logged on to the console of a Gateway or a DHCP Enforcer appliance as a superuser before you can execute this command.</td>
</tr>
<tr>
<td></td>
<td>See “Logging on to an Enforcer appliance” on page 82.</td>
</tr>
<tr>
<td>on-demand banner</td>
<td>Enables you to edit the default banner on the Welcome page of the Symantec Network Access Control On-Demand clients.</td>
</tr>
<tr>
<td></td>
<td>You must be logged on to the console of a Gateway or a DHCP Enforcer appliance as a superuser before you can execute this command.</td>
</tr>
<tr>
<td></td>
<td>See “Logging on to an Enforcer appliance” on page 82.</td>
</tr>
<tr>
<td></td>
<td>See “Editing the banner on the Welcome page” on page 202.</td>
</tr>
<tr>
<td></td>
<td>See “On-Demand banner command” on page 277.</td>
</tr>
<tr>
<td>on-demand spm-domain</td>
<td>Allows you to configure the domain ID on the console of a Gateway or DHCP Enforcer appliance. Otherwise the On-Demand Client installation fails.</td>
</tr>
<tr>
<td></td>
<td>See “Enabling Symantec Network Access Control On-Demand clients to temporarily connect to a network” on page 197.</td>
</tr>
<tr>
<td></td>
<td>After connection with the , the domain ID appears on the Enforcer appliance.</td>
</tr>
<tr>
<td></td>
<td>See the Administration Guide for Symantec Endpoint Protection and Symantec Network Access Control on how to locate the domain ID.</td>
</tr>
<tr>
<td></td>
<td>You must be logged on to the console of a Gateway or a DHCP Enforcer appliance as a superuser before you can execute this command.</td>
</tr>
<tr>
<td></td>
<td>See “Logging on to an Enforcer appliance” on page 82.</td>
</tr>
<tr>
<td></td>
<td>See “On-Demand spm-domain command” on page 288.</td>
</tr>
</tbody>
</table>
Table 11-2  Summary of CLI commands (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>on-demand dot1x</td>
<td>Allows you to enable your configuration of port-based 802.1x network access control authentication for On-Demand Client sessions.</td>
</tr>
<tr>
<td></td>
<td>You must be logged on to the console of a Gateway or a DHCP Enforcer appliance as a superuser before you can execute this command.</td>
</tr>
<tr>
<td></td>
<td>See “Logging on to an Enforcer appliance” on page 82.</td>
</tr>
<tr>
<td>on-demand dot1x default-user</td>
<td>Allows you to configure anonymous port-based 802.1x network access control authentication for On-Demand Client sessions.</td>
</tr>
<tr>
<td></td>
<td>You must be logged on to the console of a Gateway or a DHCP Enforcer appliance as a superuser before you can execute this command.</td>
</tr>
<tr>
<td></td>
<td>See “Logging on to an Enforcer appliance” on page 82.</td>
</tr>
<tr>
<td>on-demand dot1x certificate</td>
<td>Allows you to configure an 802.1x authentication root and user certificate.</td>
</tr>
<tr>
<td></td>
<td>You must be logged on to the console of a Gateway or a DHCP Enforcer appliance as a superuser before you can execute this command.</td>
</tr>
<tr>
<td></td>
<td>See “Logging on to an Enforcer appliance” on page 82.</td>
</tr>
<tr>
<td></td>
<td>See “On-Demand dot1x certificate commands” on page 278.</td>
</tr>
<tr>
<td>on-demand dot1x certificate import</td>
<td>Allows you to import an 802.1x authentication certificate.</td>
</tr>
<tr>
<td></td>
<td>You must be logged on to the console of a Gateway or a DHCP Enforcer appliance as a superuser before you can execute this command.</td>
</tr>
<tr>
<td></td>
<td>See “Logging on to an Enforcer appliance” on page 82.</td>
</tr>
<tr>
<td></td>
<td>See “On-Demand dot1x certificate import” on page 279.</td>
</tr>
<tr>
<td>on-demand dot1x certificate remove</td>
<td>Allows you to delete an 802.1x authentication certificate.</td>
</tr>
<tr>
<td></td>
<td>You must be logged on to the console of a Gateway or a DHCP Enforcer appliance as a superuser before you can execute this command.</td>
</tr>
<tr>
<td></td>
<td>See “Logging on to an Enforcer appliance” on page 82.</td>
</tr>
<tr>
<td></td>
<td>See “On-Demand dot1x certificate remove command” on page 280.</td>
</tr>
<tr>
<td>on-demand dot1x peap</td>
<td>Allows you to configure an 802.1x Protected Extensible Authentication Protocol (PEAP) to authenticate an On-Demand Client into the protected network.</td>
</tr>
<tr>
<td></td>
<td>You must be logged on to the console of a Gateway or a DHCP Enforcer appliance as a superuser before you can execute this command.</td>
</tr>
<tr>
<td></td>
<td>See “Logging on to an Enforcer appliance” on page 82.</td>
</tr>
<tr>
<td></td>
<td>See “On-Demand dot1x peap command” on page 281.</td>
</tr>
</tbody>
</table>
Table 11-2  Summary of CLI commands (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| on-demand dot1x peap validate-svr enable | Allows you to enable the validation of an 802.1x Protected Extensible Authentication Protocol (PEAP) server certificate for On-Demand Client access to the protected network.  
You must be logged on to the console of a Gateway or a DHCP Enforcer appliance as a superuser before you can execute this command.  
See “Logging on to an Enforcer appliance” on page 82.  
See “On-Demand dot1x peap cert-svr command” on page 282. |
| on-demand dot1x peap validate-svr disable | Allows you to disable validation of an 802.1x Protected Extensible Authentication Protocol (PEAP) server certificate for On-Demand Client access to the protected network.  
You must be logged on to the console of a Gateway or a DHCP Enforcer appliance as a superuser before you can execute this command.  
See “Logging on to an Enforcer appliance” on page 82.  
See “On-Demand dot1x peap cert-svr command” on page 282. |
| on-demand dot1x peap cert-svr | Allows you to configure an 802.1x Protected Extensible Authentication Protocol (PEAP) root server certificate as well as a user certificate for On-Demand Client access to the protected network.  
You must be logged on to the console of a Gateway or a DHCP Enforcer appliance as a superuser before you can execute this command.  
See “Logging on to an Enforcer appliance” on page 82. |
| on-demand dot1x peap fast-reconn enable | Allows you to enable 802.1x Protected Extensible Authentication Protocol (PEAP) fast reconnection to the root server certificate for On-Demand Client access to the protected network.  
You must be logged on to the console of a Gateway or a DHCP Enforcer appliance as a superuser before you can execute this command.  
See “Logging on to an Enforcer appliance” on page 82. |
| on-demand dot1x peap fast-reconn disable | Allows you to disable 802.1x Protected Extensible Authentication Protocol (PEAP) fast reconnection to the root server certificate for On-Demand Client access to the protected network.  
You must be logged on to the console of a Gateway or a DHCP Enforcer appliance as a superuser before you can execute this command.  
See “Logging on to an Enforcer appliance” on page 82. |
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>on-demand dot1x peap show</td>
<td>Allows you to display the configuration settings for an 802.1x Protected Extensible Authentication Protocol (PEAP) authentication for an On-Demand Client to confirm that the active protocol is PEAP.</td>
</tr>
<tr>
<td></td>
<td>You must be logged on to the console of a Gateway or a DHCP Enforcer appliance as a superuser before you can execute this command.</td>
</tr>
<tr>
<td></td>
<td>See “Logging on to an Enforcer appliance” on page 82.</td>
</tr>
<tr>
<td>on-demand dot1x peap exit</td>
<td>Allows you to exit the command line interface configuration hierarchy for 802.1x Protected Extensible Authentication Protocol (PEAP).</td>
</tr>
<tr>
<td></td>
<td>You must be logged on to the console of a Gateway or a DHCP Enforcer appliance as a superuser before you can execute this command.</td>
</tr>
<tr>
<td></td>
<td>See “Logging on to an Enforcer appliance” on page 82.</td>
</tr>
<tr>
<td>on-demand dot1x protocol</td>
<td>Allows you to configure an 802.1x Protected Extensible Authentication Protocol (PEAP) for On-Demand Client access to the protected network as either PEAP or TLS.</td>
</tr>
<tr>
<td></td>
<td>You must be logged on to the console of a Gateway or a DHCP Enforcer appliance as a superuser before you can execute this command.</td>
</tr>
<tr>
<td></td>
<td>See “Logging on to an Enforcer appliance” on page 82.</td>
</tr>
<tr>
<td>on-demand dot1x show</td>
<td>Allows you to display at the command line interface the 802.1x Protected Extensible Authentication Protocol (PEAP) configuration for an On-Demand Client and confirm that the configured protocol is either PEAP or TLS.</td>
</tr>
<tr>
<td></td>
<td>You must be logged on to the console of a Gateway or a DHCP Enforcer appliance as a superuser before you can execute this command.</td>
</tr>
<tr>
<td></td>
<td>See “Logging on to an Enforcer appliance” on page 82.</td>
</tr>
<tr>
<td>on-demand dot1x tls</td>
<td>Allows you to enter configuration mode for 802.1x transport layer security (TLS) protocol.</td>
</tr>
<tr>
<td></td>
<td>You must be logged on a Gateway or a DHCP Enforcer console as a superuser before you can execute this command.</td>
</tr>
<tr>
<td></td>
<td>See “Logging on to an Enforcer appliance” on page 82.</td>
</tr>
<tr>
<td>on-demand dot1x tls validate-svr enable</td>
<td>Allows you to enable the validation of a root server certificate for an 802.1x transport layer security (TLS) protocol configuration.</td>
</tr>
<tr>
<td></td>
<td>You must be logged on a Gateway or a DHCP Enforcer console as a superuser before you can execute this command.</td>
</tr>
<tr>
<td></td>
<td>See “Logging on to an Enforcer appliance” on page 82.</td>
</tr>
<tr>
<td></td>
<td>See “On-Demand dot1x peap cert-svr command” on page 282.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>on-demand dot1x tls validate-svr disable</td>
<td>Allows you to disable the validation of a root server certificate for an 802.1x transport layer security (TLS) protocol configuration. You must be logged on a Gateway or a DHCP Enforcer console as a superuser before you can execute this command. See “Logging on to an Enforcer appliance” on page 82.</td>
</tr>
<tr>
<td>on-demand dot1x tls cert-svr enable</td>
<td>Allows you to configure a root server certificate for an 802.1x transport layer security (TLS) protocol for On-Demand Client authentication. You must be logged on a Gateway or a DHCP Enforcer console as a superuser before you can execute this command. See “Logging on to an Enforcer appliance” on page 82.</td>
</tr>
<tr>
<td>on-demand dot1x tls cert-svr disable</td>
<td>Disable TLS certificate server.</td>
</tr>
<tr>
<td>on-demand dot1x tls cert-svr host</td>
<td>Set TLS certificate server's hostname.</td>
</tr>
<tr>
<td>on-demand dot1x tls show</td>
<td>Allows you to view configuration settings for an 802.1x transport layer security (TLS) protocol for On-Demand Client authentication. You must be logged on the Gateway or DHCP Enforcer console as a superuser before you can execute this command. See “Logging on to an Enforcer appliance” on page 82.</td>
</tr>
<tr>
<td>on-demand dot1x tls exit</td>
<td>Allows you to exit the command line interface mode for 802.1x TLS configuration. You must be logged on a Gateway or a DHCP Enforcer console as a superuser before you can execute this command. See “Logging on to an Enforcer appliance” on page 82.</td>
</tr>
</tbody>
</table>
Table 11-2 Summary of CLI commands (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>on-demand client-group</td>
<td>Enables you to configure the preferGroup on the Gateway or DHCP Enforcer console and on the Console. Otherwise the installation fails. Although it is optional to set up a separate group for the Symantec Network Access Control On-Demand clients, it is recommend that you do so. If you do not set up a separate group, all Symantec Network Access Control On-Demand clients automatically become a member of the Default group on the Symantec Endpoint Protection Manager Console.</td>
</tr>
<tr>
<td></td>
<td>You must be logged on a Gateway or a DHCP Enforcer console as a superuser before you can execute this command.</td>
</tr>
<tr>
<td></td>
<td>See “Logging on to an Enforcer appliance” on page 82.</td>
</tr>
<tr>
<td></td>
<td>See “Enabling Symantec Network Access Control On-Demand clients to temporarily connect to a network ” on page 197.</td>
</tr>
<tr>
<td></td>
<td>See “On-Demand client-group command” on page 277.</td>
</tr>
<tr>
<td></td>
<td>See the Administration Guide for Symantec Endpoint Protection and Symantec Network Access Control On-Demand clients on how to set up a group for the Symantec Network Access Control On-Demand clients or guest clients.</td>
</tr>
<tr>
<td>on-demand mac-compliance</td>
<td>Enables you to configure the Symantec Network Access Control On-Demand client on a Macintosh platform from having an end user install unauthorized programs and files.</td>
</tr>
<tr>
<td></td>
<td>You must be logged on the Gateway or DHCP Enforcer console as a superuser before you can execute this command.</td>
</tr>
<tr>
<td></td>
<td>See “On-Demand mac-compliance commands” on page 289.</td>
</tr>
<tr>
<td>on-demand mac-compliance enable</td>
<td>Allows you to configure the host integrity options for an On-Demand Client Macintosh platform.</td>
</tr>
<tr>
<td></td>
<td>You must be logged on the Gateway or DHCP Enforcer console as a superuser before you can execute this command.</td>
</tr>
<tr>
<td></td>
<td>See &quot;On-Demand mac-compliance commands&quot; on page 289.</td>
</tr>
<tr>
<td>on-demand mac-compliance disable</td>
<td>Allows you to disable the host integrity configuration for an On-Demand Client Macintosh platform.</td>
</tr>
<tr>
<td></td>
<td>You must be logged on the Gateway or DHCP Enforcer console as a superuser before you can execute this command.</td>
</tr>
<tr>
<td></td>
<td>See &quot;Logging on to an Enforcer appliance&quot; on page 82.</td>
</tr>
</tbody>
</table>
Table 11-2  Summary of CLI commands (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>on-demand mac-compliance show</td>
<td>Allows you to configure the list of host integrity software options for an On-Demand Client Macintosh platform.</td>
</tr>
<tr>
<td></td>
<td>See “On-Demand mac-compliance commands” on page 289.</td>
</tr>
<tr>
<td></td>
<td>You must be logged on the Gateway or DHCP Enforcer console as a superuser before you can execute this command.</td>
</tr>
<tr>
<td></td>
<td>See “Logging on to an Enforcer appliance” on page 82.</td>
</tr>
<tr>
<td>on-demand mac-compliance interval</td>
<td>Allows you to set compliance checking interval (in minutes) for Symantec Network Access Control On-demand Client.</td>
</tr>
<tr>
<td>password</td>
<td>Changes the password to log on to the Enforcer appliance.</td>
</tr>
<tr>
<td></td>
<td>See “Password” on page 235.</td>
</tr>
<tr>
<td>ping</td>
<td>Sends an ICMP echo to a remote host.</td>
</tr>
<tr>
<td></td>
<td>See “Ping” on page 235.</td>
</tr>
<tr>
<td>reboot</td>
<td>Restart the Enforcer appliance.</td>
</tr>
<tr>
<td></td>
<td>See “Reboot” on page 236.</td>
</tr>
<tr>
<td>show</td>
<td>Shows Enforcer appliance configuration and status information.</td>
</tr>
<tr>
<td></td>
<td>See “Show” on page 236.</td>
</tr>
<tr>
<td>shutdown</td>
<td>Turns off an Enforcer appliance.</td>
</tr>
<tr>
<td></td>
<td>See “Shutdown” on page 236.</td>
</tr>
<tr>
<td>snmp disable</td>
<td>Disable SNMP.</td>
</tr>
<tr>
<td>snmp enable</td>
<td>Enable SNMP.</td>
</tr>
<tr>
<td>snmp heartbeat</td>
<td>Set the heartbeat for SNMP.</td>
</tr>
<tr>
<td>snmp receiver</td>
<td>SNMP receiver settings.</td>
</tr>
<tr>
<td>snmp show</td>
<td>Show the configuration and status of SNMP.</td>
</tr>
<tr>
<td>snmp trap</td>
<td>SNMP try times and timeout value setting.</td>
</tr>
<tr>
<td>start</td>
<td>Starts an Enforcer &amp;; service.</td>
</tr>
<tr>
<td></td>
<td>See “Start” on page 238.</td>
</tr>
</tbody>
</table>
### Table 11-2  Summary of CLI commands (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| **stop** | Stops an Enforcer service.  
See “Stop” on page 238. |
| **traceroute** | Prints the route that packets take to the network host.  
See “Traceroute” on page 238. |
| **update** | Updates the Enforcer appliance software.  
See “Update” on page 238. |

---

**Top-level commands**

Top-level commands are available at the Enforcer CLI. They are general administration commands. Some of the commands, such as clear, exit, help, and show, are available from all levels of the hierarchy.

### Clear

The clear command clears the contents of the screen.

The following is an example of the syntax:

```
Enforcer# clear
```

### Date

The date command sets the system time or time zone for the appliance.

The following is an example of the syntax:

```
date {day <MM/DD/YY> | time <HH:MM:SS> |timezone}
```

### Exit

The exit command exits the console, when used as a main command, or exits a command group when used from within a command group. You can also use Ctrl+D instead of the exit command.

The following is an example of the syntax:

```
Enforcer# exit
```
Help

The help command displays help information for a specified command. If you want to display help for all available commands, type a question mark (?) or press Tab.

**Note:** A few commands are specific only to the Gateway Enforcer or only to the DHCP Enforcer. These commands do not appear on the other Enforcers.

The following is an example of the syntax for the Main Command Group:

```
help {capture | clear | configure | console | date |
debug | exit | hostname | mab | monitor | on-demand |
password | ping | reboot | show | shutdown | start |
stop | traceroute | update | snmp}
```

When you use the Help command within a command group, it displays help information for an individual command in the group. To display help for all commands in the group, you can type a question mark (?) or press Tab.

The following is an example of the syntax for the Capture Command Group:

```
help {clear | compress | exit | filter | show | start |
verbose | ymodem | upload}
```

The following is an example of the syntax for the Configure Command Group:

```
help {advanced | clear | dns | exit | interface |
interface-role | route | show | spm | redirect | ntp}
```

The following is an example of the syntax for the Configure Advanced Command Group:

```
help {catos | check-uid | clear | dnsspoofing | exit |
failover |
legacy | legacy-uid | local-auth | snacs | user-class | show |
trunking}
```

The following is an example of the syntax for the Console Command Group:

```
help {baud-rate | clear | dimensions | exit |
re-initialize | show | ssh | sshkey}
```

The following is an example of the syntax for the Debug Command Group:
help {clear | compress | destination | exit | level | show | ymodem | upload}

The following is an example of the syntax for the Monitor Command Group:

help {refresh | show connected-guests | show blocked-hosts | show connected-users}

Hostname

The hostname command changes the host name of the Enforcer appliance. The default host name is Enforcer. If you change the name of an Enforcer appliance, you can distinguish between multiple Enforcer appliances on the Symantec Endpoint Protection Manager and in the Enforcer logs.

The host name is automatically registered on the Symantec Endpoint Protection Manager during the next heartbeat. If you change the host name of an Enforcer appliance, you may also need to change the entry on the DNS server.

The following is an example of syntax for the hostname command:

hostname hostname

Password

The password command changes the account password. You must confirm the existing password before specifying and confirming the new password. The new password must contain one lowercase letter, one uppercase letter, one digit, and one symbol.

The following is an example of syntax for the password:

password

Ping

The ping command verifies the connections to a remote host that have been specified with an IP address or host name. The command uses an ICMP echo request and echo reply packets to determine whether a particular IP system on a network is functional. You can use the ping command for diagnosing IP network or router failures. The ping command enables you to check whether or not an Enforcer appliance can communicate with the Symantec Endpoint Protection Manager.

The following is an example of the syntax for the ping command:
ping ip-address | hostname

Example

ping 192.168.0.1

PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
64 bytes from 192.168.0.1: icmp_seq=0 ttl=64 time=0.585 ms
64 bytes from 192.168.0.1: icmp_seq=1 ttl=64 time=0.149 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=64 time=0.131 ms
64 bytes from 192.168.0.1: icmp_seq=3 ttl=64 time=0.128 ms

--- 192.168.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 57ms

rtt min/avg/max/mdev = 0.128/0.248/0.585/0.194 ms, pipe 2,
ipg/ewma 19.043/0.436 ms

Reboot

The reboot command restarts the Enforcer appliance.
The following is an example of the syntax for the reboot command:
reboot

Shutdown

The shutdown command shuts down the Enforcer appliance.
The following is an example of the syntax for the shutdown command:
shutdown

Show

The show command shows the information about the Enforcer appliance configuration or status.
The following is an example of syntax for the show command:
show { capture | configure | console | date | debug |
hostame | status | update | version }

where:

capture Display the packet capture settings such as protocol, filters, and compression
configure Shows the Enforcer network and the Symantec Endpoint Protection Manager configuration
consolle Shows the console configuration
status Shows the Enforcer service detail status
update Shows the update available for installation from tftp, CD-ROM, or USB drive
version Shows the Enforcer version and copyright information
date Display local time and UTC time
debug Display the Enforcer debug configuration
hostname Display the appliance hostname

The following example lists the output of the show status command:

show status
Enforcer Status: ONLINE(ACTIVE)
Policy Manager Connected: NO
Policy Manager: 192.168.0.64 HTTP 80
Packets Received: 26
Packets Transmitted: 1
Packets Rx. Failed: 0
Packets Tx. Failed: 0
Enforcer Health: EXCELLENT
Enforcer Uptime: 0 days 00:00:28
Policy ID:

The following example lists the output of the show version command on a DHCP Enforcer appliance:

show version
Symantec Network Access Control Enforcer 6100 Series - v11.0.1
build XXXX, 2007-11-29,19:09
DHCP Enforcer mode
Start

The start command starts the Enforcer service.

The following is an example of the syntax for the start command:

```
Enforcer# start
```

Stop

The stop command stops the Enforcer service.

The following is an example of the syntax for the stop command:

```
Enforcer# Stop
```

Traceroute

The traceroute command traces the route that packets take to get to a remote host. The remote host has been specified with an IP address or host name.

The following is an example of the syntax for the traceroute command:

```
traceroute [ ip-address | hostname ]
```

Example

```
traceroute 10.50.0.180

traceroute to 10.50.0.180 (10.50.0.180), 30 hops max, 38-byte packets

  1 192.168.0.1 (192.168.0.1) 0.391 ms 0.132 ms 0.111 ms
  2 10.50.2.1 (10.50.2.1) 0.838 ms 0.596 ms 0.589 ms
  3 oldserver1.sygate.dev (10.50.0.180) 1.170 ms 0.363 ms 0.469 ms
```

Update

The update command updates the Enforcer software package from a tftp server, USB hard disk, or CD-ROM.

The following is an example of the syntax for the update command:

```
Enforcer:# update
```
Capture commands

Commands in the Enforcer appliance capture command group allow you to capture packets on the Enforcer appliance NICs. The packets are saved to a file. Additional commands allow you to send the file in plain or compressed format to a client by various file-transfer protocols (tftp). The Enforcer appliance must be connected to the client by using the serial cable that is provided.

All commands in this group are listed and described except the capture exit and the capture help commands. The capture exit command exits the command group. The capture help commands displays help information on all the commands in the group.

Capture Compress

The capture compress command compresses the file

The capture compress command uses the following syntax:

\[
\text{compress \{on | off\}}
\]

where:

on Enables compressions.

off Disables compressions.

The following example describes the syntax for the filter compress on command on the console of an Enforcer appliance:

```
Enforcer# capture
Enforcer(capture)# compress on
```

Capture Filter

The capture filter command sets a filter that specifies which packets are captured.

The capture filter command uses the following syntax:

\[
\text{filter [auth] [spm] [failover] [all] [client ip-range]}
\]

where:

Enforcer:
auth: Captures the authentication packets that are sent among the client, Enforcer appliance, and the Symantec Endpoint Protection Manager.

The default argument is auth.

spm: Captures the communication packets between the Symantec Endpoint Protection Manager and an Enforcer; capture an Enforcer profile by downloading from the Symantec Endpoint Protection Manager and log uploading packets.

failover: Captures the Enforcer failover packets (sent out periodically to search for another Enforcer on the network). Failover is not accessible with failopen card installed.

all: Captures all the packets that are specified.

clientip-range: This option is only available with the Gateway and DHCP Enforcers.

Sets the client IP range for capturing authentication packets on Gateway and LAN Enforcers only. The ip-range can be a combination of IP addresses, IP range, and subnet/mask. A comma with no spaces separates the arguments. You can format it as follows:

- IP address is formatted as nnn.nnn.nnn.nnn
- IP range is formatted as nnn.nnn.nnn.nnn-nnn.nnn.nnn.nnn
- Subnet/mask is formatted as nnn.nnn.nnn.nnn/nnn.nnn.nnn.nnn

The following example describes the syntax for the capture filter command:

```
Enforcer# capture filter auth client
192.168.0.1,192.168.0.10-192.168.0.100,192.168.1.1/255.255.255.0
```

This command filters all authentication packets for clients with the IP address 192.168.0.1. It filters the clients whose IP address is in the range 192.168.0.10 to 192.168.0.100, and clients in the subnet 192.168.1.1 with a netmask of 255.255.255.0.

**Capture Show**

The capture show command displays the capture configuration and lists the files that are captured.

The capture show command uses the following syntax:
show {compress | files | filter | verbose | ymodem}

where:

compress  Shows if file compression is on or off
files     Shows all captured files in the Enforcer appliance's capture folder
filter    Shows the current filter configuration
verbose   Shows the current verbose configuration
ymodem    Shows the Ymodem protocol option settings

Example:

capture show

Capture Filter:  auth
Client IP Range:  
Capture Verbose is ON.
Compress capture files before sending is ON.
YMODEM protocol option is YMODEM-g.

Capture Start

The capture start command starts packet capture. To stop, press Esc

The capture start command uses the following syntax:

capture [start]

Example

Enforcer# capture
Enforcer(capture)# start

Captured packets are saved to /opt/GatewayEnforcer/bin/../capture/Dec-07-200

5-12-24-23.cap.

Press ESC to stop capture...
0  0.000000 192.168.0.25 -> 192.168.0.211 UDP Heartbeat Ver 5.1.1915
Start Session to Agent. SEQ: 0f495cd8.
1 0.000000 192.168.0.25 -> 192.168.0.64 UDP RADIUS Access Request.
ID 64 192.168.0.211  Query Status

2 0.000000 192.168.0.211 -> 192.168.0.25 UDP Heartbeat Ver 5.0.0
Keep Alive to Enforcer. SEQ: 0f495cd8. HI Disabled.
Profile 85E0-10/20/2005 11:30:00 812.
Host Integrity check is disabled. Host Integrity policy is disabled by
administrator.

3 0.000000 192.168.0.64 -> 192.168.0.25 UDP RADIUS Access Accept. ID 64
192.168.0.211  Profile 85E0-10/20/2005 11:30:00 812
4 packets were captured.

Captured packets were saved to /opt/GatewayEnforcer/bin/../capture/
Mar-07-2006-1
2-24-23.cap.

Capture Upload
The capture upload command uses the tftp protocol to send a file or files.
The capture upload command uses the following syntax:
capture upload {tftp://nnn.nnn.nnn.nnn filename}
Example:
Enforcer# capture
Enforcer(capture)# upload tftp://10.200.38.221 test.tar.gz

Capture Verbose
The capture verbose command enables or disables the display of packet details
while the capture occurs.
The capture verbose command uses the following syntax:
verbose {on | off}
where:
on Displays packet details
Configure commands

Commands in the Enforcer appliance CLI configure group allow you to view and configure the network interface settings and the connection to the Symantec Endpoint Protection Manager.

All commands in this group are listed and described except for the exit and help commands. The exit command exits the command group. The help command displays help information on individual commands in the group.

The configure group contains a command called advanced that gives access to a set of advanced configuration options.

See “Configure advanced commands” on page 243.

Configure advanced commands

Commands in the Enforcer appliance CLI advanced group are part of the configure group. They enable you to configure Enforcer advanced configuration settings.

All the commands in this group are described except the exit and help commands. The exit command exits the command group. The help command displays help information on the individual commands in the group.

Advanced CATOS

The advanced CATOS command enables or disables Cisco CATOS support.

The advanced catos command uses the following syntax (LAN Enforcer): 

advanced catos {enable | disable}

Advanced check-uid

The advanced check-uid command enables or disables UID checking for legacy agents.

The advanced check-uid command uses the following syntax (Gateway and DHCP Enforcer):

advanced check-uid {enable | disable}
Advanced DNS spoofing

The advanced DNSspoofing command configures a DNS spoofing IP address and enables or disables it in the DHCP Enforcer. Disabling deletes the DNS spoofing IP address and disables it in the DHCP Enforcer.

The advanced dnsspoofing command uses the following syntax (DHCP Enforcer):

```
advanced dnsspoofing enable ip ip address | disable
```

Advanced failover

The advanced failover command enables or disables Enforcer appliance failover and configures the failover port and sensitivity level.

This command is not accessible if Failopen is enabled.

The advanced failover command uses the following syntax (Gateway or DHCP Enforcer appliances):

```
advanced failover disable | {enable [port <port-number>] [sensitive <sensitive-level>]]}
```

where:

- `disable` Disables the Enforcer appliance failover
- `enable` Enables the Enforcer appliance failover
  The default setting is enable.
- `port portnumber` Specifies an Enforcer failover port number from 1 to 65535
- `sensitive sensitivity level` Specifies an Enforcer appliance failover sensitivity level from 0 to 4 to indicate how often to check for other Enforcers

Gateway and DHCP Enforcers appliances have the following default configuration settings:

- Failover is enabled.
- The UDP port that the failover Enforcers use to communicate with each other is 39999.
- The default failover sensitivity level is High (less than 5 seconds).
  This setting determines how quickly the standby Enforcer appliance becomes the primary Enforcer appliance if it detects that the primary Enforcer has become disabled. The higher the level that is specified, the shorter the delay before the standby Enforcer appliance takes over. At the same time more overhead is introduced in both networking and CPU processing.
The following levels are available:

- **Very High (0)**  Fewer than 2 seconds
- **High (1)**  Fewer than 5 seconds
- **Medium (2)**  Fewer than 10 seconds
- **Low (3)**  Fewer than 15 seconds
- **Very low (4)**  Fewer than 30 seconds

### Advanced legacy

The advanced legacy command enables or disables support for legacy agents. Legacy agent support is enabled by default.

Legacy agents refers to Agents that run pre-5.x Sygate Security Agent software. For LAN Enforcer appliances, legacy agent represents Sygate Security Agents that run version 4.1 and later.

Legacy agent represents Sygate Security Agents that run version 3.5 or 4.x and do not include versions 2.x, 3.0, and 3.1.

**Note:** Support for legacy agents applies only to DHCP or Gateway Enforcer appliances.

The advanced legacy command uses the following syntax:

`advanced legacy {allow | block}`

where:

- **allow**  Allows the legacy agents
  - The default setting is allow.
- **block**  Block legacy agents

You can use Enforcer appliances on the sites that run earlier (legacy) versions of agents. If you allow legacy agents, the Enforcer appliance confirms that the legacy agent runs and then verifies the results of the Host Integrity check. If the agent passes the Host Integrity check, the agent can connect to the network. For legacy agents, the Enforcer appliance does not check the agent identifier to verify that it is a valid agent. It also does not check its profile serial number to confirm that its policies are up-to-date.
Advanced legacy-uid

The advanced legacy-uid command specifies the legacy client GUID.

The advanced legacy-uid command uses the following syntax (Gateway and DHCP Enforcer appliances):

```
advanced legacy-uid uid-string
```

Advanced local-auth

The advanced local-auth command enables or disables the Enforcer’s authentication of the client. Use this command for troubleshooting.

Client authentication is disabled by default.

The advanced local-auth command uses the following syntax:

```
advanced local-auth {disable | enable}
```

where:

- **Enable**: Verifies the client with the Symantec Endpoint Protection Manager and blocks the client if it is unable to connect to a Symantec Endpoint Protection Manager.
  
  The default setting for client authentication is enable.

- **Disable**: Disables the verification of the client and performs Host Integrity validation only.

By default, the Gateway Enforcer appliance verifies the unique identifier (UID) 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 UID, it blocks the client. Although it is not recommended as a troubleshooting step, you can stop the Gateway Enforcer appliance from verifying the UID.

By default, the Gateway Enforcer appliance verifies the UID. Instead, the Gateway Enforcer appliance only performs a Host Integrity validation check. Be sure to re-enable this setting if you want the Gateway Enforcer appliance to verify the UID.

Advanced Radius

The advanced Radius command configures, enables, or disables Radius accounting proxy support.

The advanced radius command uses the following syntax (LAN Enforcer appliance):

```
advanced radius acc_proxy {enable | disable} | acc_port <1811-1813>
```
The following example describes the syntax for the advanced radius command (LAN Enforcer appliance):

```
Enforcer(advanced)# radius proxy {enable | disable}
```

**Advanced Re-initialize**

The advanced re-initialize command enables the switch to different Enforcer types by re-initializing the Enforcer configuration. This command is not available if you are logged into an SSH session.

The advanced re-initialize command uses the following syntax:

```
advanced re-initialize
```

**Advanced Symantec Network Access Control Server Scanner**

The advanced snacs command sets the IP address of the Symantec Network Access Control scanner, port number, and pre-share key. You can use this command to re-enable the Symantec Network Access Control scanner if it has been disabled.

**Note:** Symantec Network Access Control Scanner does not support a printer connection to a Symantec DHCP Enforcer appliance. Printers do not accept the static routes that are configured for a Symantec DHCP Enforcer appliance. Therefore, the Symantec Network Access Control Scanner cannot communicate with a printer that is connected to a Symantec DHCP Enforcer appliance.

The advanced snacs command uses the following syntax (Gateway Enforcer appliance and DHCP Enforcer appliance):

```
advanced snacs enable | disable | set [ip <ipaddress>] [port <1811-1813>] [key <string>]
```

The following example describes the syntax for the advanced snacs command (Gateway Enforcer appliance and DHCP Enforcer appliance):

```
Enforcer(advanced)# snacs
```

```
disable  disable snacs
set ip   set ip IP address
set key  set key string
```
Advanced Show

The advanced show command shows the configuration settings for the Enforcer advanced commands.

The show command uses the following syntax:

```
show
```

Example:

```
Enforcer# configure advanced show
Failover Status: ENABLED
Failover Port: 39999
Failover Sensitivity Level: 1
Legacy Client: ALLOW
Local Authentication: ENABLED
```

Advanced User-class

The advanced user-class command enables or disables the user class ID SYGATE_ENF on the Enforcer appliance.

The advanced user_class command uses the following syntax (DHCP Enforcer):

```
advanced user_class {disable | enable}
```

where:

```
disable     Disables the Enforcer appliance user class ID
Enable       Disables the Enforcer appliance user class ID
```

If you want to use one DHCP server as both the normal and quarantine DHCP server, you must complete the following configuration steps:

- After you install the Enforcer appliance, use the advanced user_class command to enable the user class ID.
  After you enable the user class ID, the Enforcer appliance includes the user class ID SYGATE_ENF in the DHCP request. The Enforcer appliance then sends the DHCP request to the DHCP server for the clients that require a quarantine configuration.

- Add the SYGATE_ENF user class to the DHCP server and configure the DHCP server. Consequently, when the DHCP server receives a request with the user class ID SYGATE_ENF, it provides a quarantine IP address and network configuration.
Advanced trunking

The advanced trunking command configures the trunking feature.

The advanced trunking command uses the following syntax:

```
advanced trunking enable | disable |
chall-vlist <vlan-list> | nat-vid <vlan-id> | fail-vid <vlan-id> | mgmt-vid <vlan-id>
```

where:

- `chall-vlist`: Specify the list of VLANs that Gateway Enforcer should challenge.
  Format: n[-n][,n[-n]]... n:<1-4096> e.g. 1,2,3-6,8,10-15
- `disable`: Disable trunking feature
- `enable`: Enable trunking feature
- `fail-vid`: Specify where Gateway Enforcer should send out or receive from those failover packets
- `mgmt-vid`: Specify the management VLAN ID
- `nat-vid`: Specify the VLAN id of those non-tagged packets

Configure DNS

The configure DNS command adds or deletes a Domain Name Service (DNS) server entry. For example, you need to add a DNS entry if you want to specify a Symantec Endpoint Protection Manager with a host name.

The configure DNS command uses the following syntax:

```
configure {add | delete} <ipaddress>
```

where:

- `add`: Enables you to add an IP address of a DNS server.
- `delete`: Enables you to delete an IP address of a DNS server.

The following example describes how to add the IP address of a DNS server on the console of an Enforcer appliance:
Configure Interface

The configure interface command starts or shuts down a network interface card (NIC). It also configures the IP address of a NIC or configures a NIC as a DHCP client.

The configure interface command uses the following syntax:

```
configure interface up <nic-name> | down <nic-name> | failopen | set <nic-name> ip <ipaddress> [netmask <netmask>]
```

where:

- **up nic-name**  
  Name of the NIC to start, such as eth0 or eth1.  
  eth0 or eth1 are case sensitive.

- **down nic-name**  
  Name of the NIC to stop, such as eth0 or eth1.  
  eth0 or eth1 are case sensitive.

- **failopen [enable | disable ]**  
  Enables or disables the Bypass mode for the fail-open Ethernet card. If a Gateway Enforcer appliance that is configured as a gateway fails, the configuration enables the Bypass state on the Gateway appliance.

- **set nic-name**  
  Name of the NIC, such as eth0 or eth1, to be configured as a DHCP client.  
  The name is case sensitive.

- **set IP address IP address netmask**  
  Name of the NIC (eth0 or eth1, case sensitive) for which to configure a static IP address and subnet mask:
  - IP address **IP address**—IP address of the NIC
  - netmask **netmask**—Subnet mask of the NIC

- **set gateway IP address**  
  Name of the NIC, such as eth0 or eth1, that you can configure as a gateway if you want to implement a bypass mode.  
  eth0 or eth1 are case sensitive.

Example:
configure interface set eth0 ip 10.0.0.1 netmask 255.0.0.0

This command sets the IP address of eth0 to 10.0.0.1 with a netmask of 255.0.0.0. Replace the IP address and netmask with the values that you want to use. You must configure a second NIC (eth1) for Gateway and DHCP Enforcer appliances.

Configure interface-role

The configure interface-role command specifies the NIC that represents the internal NIC.

You can also specify the external NIC (Gateway Enforcer appliance and DHCP Enforcer appliance only).

You can also specify the NIC that communicates with the Symantec Endpoint Protection Manager (DHCP Enforcer appliance only).

The configure interface-role command uses the following syntax:

```
interface-role internal <nic-name> | external <nic-name> | manager <nic-name> (DHCP Enforcer only)
```

where:

- **internal nic-name**: Name, such as eth0 or eth1 of the NIC that connects to the internal network. The name is case sensitive.
- **external nic-name**: Name, such as eth0 or eth1 of the NIC that connects to an external network. The name is case sensitive.
- **manager nic-name (DHCP Enforcer only)**: Name, such as eth0 or eth1 of the NIC that connects to the Symantec Endpoint Protection Manager. The name is case sensitive.

Configure NTP

The configure ntp string command establishes communication between an Enforcer appliance and a Network Time Server by specifying an IP address, domain name, or web address.

The configure ntp enable or configure ntp disable command starts and stops the synchronization of time between an Enforcer appliance and a Network Time Server with the Network Time Protocol.

The configure ntp server command uses the following syntax:

```
ntp enable | disable | server <hostname>
```
where:

ntp server <hostname>  You can establish communication between an Enforcer appliance and a Network Time Server by specifying an IP address, domain name, or Web address.

ntp enable          You can start synchronizing time between an Enforcer appliance and a Network Time Server with the Network Time Protocol.

ntp disable         You can stop synchronizing time between an Enforcer appliance and a Network Time Server with the Network Time Protocol.

### Configure Redirect

The configure redirect command specifies an HTTP redirect address when a client is not installed on an endpoint. (Gateway Enforcer appliance only. Not applicable if a Symantec Endpoint Protection Manager is deployed in a network environment.)

The configure redirect command uses the following syntax:

```
configure redirect <url-string>
```

### Configure Route

The configure route command adds or deletes a route table entry. You can configure multiple entries.

The configure route command uses the following syntax:

```
configure route {add | delete} <ipaddress>
netmask <netmask> device <nic-name> [gateway <ipaddress>] [metric <metric-number>]
```

where:

- add <ipaddress>  IP address and subnet mask of the entry to be added to the route table
- netmask <netmask>  IP address and subnet mask of the entry to be deleted from the route table
- delete <ipaddress>
- netmask <netmask>  Interface name (eth0 or eth1, case sensitive) of the entry
- device <nic-name>  IP address of the gateway for the entry
- gateway <ipaddress>  Metric of the entry, an integer from 1 to 32
- metric <metric-number>
The following example adds an entry in a route table with an IP address, a subnet mask, a NIC name, and a gateway IP address:

```
Enforcer# configure

Enforcer(configure)# route

Enforcer(route)# add 192.168.45.0 netmask 255.255.255.0 device eth0 gateway 192.168.40.1
```

## Configure Show

The configure show command displays the current configuration of each command in the configure group. If no argument is specified, all settings appear.

The configure show command uses the following syntax (Gateway or DHCP Enforcer appliance only):

```
configure dns | interface [<nic-name>] | interface-role | ntp | redirect | route | spm
```

## Configure SPM

The configure SPM command sets up the connection between the Enforcer appliance 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 <port-number>] | [key <key-name>] | [del key <shared-key>]
```

where:

- `ip <ipaddress>` Enables you to add the IP address of the Symantec Endpoint Protection Manager.
- `del key <shared-key>` Delete shared secret key.
- `group <group-name>` Enables you to specify a preferred group name for the Enforcer appliance. Therefore it is recommended that you assign a unique group name to distinguish the Enforcer appliances on the console of the Symantec Endpoint Protection Manager.
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 80.

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 HTTPS protocol.

The default port number for the HTTPS protocol is 443.

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 how to configure an Enforcer appliance to communicate with the Symantec Endpoint Protection Manager at IP address 192.168.0.64 in an Enforcer group called CorpAppliance. It uses HTTP protocol on port 80 with an encrypted password of “security.”

```
configure spm ip 192.168.0.64 group CorpAppliance http 80 key security
```

**Console commands**

Commands in the Enforcer appliance CLI console group allow you to configure console settings.

All the commands in this group are listed and described except for the `exit` and `help` commands. The `exit` command exits the command group. The `help` command displays help information on individual commands in the group.

**Console Baud-rate**

The console baud-rate command specifies the baud rate that the console uses to communicate with a client by the serial port. The baud rate that is set on the Enforcer appliance should match the baud rate that is set for this communication connection on the client.

The default baud rate is 9600.

The console baud-rate command uses the following syntax:

```
console baud-rate {9600 | 19200 | 38400 | 57600 | 115200}
```
Console SSH

The console SSH command starts or stops SSH remote logon service. This command also specifies whether to start ssh service when computer starts.

The console ssh command uses the following syntax:

```
console ssh {start | stop} {off | on}
```

Console SSHKEY

The console sshkey command sets and deletes the public key for ssh remote logon without a password.

The console sshkey command uses the following syntax:

```
console sshkey set | delete
```

Example:

```
Enforcer(console)# sshkey set
Enforcer(console)# sshkey delete
```

Console Show

The console show command shows the console configuration settings.

The console show command uses the following syntax:

```
show
```

The following is an example of the syntax for the console show command:

```
Enforcer# console show
Serial Port Number: 1
Baud Rate: 9600
Flow Control: NONE
Console Width: 80
Console Height: 24
```

Debug Commands

Commands in this group allow the user to configure Enforcer debug settings and transfer debug files in plain or compressed form.
All the commands in this group are listed except the `exit` and `help` commands. The `exit` command exits the command group. The `help` displays help information on individual commands in the group.

### Debug Destination

The debug destination command configures where an Enforcer appliance can store debug files.

The debug destination command uses the following syntax:

```
destination {both | disk | memory}
```

where:

- **Both** Stores debug files both in memory and on disk
  The default setting is both
- **Disk** Stores debug files on hard disk only
- **Memory** Stores debug files in memory only

### Debug Level

The debug level command configures the level of debug information that the Enforcer stores.

The debug level command uses the following syntax:

```
level {disabled | fatal | error | information | support | engineer}
```

where:

- **disabled** Does not save debug information
- **fatal** Enables debug and set level to FATAL (save fatal debug messages only)
- **error** Enables debug and set level to ERROR (save fatal and error debug messages)
  The default argument is set to error.
- **information** Enables debug and set level to INFORMATION (save fatal, error, and information debug messages)
- **support** Enables debug and set level to SUPPORT (save fatal, error, information, and support debug messages)
engineer Enables debug and set level to ENGINEER (save all debug messages)

Debug Show

The debug show command shows the configuration of debug settings.
The debug show command uses the following syntax:

```
show [compress | destination | file |
files | kernel | kernel live |
level | user | user live | ymodem]
```

where:

- **compress**: Shows if compress is on
- **destination**: Shows debug destination
- **file**: Shows specified debug file name
- **files**: Lists all debug files
- **kernel**: Shows the kernel debug file
- **kernel_live**: Shows the kernel debug file with live update
- **user**: Shows the user debug file
- **user_live**: Shows the user debug file with live update
- **ymodem**: Displays the ymodem protocol setting

Debug Upload

The debug upload command uses the tftp protocol to transfer a debug file from an Enforcer appliance to a remote host.
The debug upload command uses the following syntax:

```
depbug upload tftp <ipaddress> filename <filename>
```

Example:

```
Enforcer# debug upload tftp 10.200.39.251 filename debug_file
```
MAB commands

The mab commands enable you to implement a Media Access Control (MAC) Authentication Bypass (MAB) with a LAN Enforcer appliance on the following 802.1x-aware switches:

- Cisco Catalyst Switch 3550 Series
- Extreme Networks
- Hewlett-Packard ProCurve Switch 2600 Series
- Foundry Networks

When a LAN Enforcer appliance receives a MAB request, it looks up the address in the local MAB database first. If the entry is located in the local MAB database, the LAN Enforcer appliance authenticates the client based on 802.1x-aware switch model. If an entry cannot be located in the local MAB database, the LAN Enforcer appliance then tries to connect to any available LDAP server.

If an LDAP server is not available to authenticate a client's MAC address or a client's MAC address is not available in the database of the LDAP server, the LAN Enforcer appliance then tries to connect to any available RADIUS server. After the LAN Enforcer appliance receives the authentication result, it then sends a message to the RADIUS server to accept or reject the packet. The LAN Enforcer appliance then completes the authentication session.

MAB database commands

The MAB database commands provide access to all commands that add and manage local MAB database entries on a LAN enforcer appliance.

**MAB database add command**

If you enable MAB, you must add the MAC addresses of all designated MAB client computers to a local database on the LAN Enforcer appliance.

If you want to execute this command, you must be logged on as a superuser.

The mab database command uses the following syntax (LAN Enforcer appliance only):

```plaintext
mab database {add string}
```

where `string` represents:
**add MAC address, MAC address**
Adds one or more MAC addresses into the local MAB database on a LAN Enforcer appliance.

For example, 11:22:33:44:55:66

The delimitation inside a MAC address is represented by a colon. Multiple MAC addresses are separated by a comma and a space.

**add MAC address nx - MAC address ny, MAC address na - MAC address nb**
Adds one or more MAC address ranges into the local MAB database on a LAN Enforcer appliance.


The delimitation inside a MAC address is represented by a colon. The starting and ending MAC addresses for a range are separated by a hyphen. Multiple MAC address ranges are separated by a comma and a space.

**add MAC address/MAC mask, MAC address/MAC mask**
Adds one or more MAC addresses and MAC address masks into the local MAB database on a LAN Enforcer appliance.

For example, 11:00:00:00:00:00/ff:00:00:00:00:00.

The delimitation inside a MAC address is represented by a colon. The MAC address ranges and MAC address mask are separated by a forward slash. The MAC address mask must be in hexadecimal format. Multiple sets of MAC addresses and MAC address masks are separated by a comma and a space.

---

**MAB database clean command**

The MAB database clean command clears all of the MAC entries from the local MAB database on a LAN Enforcer appliance.

You can only remove entries in the local MAB database on a LAN Enforcer appliance if the following conditions have previously been met:

- MAB was enabled.
- MAB entries were added to the local MAB database.

The `mab database clean` command uses the following syntax (LAN Enforcer appliance only):

```
mab database clean
```

The following example explains how to remove existing entries from a local MAB database on a LAN Enforcer appliance:

```
Enforcer:# mab
Enforcer(mab):# database clean
```
MAB database download command

The MAB database download command enables you to download all MAB entries from a TFTP server to the local MAB database on a LAN Enforcer appliance.

The `mab database download` command uses the following syntax (LAN Enforcer appliance only):

```
mab database download filename ip ip address
```

where:

- `filename` Represents the name of the file that includes all of the MAB entries that the tftp server downloads to the LAN Enforcer appliance.
- `ip` Represents the IP address of a location, such as a tftp server, from which to download the MAB database to the LAN Enforcer appliance.

For example, `tftp://nnn.nnn.nnn.nnn`

The following example explains how to copy a file that includes MAC addresses for clients from a location, such as a TFTP server, to a local MAB database on a LAN Enforcer appliance:

```
download mab_database_file tftp://192.192.192.10
```

MAB database upload command

The MAB database upload command enables you to copy all MAB entries from a LAN Enforcer appliance to a location, such as a TFTP server.

The `mab database upload` command uses the following syntax (LAN Enforcer appliance only):

```
mab database upload filename ip ip address
```

The following example explains how to download a file that includes MAC addresses for clients from a local MAB database on a LAN Enforcer appliance to a location, such as a TFTP server:

```
Enforcer: mab
Enforcer(mab): upload mab_database_file tftp://192.192.192.10
```

MAB disable command

The MAB disable command disables MAC Authentication Bypass (MAB) on a LAN Enforcer appliance.
The mab disable command uses the following syntax (LAN Enforcer appliance only):

```
mab disable
```

The following example explains how to disable MAC Authentication Bypass (MAB) on a LAN Enforcer appliance:

```
Enforcer: mab
Enforcer(mab)#disable
```

**MAB enable command**

The MAB enable command enables MAC Authentication Bypass (MAB) on a LAN Enforcer appliances.

The mab enable command uses the following syntax (LAN Enforcer appliance only):

```
mab enable
```

The following example explains how to enable MAC Authentication Bypass (MAB) on a LAN Enforcer appliance:

```
Enforcer: mab
Enforcer(mab)#enable
```

**MAB LDAP commands**

The MAB LDAP commands establish communication between a LAN Enforcer appliance and a LDAP server. After you establish communication between these two devices, you can enable MAC Authentication Bypass (MAB) to authenticate clients by using the database on an LDAP server instead of the local MAB database on a LAN Enforcer appliance.

**MAB LDAP disable command**

The MAB LDAP disable command disables MAC Authentication Bypass (MAB) on a LDAP server instead of a LAN Enforcer appliance.

The mab LDAP disable command uses the following syntax (LAN Enforcer appliance only):

```
mab ldap disable
```

The following example explains how to disable MAC Authentication Bypass (MAB) on a LDAP server instead of a LAN Enforcer appliance:
MAB LDAP enable command

The MAB LDAP enable command disables MAC Authentication Bypass (MAB) on a LDAP server instead of a LAN Enforcer appliance.

The mab LDAP enable command uses the following syntax (LAN Enforcer appliance only):

```
mab ldap enable
```

The following example explains how to disable MAC Authentication Bypass (MAB) on a LDAP server instead of a LAN Enforcer appliance:

```
Enforcer:# mab
Enforcer(mab):# ldap enable
```

MAB LDAP host command

The mab ldap host command specifies the host name of a LDAP server if you plan to authenticate clients by using MAC Authentication Bypass (MAB) on a LDAP server instead of a LAN Enforcer appliance.

The mab ldap host command uses the following syntax (LAN Enforcer appliance only):

```
mab ldap host string
```

where:

string represents the host name of a designated LDAP server with which the LAN Enforcer appliances must establish a connection.

The following example explains how to specify the host name for a LDAP server if you plan to authenticate clients by using MAC Authentication Bypass (MAB) on a LDAP server instead of a LAN Enforcer appliance:

```
Enforcer: mab
Enforcer(mab): ldap host www.symantec.com
```

MAB LDAP password command

The mab ldap password command specifies the password on a LDAP server if you plan to authenticate clients by using MAC Authentication Bypass (MAB) on a LDAP server instead of a LAN Enforcer appliance.
The `mab ldap password` command uses the following syntax (LAN Enforcer appliance only):

```
mab ldap password string
```

where:

`string` represents the password that enables the LAN Enforcer appliance to connect to a designated LDAP server.

The following example explains how to specify the password for a LDAP server if you plan to authenticate clients by using MAC Authentication Bypass (MAB) on a LDAP server instead of a LAN Enforcer appliance:

```
Enforcer: mab
Enforcer(mab): ldap password symantec
```

**MAB LDAP port command**

The `mab ldap port` command specifies the port number on a LDAP server if you plan to authenticate clients by using MAC Authentication Bypass (MAB) on a LDAP server instead of a LAN Enforcer appliance.

The `mab ldap port` command uses the following syntax (LAN Enforcer appliance only):

```
ldap enable | disable | host <hostname> | password <string> | port <number>
```

where:

- `disable` Disable Enforcer MAB LDAP lookup feature
- `enable` Enable Enforcer MAB LDAP lookup feature
- `host` Configure the host of the LDAP server
- `password` Configure the key to access the LDAP server
- `port` Configure the port of the LDAP server

The following example explains how to specify the port number on a LDAP server if you plan to authenticate clients by using MAC Authentication Bypass (MAB) on a LDAP server instead of a LAN Enforcer appliance:

```
Enforcer: mab
Enforcer(mab): ldap port 45298
```
MAB show command

The mab show command enables you to display the following information:

- Whether the MAC authentication bypass is enabled or disabled.
- Whether lookup in the MAC LDAP database on the LDAP server is enabled or disabled.
- Host name of a LDAP server
- Port number of a LDAP server
- Password for a LDAP server

The mab show command uses the following syntax:

```
show [ldap]
```

where:

- `ldap` Show LDAP server configuration

```
Enforcer(mab)# show
MAC Address Bypass: Disable
MAC LDAP lookup: Disable
LDAP server host: www.symantec.com
LDAP server port: 1283
LDAP server password: symantec
```

Monitor commands

The monitor command enables you to display the following information about a managed or unmanaged client:

- IP address
- Host name
- User name (Gateway Enforcer only)
- Policy ID
- MAC address (DHCP Enforcer only)

If you want to execute any of the commands in the monitor group, you must be logged on as a superuser.
Monitor refresh command

The monitor refresh command updates information about the client (Gateway and DHCP Enforcer appliances only).

If you want to execute this command, you must be logged on as a superuser.

The monitor refresh command uses the following syntax:

```
monitor refresh
```

Monitor show command

The monitor show command enables you to display different types of information. The default is to show all monitor information that is available.

Monitor show blocked-hosts command

The monitor show blocked-hosts command displays a blocked client's IP address, host name, username, client profile, required profile, blocked status, host integrity status (Gateway Enforcer appliance only). A blocked client includes information about managed users and connected clients.

This command displays a blocked client's IP address, host name, username, MAC address, client profile, required profile, blocked status, host integrity status (DHPC Enforcer appliance only).

If you want to execute this command, you must be logged on as a superuser.

The monitor show blocked-hosts command uses the following syntax (Gateway and DHCP Enforcer appliances only):

```
monitor [show blocked-hosts {all | ip <ipaddress>}] 
```

where:

- **all**: Displays all blocked clients' IP addresses, host names, user names, client profiles, required profiles, blocked status, host integrity status on Gateway and DHCP Enforcers. In addition, all blocked clients' MAC addresses appear on a DHCP Enforcer.

- **ip <ipaddress>**: Displays a blocked client's IP address, host name, username, client profile, required profile, blocked status, host integrity status on Gateway and DHCP Enforcers. In addition, a blocked client's MAC address appears on a DHCP Enforcer.

The following example provides information about a blocked client's status on a Gateway Enforcer:
monitor
show blocked-hosts ip 100.0.0.242

Authentication blocked host statistics
IP address: 100.0.0.242
Hostname: SNA-7D7911D97BA
Username: guest
Client Profile: Valid-DB1B 12/29/2007 12:35:00
Required Profile: Valid-DB1B 12/29/2007 12:35:00
Blocked: Host Integrity or Policy check failed
HI status: Host Integrity check failed.

The following example provides information about a blocked client's status on a DHCP Enforcer:

monitor
show blocked-hosts ip 100.0.0.242

Authentication blocked host statistics
IP address: 100.0.0.242
Hostname: SNA-7D7911D97BA
Username: guest
MAC address: 0-12-3f-10-a5-99
Client Profile: Valid-DB1B 12/29/2007 12:35:00
Required Profile: Valid-DB1B 12/29/2007 12:35:00
Blocked: Host Integrity or Policy check failed
HI status: Host Integrity check failed.

Monitor show connected-guests commands

The monitor show connected-guests command displays a connected guest's or on-demand client's IP address, host name, username, and policy ID (Gateway Enforcer only). In addition, this command displays a noncompliant client's MAC address for a DHCP Enforcer.

A connected guest or an on-demand client supports the Symantec Network Access Control software on both the Windows and Macintosh platforms. The connected guest or an on-demand client must have been authenticated or set up as a trusted client on the Symantec Endpoint Protection Manager. Otherwise, the monitor show connected-guests command does not display any information about the on-demand clients.

If you want to execute this command, you must be logged on as a superuser.
The monitor show connected-guests command uses the following syntax (Gateway Enforcer appliance and DHCP Enforcer appliance):

```
monitor [show connected-guests { all | ip <ipaddress>}]
```

where:

- **all** Displays all blocked clients’ IP addresses, host names, user names, client profiles, required profiles, connected status, host integrity status on Gateway and DHCP Enforcers. In addition, all blocked clients’ MAC addresses appear on a DHCP Enforcer.

- **ip <ipaddress>** Displays a blocked client’s IP address, host name, username, client profile, required profile, connected status, host integrity status on Gateway and DHCP Enforcers. In addition, a blocked client’s MAC address appears on a DHCP Enforcer.

The following example provides information about a blocked client’s status on a Gateway Enforcer:

```
monitor
show connected-guests ip 100.0.0.242
```

**Authentication connected guests statistics**
- **IP address:** 100.0.0.242
- **Hostname:** SNA-7D7911D97BA
- **Username:** guest
- **Client Profile:** Valid-DB1B 12/29/2007 12:35:00
- **Required Profile:** Valid-DB1B 12/29/2007 12:35:00
- **Connected:** Authenticated
- **HI status:** Host Integrity check passed.

The following example provides information about a blocked client’s status on a DHCP Enforcer:

```
monitor
show connected-guests ip 100.0.0.242
```

**Authentication connected guests statistics**
- **IP address:** 100.0.0.242
- **Hostname:** SNA-7D7911D97BA
- **Username:** guest
- **MAC address:** 0-12-3f-10-a5-99
- **Client Profile:** Valid-DB1B 12/29/2007 12:35:00
- **Required Profile:** Valid-DB1B 12/29/2007 12:35:00
Monitor show connected-users command

The monitor show connected-users command displays a connected user's or a managed client's IP address, host name, username, and policy ID (Gateway Enforcer appliance only). In addition, this command displays a connected user's or a managed client's MAC address for a DHCP Enforcer.

A connected user or a managed client supports Symantec Endpoint Protection client software and Symantec Network Access Control client software. The connected user or managed client must have been authenticated or the monitor show connected-users command does not display any information about the client.

You must be logged on a Gateway or DHCP Enforcer appliance console as a superuser before can execute this command.

The monitor show connected-users command uses the following syntax (Gateway Enforcer appliance and DHCP Enforcer appliance):

```
monitor [show connected-user {all|ip <ipaddress>}
```

where:

- **all**: Displays all connected clients' IP addresses, host names, and policy IDs (GatewayEnforcer appliance and DHCP Enforcer appliance). All noncompliant clients' MAC addresses are also displayed (DHCP Enforcer appliance only).
- **ip <ipaddress>**: Displays a connected client's IP address, host name, and policy ID (GatewayEnforcer appliance and DHCP Enforcer appliance). A noncompliant client’s MAC address is also displayed (DHCP Enforcer appliance only).

**SNMP commands**

The following SNMP commands allow you to work with Simple Network Management Protocol.

**SNMP disable command**

Allows you to disable the Simple Network Management Protocol feature.

The SNMP disable command uses the following syntax:
The following example shows how to disable SNMP:

```
Enforcer(snmp)#disable
```

### SNMP enable command

 Allows you to enable the Simple Network Management Protocol feature. The SNMP enable command uses the following syntax:

```
snmp enable
```

The following example shows how to enable SNMP:

```
Enforcer(snmp)#enable
```

### SNMP heartbeat command

 Allows you to set the heartbeat for the Simple Network Management Protocol feature. The SNMP heartbeat command uses the following syntax:

```
heartbeat <seconds>
```

where:

- The seconds represent time, ranging from 30 to 86400.
- The default number of seconds is 30.

The following example shows how to set the heartbeat for SNMP to 100 seconds:

```
Enforcer(snmp)#heartbeat 100
```

### SNMP receiver command

 Allows you to add or delete an SNMP receiver. The SNMP receiver command uses the following syntax:

```
receiver {add <hostname>::<port> | delete <hostname>::<port>}
```

where:

- add

  Add an SNMP receiver in the format `<host[:port]>`
Delete an SNMP receiver in the format `<host[:port]>`

The following example shows how to add or delete an SMTP receiver:

```
Enforcer(snmp)# receiver add abc
```

```
Enforcer(snmp)# receiver delete abc
```

### SNMP show command

Show the configuration and the status of SNMP.

The SNMP show command uses the following syntax:

```
show configure | status
```

The following examples demonstrate how to use the show command:

```
Enforcer(snmp)# show configure

SNMP Trap : ENABLED
Heartbeat  : 30 second(s)
Timeout   : 1 second(s)
Retry      : 0 time(s)
Trap Receiver : abc:162
```

```
Enforcer(snmp)# show status

CPU usage 3%
Memory usage 97%
lo rec/trans:9386498/9386498 byte
eth0 rec/trans:704234599/288693960 byte
eth1 rec/trans:228648902/179921169 byte
Connected to Symantec Endpoint Protection Manager
```

### SNMP trap command

Allows you to set SNMP try times and timeout value.

The SNMP trap command uses the following syntax:

```
trap retry <times> | timeout <seconds>
```

where:

```
retry Number of times to retry
```
The following example shows how to set SNMP try times and timeout value:

```
Enforcer(snmp)# trap retry 3
Enforcer(snmp)# trap timeout 3
```

### On-Demand commands

The on-demand commands in the Enforcer appliance CLI enable you to configure the automatic downloading of the Symantec Network Access Control On-Demand client on the Windows and Macintosh platforms. You can only execute the on-demand commands on a Gateway Enforcer and a DHCP Enforcer appliance.

All the commands in this group are described except the `exit` and `help` commands. The `exit` command exits the command group. The `help` command displays help information on the individual commands in the group.

### On-Demand authentication commands

Most enterprises may want to set up authentication for Symantec Network Access Control On-Demand clients.

If you want to authenticate Symantec Network Access Control On-Demand clients on the Windows and Macintosh platforms, you can use any of the following types of databases:

- **Local database** that is resident on a Gateway or a DHCP Enforcer appliance. If you do not support an Active Directory server in a network environment, you can use the local on-board database to add user names and passwords for individual users.

- **Active Directory server**
  You must connect to a Microsoft Windows Server 2003 Active Directory.

Table 11-3 provides information about the on-demand authentication command.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ad</code></td>
<td>Enables authentication through the use of an Active Directory server instead of the on-board local database on a Gateway and DHCP Enforcer appliance. See “On-demand authentication ad commands” on page 272.</td>
</tr>
</tbody>
</table>
Table 11-3  On-demand authentication arguments (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables authentication of the Symantec Network Access Control On-Demand clients on the Gateway and DHCP Enforcer appliances. If you enable authentication on the Enforcer, an end user must pass the authentication (input correct username and password) before downloading of the Symantec Network Access Control On-Demand clients. See “On-demand authentication enable command” on page 274.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables authentication of the Symantec Network Access Control On-Demand clients on the Gateway and DHCP Enforcer. End users can trigger the automatic downloading of the Symantec Network Access Control On-Demand clients on a client computer without authentication. See “On-demand authentication disable command” on page 274.</td>
</tr>
<tr>
<td>local-db</td>
<td>Enables authentication through the use of the on-board local database instead of an Active Directory server on the Gateway and DHCP Enforcer appliance. See “On-Demand authentication local-db commands” on page 275.</td>
</tr>
<tr>
<td>show</td>
<td>Lists the status information about the different options and arguments of the authentication command.</td>
</tr>
<tr>
<td>upload</td>
<td>Upload authentication-related files to a server.</td>
</tr>
</tbody>
</table>

**On-demand authentication ad commands**

If an enterprise network supports a Microsoft Windows Server 2003 Active Directory, you can authenticate users with an Active Directory server. Otherwise you must set up the on-board database to authenticate users.

**On-demand authentication ad disable command**

The on-demand authentication ad disable command uses the following syntax to disable the authentication of clients with a Microsoft Windows Server 2003 Active Directory:

You must be logged on to the console of a Gateway or a DHCP Enforcer appliance as a superuser before you can execute this command.

See “Logging on to an Enforcer appliance” on page 82.
The following example describes how to disable the authentication for an On-Demand Client with a Microsoft Windows Server 2003 Active Directory:

```
on-demand authentication ad disable
```

**On-demand authentication ad domain command**

The on-demand authentication ad domain command uses the following syntax to specify the domain ID or the domain ID address of a Microsoft Windows Server 2003 Active Directory:

```
on-demand authentication ad domain
<Active Directory Domain server name> | 
<Active Directory Domain server IP address>
```

where:

- **Active Directory Domain server name** Represents the domain name of a Microsoft Windows Server 2003 Active Directory.
- **Active Directory Domain server IP address** Represents the domain IP address of a Microsoft Windows Server 2003 Active Directory.

The following example describes how to specify the domain ID of a Microsoft Windows Server 2003 Active Directory:

```
Enforcer# on-demand
Enforcer (on-demand)# authentication
Enforcer (authentication)# ad domain symantec.com
```

where:

- **symantec.com** represents the domain name of the Microsoft Windows Server 2003 Active Directory Server.

**On-demand authentication ad enable command**

The on-demand authentication ad enable command uses the following syntax for enabling the authentication of end users with a Microsoft Windows Server 2003 Active Directory:

```
on-demand authentication ad enable
```

The following example describes how to enable authentication for an On-Demand Client with a Microsoft Windows Server 2003 Active Directory:
On-demand authentication disable command

You can stop the authentication process—the auth-daemon—on the console of a Gateway or DHCP appliance for a Symantec Network Access Control On-Demand client.

The on-demand authentication disable command uses the following syntax:

```
on-demand authentication disable
```

You must be logged on a Gateway or DHCP Enforcer appliance console as a superuser before you can execute this command.

See “Logging on to an Enforcer appliance” on page 82.

The following example describes how to disable authentication for a Symantec Network Access Control On-Demand client on the console of a Gateway or DHCP Enforcer appliance:

```
Enforcer# on-demand
Enforcer (on-demand)# authentication disable
```

On-demand authentication enable command

You can start the authentication process—the auth-daemon—on the console of a Gateway or DHCP appliance for a Symantec Network Access Control On-Demand client.

The on-demand authentication enable command uses the following syntax:

```
on-demand authentication enable
```

You must be logged on a Gateway or DHCP Enforcer appliance console as a superuser before you can execute this command.

See “Logging on to an Enforcer appliance” on page 82.

The following example describes how to enable authentication for a Symantec Network Access Control On-Demand client on the console of a Gateway or DHCP Enforcer appliance:

```
Enforcer# on-demand
Enforcer (on-demand)# authentication enable
```
On-Demand authentication local-db commands

If an enterprise network does not support a Microsoft Windows Server 2003 Active Directory, you must authenticate users with the on-board database that you can set up on a Gateway Enforcer appliance or a DHCP Enforcer appliance.

On-Demand authentication local-db add command

If you must authenticate users with the on-board database, you must add user accounts for each client on a Gateway Enforcer appliance or a DHCP Enforcer appliance.

See “Setting up authentication with a local on-board database” on page 199.

You must be logged on the console of a Gateway or a DHCP Enforcer appliance as a superuser before you can execute this command.

See “Logging on to an Enforcer appliance” on page 82.

The on-demand local-db authentication add command uses the following syntax to add a user account to the on-board database that you set up on a Gateway Enforcer appliance or a DHCP Enforcer appliance:

on-demand authentication local-db add user username

where:

username represent a user account that you can add to the on-board database.

The on-demand local-db add user command uses the following syntax:

Enforcer# on-demand
Enforcer (on-demand)# authentication
Enforcer (authentication)# local-db add user jim

On-Demand authentication local-db disable command

The on-demand local-db authentication disable command uses the following syntax to disable the on-board database that you set up on a Gateway Enforcer appliance or a DHCP Enforcer appliance:

on-demand authentication local-db disable

The on-demand authentication local-db enable command uses the following syntax:

Enforcer# on-demand
Enforcer (on-demand)# authentication
Enforcer (authentication)# local-db disable
On-Demand authentication local-db enable command

The on-demand local-db authentication enable command uses the following syntax to enable the on-board database that you can set up on a Gateway Enforcer appliance or a DHCP Enforcer appliance:

```
on-demand authentication local-db enable
```

The on-demand authentication local-db enable command uses the following syntax:

```
Enforcer# on-demand
Enforcer (on-demand)# authentication
Enforcer (authentication)# local-db enable
```

On-Demand authentication local-db username commands

The on-demand local-db authentication username commands allow you to add, delete, and edit usernames:

```
local-db add username <string> password <string>
llocal-db delete username <string>
llocal-db edit username <string> password <string>
llocal-db enable |disable | clear
```

where:

- **add**: Create a new user account to the local database
- **clear**: Clean up all user accounts from the local database
- **delete**: Remove an existing user from the local database
- **disable**: Disable the local database authentication
- **edit**: Modify an existing user account
- **enable**: Enable local database authentication

The following example describes how to configure local database authentication for a Symantec Network Access Control On-Demand client on the console of a Gateway or DHCP Enforcer appliance:

```
Enforcer# on-demand
Enforcer (on-demand)# authentication
Enforcer (authentication)# local-db disable
```

Enforcer appliance command-line interface reference

On-Demand commands
Local database authentication is disabled.

Enforcer(authentication)# local-db enable
Local database authentication is enabled.

Enforcer(authentication)# local add username test password test

Enforcer(authentication)# local-db delete username test
Your action will delete the user account "test" permanently.
Please confirm. [Y/N]y

Enforcer(authentication)# local-db edit username test password b

Enforcer(authentication)# local-db clear
Notice that your action will remove ALL user account permanently!
Please confirm. [Y/N]y

On-Demand banner command

You can edit the default banner on the Welcome page of the Symantec Network Access Control On-Demand clients.

You must be logged on a Gateway or DHCP Enforcer appliance console as a superuser before you can execute this command.

See “Logging on to an Enforcer appliance” on page 82.

The on-demand banner command uses the following syntax:

Enforcer(on-demand)# banner

Type the new banner text that cannot exceed 1024 characters, and press Ctrl-D to end:

At the Enforcer appliance command prompt, replace the default banner text with wording of your choice.

The banner text cannot exceed 1024 characters.

On-Demand client-group command

The On-Demand client-group command enables you to configure the name of an Enforcer group on the console of a Gateway or DHCP Enforcer appliance. You do not need to configure the name of the Enforcer on the Enforcer console if you have already configured it on the console of the Symantec Endpoint Protection Manager.
You must be logged on to the console of a Gateway or DHCP Enforcer appliance as a superuser before you can execute this command.

The on-demand client-group command uses the following syntax:

```
Enforcer# on-demand
Enforcer(on-demand)# client-group <groupname> enable|disable
```

The following example describes how to add the name of an Enforcer appliance group on the console of a Gateway or DHCP Enforcer appliance:

```
Enforcer# on-demand
Enforcer(on-demand)# client-group My Company/On-Demand
```

where:

name of group represents the Enforcer group name on the Symantec Endpoint Protection Manager for a particular group of On-Demand Client computers.

**On-Demand dot1x commands**

You must configure the dot1x command on the console of a Gateway or DHCP Enforcer appliance if the end user uses dot1x authentication in LAN environment.

You must be logged on the console of a Gateway or DHCP Enforcer appliance as a superuser before you can execute this command.

See “Logging on to an Enforcer appliance” on page 82.

**On-Demand dot1x certificate commands**

The On-Demand dot1x certificate command provides access to a number of commands that enable you to:

- Import and configures a root server certificate to authenticate an On-Demand Client with an 802.1x-aware switch.
- Remove a root server certificate.
- Display configuration criteria about the root server certificate.

You must be logged on to the console of a Gateway or DHCP Enforcer appliance as a superuser before you can execute this command.

See “Logging on to an Enforcer appliance” on page 82.

The on-demand dot1x certificate command uses the following syntax:

```
on-demand dot1x certificate
{import| remove | show}
```
where:

import Imports a root server certificate from a designated location.
remove Removes a root server certificate for an 802.1x transport layer security (TLS) protocol.
show Displays the configuration parameters of a root server certificate for an 802.1x transport layer security (TLS) protocol.

The following example describes how to access the on-demand dot1x certificate command:

```
Enforcer# on-demand
Enforcer(on-demand)# dot1x
Enforcer(dot1x)# certificate
Enforcer(certificate)#
```

**On-Demand dot1x certificate import**

The on-demand dot1x certificate import command imports and configures a root server certificate to authenticate an On-Demand Client with an 802.1x-aware switch.

You must be logged on to the console of a Gateway or DHCP Enforcer appliance as a superuser before you can execute this command.

See “Logging on to an Enforcer appliance” on page 82.

The on-demand dot1x certificate import command uses the following syntax:

```
import tftp <ipaddress> username <string>
password <string> root-cert <string> user-cert <string>
```

where:

- `import tftp <ipaddress>` Represents the IP address of the computer from which the Enforcer appliance imports the certificate.
- `password <string>` Represents the password that you must configure to connect to the TFTP server.
- `username <string>` Represents the user logon name that you must use to log on to the On-Demand Client computer.
- `user-cert <string>` Represents the name of the user certificate to be imported.
root-cert <string>  Represents the name of the server certificate to be imported.

The following example describes how to import and configure a root server certificate to authenticate an On-Demand Client with an 802.1x-aware switch:

Enforcer# on-demand
Enforcer(on-demand)# dot1x
Enforcer(dot1x)# certificate
Enforcer(certificate)# import tftp:10.200.39.251
password symantec username janedoe user-cert name.pfx
root-cert name.cer

where:

10.200.39.251  Represents the computer from which the Enforcer appliance imports the certificate.
password symantec  Represents the password that you must configure to connect to the TFTP server.
username janedoe  Represents the user logon name that you must use to log on to the On-Demand Client computer.
user-cert name.pfx  Represents the name of the user certificate to be imported.
root-cert name.cer  Represents the name of the server certificate to be imported.

On-Demand dot1x certificate remove command

You can use the on-demand dot1x certificate remove command to delete the name of a dot1x certificate.

The on-demand dot1x certificate remove command uses the following syntax:

on-demand dot1x certificate remove <string>

where:

string represents the name of the dot1x certificate that you want to remove.

The following example describes how to remove a dot1x certificate with a file name called packagelist.

Enforcer# on-demand
Enforcer(on-demand)# dot1x
Enforcer(dot1x)# certificate
Enforcer(certificate)# remove packagelist
Are you sure that you want to remove "packagelist"? [Y/N] Y

**On-Demand dot1x show certificate command**

You can use the on-demand dot1x show certificate command to display information about the dot1x certificate.

The on-demand dot1x show certificate command uses the following syntax:

```plaintext
on-demand dot1x certificate show
```

The following example describes how to remove a dot1x show certificate.

```plaintext
Enforcer# on-demand
Enforcer(on-demand)# dot1x
Enforcer(dot1x)# certificate
Enforcer(certificate)# show
Certificates: packagelist
```

**On-Demand dot1x peap command**

The On-Demand dot1x peap command enables you to configure an 802.1x Protected Extensible Authentication Protocol (PEAP) to authenticate an On-Demand Client into the protected network.

You must log on to the console of a Gateway or DHCP Enforcer as a superuser before you configure this command.

The on-demand dot1x peap command uses the following syntax:

```plaintext
on-demand dot1x peap { cert-svr | fast-reconn| validate-svr | show }
```

The following example describes how to configure an 802.1x PEAP protocol on the console of a Gateway or DHCP Enforcer appliance:

```plaintext
Enforcer# on-demand
Enforcer(on-demand)# dot1x peap
```

where:

```
peap specifies a Protected Extensible Authentication Protocol (PEAP) configuration as your On-Demand Client dot1x authentication protocol.
```

**On-Demand dot1x peap validate-svr command**

The On-Demand dot1x peap validate-svr command enables you to enable or disable the validation of a root server certificate for an 802.1x Protected Extensible Authentication Protocol (PEAP) protocol configuration.
You must be logged on the console of a Gateway or DHCP Enforcer appliance as a superuser before you can execute this command.

The on-demand dot1x peap peap validate-svr command uses the following syntax:

```
on-demand dot1x peap validate-svr [enable | disable]
```

The following example describes how to enable the validation of a root server certificate for the 802.1x PEAP protocol on the console of a Gateway or DHCP Enforcer appliance:

```
Enforcer# on-demand
Enforcer(on-demand)# dot1x
Enforcer(dot1x)# peap validate-svr enable
```

where:

validate-svr enable sets the validation of a root server certificate for an 802.1x Protected Extensible Authentication Protocol (PEAP) configuration.

**On-Demand dot1x peap cert-svr command**

The On-Demand dot1x peap cert-svr command enables you to import and configure a root server certificate for an 802.1x Protected Extensible Authentication Protocol (PEAP) for On-Demand Client authentication.

You must be logged on the console of a Gateway or DHCP Enforcer as a superuser before you can execute this command.

The on-demand dot1x peap cert-svr command uses the following syntax:

```
Enforcer# on-demand
Enforcer(on-demand)# dot1x peap cert-svr
```

The following example describes how to import and configure a certificate for the 802.1x PEAP protocol on the console of a Gateway or DHCP Enforcer appliance:

```
Enforcer# on-demand
Enforcer(on-demand)# dot1x peap cert-svr
Enforcer(peap)# cert-svr host snac
Enforcer(peap)# cert-svr disable
Enforcer(peap)# cert-svr enable
```

where:

- `disable` Disable PEAP certificate server
- `enable` Enable PEAP certificate server
Set PEAP certificate server’s hostname

**On-Demand dot1x peap fast-reconn command**

The On-Demand dot1x peap fastreconn command allows you to enable or disable fast reconnection of an 802.1x Protected Extensible Authentication Protocol (PEAP) configuration for On-Demand Clients.

You must be logged on the console of a Gateway or DHCP Enforcer appliance as a superuser before you can execute this command.

The on-demand dot1x peap fastreconn command uses the following syntax:

```
Enforcer# on-demand
Enforcer(on-demand)# dot1x peap fastreconn {enable|disable}
```

The following example describes how to validate a root server certificate for an 802.1x Protected Extensible Authentication Protocol (PEAP) on the console of a Gateway or a DHCP Enforcer appliance:

```
Enforcer# on-demand
Enforcer(on-demand)# dot1x peap fastreconn enable
```

where:

- `validate-svr enable` sets the validation of a root server certificate for an 802.1x Protected Extensible Authentication Protocol (PEAP) configuration.

**On-Demand dot1x peap show command**

The On-Demand dot1x peap show command allows you to display the configuration settings for an 802.1x Protected Extensible Authentication Protocol (PEAP) authentication for an On-Demand Client. Use this command to confirm that the active protocol is PEAP.

You must be logged on the console of a Gateway or DHCP Enforcer as a superuser before you can execute this command.

The on-demand dot1x peap show command uses the following syntax:

```
show
```

The following example describes how to display the configuration settings for an 802.1x Protected Extensible Authentication Protocol authentication on the console of a Gateway or DHCP Enforcer appliance:

```
Enforcer(peap)# show
PEAP Validate Server Certificate: DISABLED
PEAP Certificate Server: DISABLED
```
On-Demand dot1x tls command

The On-Demand dot1x tls command allows you to configure the 802.1x transport layer security (TLS) protocol for On-Demand Client sessions.

You must log on to the console of a Gateway or DHCP Enforcer as a superuser before you configure this command.

The on-demand dot1x tls command uses the following syntax:

```
on-demand dot1x tls {cert-svr | validate-svr | show}
```

The following example describes the syntax for the on-demand dot1x tls command on the Gateway or DHCP Enforcer appliance console:

```
Enforcer# on-demand
Enforcer(on-demand)# dot1x tls

where:

tls specifies a Transport Layer Security (TLS) configuration for your On-Demand Client dot1x authentication protocol configuration.

On-Demand dot1x tls validate-svr command

The On-Demand dot1x tls validate-svr command enables or disables the validation of a root server certificate for an 802.1x transport layer security (TLS) protocol configuration.

You must be logged on the console of a Gateway or DHCP Enforcer appliance as a superuser before you can execute this command.

The on-demand configure dot1x tls validate-svr command uses the following syntax:

```
Enforcer# on-demand
Enforcer(on-demand)# dot1x
Enforcer(dot1x)# tls validate-svr [enable|disable]
```

The following example describes the syntax for the on-demand dot1x tls validate-svr command on the console of a Gateway or DHCP Enforcer appliance:

```
Enforcer# on-demand
Enforcer(on-demand)# dot1x tls validate-svr enable

where:
```
validate-svr enable sets the validation of a root server certificate for an 802.1x transport layer security (TLS) protocol configuration.

**On-Demand dot1x tls cert-svr command**

The On-Demand dot1x tls cert-svr command enables you to import and configure a root server certificate for an 802.1x transport layer security (TLS) protocol for On-Demand Client authentication.

You must be logged on to the console of a Gateway or DHCP Enforcer as a superuser before you can execute this command.

The on-demand dot1x tls cert-svr command uses the following syntax:

```
Enforcer# on-demand
Enforcer(on-demand)# dot1x tls cert-svr
```

The following example describes the syntax for the on-demand dot1x tls certificate command on the console of a Gateway or DHCP Enforcer appliance console:

```
Enforcer# on-demand
Enforcer(on-demand)# dot1x
Enforcer(dot1x)# tls
Enforcer(tls)# cert-svr host snac
Enforcer(tls)# cert-svr disable
Enforcer(tls)# cert-svr enable
```

where:

- disable
  - Disable TLS certificate
- enable
  - Enable TLX certificate
- host
  - Set TLS certificate server’s hostname

**On-Demand dot1x tls show command**

The On-Demand dot1x tls show command allows you to view configuration settings for an 802.1x transport layer security (TLS) protocol for On-Demand Client authentication. Use this command to make sure that the tls server certificate is enabled.

You must be logged on the console of a Gateway or DHCP Enforcer as a superuser before you configure this command.

The on-demand dot1x tls show command uses the following syntax:

```
Enforcer# on-demand
Enforcer(on-demand)# dot1x show [tls | peap]
```
The following example describes how to display the configuration settings for an 802.1x transport layer security protocol authentication on the console of a Gateway or DHCP Enforcer appliance:

Enforcer(tls)# show
TLS Validate Server Certificate: DISABLED
TLS Certificate Server: ENABLED
TLS Certificate Server: snac

**On-Demand dot1x protocol command**

The On-Demand dot1x protocol command enables you to set the active authentication protocol to either Extensible Authentication Protocol (PEAP) or Transport Layer Security (TLS) protocol to authenticate On-Demand Clients with an 802.1x-aware switch that has dot1x-enabled ports.

You must be logged on to the console of a Gateway or DHCP Enforcer appliance as a superuser before you configure this command.

The on-demand dot1x protocol command uses the following syntax:

```
on-demand dot1x protocol [tls | peap]
```

The following example describes how to set the active authentication protocol to Extensible Authentication Protocol (PEAP) to authenticate On-Demand Clients with an 802.1x-aware switch that has dot1x-enabled ports:

```
Enforcer# on-demand
Enforcer(on-demand)# dot1x
Enforcer(dot1x)# protocol peap
```

The following example describes how to set the active authentication protocol to Transport Layer Security (TLS) protocol to authenticate On-Demand Clients with an 802.1x-aware switch that has dot1x-enabled ports:

```
Enforcer# on-demand
Enforcer(on-demand)# dot1x
Enforcer(dot1x)# protocol tls
```

**On-Demand dot1x default-user command**

The On-Demand dot1x default-user command allows you to set the active authentication protocol as anonymous for On-Demand Client 802.1x authentication.

You must be logged on the Gateway or DHCP Enforcer console as a superuser before you configure this command.
The on-demand configure dot1x default-user command uses the following syntax:

```
default-user username <string> password <string>
```

The following example describes the syntax for the on-demand dot1x anonymity command on the Gateway or DHCP Enforcer appliance console:

```
Enforcer(dot1x)# default-user username snac password snac
```

**On-Demand dot1x show command**

The On-Demand dot1x show command allows you to view 802.1x authentication settings for On-Demand Client authentication.

You must be logged on the Gateway or DHCP Enforcer console as a superuser before you configure this command.

The On-Demand dot1x show command uses the following syntax:

```
show protocol | peap | tls | certificate | default-user
```

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>certificate</td>
<td>List imported authentication certificates</td>
</tr>
<tr>
<td>default-user</td>
<td>Show default user information</td>
</tr>
<tr>
<td>peap</td>
<td>Show the PEAP authentication settings</td>
</tr>
<tr>
<td>protocol</td>
<td>Show the current active 802.1x protocol</td>
</tr>
<tr>
<td>tls</td>
<td>Show the TLS authentication settings</td>
</tr>
</tbody>
</table>

The following example describes how to display the protocol on the console of a Gateway or DHCP Enforcer appliance:

```
Enforcer(dot1x)# show peap
PEAP Validate Server Certificate: DISABLED
PEAP Certificate Server: DISABLED
PEAP Certificate Server: snac
PEAP Fast Reconnected: ENABLED
```

**On-Demand show command**

The On-Demand show command allows you to display the configuration settings for On-Demand Clients.

You must be logged on the console of a Gateway or DHCP Enforcer as a superuser before you configure this command.
The on-demand show command uses the following syntax:

```
show [ banner | authentiction | dot1x | status | configuration ]
```

The following example describes the syntax for the on-demand show command on the Gateway or DHCP Enforcer appliance console:

```
Enforcer(on-demand)# show
On-Demand: ENABLED
Policy Manager Connected: YES
Policy Manager Domain ID: BD751DAE0AC827F7015EFE3443254960
Client Group: My Company/My Group

Authentication: DISABLED
Local Database Authentication: DISABLED
Active Directory Authentication: DISABLED
Active Directory Domain ID: (NULL)

Active Protocol: TLS
Banner: (NULL)
```

**On-Demand spm-domain command**

You must configure the spm-domain on a Gateway or DHCP Enforcer appliance console. Otherwise the installation fails. The spm-domain may be automatically sent to a Symantec Endpoint Protection Manager. If you have installed version 11.2 or later of a Symantec Endpoint Protection Manager, the spm-domain is automatically sent to a Symantec Endpoint Protection Manager. You can autocomplete the spm-domain on the console of any Enforcer appliance.

Any version of a Symantec Endpoint Protection Manager that precedes 11.2 must be configured with the on-demand spm-domain command on a Gateway or DHCP Enforcer appliance console.

See “Enabling Symantec Network Access Control On-Demand clients to temporarily connect to a network” on page 197.

The spm-domain appears in the Clients page on the Symantec Endpoint Protection Manager Console.

See the Administration Guide for Symantec Endpoint Protection and Symantec Network Access Control on how to locate the spm-domain.

You must be logged on the console of a Gateway or DHCP Enforcer appliance as a superuser before you configure this command.

See “Logging on to an Enforcer appliance” on page 82.
The on-demand spm-domain command uses the following syntax:

```
spm-domain {name <string> | id <string>}
```

The following example describes the syntax for the on-demand spm-domain command on the console of a Gateway or DHCP Enforcer appliance:

```
Enforcer# on-demand
Enforcer(on-demand)# spm-domain id BD751DAE0AC827F7015EFE3443254960
Enforcer(on-demand)# spm-domain name Default
```

where:

BD751DAE0AC827F7015EFE3443254960 represents the spm-domain that is located in the Clients page on the console of the Symantec Endpoint Protection Manager.

### On-Demand mac-compliance commands

You must configure the mac-compliance command on a Gateway or DHCP Enforcer appliance console. Additionally, you only need to execute the mac-hi command if Symantec Network Access Control On-Demand client on a Macintosh platform needs to be supported. Otherwise the installation fails.

You must be logged on the Gateway or DHCP Enforcer console as a superuser before you configure this command.

See “Logging on to an Enforcer appliance” on page 82.

The on-demand mac-compliance command uses the following syntax:

```
on-demand mac-compliance {disable| enable| interval| show}
```

where:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disable</td>
<td>Disable compliance checking rules for Symantec Network Access Control On-demand Client for Mac</td>
</tr>
<tr>
<td>enable</td>
<td>Enable HI rules for Symantec Network Access Control On-demand Client for Mac</td>
</tr>
<tr>
<td>interval</td>
<td>Set compliance checking interval (minutes) for Symantec Network Access Control On-demand Client for Mac</td>
</tr>
</tbody>
</table>
show

Show compliance checking configuration for Symantec Network Access Control
On-demand Client for Mac

exit

Exit the Macintosh compliance setting

clear

Clear the screen

help

Display Help for a command

On-demand mac-compliance disable command

The on-demand mac-compliance disable command uses the following syntax:

on-demand mac-compliance disable <rule-number>

The following example describes the syntax for the on-demand mac-compliance disable command on the console of a Gateway or DHCP Enforcer appliance:

Enforcer(mac-compliance)# disable 1

where the user may select any of the following rules by entering the number that is associated with the rule, as shown in this example:

<table>
<thead>
<tr>
<th>Number</th>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ENABLED</td>
<td>Check system updated</td>
</tr>
<tr>
<td>2</td>
<td>ENABLED</td>
<td>Check SAV installed</td>
</tr>
<tr>
<td>3</td>
<td>ENABLED</td>
<td>Check SAV auto-protect started</td>
</tr>
<tr>
<td>4</td>
<td>ENABLED</td>
<td>Check IP firewall started</td>
</tr>
<tr>
<td>5</td>
<td>ENABLED</td>
<td>Check Norton confidential installed</td>
</tr>
<tr>
<td>6</td>
<td>ENABLED</td>
<td>Check screen saver inactivity/lock</td>
</tr>
</tbody>
</table>

Note: The Check system updated command is optional. Host Integrity will pass regardless of its state. The purpose of the command is to remind users to update their systems.

On-demand mac-compliance enable command

The on-demand mac-compliance enable command uses the following syntax:

on-demand mac-compliance disable <rule-number>

The following example describes the syntax for the on-demand mac-compliance enable command on the console of a Gateway or DHCP Enforcer appliance:

Enforcer(mac-compliance)# enable 1
where the user may select any of the following rules by entering the number that is associated with that number, as shown in this example:

<table>
<thead>
<tr>
<th>&lt;Number&gt;</th>
<th>&lt;State&gt;</th>
<th>&lt;Description&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>DISABLED</td>
<td>Check system updated</td>
</tr>
<tr>
<td>2</td>
<td>DISABLED</td>
<td>Check SAV installed</td>
</tr>
<tr>
<td>3</td>
<td>DISABLED</td>
<td>Check SAV auto-protect started</td>
</tr>
<tr>
<td>4</td>
<td>DISABLED</td>
<td>Check IP firewall started</td>
</tr>
<tr>
<td>5</td>
<td>DISABLED</td>
<td>Check Norton confidential installed</td>
</tr>
<tr>
<td>6</td>
<td>DISABLED</td>
<td>Check screen saver inactivity/lock</td>
</tr>
</tbody>
</table>

**Note:** The Check system updated command is optional. Host Integrity will pass regardless of its state. The purpose of the command is to remind users to update their systems.

---

**On-demand mac-compliance interval command**

The on-demand mac-compliance interval command uses the following syntax:

```
on-demand mac-compliance interval <minutes>
```

where:

The user may set the compliance-checking interval in minutes for Symantec Network Access Control On-demand Client for Mac, in the range of 1-14398560 minutes.

**On-demand mac-compliance show command**

The on-demand mac-compliance show command uses the following syntax:

```
on-demand mac-compliance show { rules | interval}
```

The following example shows the on-demand mac-compliance show command on the console of a Gateway or DHCP Enforcer appliance:

```
Enforcer(mac-compliance)# show rules
1   ENABLED        Check system updated
2   ENABLED        Check SAV installed
3   ENABLED        Check SAV auto-protect started
4   ENABLED        Check IP firewall started
5   ENABLED        Check Norton confidential installed
6   ENABLED        Check screen saver inactivity/lock
```
Enforcer(mac-compliance)# show interval
Interval: 3 (minutes)
Troubleshooting an Enforcer appliance

This chapter includes the following topics:

- About troubleshooting an Enforcer appliance
- General troubleshooting topics and known issues
- About debug information transfer over the network

About troubleshooting an Enforcer appliance

You may need to troubleshoot communication problems with between Enforcers and the Symantec Endpoint Protection Manager.

See “Enforcement questions” on page 297.

Select any of the following topics:

- Enforcer cannot register with the Symantec Endpoint Protection Manager
- Delay in connecting to the network through an Enforcer
- Gateway Enforcer appliance blocks clients
- DHCP Enforcer appliance blocks clients
- Same LAN Enforcer appliance registers twice on the Symantec Endpoint Protection Manager Console
- Client disconnected events in the LAN Enforcer appliance's Client Log
- LAN Enforcer appliance does not switch clients to the correct VLAN
General troubleshooting topics and known issues

The following topics are broader and may also provide help:

<table>
<thead>
<tr>
<th>Table 12-1</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Symptom</strong></td>
</tr>
<tr>
<td>Enforcer root password is shown as invalid when set using the command-line interface</td>
</tr>
<tr>
<td>Time synchronization fails when installing a LAN Enforcer with NTP enabled and configured on Dell 850</td>
</tr>
<tr>
<td>Changing memory on the R200 causes hardware errors</td>
</tr>
<tr>
<td>Some settings (Debug Level, Capture) return to default when the Enforcer is upgraded</td>
</tr>
<tr>
<td>Problems appear when running SNMP with the Enforcer and HP OpenView</td>
</tr>
</tbody>
</table>
| | ■ Load the Symantec MIB file, using **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**. |

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[08-01-2008-14-30-03].xml
2008-08-01 14:29:59  ServerProfile[08-01-2008-14-29-59].xml
Enforcer(debug)# upload tftp 10.1.1.1 filename kernel.log
```
About debug information transfer over the network
Frequently asked questions about the Gateway, DHCP, or LAN Enforcer appliances

This chapter includes the following topics:

- Enforcement questions

Enforcement questions

The following issues provide answers about enforcement issues on the Gateway Enforcer appliance, DHCP Enforcer appliance, or LAN Enforcer appliance:

- See “Which antivirus software provides support for host integrity?” on page 297.
- See “Can Host Integrity policies be set at the group level or the global level?” on page 299.
- See “Can you create a custom host integrity message?” on page 299.
- See “What happens if Enforcer appliances cannot communicate with Symantec Endpoint Protection Managers?” on page 299.
- See “Is a RADIUS server required when a LAN Enforcer appliance runs in transparent mode?” on page 300.
- See “How does enforcement manage computers without clients?” on page 300.

Which antivirus software provides support for host integrity?

Symantec Network Access Control supports the following antivirus software:

- AVG Anti-Virus Free Edition 8.0
AVG Internet Security Edition 8.0
BitDefender Internet Security 2008
BitDefender Total Security 2008
CA Internet Security Suite Plus 2008
CA Personal Firewall 2008
eTrust EZ Antivirus 7.1.129
eTrust EZ Antivirus 7.014
Lavasoft Ad-Aware Pro 2008
McAfee Internet Security Suite 2008
McAfee VirusScan Professional 7.02
McAfee VirusScan Corp Edition 7.1.0
McAfee VirusScan Enterprise 8.0i
McAfee VirusScan Enterprise 8.5i
McAfee VirusScan Professional 8.0
McAfee VirusScan Home Edition 8.0
McAfee VirusScan Home Edition 9.0
McAfee VirusScanPlus 2008
Norton 360 All in One Security
Norton AntiVirus 2004
Norton AntiVirus 2005
Norton AntiVirus 2008
Norton AntiVirus 9.0
Norton Internet Security 2005
Norton Internet Security 2006
Norton Internet Security 2007
Norton Internet Security 2008
Panda Internet Security 2008
Panda Platinum Antivirus 7.0
Panda Security Panda Antivirus + Firewall 2008
Panda Titanium Antivirus 2004
Can Host Integrity policies be set at the group level or the global level?

You can assign Host Integrity policies by group and by location on the console of the Symantec Endpoint Protection Manager.

Can you create a custom host integrity message?

Symantec Network Access Control can create custom Host Integrity messages for each Host Integrity rule. You can customize the message, including the icon and the title. You can perform this customization through a custom Host Integrity rule.

What happens if Enforcer appliances cannot communicate with Symantec Endpoint Protection Managers?

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 246.

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.

How does enforcement manage computers without clients?

Symantec Network Access Control 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 client firewall has no effect on the systems without clients in the network.
### 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 could be to place non-critical servers on the same side of the gateway. This configuration simplifies the network design without seriously compromising security.

### DHCP enforcement

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.
LAN enforcement

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 as 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.

Universal enforcement API

When you use the Universal Enforcement API, the third-party vendor’s implementation of the API handles the exceptions.

Enforcement by using Cisco NAC

When you use the Symantec solution to interface with Cisco NAC, the Cisco NAC architecture handles any exclusions.
Installing the Symantec NAC Integrated Enforcer for Microsoft DHCP Servers

- Chapter 14. Introducing the Symantec NAC Integrated Enforcer for Microsoft DHCP Servers
- Chapter 15. Planning for the installation of the Symantec NAC Integrated Enforcer for Microsoft DHCP Servers
- Chapter 16. Installing the Symantec NAC Integrated Enforcer for Microsoft DHCP Servers
Introducing the Symantec NAC Integrated Enforcer for Microsoft DHCP Servers

This chapter includes the following topics:

- About the Symantec NAC Integrated Enforcer for Microsoft DHCP Servers
- How an Integrated Enforcer for Microsoft DHCP Servers works
- How to get started with the installation of an Integrated Enforcer for Microsoft DHCP Servers
- Where to find more information about related documentation for an Integrated Enforcer for Microsoft DHCP Servers

About the Symantec NAC Integrated Enforcer for Microsoft DHCP Servers

The Symantec NAC Integrated Enforcer for Microsoft DHCP Servers works in concert with the Microsoft Windows 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 works 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 either Symantec Endpoint Protection or Symantec Network Access Control client installations on all the DHCP clients that the DHCP server manages. It then enforces policies for those clients as configured on the Symantec Endpoint Security Manager.

The Integrated Enforcer for Microsoft DHCP Servers also authenticates the client for an agent existence, Globally Unique Identifier (GUID), Host Integrity, and profile version for each configured policies. It then either allows or quarantines the client by using its authentication result.

The Integrated Enforcer for Microsoft DHCP Servers uses a plug-in to interact with the Microsoft DHCP Server. Although the Integrated Enforcer for Microsoft DHCP Servers and the DHCP Server must be installed on the same computer, the Integrated Enforcer for Microsoft DHCP Servers is not dependent on the DHCP server.

**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. By having the Integrated Enforcer for Microsoft DHCP Servers reside on the same computer as the DHCP Server, the Integrated Enforcer for Microsoft DHCP Servers eliminates the need for additional hardware.

You use the Symantec Endpoint Protection Manager to configure the security policies. However, the Integrated Enforcer for Microsoft DHCP Servers enforces the security policies.

The Integrated Enforcer for Microsoft DHCP Servers authenticates the client computers by checking for the response regarding the following criteria:

- Does the Symantec Endpoint Protection client or the Symantec Network Access Control client run on a client computer?

- Does the Symantec Endpoint Protection client or the Symantec Network Access Control client have the correct Globally Unique Identifier (GUID)?
  The GUID is a 128-bit hexadecimal number that 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 is initially connected.

- Does the client comply with the latest Host Integrity policy that the administrator set up on the console of the Symantec Endpoint Protection Manager?
The client received the latest security policy.

The client is trusted by a Network Access Control Scanner, has a trusted MAC, or is running a trusted operating system, if configured.

If the Integrated Enforcer for Microsoft DHCP Servers cannot authenticate the client, access to a quarantined area with limited network resources is provided 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 allows them to become security compliant.

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:

- Review the components that are needed for the installation of an Integrated Enforcer for Microsoft DHCP Servers.
  See “Required components for an Integrated Enforcer for Microsoft DHCP Servers” on page 312.

- Review the hardware requirements for an Integrated Enforcer for Microsoft DHCP Servers.
  See “Hardware requirements for an Integrated Enforcer for Microsoft DHCP Servers” on page 312.

- Review the operating system requirements that for an Integrated Enforcer for Microsoft DHCP Servers.
  See “Operating system requirements for an Integrated Enforcer for Microsoft DHCP Servers” on page 313.

- Where to place an Integrated Enforcer for Microsoft DHCP Servers in a network environment.
  See “Planning for the placement of an Integrated Enforcer for Microsoft DHCP Servers” on page 313.

- Install an Integrated Enforcer for Microsoft DHCP Servers.
  See “Installing an Integrated Enforcer for Microsoft DHCP Servers” on page 316.

- Configure the connections and settings of an Integrated Enforcer for Microsoft DHCP Servers on an Enforcer console.
  See “About configuring the Symantec NAC Integrated Enforcer on an Enforcer console” on page 344.
Where to find more information about related documentation for an Integrated Enforcer for Microsoft DHCP Servers

The Symantec NAC Integrated Enforcer for Microsoft DHCP Servers is part of the Symantec Network Access Control software.

Table 14-1 provides the additional information about the tasks that you may need to perform before or after the installation of an Integrated Enforcer for Microsoft DHCP Servers.

Table 14-1 Related documentation for an Integrated Enforcer for Microsoft DHCP Servers

<table>
<thead>
<tr>
<th>Title of document</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Installation Guide for Symantec Endpoint Protection and Symantec Network Access</em></td>
<td>Describes how to install the following software components:</td>
</tr>
<tr>
<td><em>Control</em></td>
<td>■ Symantec Endpoint Protection Manager</td>
</tr>
<tr>
<td></td>
<td>■ Symantec Endpoint Protection client</td>
</tr>
<tr>
<td></td>
<td>■ Symantec Network Access Control client</td>
</tr>
<tr>
<td></td>
<td>It also explains how to install and configure the embedded and Microsoft SQL database, as well as how to set up replication.</td>
</tr>
<tr>
<td><em>Administration Guide for Symantec Endpoint Protection and Symantec Network Access</em></td>
<td>Describes how to configure and administer the following software components:</td>
</tr>
<tr>
<td><em>Control</em></td>
<td>■ Symantec Endpoint Protection Manager</td>
</tr>
<tr>
<td></td>
<td>■ Symantec Endpoint Protection client</td>
</tr>
<tr>
<td></td>
<td>■ Symantec Network Access Control client</td>
</tr>
<tr>
<td></td>
<td>It also describes how to set up the Host Integrity policies that an Enforcer uses to implement compliance on client computers.</td>
</tr>
<tr>
<td><em>Online Help for Symantec Endpoint Protection and Symantec Network Access Control</em></td>
<td>Explains how to use the Symantec Endpoint Protection Manager.</td>
</tr>
</tbody>
</table>
Table 14-1  Related documentation for an Integrated Enforcer for Microsoft DHCP Servers (continued)

<table>
<thead>
<tr>
<th>Title of document</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sep_readme.txt and snac_readme.txt files</td>
<td>Includes the latest information about the critical Enforcer-related defects that may also affect the Symantec Endpoint Protection Manager. See the sep_readme.txt file that is located on the installation CD called CD1 for information about defects regarding Symantec Endpoint Protection. See the snac_readme that is located on installation CD called CD2 for information about defects regarding Symantec Network Access Control.</td>
</tr>
<tr>
<td>Client Guide for Symantec Endpoint Protection and Symantec Network Access Control</td>
<td>Describes how to use the following software components: ■ Symantec Endpoint Protection client ■ Symantec Network Access Control client</td>
</tr>
<tr>
<td>Online Help for a Symantec Endpoint Protection and a Symantec Network Access Control client</td>
<td>Describes how to use the following software components: ■ Symantec Endpoint Protection client ■ Symantec Network Access Control client</td>
</tr>
<tr>
<td>Online Help for an Integrated Enforcer for Microsoft DHCP Servers</td>
<td>Describes how to configure an Integrated Enforcer for Microsoft DHCP Servers.</td>
</tr>
</tbody>
</table>
Introducing the Symantec NAC Integrated Enforcer for Microsoft DHCP Servers

Where to find more information about related documentation for an Integrated Enforcer for Microsoft DHCP Servers
Planning for the installation of the Symantec NAC Integrated Enforcer for Microsoft DHCP Servers

This chapter includes the following topics:

■ About planning for the installation of an Integrated Enforcer for Microsoft DHCP Servers
■ Required components for an Integrated Enforcer for Microsoft DHCP Servers
■ Hardware requirements for an Integrated Enforcer for Microsoft DHCP Servers
■ Operating system requirements for an Integrated Enforcer for Microsoft DHCP Servers
■ Planning for the placement of an Integrated Enforcer for Microsoft DHCP Servers

About planning for the installation of an Integrated Enforcer for Microsoft DHCP Servers

You must meet a number of requirements before the Symantec NAC Integrated Enforcer for Microsoft DHCP Servers can become operational. The requirements apply to both hardware and software, as well as other software components, including third-party applications.
The type of Enforcer that you can implement depends on the type of Symantec Network Access Control product that you purchased.

See your license agreement for more information.

**Required components for an Integrated Enforcer for Microsoft DHCP Servers**

The Integrated Enforcer for Microsoft DHCP Servers works with the Microsoft DHCP server, the Symantec Endpoint Protection Manager, and the Symantec Network Access Control client. It verifies the clients that try to connect to the network comply with configured security policies.

Install the following required components before you use the 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>Required component to create security policies in a centralized location and assign them to clients.</td>
</tr>
<tr>
<td>Symantec Network Access Control client</td>
<td>Required component if you want end users to be protected by the enforcement of security policies that the Integrated Enforcer for Microsoft DHCP Servers provides.</td>
</tr>
<tr>
<td>Microsoft Windows DHCP Server</td>
<td>Required component if you want end users to be protected by the security policies that the Integrated Enforcer for Microsoft DHCP Servers enforces.</td>
</tr>
<tr>
<td>Integrated Enforcer for Microsoft DHCP Servers (installed on the same computer as the DHCP service)</td>
<td>Required component to authenticate clients and enforce security policies.</td>
</tr>
</tbody>
</table>

**Hardware requirements for an Integrated Enforcer for Microsoft DHCP Servers**

The Integrated Enforcer for Microsoft DHCP Servers includes RAM, processor, storage, monitor, network adapter, and network interface card hardware requirements.

For installations of up to 10,000 users, use the following recommended requirements:

- Pentium III 750 MHz
■ 256-MB memory
■ 120-MB 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 memory
■ 512-MB disk space
■ 1-GB network adapters
■ 800 x 600 resolution monitor with 256 colors (minimum)
■ One network interface card (NIC) with TCP/IP installed

Operating system requirements for an Integrated Enforcer for Microsoft DHCP Servers

The Symantec Integrated Enforcer requires that one of the following operating systems be installed before you can install the Integrated Enforcer for Microsoft DHCP Servers:
■ Windows Server 2000 Service Pack 4 with Microsoft DHCP server
■ Windows Server 2003 Service Pack with Microsoft DHCP server
■ Windows Server 2003 Service Pack 1 and Microsoft DHCP server

Planning for the placement of an Integrated Enforcer for Microsoft DHCP Servers

Figure 15-1 illustrate 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.
Planning for the installation of the Symantec NAC Integrated Enforcer for Microsoft DHCP Servers

Planning for the placement of an Integrated Enforcer for Microsoft DHCP Servers

**Figure 15-1** Placement of Symantec NAC Integrated Enforcer for Microsoft DHCP Servers
Installing the Symantec NAC Integrated Enforcer for Microsoft DHCP Servers

This chapter includes the following topics:

- Before you install the Integrated Enforcer for Microsoft DHCP Servers
- Installing an Integrated Enforcer for Microsoft DHCP Servers
- Upgrading the integrated Enforcer for Microsoft DHCP Servers

Before you install the Integrated Enforcer for Microsoft DHCP Servers

Before you begin to install the Symantec Integrated Enforcer, you must have completed the following installation and configuration tasks:

- Installation of the Symantec Endpoint Protection Manager

**Note:** It is recommended that you install the Symantec Endpoint Protection Manager before you install the Integrated Enforcer for Microsoft DHCP Servers. The Symantec Endpoint Protection Manager must be installed before the Integrated Enforcer for Microsoft DHCP Servers can work properly.

See the *Installation Guide for Symantec Enterprise Protection and Symantec Network Access Control* for information on how to install the Symantec Endpoint Protection Manager.
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 Microsoft Windows server operating system along with the DHCP Service. You must log in as an administrator or 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.

You can install the Integrated Enforcer for Microsoft DHCP Servers by using any of the following installation methods:

- **Installation Wizard**
  See “To install the Integrated Enforcer for Microsoft DHCP Servers with a Wizard” on page 317.

- **Command line**
  See “To install the Integrated Enforcer for Microsoft DHCP Servers from the command line” on page 318.
To install the Integrated Enforcer for Microsoft DHCP Servers with a Wizard

1 Insert the installation CD2.
  
  If the installation does not start automatically, double-click `IntegratedEnforcerInstaller.exe`.

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 NAC 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 asked whether you want 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 “To stop and start the Microsoft DHCP Server manually” on page 319.

9 Click **Finish**.

If you need to reinstall the Integrated Enforcer, you must first uninstall it. See “To uninstall the Integrated Enforcer for Microsoft DHCP Servers” on page 318.

See “To uninstall the Integrated Enforcer for Microsoft DHCP Servers from the command line” on page 319.

**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 C:\Program Files\Symantec\Integrated Enforcer.

3 Type `IntegratedEnforcerInstaller.exe /qr` at the command line and type: `Enter`.

**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 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 one of the following depending on the installed version:

   **version 11.0.0000**
   ```
   MsiExec.exe /qn /X
   {C58BCCDF-A390-46CF-A328-323572E35735}
   ```

   **version 11.0.1000 or higher**
   ```
   msieexec.exe /qn /X <filename>
   filename should be under Program Files\Common Files\Wise Installation Wizard.
   ```

To stop and start the Microsoft DHCP Server manually

1. On the Windows taskbar, click **Start > Control Panel > Administrative Tools > Services**.
2. Click **DHCP Server**.
3. Right-click, and then click **Stop**.
4. Click **Start**.

**Upgrading the integrated Enforcer for Microsoft DHCP Servers**

The following tasks detail how to upgrade to a Symantec NAC Integrated Enforcer:
To upgrade your Symantec NAC Integrated Enforcer

1  Uninstall the existing version of the Integrated Enforcer.
   See “To uninstall the Integrated Enforcer for Microsoft DHCP Servers” on page 318.
   See “To uninstall the Integrated Enforcer for Microsoft DHCP Servers from the command line” on page 319.

   **Note:** Make sure you restart the DHCP service before you install the new version of the Integrated Enforcer.

2  Install the new version of the Integrated Enforcer.
   See “To install the Integrated Enforcer for Microsoft DHCP Servers with a Wizard” on page 317.
   See “To install the Integrated Enforcer for Microsoft DHCP Servers from the command line” on page 318.
Installing the Symantec NAC Integrated Enforcer for Alcatel-Lucent VitalQIP DHCP Servers (Integrated Lucent Enforcer)
Introducing the Symantec NAC Integrated Lucent Enforcer

This chapter includes the following topics:

- About the Integrated Enforcer for Alcatel-Lucent VitalQIP DHCP Servers (Integrated Lucent Enforcer)
- What you can do with the Integrated Lucent Enforcer
- How the Integrated Lucent Enforcer works
- Where to find more information about related documentation for an Integrated Lucent Enforcer

About the Integrated Enforcer for Alcatel-Lucent VitalQIP DHCP Servers (Integrated Lucent Enforcer)

The Integrated Lucent Enforcer works with the Lucent VitalQIP DHCP Server, version 6.2.

The Integrated Lucent Enforcer and the Symantec Endpoint Protection Manager ensure that the following applications comply with configured security policies:

- Symantec Endpoint Protection client
- Symantec Network Access Control client

The Integrated Lucent Enforcer verifies the compliance of client computers with the security policies that the administrator configures. It achieves security by intercepting and checking DHCP messages from each client that receives a dynamic...
IP address through the Lucent VitalQIP Enterprise DHCP Server. The Integrated Lucent Enforcer then groups non-secure computers into a quarantine class. It also provides non-secure computers with available but limited resources for each established security policy.

What you can do with the Integrated Lucent Enforcer

You can perform the following key tasks on the Integrated Lucent Enforcer console:

- Configure a connection to a Symantec Endpoint Protection Server.
- Start and stop the Enforcer service.
- Configure connections to Network Access Control Scanners.
- Configure automatic quarantines.
- View the connection status.
- View the Client log and the System log.
- View DHCP trusted vendors.

How the Integrated Lucent Enforcer works

The Integrated Lucent Enforcer checks on a client computer for the presence of Symantec Endpoint Protection and Symantec Network Access Control clients that the Lucent VitalQIP Enterprise DHCP Server manages. The Integrated Lucent Enforcer then enforces policies for those clients as configured on the Symantec Endpoint Protection Manager, the so-called management server.

The Integrated Lucent Enforcer authenticates the client computers by checking for the response regarding the following criteria:

- Does the Symantec Endpoint Protection client or the Symantec Network Access Control client run on a client computer?
- Does the Symantec Endpoint Protection client or the Symantec Network Access Control client have the correct Globally Unique Identifier (GUID)? The GUID is a 128-bit hexadecimal number that 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 is initially installed.
- Host Integrity (HI) policy
  A Host Integrity policy ensures that the client computer runs the required applications and data files when the client computer tries to connect to the network.
The profile serial number that is based on the latest configured security policies, including the latest Host Integrity policy. The Integrated Lucent Enforcer verifies that the client computer has received the latest security policies from the management server. If the profile serial number does not match, then the Integrated Lucent Enforcer notifies the client computer to update its security policies.

**Note:** The Integrated Lucent Enforcer uses a plug-in to interact with a Lucent VitalQIP Enterprise DHCP Server. The Integrated Lucent Enforcer is dependent on the Lucent VitalQIP Enterprise DHCP Server. If the Lucent VitalQIP Enterprise DHCP Server is not present, the Integrated Lucent Enforcer cannot be installed.

If you stop the Lucent VitalQIP Enterprise DHCP Server, the Integrated Lucent Enforcer continues to operate. If you stop the Integrated Lucent Enforcer, the Lucent VitalQIP Enterprise DHCP Server continues to operate. By having the Integrated Lucent Enforcer and the Lucent VitalQIP Enterprise DHCP Server installed on the same computer, the need for additional hardware is eliminated.

You use the management server to configure the security policies that the Integrated Lucent Enforcer enforces. Before the Integrated Lucent Enforcer enables a client to connect to a network, it authenticates the client by verifying the following conditions:

- The client computer must have installed and run the Symantec Endpoint Protection client or the Symantec Network Access Control client.
- The client has the correct GUID.
- The client complies with the latest default Host Integrity policies or your custom Host Integrity policy.
- The client received the latest security policy.
- The client is trusted by a Network Access Control Scanner, has a trusted MAC, or is running a trusted operating system, if configured.

If the Integrated Lucent Enforcer cannot authenticate the client, access to a quarantined area with limited network resources is provided to the client. The quarantine area is configured on the same computer as the Integrated Lucent Enforcer and the Lucent VitalQIP Enterprise DHCP Server.

You can also set up access to a remediation server. The remediation server provides clients with links to software that allows them to become security compliant.
Where to find more information about related documentation for an Integrated Lucent Enforcer

The Integrated Lucent Enforcer is part of the Symantec Network Access Control software.

Table 17-1 provides the additional information about the tasks that you may need to perform before or after the installation of an Integrated Lucent Enforcer.

**Table 17-1**  Related documentation for an Integrated Lucent Enforcer

<table>
<thead>
<tr>
<th>Title of document</th>
<th>Description</th>
</tr>
</thead>
</table>
| *Installation Guide for Symantec Endpoint Protection and Symantec Network Access Control* | Describes how to install the following software components:  
- Symantec Endpoint Protection Manager  
- Symantec Endpoint Protection client  
- Symantec Network Access Control client  
It also explains how to install and configure the embedded and Microsoft SQL database, as well as how to set up replication. |
| *Administration Guide for Symantec Endpoint Protection and Symantec Network Access Control* | Describes how to configure and administer the following software components:  
- Symantec Endpoint Protection Manager  
- Symantec Endpoint Protection client  
- Symantec Network Access Control client  
It also describes how to set up the Host Integrity policies that an Enforcer uses to implement compliance on client computers. |
| Online Help for Symantec Endpoint Protection and Symantec Network Access Control   | Explains how to use the Symantec Endpoint Protection Manager. |
| readme.txt files                                                                   | Includes the latest information about the critical Enforcer-related defects that may also affect the Symantec Endpoint Protection Manager.  
See the readme.txt file that is located on the installation CD called CD1 for information about defects regarding Symantec Endpoint Protection.  
See readme that is located on installation CD called CD2 for information about defects regarding Symantec Network Access Control. |
Table 17-1  Related documentation for an Integrated Lucent Enforcer (continued)

<table>
<thead>
<tr>
<th>Title of document</th>
<th>Description</th>
</tr>
</thead>
</table>
| Client Guide for Symantec Endpoint Protection and Symantec Network Access Control | Describes how to use the following software components:  
  ■ Symantec Endpoint Protection client  
  ■ Symantec Network Access Control client |
| Online Help for a Symantec Endpoint Protection and a Symantec Network Access Control client | Describes how to use the following software components:  
  ■ Symantec Endpoint Protection client  
  ■ Symantec Network Access Control client |
| Online Help for an Integrated Lucent Enforcer           | Describes how to configure an Integrated Lucent Enforcer.                                         |
| Online Help for an Integrated Enforcer for Microsoft DHCP Servers | Describes how to configure an Integrated Enforcer for Microsoft DHCP Servers.                   |
Introducing the Symantec NAC Integrated Lucent Enforcer

Where to find more information about related documentation for an Integrated Lucent Enforcer
Planning for the installation of the Symantec NAC Integrated Lucent Enforcer

This chapter includes the following topics:

- About planning for the installation of an Integrated Lucent Enforcer
- Required components for an Integrated Lucent Enforcer
- Planning for the placement of an Integrated Lucent Enforcer
- Hardware requirements for an Integrated Lucent Enforcer
- Operating system requirements for an Integrated Lucent Enforcer

About planning for the installation of an Integrated Lucent Enforcer

You must meet a number of requirements before the Integrated Lucent Enforcer can become operational. The requirements apply to both hardware and software, as well as other software components, including third-party applications.

The type of Enforcer that you can implement depends on the type of Symantec Network Access Control product that you purchased.

See your license agreement for more information.
Required components for an Integrated Lucent Enforcer

You must have already installed and configured the following components before you can install the Symantec Integrated Lucent Enforcer:

- **Lucent VitalQIP Enterprise DHCP 6.2 Server**
  See the accompanying Lucent VitalQIP Enterprise DHCP 6.2 Server documentation for information on how to install and configure the Lucent VitalQIP Enterprise DHCP 6.2 Server.

- **Sybase Adaptive Server Enterprise Suite 12.5.2**
  See the accompanying Sybase documentation for information on how to install and configure the Sybase database.

- **Symantec Endpoint Protection Manager, version 11.0.3**
  See the *Installation Guide for Symantec Endpoint Protection and Symantec Network Access Control* for information on how to install the Symantec Endpoint Protection Manager.

- **Symantec Network Access Control clients, version 11.0.3**
  See the *Installation Guide for Symantec Endpoint Protection and Symantec Network Access Control* for information on how to install the Symantec Network Access Control clients.
  See the *Administration Guide for Symantec Endpoint Protection and Symantec Network Access Control* for information on how to upgrade Symantec Network Access Control clients.

- **See the *Client Guide for Symantec Endpoint Protection and Symantec Network Access Control*** for information on how to use the Symantec Network Access Control client.

*Table 18-1* must be installed before you can successfully protect any clients.

**Table 18-1** Required components for the Symantec NAC Integrated Lucent Enforcer

<table>
<thead>
<tr>
<th>Name of component</th>
<th>Function of component</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symantec Endpoint Protection Manager, version 11.0.3</td>
<td>The Symantec Endpoint Protection Manager is required to create security policies in a centralized location and assign them to Symantec Network Access Control clients.</td>
</tr>
</tbody>
</table>
Table 18-1  Required components for the Symantec NAC Integrated Lucent Enforcer (continued)

<table>
<thead>
<tr>
<th>Name of component</th>
<th>Function of component</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symantec Network Access Control client, version 11.0.3</td>
<td>The Symantec clients are required to be installed and deployed on the client computers before the security policies can protect them. You configure the Host Integrity policies on the Symantec Endpoint Protection Manager.</td>
</tr>
<tr>
<td>Sybase Adaptive Server Enterprise Suite 12.5.2</td>
<td>This Sybase suite is required.</td>
</tr>
<tr>
<td>Lucent VitalQIP Enterprise DHCP 6.2 Server</td>
<td>The Lucent VitalQIP Enterprise DHCP 6.2 Server is required for the assignments of DHCP leases and IP addresses.</td>
</tr>
<tr>
<td>Symantec NAC Integrated Lucent Enforcer</td>
<td>The Symantec NAC Integrated Lucent Enforcer is required to authenticate a client’s credentials and to enforce a client’s compliance with a security policy.</td>
</tr>
</tbody>
</table>

Planning for the placement of an Integrated Lucent Enforcer

*Figure 18-1* illustrate how to place the Integrated Lucent Enforcer, the Lucent VitalQIP Enterprise DHCP 6.2 Server, and the Symantec Endpoint Protection Manager, as well as internal or remote clients in a network.
Figure 18-1  Placement of Integrated Enforcer for Alcatel-Lucent VitalQIP Servers with a Lucent VitalQIP Enterprise DHCP 6.2 Server
Hardware requirements for an Integrated Lucent Enforcer

The Integrated Lucent Enforcer includes RAM, processor, storage, monitor, network adapter, and network interface card hardware requirements.

For installations of up to 10,000 users, use the following recommended requirements:

- Pentium III 750 MHz
- 256-MB memory
- 120-MB 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 memory
- 512-MB disk space
- 1-GB network adapters
- 800 x 600 resolution monitor with 256 colors (minimum)
- One network interface card (NIC) with TCP/IP installed

Operating system requirements for an Integrated Lucent Enforcer

Before you can install the Integrated Lucent Enforcer on the same computer as the Lucent VitalQIP Enterprise DHCP 6.2 Server, you must install one of the following operating systems:

- Windows 2000 Advanced Server with Service Pack 4 and Lucent VitalQIP Enterprise DHCP 6.2 Server or later
■ 32-bit Windows Server 2003 Advanced Edition and Lucent VitalQIP Enterprise DHCP 6.2 Server or later
■ 32-bit Windows Server 2003 Advanced Edition with Service Pack 1 and Lucent VitalQIP Enterprise DHCP 6.2 Server or later
■ 32-bit Windows Server 2003 Advanced Edition with Service Pack 2 and Lucent VitalQIP Enterprise DHCP 6.2 Server or later
Installing the Symantec NAC Integrated Lucent Enforcer

This chapter includes the following topics:

- Before you install the Integrated Lucent Enforcer
- Installing an Integrated Lucent Enforcer
- Uninstalling an Integrated Lucent Enforcer
- Stopping and starting the Lucent VitalQIP Enterprise DHCP Server

**Before you install the Integrated Lucent Enforcer**

Before you begin to install the Integrated Lucent Enforcer, you must have completed the following tasks:

- Completed the installation of Symantec Network Access Control that includes the Symantec Endpoint Protection Manager

**Note:** The Symantec Endpoint Protection Manager must be installed before the Integrated Lucent Enforcer can work properly.

See the *Installation Guide for Symantec Enterprise Protection and Symantec Network Access Control* for information on how to install the Symantec Endpoint Protection Manager.

- Completed the configuration, deployment, and installation of the Symantec Network Access Control client
See the *Installation Guide for Symantec Enterprise Protection and Symantec Network Access Control* for information on how to install the Symantec Network Access Control client.

- Verified the system requirements for the computer on which you plan to install the following components:
  - Sybase database
  - Lucent VitalQIP Enterprise DHCP Server
  - Integrated Lucent Enforcer

See the documentation that accompanies the Sybase database for more information on how to install and configure the database.

See the documentation that accompanies the Lucent VitalQIP Enterprise DHCP Server for more information on how to install and configure the DHCP service.

---

## Installing an Integrated Lucent Enforcer

You must install the Integrated Lucent Enforcer on the same computer on which you have already installed the following software:

- Microsoft Windows server operating system
- Sybase database
- Lucent VitalQIP Enterprise DHCP 6.2 Server

You must log in as an administrator or as a user in the administrators group.

---

**Note:** After you completed the installation of the Integrated Lucent Enforcer, you must configure it. The Integrated Lucent Enforcer must be able to establish a connection to the Symantec Endpoint Protection Manager that is also known as the management server.

You can install the Integrated Lucent Enforcer by using any of the following installation methods:

- Installation Wizard
- Command line
To install an Integrated Lucent Enforcer with a Wizard

1 Insert the installation CD that is labeled CD2.
   If the installation does not start automatically, double-click IntegratedEnforcerInstaller.exe.

2 If the Lucent VitalQIP Enterprise DHCP Server is already installed, in the Welcome panel of the Symantec Integrated Lucent Enforcer Installation Wizard, 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 Alcatel-Lucent VitalQIP® DHCP Server and click Next.
   The Role Selection panel only appears if more than one type of Symantec NAC 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 asked whether you want to restart the Lucent VitalQIP Enterprise DHCP Server, perform one of the following tasks:
   ■ To restart the Lucent VitalQIP Enterprise DHCP Server immediately, click Yes.
   ■ To restart the Lucent VitalQIP Enterprise DHCP Server manually later, click No.
     If you restart the Lucent VitalQIP Enterprise DHCP Server later, you must stop and then start it.
   You must restart the Lucent VitalQIP Enterprise DHCP Server or the Integrated Lucent Enforcer does not function.
   See “Stopping and starting the Lucent VitalQIP Enterprise DHCP Server” on page 339.

9 Click Finish.
   If you need to reinstall the Integrated Lucent Enforcer, you must first uninstall it.
   See “Uninstalling an Integrated Lucent Enforcer” on page 338.
To install an Integrated Lucent Enforcer 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 Lucent Enforcer Installer is located.
   The install location defaults to C:\Program Files\Symantec\Integrated Enforcer.

3. Type `IntegratedEnforcerInstaller.exe /qr` at the command line and press Enter.

Uninstalling an Integrated Lucent Enforcer

You may need to uninstall the Integrated Lucent Enforcer at times. You can uninstall the Integrated Lucent Enforcer by using the utility in the Control Panel or from the command line.

To uninstall an Integrated Lucent Enforcer

1. On the Windows taskbar, click Start > Control Panel > Add or Remove Programs.

2. Click Symantec 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 Lucent VitalQIP Enterprise DHCP Server, perform one of the following tasks:
   - To restart the Lucent VitalQIP Enterprise DHCP Server immediately, click Yes.
   - To restart the Lucent VitalQIP Enterprise DHCP Server manually later (the default), click No.
     If you restart the Lucent VitalQIP Enterprise DHCP Server later, you must stop and then start it.
     You must restart the Lucent VitalQIP Enterprise DHCP Server to completely uninstall the Integrated Lucent Enforcer.

To uninstall an Integrated Lucent Enforcer

1. Open a DOS command prompt.

2. At the command prompt, type: `MsiExec.exe /qn /X{A145EB45-0852-4E18-A9DC-9983A6AF2329}`
Stopping and starting the Lucent VitalQIP Enterprise DHCP Server

You may need to stop and start the Lucent VitalQIP Enterprise DHCP Server at times.

To stop and start the Lucent VitalQIP Enterprise DHCP Server

2. Click Lucent DHCP Service.
3. Right-click, and then click Stop.
4. Click Start.
Installing the Symantec NAC Integrated Lucent Enforcer

Stopping and starting the Lucent VitalQIP Enterprise DHCP Server
Chapter 20. Configuring the Symantec NAC Integrated Enforcers on the Enforcer console
This chapter includes the following topics:

- About configuring the Symantec NAC Integrated Enforcer on an Enforcer console
- Establishing or changing communication between a Symantec NAC Integrated Enforcer and Symantec Endpoint Protection Manager servers
- Configuring automatic quarantine
- Configuring Symantec NAC Integrated Enforcer basic settings
- Editing a Symantec Endpoint Protection Manager connection
- Configuring a trusted vendor list
- Viewing Enforcer logs on an Enforcer console
- Configuring logs for the Symantec NAC Integrated Enforcer
- Configuring Symantec NAC Integrated Enforcer authentication settings
- Establishing communication between a Symantec NAC Integrated Enforcer and a Network Access Control Scanner on an Enforcer console
- Configuring Symantec NAC Integrated Enforcer advanced settings
- Stopping and starting communication services between an Integrated Enforcer and a management server
About configuring the Symantec NAC Integrated Enforcer on an Enforcer console

After you complete the installation of a Symantec NAC Integrated Enforcer, there are two stages of configuration. First, configure the settings on the Integrated Enforcer console. Secondly, move to the Symantec management console of the Symantec Endpoint Protection Manager to make any desired changes to the configuration settings for the group that the Integrated Enforcer is part of. These tasks are outlined below.

- On the Enforcer console of an Integrated Enforcer for Microsoft DHCP Servers, establish communication between the Integrated Enforcer and a management server. See “Establishing or changing communication between a Symantec NAC Integrated Enforcer and Symantec Endpoint Protection Manager servers” on page 344.
- On the management console of a Symantec Endpoint Protection Manager, configure the Symantec NAC Integrated Enforcer configuration settings.

- Set up the DHCP server with a quarantine configuration. You must configure a quarantine user class and add resources to the quarantine class for each subnet. Alternatively, you can use the Integrated Enforcer Automatic Quarantine Configuration option. This option allows the Integrated Enforcer for Microsoft DHCP Servers to configure user class and resources, but only if there is no quarantine class configured previously. See “Configuring automatic quarantine” on page 347.
- If you did not restart the DHCP service on the DHCP server when you installed the Integrated Enforcer, stop and start it manually now.

Establishing or changing communication between a Symantec NAC Integrated Enforcer and Symantec Endpoint Protection Manager servers

You must specify one or more Symantec Endpoint Protection Managers 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.

See the Administration Guide for Symantec Endpoint Protection and Symantec Network Access Control for more information about management server lists.

To establish communication between an Integrated Enforcer and a Symantec Endpoint Protection Manager server from the Symantec NAC Integrated Enforcer console


   The Symantec NAC 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 the Integrated Enforcer is actively connected to the management server. A red light indicates that the connection is disabled.

2. In the left-hand panel, click Symantec Integrated Enforcer > Configure > Management Servers.

3. In the Management Servers panel, click Add in the icon column that is located at the right of the management servers list.

4. In the Add/Edit 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 will be resolved correctly by the domain name server (DNS server).

5. In the Add/Edit 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.

6. Click OK.
7 Click either the Move up arrow or Move down arrow from the icon column that is located to the right of the management servers list to optionally change the order of the management servers that the Symantec NAC Integrated Enforcer uses to connect to a Symantec Endpoint Protection Manager.

The first time the Symantec NAC Integrated Enforcer connects to Symantec Endpoint Protection Manager, it tries to connect to the first server that is listed in the management server list. If the management server is not available, the Symantec NAC Integrated Enforcer connects to the next management server that appears in the management server list.

8 In the Encrypted password text box, type the password of the Symantec Endpoint Protection Manager you are connecting to.

The Symantec Endpoint Protection Manager and Integrated Enforcer must use the same encrypted password for communication.

To display the letters and numbers of the preshared key instead of asterisks, check Unmask.

9 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 NAC Integrated Enforcer to a default Enforcer group with default settings. The default group name is I-DHCP. However, a Symantec NAC 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 View Servers page.

10 To specify the protocol that the Symantec NAC 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 Symantec Endpoint Protection Manager’s certificate with a trusted third-party certificate authority, check Verify certificate when using HTTPS protocol.

11 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.

Either the Symantec NAC Integrated Enforcer can perform the quarantine configuration based on allowed IP addresses or you can configure a quarantine user class and add resources to it for each subnet from inside 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 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.
To set up a quarantine configuration on a DHCP server (advanced optional task)

1. On the DHCP server, click **Start > Administrative Tools > DCHP**.

   To renew the request with a quarantine configuration, the Integrated Enforcer dynamically appends a quarantine DHCP user class to the DHCP messages that come from the non-compliant clients. You define the quarantine user class by adding an ID called: **SYGATE_ENF**. Then you assign the user class various resources, which includes a gateway IP address, lease time, a DNS server, and enough static routes for remediation.

2. In the tree of the DHCP dialog box, right-click the DHCP server, and click **Define User Classes**.

3. In the DHCP User Classes dialog box, click **Add**.

4. In the New Class dialog box, type a display name that identifies this quarantine user class as the quarantine configuration, and an optional description.

   For example, you can identify a quarantine user class, such as QUARANTINE.

5. To define a new user class, click the ASCII column and type **SYGATE_ENF** in uppercase letters.

6. Click **OK**.

7. Click **Close**.

To configure scope options on a DHCP server (advanced optional task)

1. In the tree, right-click **Server Options**.

2. Click **Configure Options....**

3. On the General tab, check **003 Router** and configure the IP address of the router that is associated with the DHCP relay client.

4. On the Advanced tab, in the Vendor class drop-down list, click **DHCPStandard Options**.

5. On the Advanced tab, in the User class drop-down list, click **QUARANTINE**.

6. Check **003 Router**.

7. In the IP address field, type **127.0.0.1** (recommended). However, it is up to the administrator to decide which router IP, if any, to assign to quarantined clients.

8. Check **051 Lease**.

9. Type the hexadecimal value of the lease time in seconds.

   For example, for 2 minutes, type **0x78**.
Configuring Symantec NAC Integrated Enforcer basic settings

You can add or edit the description of a Symantec NAC Integrated Enforcer or an Integrated Enforcer group in the Symantec Endpoint Protection Manager Console. 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 NAC Integrated Enforcer” on page 350.

You can add or edit the IP address or host name of an Integrated Enforcer in a management server list.

See “Adding or editing the IP address or host name of a Symantec NAC Integrated Enforcer” on page 350.

However, you cannot add or edit the name of an Integrated Enforcer group in the Symantec Endpoint Protection Manager Console. You cannot add or edit the IP address or host name of an Integrated Enforcer in the Symantec Endpoint Protection Manager Console. Instead, you must perform these tasks on the Enforcer console.

See “Adding or editing the name of an Enforcer group for Symantec NAC Integrated Enforcer” on page 349.

You must connect the Integrated Enforcer to a Symantec Endpoint Protection Manager.

See “Connecting the Symantec NAC Integrated Enforcer to a Symantec Endpoint Protection Manager” on page 351.

Adding or editing the name of an Enforcer group for Symantec NAC 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.
Adding or editing the description of an Enforcer group with a Symantec NAC Integrated Enforcer

You can add or edit the description of an Enforcer group of which a Symantec NAC 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 NAC Integrated Enforcer

1. In the Symantec Endpoint Protection Manager Console, click Admin.
2. In the Admin page, click Servers.
3. In the Admin page, under View Servers, select and expand the Enforcer group whose name you want to add or edit.
4. In the Admin page, 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. In the Settings dialog box, click OK.

Adding or editing the IP address or host name of a Symantec NAC Integrated Enforcer

You can only change the IP address or host name of an Integrated Enforcer on the Enforcer console during the installation. If you want to change the IP address or host name of an Integrated Enforcer at a later time, you can do so on the Integrated Enforcer console.

Adding or editing the description of a Symantec NAC Integrated Enforcer

You can add or edit the description of a Symantec NAC Integrated Enforcer. You can perform this task on the Symantec Endpoint Protection Manager Console 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 NAC Integrated Enforcer

1. In the Symantec Endpoint Protection Manager Console, click **Admin**.
2. In the Admin page, click **Servers**.
3. Under View Servers, 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 NAC Integrated Enforcer to a Symantec Endpoint Protection Manager

Enforcers must be able to connect to servers on which the Symantec Endpoint Protection Manager is installed. The Symantec Endpoint Protection Manager includes a file that helps manage the traffic between clients, Symantec Endpoint Protection Managers, 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 server an Integrated Enforcer connects. It also specifies to which Symantec Endpoint Protection server 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 Symantec Endpoint Protection Managers 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.
See the Administration Guide for Symantec Endpoint Protection and Symantec Network Access Control for more information on how to customize management server lists.

To connect the Symantec NAC Integrated Enforcer to a Symantec Endpoint Protection Manager

1. In the Symantec Endpoint Protection Manager Console, click Admin.
2. In the Admin page, click Servers.
3. Under View Servers, 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.
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.
   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.

Editing a Symantec Endpoint Protection Manager connection

You can update the Symantec Endpoint Protection Manager server 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, click Edit from the icon column that is located to the right of the management servers list.
In the Add/Edit 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, the Symantec NAC Integrated Enforcer must connect to a domain name server (DNS) server.

Click OK.

Configuring a trusted vendor list

Agents 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 NAC 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 NAC 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**.

**Configuring logs for the Symantec NAC Integrated Enforcer**

Logs for the Symantec NAC Integrated Enforcer are stored on the same computer on which you installed the Symantec NAC Integrated Enforcer. Enforcer logs are generated by default.

If you want to view Enforcer logs on the Symantec Endpoint Protection Manager Console, you must enable the sending of logs on the Symantec Endpoint Protection Manager Console. If this option is enabled, the log data is sent from the Integrated Enforcer to the Symantec Endpoint Protection Manager and stored in a database.

You can modify the log settings for the Integrated Enforcer on 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 Integrated Enforcer generates:

- **Enforcer Server log**
  The Enforcer Server log provides the information that is related to the functioning of an Enforcer.

- **Enforcer Client log**
  The Client 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 Symantec NAC 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 20-1 provides more information about the options on the Authentication tab.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum number of packets per authentication session</td>
<td>The maximum number of challenge packets that the Integrated Enforcer sends in each authentication session. The default number is 10. See “Specifying the maximum number of challenge packets during an authentication session” on page 358.</td>
<td></td>
</tr>
<tr>
<td>Time between packets in authentication session</td>
<td>The time (in seconds) between each challenge packet that the Enforcer sends. The default value is 3 seconds. See “Specifying the frequency of challenge packets to be sent to clients” on page 358.</td>
<td></td>
</tr>
<tr>
<td>Allow all clients, but continue to log which clients are not authenticated</td>
<td>If this option is enabled, the Enforcer authenticates all users by checking that they are running a client. It then forwards the Integrated 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 359.</td>
<td></td>
</tr>
<tr>
<td>Allow all clients with non-Windows operating systems</td>
<td>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 360.</td>
<td></td>
</tr>
</tbody>
</table>
Table 20-1  Authentication configuration settings for a Symantec NAC Integrated Enforcer (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 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 Integrated request to receive a quarantine network configuration.  
If this option is not enabled and if the Host Integrity check is successful, 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 NAC Integrated Enforcer check the Policy Serial Number on a client” on page 361.                                                                                                                                 |
| Enable pop-up message on client if Client is not running  | This option is displayed but currently unavailable for Symantec NAC Integrated Enforcer.  
See “Sending a message from a Symantec NAC Integrated Enforcer to a client about non-compliance” on page 362.                                                                                                                                                                              |

About authentication sessions

When a client tries to access the internal network, the Symantec NAC Integrated Enforcer first detects whether the client is running a 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 10.

The frequency (3 seconds) times the number of packets (10) 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 three seconds.

The client sends information to the Integrated Enforcer that contains the following items:

- Unique identification (UID)
- Its current Profile Serial Number
- The results of the Host Integrity check

The Integrated Enforcer verifies the client UID and the Policy Serial Number with the 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.

If the client information passes the authentication requirements, the Symantec NAC Integrated Enforcer forwards its DHCP request to the DHCP server. The Integrated Enforcer expects to receive a normal DHCP network configuration. Otherwise the Integrated Enforcer forwards it to the quarantine DHCP server to receive a quarantine network configuration.

You can install one DHCP server on one computer and configure it to provide both a normal and a quarantine network configuration.

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 sends a message to the DHCP server. The message is a request for the release of the current IP address. The Integrated Enforcer then sends a DHCP message to the client. The client then sends a request for a new IP address and network configuration to the Integrated Enforcer. The Integrated Enforcer forwards this request to the quarantine DHCP server.
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 10 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 the Symantec Endpoint Protection Manager Console, click **Admin**.
2. In the Admin page, click **Servers**.
3. Under View Servers, 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.
   
   The default setting is 10.
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 3 seconds.
To specify the frequency of challenge packets to be sent to clients

1. In the Symantec Endpoint Protection Manager Console, click **Admin**.
2. In the Admin page, click **Servers**.
3. Under View Servers, 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.
   The default setting is 10.
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 may want to 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 Integrated 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. It forwards the DHCP requests to receive the normal DHCP server network configuration instead of the quarantine network configuration. 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 the Symantec Endpoint Protection Manager Console, click Admin.
2. In the Admin page, click Servers.
3. Under View 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 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 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 the Symantec Endpoint Protection Manager Console, click Admin.
2. In the Admin page, click Servers.
3. Under View Servers, 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.
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 In the Settings dialog box, on the Authentication tab, click **OK**.

**Having the Symantec NAC Integrated Enforcer check 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 Integrated Enforcer, the Integrated Enforcer retrieves the Policy Serial Number from the 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 NAC Integrated Enforcer 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 Under View Servers, select and expand the group of Enforcers.

   The Enforcer group must include the Integrated Enforcer that checks the Policy Serial Number on a client.
4 Under Tasks, click **Edit Group Properties**.
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 In the Settings dialog box, on the Authentication tab, click **OK**.

**Sending a message from a Symantec NAC Integrated Enforcer to a client about non-compliance**

Although this option is displayed, it is currently unavailable for Symantec NAC Integrated Enforcer configuration.

**Establishing communication between a Symantec NAC Integrated Enforcer and a Network Access Control Scanner on an Enforcer console**

The Integrated Enforcer can be configured to connect to Network Access Control Scanners. When Network Access Control Scanner is enabled, it checks client security. If the scanner determines that a client is not running on the client computer, the policy rule is engaged. The client is either allowed or denied access to the internal network.

---

**Note:** Symantec Network Access Control Scanner does not support a printer connection to Symantec NAC Integrated Enforcers. Printers do not accept the static routes that are configured for a Symantec NAC Integrated Enforcer. Therefore the Symantec Network Access Control Scanner cannot communicate with a printer that is connected to an Integrated Enforcer.

---

**Note:** The Integrated Enforcer service needs to be restarted after you enable or disable the scanner.

---

**To establish communication between a Symantec NAC Integrated Enforcer and a Network Access Control Scanner from the Enforcer console**

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 > Network Access Control Scanner**.
3 To enable network scanners, check **Turn on NAC scanner**.

4 To add or edit a Network Access Control Scanner, click **Add**.

5 Enter the address, hostname, or DNS name in the Add/Edit management server dialog of the NAC scanner and click **OK**.

6 Enter the encryption password that is configured on the scanner.

   The preshared secret or encrypted password must match the preshared secret or encrypted password that is defined on the scanner.

   To display the letters and numbers of the preshared key instead of asterisks, check **Unmask**.

7 After scanner addresses are added to the Address list, you may modify the list by clicking **Edit, Remove, Remove all, Move Up, or Move down**.

   The Integrated Enforcer connects to the NAC scanners in the order they are listed in the NAC Scanner Address list.

8 Click **OK** to complete NAC Scanner Address list and configuration.

   The Integrated Enforcer service needs to be restarted after you enable or disable the scanner.

---

**Configuring Symantec NAC 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 NAC Integrated Enforcer configuration.

- MAC addresses for the trusted hosts that the Integrated Enforcer allows to connect to the normal DHCP server without authentication
  See “**Enabling servers, clients, and devices to connect to the network as trusted hosts without authentication**” on page 364.

- Enabling local authentication

When you apply any of these configuration settings, the changes are sent to the selected Symantec NAC Integrated Enforcer during the next heartbeat.
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 to the normal DHCP server without authenticating the trusted host.

To enable servers, clients, and devices to connect to the network as trusted hosts without authentication

1. In the Symantec Endpoint Protection Manager Console, click **Admin**.
2. In the Admin page, click **Servers**.
3. Under View 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, under Trusted Hosts, 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.

   You can also copy a set of MAC addresses from a text file.

   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-**-66 does not represent the correct use of the wildcard character.

8. Click **OK**.
9 In the Settings dialog box, on the Advanced tab, click **OK**.

The MAC address for the trusted host that you added now appears in the Settings dialog box in the MAC Address area.

10 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 the 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 the Symantec Endpoint Protection Manager server, it always asks the Symantec Endpoint Protection Manager server to verify the client’s UID regardless of whether local authentication is enabled or disabled.

**To enable local authentication on the Integrated Enforcer**

1 In the Symantec Endpoint Protection Manager Console, click **Admin**.

2 In the Admin page, click **Servers**.

3 Under View 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**.

### 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. This information is stored in the local cache (but only if cache is enabled). It automatically authenticates new clients (based on their host integrity status) but it skips the GUID and policy verification.

As soon as the communication to the Symantec Endpoint Protection Manager is reestablished, the Integrated Enforcer updates the policy version. It also authenticates the clients that have been added since the connection was lost.

**Note:** You can configure the Symantec NAC Integrated Enforcer to quarantine new clients instead of authenticating them while the Symantec Endpoint Protection Manager connection is unavailable. You accomplish this goal by changing the default value of the DetectEnableUidCache key in the registry.

Stopping the Integrated Enforcer does not affect 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 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 NAC Integrated Enforcer.
2. Click **Symantec NAC Integrated Enforcer**.
3. 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 NAC 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 NAC 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.

### Disconnecting an Integrated Lucent Enforcer from a management server on an Enforcer console

You may need to disconnect an Integrated Lucent Enforcer from a management server under the following circumstances:

- Troubleshooting an Integrated Lucent Enforcer.
- Troubleshooting a management server.

**Warning:** Be sure to stop the Enforcer service before you try to disconnect an Integrated Lucent Enforcer from a management server. Clients may no longer be able to connect to the network unless you have set up failover management servers.

If you want to disconnect an Integrated Lucent Enforcer from a management server, you need to delete the IP address, host name, or domain name from the designated management server list.

You can perform this task on an Enforcer console or on a management server console.

**To disconnect an Integrated Lucent Enforcer from a management server on an Enforcer console**

2. In the left-hand panel, expand Symantec Lucent Enforcer.
3. Expand Configure.
4. Click Management Servers.
5 In the Management Servers panel, select the management server that you want to disconnect from the Integrated Lucent Enforcer.

6 In the icon column that is located to the right of the management servers list, click Remove or Remove All.

7 Click Save.

Configuring a secure subnet mask

The Integrated Enforcer Advanced Settings configuration page allows users to bypass quarantine and communicate with the legacy 5.1.x Symantec Policy Manager server.

Note: The secure subnet mask (255.255.255.255) option is only available with the Symantec NAC Integrated Enforcer for Microsoft DHCP Servers.

To connect to a legacy Symantec Endpoint Protection Manager server

1 Check the option to Use secure subnet mask (255.255.255.255) for quarantine IP address, or uncheck to use the default subnet 255.255.255.0

2 Click OK to save your configurations.
Installing and configuring the Symantec NAC Integrated Enforcer for Microsoft Network Access Protection

- Chapter 21. Introducing the Symantec NAC Integrated Enforcer for Microsoft Network Access Protection
- Chapter 22. Planning for the installation of the Symantec NAC Integrated Enforcer for Microsoft Network Access Protection
- Chapter 23. Installing the Symantec NAC Integrated Enforcer for Microsoft Network Access Protection
- Chapter 24. Configuring the Symantec NAC Integrated Enforcer for Microsoft Network Access Protection on an Enforcer console
- Chapter 25. Configuring the Symantec NAC Integrated Enforcer for Microsoft Network Access Protection on a Symantec Endpoint Protection Manager console
Introducing the Symantec NAC Integrated Enforcer for Microsoft Network Access Protection

This chapter includes the following topics:

- About the Integrated Enforcer for Microsoft Network Access Protection

About the 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. 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 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 health 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 until their configuration is updated and brought into compliance with a policy. Depending on how you choose to deploy NAP, noncompliant clients can be automatically updated so that users can quickly regain full network access without manually updating or reconfiguring their computers.

If you configure a Network Policy Server (NPS) as a Network Access Protection (NAP) policy server, NPS evaluates statements of health (SoH) that are sent by NAP-capable client computers that want to connect to the network. You can configure NAP policies on NPS that allow client computers to update their configuration to become compliant with your organization’s network policy.

NAP can help you solve the following problems by:

- Checking adherence to endpoint security policies
- Controlling guest access
- Authenticating end users
Planning for the installation of the Symantec NAC Integrated Enforcer for Microsoft Network Access Protection

This chapter includes the following topics:

- About planning for the installation of the Symantec Integrated NAP Enforcer
- Required components for an Symantec Integrated NAP Enforcer
- Hardware requirements for a Symantec Integrated NAP Enforcer
- Operating system requirements for a Symantec Integrated NAP Enforcer
- Operating system requirements for a Symantec Network Access Control client

About planning for the installation of the Symantec Integrated NAP Enforcer

You must meet a number of requirements before the Integrated Enforcer for Microsoft Network Access Protection (NAP) can become operational. The requirements apply to both hardware and software, as well as other software components, including third-party applications.
The type of Enforcer that you can implement depends on the type of Symantec Network Access Control product that you purchased.

See your license agreement for more information.

**Required components for an Symantec Integrated NAP Enforcer**

The Symantec Integrated NAP Enforcer works with the Microsoft DHCP Server, the Symantec Endpoint Protection Manager, and the Symantec Network Access Control client with Network Access Protection enabled. The Symantec Integrated NAP Enforcer 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 NAP Enforcer:

- **Symantec Endpoint Protection Manager version 11.0.2**
  Required to create security policies in a centralized location and assign them to clients.

- **Windows 2008 server**
  Required installation of the Microsoft Windows Server with the DHCP Server service and the Network Policy Server service. These two services must be installed and configured before you can install the Symantec Integrated NAP Enforcer.

- **DHCP Server service as well as the Network Policy Server (NPS) service must also be installed on the same computer**

- **Domain Controller**
  Required installation of the Domain Controller on the same computer as the Symantec Endpoint Protection Manager or on a different computer that supports Microsoft Windows Server 2003.

- **Symantec Integrated NAP Enforcer**
  Required to authenticate clients and enforce security policies.

- **Symantec Network Access Control client**
  Required installation of the Symantec Network Access Control client.

**Hardware requirements for a Symantec Integrated NAP Enforcer**

The Symantec Integrated NAP Enforcer includes RAM, processor, storage, monitor, network adapter, and network interface card hardware requirements.
For installations of up to 10,000 users, use the following recommended requirements:

- Pentium III 750 MHz
- 256-MB memory
- 120-MB 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 memory
- 512-MB disk space
- 1-GB network adapters
- 800 x 600 resolution monitor with 256 colors (minimum)
- One network interface card (NIC) with TCP/IP installed

Operating system requirements for a Symantec Integrated NAP Enforcer

The Symantec Integrated NAP Enforcer requires that the following operating system and services are installed:

- You can select one of the following configurations:
  - Windows Server 2008 DHCP service if you plan to use DHCP enforcement
    The Windows 2008 DHCP service should be located on the same computer as the Windows Server 2008 Network Policy Server.
  - 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.
  - Windows Server 2008 Network Policy Server (NPS) service
Operating system requirements for a Symantec Network Access Control client

The Symantec Network Access Control client requires one of the following operating systems to be installed on the client computer:


■ XP Professional with Service Pack 3
Installing the Symantec NAC Integrated Enforcer for Microsoft Network Access Protection

This chapter includes the following topics:

■ Before you install the Symantec Integrated NAP Enforcer
■ Installing the Symantec Integrated NAP Enforcer

Before you install the Symantec Integrated NAP Enforcer

Before you install the Symantec Integrated NAP Enforcer, you must have completed the following installation and configuration tasks:

■ Installation of the Symantec Endpoint Protection Manager

Note: It is recommended that you install the Symantec Endpoint Protection Manager before you install the Symantec Integrated NAP Enforcer. The Symantec Endpoint Protection Manager must be installed before the Symantec Integrated NAP Enforcer can work properly.

See the Installation Guide for Symantec Enterprise Protection and Symantec Network Access Control on how to install the Symantec Endpoint Protection Manager.
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 NAP Enforcer

See “Required components for an Symantec Integrated NAP Enforcer” on page 374.

Installing the Symantec Integrated NAP Enforcer

You must install the Symantec Integrated NAP Enforcer on the same computer on which you have already installed the Microsoft Windows server operating system. The DHCP Server service and the Network Access Protection Server service should have already been installed and configured on the same computer. 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 the Symantec Endpoint Protection Manager.

You can install the Symantec Integrated NAP Enforcer by using the Installation Wizard.

See “To install the Symantec Integrated NAP Enforcer with the Installation Wizard” on page 378.

To install the Symantec Integrated NAP Enforcer with the Installation Wizard

1. Insert the installation CD for Symantec Network Access Control into the CD-ROM drive to start the installation automatically.
   - If the installation does not start, click IntegratedEnforcerInstaller.exe.
   - You must exit the installation and install the NAP server if the NAP 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.

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. The application is automatically installed in the C:\Program Files\Symantec\Integrated Enforcer\ folder.

If you want to select a destination folder, click Browse to locate and select a destination folder, click OK, and then click Next.

6 If the Role Selection panel appears, select NAP Enforcement and click Next. The Role Selection panel only appears if more than one type of Symantec NAC Integrated Enforcer can be installed based on the services running on the server.

7 In the Ready to Install the Application panel, click Next. If you need to modify any of the previous settings, click Back.

8 Click Finish. If you need to reinstall the Symantec Integrated NAP Enforcer, you must first uninstall it.

9 Click Start > Programs > Symantec Enterprise Protection > Symantec Integrated Enforcer.

To Uninstall the Symantec Integrated NAP Enforcer

1 On the Windows taskbar, click Start > Control Panel > Add or Remove Programs.

2 Click Symantec 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 NAP server, do one of the following tasks:
   - To restart the NAP server immediately, click Yes.
   - To restart the NAP service manually later (the default), click No.

   If you restart the NAP service later, you must stop and then start it. You must restart the NAP service to completely uninstall the Symantec Integrated Enforcer.
To uninstall the Symantec Integrated NAP Enforcer from the command line

1. Open a DOS command prompt.
2. At the command prompt, type: `MsiExec.exe /qn /X{A145EB45-0852-4E18-A9DC-9983A6AF2329}`
3. Restart NAP Server

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 Symantec NAC Integrated Enforcer for Microsoft Network Access Protection on an Enforcer console

This chapter includes the following topics:

- About configuring a Symantec Integrated NAP Enforcer on an Enforcer console
- Connecting a Symantec Integrated NAP Enforcer to a management server on an Enforcer console
- Encrypting communication between a Symantec Integrated NAP Enforcer and a management server
- Setting up an Enforcer group name on the Symantec Integrated NAP Enforcer console
- Setting up an HTTP communication protocol on the Symantec Integrated NAP Enforcer console
About configuring a Symantec Integrated NAP Enforcer on an Enforcer console

After you complete the installation of the Symantec Integrated NAP Enforcer, you must perform the following tasks before the Symantec Integrated NAP Enforcer can become operational:

- Specify at least one Symantec Endpoint Protection Manager to which the Symantec Integrated NAP Enforcer can connect. You include the host name or IP address of the Symantec Endpoint Protection Manager in a file that is called a management server list. The Symantec Integrated NAP Enforcer must connect to an IP address or host name of a Symantec Endpoint Protection Manager. Otherwise the configuration fails. See “Connecting a Symantec Integrated NAP Enforcer to a management server on an Enforcer console” on page 382.

- Add an encrypted password or a preshared secret that you configured during the installation of the Symantec Endpoint Protection Manager. The encrypted password was previously known as a preshared key. See “Encrypting communication between a Symantec Integrated NAP Enforcer and a management server” on page 384.

- Set up an Enforcer group name
  See “Setting up an Enforcer group name on the Symantec Integrated NAP Enforcer console” on page 385.

- Set up an HTTP communication protocol
  See “Setting up an HTTP communication protocol on the Symantec Integrated NAP Enforcer console” on page 386.

Connecting a Symantec Integrated NAP Enforcer to a management server on an Enforcer console

You need to connect a Symantec Integrated Network Access Protection Enforcer to a management server on a Network Access Protection Enforcer console.
To connect a Symantec Integrated NAP Enforcer to a management server on an Enforcer console


   The Symantec Integrated NAP Enforcer console appears. The main page shows the connection status between the Symantec Integrated NAP Enforcer and the Symantec Endpoint Protection Manager. A green light indicates that Symantec Integrated NAP Enforcer is actively connected to a management server. A red light indicates that the connection failed.

2. In the left-hand panel, expand Symantec NAP Enforcer.

3. In the left-hand panel, expand Configure.

4. In the left-hand panel, click Management Servers.

5. In the Management Servers panel, click Add from the icon column that is located to the right of the management servers list.

6. In the Add/Edit 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 domain name, the Symantec Integrated NAP Enforcer must connect to a domain name server (DNS) server.

7. In the Add/Edit Management Server dialog box, edit the port number that the Symantec Integrated NAP Enforcer uses to communicate with the Symantec Endpoint Protection Manager.

   The default port number is 80 for the 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.

8. Click OK.

9. In the Add/Edit management server dialog box, select a different management server.

   You can change the order of the management servers that the Symantec Integrated NAP Enforcer uses to connect to a Symantec Endpoint Protection Manager.
10 Click Move up or Move down arrows from the icon column that is located to the right of the management servers list.

When a Symantec Integrated NAP Enforcer connects to a Symantec Endpoint Protection Manager for the first time, it tries to connect to the first management server that is listed in the management server list. If the management server is not available, the Symantec Integrated NAP Enforcer connects to the next management server that appears in the management server list.

11 To edit a management server, click Edit from the icon column and modify the management server address or port information.

To remove a Symantec Endpoint Protection Manager from a management server list on a Symantec Integrated NAP 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 To remove a Symantec Endpoint Protection Manager, click Remove or Remove All from the icon column.

Encrypting communication between a Symantec Integrated NAP Enforcer and a management server

If you want to add another layer of security, you can secure communication between the Symantec Integrated NAP Enforcer and the 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 the 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 the Symantec Endpoint Protection Manager fails.
To encrypt communication between a Symantec Integrated NAP Enforcer and a 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 the Symantec Endpoint Protection Manager.
   The encrypted password is always configured during the installation of the Symantec Endpoint Protection Manager.
6. Check **Unmask**.
   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 NAP Enforcer console**

You must add a name for the Enforcer group. After the Symantec Integrated NAP Enforcer connects to a 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 Integrated NAP 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, then all Integrated Enforcers automatically become part of the Temporary group on the management server. If you add the name of the Integrated Enforcer group on the Enforcer console, then 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 NAP Enforcer console

You need to establish a communication protocol between the Symantec Integrated NAP Enforcer and the Symantec Endpoint Protection Manager. Otherwise the communication between the Symantec Integrated NAP Enforcer and the Symantec Endpoint Protection Manager fails.

You can set up a 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 NAP 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 of the Symantec Integrated NAP Enforcer console, click HTTP.

   If you want to set up encrypted communication between the Symantec Integrated NAP Enforcer and the 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 Symantec NAC Integrated Enforcer for Microsoft Network Access Protection on a Symantec Endpoint Protection Manager console

This chapter includes the following topics:

- About configuring the Symantec Integrated NAP Enforcer on a Symantec Endpoint Protection Manager Console
- Enabling NAP enforcement for clients
- Verifying that the management server manages the client
- Verifying Security Health Validator policies
- Verifying that the clients passes the Host Integrity check
- Enabling local authentication on the Symantec Integrated NAP Enforcer
- Configuring logs for the Symantec Integrated NAP Enforcer
About configuring the Symantec Integrated NAP Enforcer on a Symantec Endpoint Protection Manager Console

If you want to support the Symantec Integrated NAP Enforcer in a network environment, you must enable NAP enforcement on the Symantec Endpoint Protection Manager. Otherwise the Enforcer will work 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.

Enabling NAP enforcement for clients

You must enable NAP enforcement for Symantec Endpoint Protection and Symantec Network Access Control clients. If you do not enable Network Access Protection (NAP) enforcement for clients, the Symantec Integrated NAP Enforcer cannot implement any Security Health Validator policies.

To enable NAP enforcement for clients

1. In the Symantec Endpoint Protection Manager Console, click Clients.
2. In the Clients page, under View Groups, select the group for which you want to enable NAP enforcement.
4. In the Settings dialog box, click Security Settings.
   The Enable NAP Enforcement setting is disabled by default.
6. Click OK.

Verifying that the management server manages the client

You can set up a verification check to ensure that the 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 the Symantec Endpoint Protection Manager Console, click **Admin**.
2. In the Admin page, click **Servers**.
3. In the Admin page, 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, check **Verify that the management server manages the client**.
   The Verify that the management server manages the client setting is disabled by default.
6. In the Client Information area on the NAP Setting tab in the I-DHCP Settings dialog, 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 the Symantec Endpoint Protection Manager Console, click **Admin**.
2. In the Admin page, click **Servers**.
3. In the Admin page, 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, 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 the clients passes the Host Integrity check

You can set up a compliance check for clients on the Symantec Endpoint Protection Manager.
To verify that the client passes the Host Integrity check
1. In the Symantec Endpoint Protection Manager Console, click **Admin**.
2. In the Admin page, click **Servers**.
3. In the Admin page, 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, 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**.

### Enabling local authentication on the Symantec Integrated NAP Enforcer

With local authentication enabled, if the Symantec Integrated NAP Enforcer loses its connection with the client on which the Symantec Endpoint Protection Manager is installed, the Symantec Integrated NAP Enforcer authenticates clients locally. In this case, the Symantec Integrated NAP Enforcer considers the client a valid user and only checks the client’s Host Integrity status.

**Note:** If the Symantec Integrated NAP Enforcer does not lose its connection with the Symantec Endpoint Protection Manager server, it always asks the Symantec Endpoint Protection Manager server to verify the client’s UID regardless of whether local authentication is enabled or disabled.

To enable local authentication on the Symantec Integrated NAP Enforcer
1. In the Symantec Endpoint Protection Manager Console, click **Admin**.
2. In the Admin page, click **Servers**.
3. Under View Servers, select and expand the group of Symantec Integrated NAP 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 logs for the Symantec Integrated NAP Enforcer

Logs for the Symantec Integrated 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 on the Symantec Endpoint Protection Manager Console, you must enable the sending of logs on the Symantec Endpoint Protection Manager Console. If this option is enabled, the log data is sent from the Symantec Integrated NAP Enforcer to the Symantec Endpoint Protection Manager and stored in a database.

You can modify the log settings for the Symantec Integrated NAP Enforcer on 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:

- Enforcer Server log
- Enforcer Client log

The Client 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 NAC Integrated Enforcer for Microsoft Network Access Protection on a Symantec Endpoint Protection Manager console

Configuring logs for the Symantec Integrated NAP Enforcer
Chapter 26. Managing Enforcers on the Symantec Endpoint Protection Manager console
Managing Enforcers on the Symantec Endpoint Protection Manager console

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
- Displaying information about the Enforcer on the management console
- Changing an Enforcer’s name and description
- Deleting an Enforcer or an Enforcer group
- Exporting and importing Enforcer group settings
- Pop-up messages for blocked clients
- About client settings and the Enforcer
- Configuring clients to use a password to stop the client service
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 you configure: Gateway, LAN, or DHCP appliance. 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.

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 400.

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 View Servers pane and edit the group properties.

How the console determines the Enforcer group name

When you set up the console connection on the Enforcer local console, you can specify a group name. The Enforcer registers itself with the console after establishing the connection. The console automatically assigns the Enforcer to the specified group and lists the Enforcer under the group name in the console View Servers pane. If you do not specify a name during setup, the console assigns the Enforcer to a default Enforcer group. The console uses the name of the Enforcer computer as the group name.

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 DHCP Enforcer or a 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 DHCP or Gateway Enforcer has exactly the same settings as the primary Enforcer.

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.

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.

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.

You can view similar information about the Enforcer on the Enforcer console. Table 26-1 describes the type of information that you can view.

<p>| Table 26-1 Information about the Enforcer appliance on the Enforcer console |</p>
<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 be 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>
</tbody>
</table>
Table 26-1 Information about the Enforcer appliance on the Enforcer console (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online Status</td>
<td>Online: The service is running and is the primary active Enforcer. Offline:</td>
</tr>
<tr>
<td></td>
<td>The service is stopped.</td>
</tr>
<tr>
<td>Failover Status</td>
<td>(Gateway and DHCP Enforcer only) Whether the Enforcer is active or on</td>
</tr>
<tr>
<td></td>
<td>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 and DHCP Enforcer only) IP address of the external network</td>
</tr>
<tr>
<td></td>
<td>interface card.</td>
</tr>
<tr>
<td>Internal MAC</td>
<td>The MAC address of the internal network interface card</td>
</tr>
<tr>
<td>External MAC</td>
<td>(Gateway and DHCP Enforcer only) The MAC address of the external network</td>
</tr>
<tr>
<td></td>
<td>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 and DHCP Enforcer only) Manufacturer and model of the external</td>
</tr>
<tr>
<td></td>
<td>network interface card.</td>
</tr>
</tbody>
</table>

Displaying information about the Enforcer on the management console

You can display information about the Enforcer from a console.

See Table 26-1 on page 398.

To display information about the Enforcer on the management console

1. In the Symantec Endpoint Protection Manager Console, on the Admin page, click Servers.
2. Under View Servers, click the name of the Enforcer about which you want to view information.

Information about the LAN Enforcer appliance do not appear in the fields that refer to the external NIC because the LAN Enforcer appliance only requires an internal NIC. No failover status is shown because a switch manages LAN Enforcer failover.
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 the console, on the Admin page, click Servers.
2. Under View 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 the console, on the Admin page, click Servers.
3. Under View 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 the Symantec Endpoint Protection console, click **Admin**.
   In the Admin page, click **Servers**.
2. Under View 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 the management console, on the Admin page, click **Servers**.
2. Under View 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**.

When you import settings, you must import them into an existing Enforcer group, which overwrites the selected group settings.

To import Enforcer group settings
1. In the management console, on the Admin page, click **Servers**.
2. Under View 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**.

Pop-up messages for blocked clients

When an Enforcer blocks a client that tries to connect to the network, the following two types of pop-up messages can be configured:
Messages for the computers that are running the client

If the Enforcer blocks computers even though they are running a client, there can be several causes. A blockage can occur because a Host Integrity check failed or because the client policy is not up-to-date. When these events occur, you can specify that a pop-up message displays on the client. That message notifies the user that the Enforcer has blocked all traffic from the client and why it was blocked. For example, the following message is displayed if the client has failed the Host Integrity check:

Symantec Enforcer has blocked all traffic from the client because the client failed Host Integrity.

You can add text to the default message. For example, you may want to tell the computer user what to do to remedy the situation. You configure this message as part of the client group policy settings rather than the Enforcer settings.

Messages for Windows computers that are not running the client (Gateway or DHCP Enforcer only)

In some cases, clients try to connect to the enterprise network without running the client. Gateway and DHCP Enforcers provide 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:** For the Gateway Enforcer only, 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.
Setting up the Enforcer messages

You can configure the Enforcer messages that appear on the clients when an Enforcer blocks the clients.

**Note:** You can modify the settings only for the groups that do not inherit settings from a parent group.

**To set up the Enforcer messages**

1. In the console, on the Clients page, select the Policies tab.
2. Under View Policies, select the group for which you want to specify a pop-up message.
3. Under Settings, select **General Settings**. The Group Settings dialog box appears with the General Settings tab selected.
4. On the Security Settings tab, select **Display a message when a client is blocked by a Symantec Enforcer**.
5. If you want to add text to the default message, click **Set Additional Text**, then type the text, and click **OK**.
6. Click **OK**.

About client settings and the Enforcer

Symantec clients work with the Enforcer with no special configuration. The exception is some 802.1x authentication settings required for the LAN Enforcer. Also, there is one situation you should be aware of when configuring clients. If an end user stops the client while it is running, a problem could occur.

Configuring clients to use a password to stop the client service

The 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 do a release and renew of 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 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.
To configure clients to use a password to stop the client service

1. In the console, on the Client page, select the client group.
2. On the Policies tab, under Settings, click **General Settings**.
3. On the Security Settings tab, under Client Password Protection, select **Require a password to stop the client service** and specify the password.
4. Click **OK**.
Working with enforcer reports and logs

- Chapter 27. Managing Enforcer reports and logs
Managing Enforcer reports and logs

This chapter includes the following topics:

- About Enforcer reports
- About Enforcer logs
- Configuring Enforcer log settings

About Enforcer reports

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.

See the Administration Guide for Symantec Endpoint Protection Manager and Symantec Network Access Control for detailed information about Enforcer reports.

See “About Enforcer logs” on page 408.
About Enforcer logs

Enforcers provide the following logs that you can use to monitor and troubleshoot system activity:

- **Enforcer Server log**
  See “About the Enforcer Server log” on page 408.

- **Enforcer Client log**
  See “About the Enforcer Client log” on page 409.

- **Enforcer Traffic log (Gateway Enforcer only)**
  See “About the Gateway Enforcer Traffic log” on page 410.

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 the 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.

---

**Note:** A system log called Enforcer Activity is also available on the Symantec Endpoint Protection Manager Console. It contains information about events such as when Enforcers start and when they connect to the Symantec Endpoint Protection Manager.

---

About the Enforcer Server log

The Enforcer Server log provides the information that is related to the functioning of an Enforcer.

*Table 27-1* describes the information that is available in the Enforcer Server log.
### Table 27-1 Enforcer Server log information

<table>
<thead>
<tr>
<th>Log column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>The date and time of the logged event. You should keep the time of the Enforcer Server log synchronized with the Linux system time on the Enforcer appliance. You may need to manually change the time on the Enforcer appliance to match changes to daylight saving time (DST).</td>
</tr>
<tr>
<td>Event Type</td>
<td>The type of event. For example, Enforcer registered or Server received Enforcer log are types of events.</td>
</tr>
<tr>
<td>Enforcer Name</td>
<td>The name of the Enforcer that this event involves.</td>
</tr>
<tr>
<td>Site</td>
<td>The name of the site that this event involves.</td>
</tr>
<tr>
<td>Server</td>
<td>The name of the server that this event involves.</td>
</tr>
</tbody>
</table>

### About the Enforcer Client log

An Enforcer Client log provides information about the interactions between an Enforcer and a client that has tried to connect to the network. It shows information about authentication, failed authentication, and disconnection.

In a peer-to-peer authentication scenario, the Enforcer Client log also shows information about authentication, failed authentication, and disconnection. The information is for interactions between the clients that act as Enforcers and remote clients. The remote clients try to connect to the network through the clients that act as Enforcers.

*Table 27-2* describes the information that is available in the Enforcer Client log.

### Table 27-2 Enforcer Client log information

<table>
<thead>
<tr>
<th>Log column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>The date and time that the interaction with the client occurred.</td>
</tr>
<tr>
<td>Enforcer Name</td>
<td>The host name of the Enforcer appliance or computer that this event involves.</td>
</tr>
<tr>
<td>Enforcer Type</td>
<td>The type of Enforcer that this event involves, either a Gateway Enforcer appliance, a DHCP Enforcer appliance, or a LAN Enforcer appliance.</td>
</tr>
</tbody>
</table>
**Table 27-2**  
Enforcer Client log information (continued)

<table>
<thead>
<tr>
<th>Log column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site</td>
<td>The name of the site that this event involves</td>
</tr>
<tr>
<td>Remote Host</td>
<td>The host name of the client that this event involves, if any</td>
</tr>
<tr>
<td>Action</td>
<td>The action that the Enforcer took. This column can contain the following actions:</td>
</tr>
</tbody>
</table>
|                 | ■ Authenticated  
The client’s unique identifier (UID) was correct. |
|                 | ■ Rejected       
The client’s UID was incorrect or no client was running. |
|                 | ■ Disconnected   
The client has disconnected from the Enforcer or the Enforcer service has stopped. |
|                 | ■ Passed         
The client passed the Host Integrity check. |
|                 | ■ Failed         
The client failed the Host Integrity check. |
| Remote MAC      | The MAC address of the client |

**About the Gateway Enforcer Traffic log**

The Traffic log records all traffic that enters through a Gateway Enforcer appliance’s external adapter and leaves through the internal adapter.

**Note:** Traffic logs are available on Gateway Enforcer appliances only. The contents depend on the Traffic log filter that is set in the Gateway Enforcer Settings dialog box.

*Table 27-3* describes the information available in the Gateway Enforcer Traffic log.

**Table 27-3**  
Gateway Enforcer appliance Traffic log information

<table>
<thead>
<tr>
<th>Log column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>The date and time of the traffic event.</td>
</tr>
<tr>
<td>Enforcer Name</td>
<td>The name of the Gateway Enforcer appliance that this event involves.</td>
</tr>
</tbody>
</table>
### Configuring Enforcer log settings

You can configure settings for Enforcer logs in the Enforcer name Settings dialog box on the Logging tab. The changes are sent to the selected Enforcer during the next heartbeat.

#### Disabling Enforcer logging on the Symantec Endpoint Protection Manager Console

By default, Enforcer logging is enabled. You can disable it on the Symantec Endpoint Protection Manager Console. If you disable logging, you can enable it from this same location.

**To disable Enforcer logging on the Symantec Endpoint Protection Manager Console**

1. In the Symantec Endpoint Protection Manager Console, click **Admin**.
2. In the Admin page, click **Servers**.
3. In the Admin page, under View Servers, select the Enforcer group for which you want to disable Enforcer logging.
4. In the Admin page, under Tasks, click **Edit Group Properties**.

---

**Table 27-3**

Gateway Enforcer appliance Traffic log information (continued)

<table>
<thead>
<tr>
<th>Log column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enforcer Type</strong></td>
<td>The name of the type of Enforcer that this event involves, either a Gateway Enforcer appliance, a DHCP Enforcer, or a LAN Enforcer.</td>
</tr>
<tr>
<td><strong>Site</strong></td>
<td>The name of the site that this event involves.</td>
</tr>
<tr>
<td><strong>Local Port</strong></td>
<td>The TCP port or UDP port of the packet destination.</td>
</tr>
<tr>
<td><strong>Local Host IP</strong></td>
<td>The IP address of the packet source.</td>
</tr>
<tr>
<td><strong>Remote Host IP</strong></td>
<td>The IP address of the packet destination.</td>
</tr>
<tr>
<td><strong>Direction</strong></td>
<td>The direction of the traffic: either inbound, which enters the Gateway Enforcer appliance, or outbound, which leaves the Gateway Enforcer appliance.</td>
</tr>
<tr>
<td><strong>Action</strong></td>
<td>The action taken. For example, the action can be authenticated or blocked.</td>
</tr>
<tr>
<td><strong>Count</strong></td>
<td>The number of times the same packet was received.</td>
</tr>
</tbody>
</table>
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.

Enabling the sending of Enforcer logs from an Enforcer to the 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 the Symantec Endpoint Protection Manager. As soon as you enable the sending of logs, you can view all Symantec logs in a central location on the Symantec Endpoint Protection Manager Console.

To enable the sending of Enforcer logs from an Enforcer to the Symantec Endpoint Protection Manager

1 In the Symantec Endpoint Protection Manager Console, click Admin.
2 In the Admin page, click Servers.
3 In the Admin page, under View Servers, select the Enforcer group for which you want to enable the sending of Enforcer logs from an Enforcer to a Symantec Endpoint Protection Manager.
4 In the Admin page, 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 the Symantec Endpoint Protection Manager.

6 Click OK.

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 the Symantec Endpoint Protection Manager Console, click Admin.
2 In the Admin page, click Servers.
3 In the Admin page, under View Servers, select the Enforcer group for which you want to set the size and age of Enforcer logs.
4 In the Admin page, under Tasks, click Edit Group Properties.
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.

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.

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 the Symantec Endpoint Protection Manager Console, click Admin.

2 In the Admin page, click Servers.

3 In the Admin page, under View Servers, select the Enforcer group for which you want to filter Traffic logs.

4 In the Admin page, under Tasks, click Edit Group Properties.

5 In the Enforcer name Settings dialog box, on the Logging tab, in the Traffic log filter list, select one of the following filter options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All traffic</td>
<td>Logs all traffic, including that which is allowed and dropped</td>
</tr>
<tr>
<td>Only blocked traffic</td>
<td>Logs only the clients that the Enforcer blocks</td>
</tr>
<tr>
<td>Only allowed traffic</td>
<td>Logs only the traffic that the Enforcer allows</td>
</tr>
</tbody>
</table>

6 Click OK.
Managing Enforcer reports and logs

Configuring Enforcer log settings
configure command  (continued)
  advanced failover 244
  advanced legacy 245
  advanced legacy UID 246
  advanced local authentication 246
  advanced RADIUS 246
  advanced re-initialize 247
  advanced show 248
  advanced SNACS 247
  advanced user-class 248
  DNS add IP address 249
  DNS delete IP address 249
  interface 250
  interface-role 251
  ntp 251
  redirect 252
  route 252
  show 253
  spm 253
configuring
  Enforcer log 411
connectors
  Enforcer appliance 73
console
  displaying Enforcer information 399
  Enforcer 398
  Enforcer management 396
  Servers page 396
console command 208, 254
  baud-rate 254
  show 255
  ssh 255
  sshkey 255
controls
  Enforcer appliance 73

DHCP Enforcer appliance
  about 27, 72, 122
  advanced user-class command 248
  authentication 127
  configuring 122
  failover 57, 72
  how it works 33
  installation 75
  installation planning 52
  IP address 54
  network interface card configuration 251
  NIC 75
  remediation server 72
DHCP request packet 117
DHCP server
  and Integrated Enforcer 315
  and non-authenticated clients 359
  as quarantine server 356
  DHCP Enforcer appliance 136
  Integrated Enforcer for Microsoft DHCP Servers 305, 344
  maximum number in network 136
  quarantine 248
  quarantined clients 136
  restarting 344
DNS request packet 117
DNS spoofing
  command 244
  enabling 143
domain name server 249

E
  encrypted password 344
  encryption
    password 177
  Symantec Integrated NAP Enforcer 384
Enforcer
  about a group 397
  changing a group 398
  changing a group name 397
  Client log 409
  console 398
    managing 396
  creating a group 398
  deleting 400
  DHCP failover 397
  editing description 400
  editing name 400
  failover 397
Enforcer (continued)

Gateway failover 397
  group
    exporting settings 401
    importing settings 401
LAN failover 397
log 408
report 407
Server log 408
settings 396
third-party vendor 38
Traffic log 410

Enforcer appliance
  alphabetical command reference 216
  back panel 74
  checking communication status 85
  command line interface 207
    help system 213
    keystroke shortcuts 211
    top-level commands 233
  configuring 78
  connectors 73
  console commands 254
  controls 73
  debug commands 255
  DHCP 26
Enforcer appliance, command line interface
  command conventions 215
frequently asked questions 297
front panel 73
Gateway 26
hardware specifications 74
indicators 73
installing 71
LAN 26
lock 80
logging on 82
mab commands 258
mab database commands 258
monitor reports 86
purpose 28
reimaging 70
showing status 86
troubleshooting 293
type of enforcement 26
use 28

Enforcer log (continued)
retention 412
  sending to management console 412
  size 412
Enforcer Server log
  name of Enforcer involved in event 409
  name of server responsible for event 409
  site where event took place 409
  time of logged event 409
  type of event 409
Enforcer Traffic log
filtering 413

Enforcers
  authenticates client with UID 31
  client settings 403
  Gateway 88
  restricting client stoppage 403
  exit command 208, 233
  exporting
    Enforcer group settings 401

F
failover
  command 244
  DHCP Enforcer appliance 57
  Gateway Enforcer appliance 45, 49
  LAN Enforcer appliance 64

G
Gateway Enforcer
  and Symantec Endpoint Protection Manager
    configuration 88
  appliance commands 216
  multiple installations 113
  network locations 42
Gateway Enforcer appliance
  about 27, 72
  ARP request packet 117
  authentication 32
  DHCP request packet 117
  DNS request packet 117
  Failover 49
  failover 45
  how it works 32
  installation 72, 75
  installation planning 42
  installing 71
  IP address 45
Gateway Enforcer appliance (continued)
  network interface card configuration 251
  network locations 72
  NIC 75
  non-Windows client 47
  non-Windows server 47
  other protocols 117
  remote access server (RAS 45
  server protection 46
  servers 43
  Traffic log 410
  VPN 43, 46
  wireless access point (WAP) 43
  wireless access points (WAP) 46

  group
  DHCP Enforcer appliance 124
  Gateway Enforcer appliance 91
  Integrated Enforcer 349
  LAN Enforcer appliance 152
  RADIUS server 156, 178

H
  hardware requirements for Integrated Lucent Enforcer 333
  hardware specifications
    Enforcer appliance 74
  heartbeat
    between Symantec Endpoint Protection Manager and Enforcer 31
  help command 208, 234
  host integrity
    check 30
    Enforcer appliance 30
    frequently asked questions 299
    message 299
    RADIUS server 148
    status 31
    supported software 297
  Host Integrity check
    and Integrated Enforcer 356
  host integrity policy
    global level 299
    group level 299
  hostname command 208, 235

I
  importing
    Enforcer group settings 401
  indicators
    Enforcer appliance 73
  installation
    DHCP Enforcer appliance 71–72, 75
    Gateway Enforcer appliance 71–72, 75
    LAN Enforcer appliance 71, 73, 75
    prerequisites 71
    Symantec Integrated Enforcer
      command line 315
    install wizard 315
    Symantec Integrated NAP Enforcer 377
  installation planning
    DHCP Enforcer appliance 52
    Gateway Enforcer appliance 42
    LAN Enforcer appliance 61
  Integrated DHCP Enforcer
    Microsoft DHCP Servers 305
  Integrated Enforcer
    and Network Access Control Scanners 362
    and policy serial number checking 361
    and Symantec Endpoint Security Manager
      communication 344
    and Symantec Network Access Control
      clients 315
    communication settings 344, 362
    connection to management server 351
    installing 315
    Microsoft DHCP Servers 26
    Microsoft NAP 26
    quarantine 347
    trusted vendors 353
  Integrated Enforcer for Alcatel-Lucent VitalQIP DHCP Servers
    component 330
    hardware requirements 333
    planning 329
    type of enforcement 28
  Integrated Enforcer for Microsoft DHCP Servers
    hardware requirements 312
    Microsoft DHCP server 344
    operating system requirement 313
    planning 313
    required component 312
    Symantec Network Access Control client 305, 344
    type of enforcement 28
  Integrated Enforcer for Microsoft NAP
    type of enforcement 28
Integrated Enforcer for Microsoft Network Access Protection
operating system requirements 374
planning 373
required component 374
Integrated Lucent Enforcer
disconnecting from management server list 367
operating system requirements 333
interface-role command 251
IP address
DHCP Enforcer appliance 54
Gateway Enforcer 98
Gateway Enforcer appliance 45
Integrated Enforcer 350
quarantine 56
trusted 108–109

K
known issues 203, 294

L
LAN Enforcer
appliance commands 216
LAN Enforcer appliance
802.1x 189
802.1x basic configuration 36
802.1x supplicant 73
802.1x wireless access points 149
about 27
configuration from Symantec Endpoint Protection Manager Console 147
configuration settings 150
dynamic VLAN switching 73, 149
failover 64
how it works 35
installation 73, 75
installation planning 61
installing 71
supported switch model 164
switch settings 163
transparent mode 36, 300
legacy client
connecting to DHCP Enforcer appliance 144
connecting to Gateway Enforcer appliance 118
connecting to LAN Enforcer appliance 188
Linux operating system 70
listening port
LAN Enforcer 153
local authentication 363
command 246
enabling on DHCP Enforcer appliance 144
enabling on Gateway Enforcer appliance 119
enabling on Integrated Enforcer 365
enabling on LAN Enforcer appliance 189
enabling on Symantec Integrated NAP Enforcer 390
log. See Enforcer Server log
compliance 408
Enforcer 408
filtering Enforcer Traffic log data 413
location of 408
sending from Enforcer to Symantec Endpoint Protection Manager 408
log-on
superuser 82
log files
debug 294
log size
Enforcer 412
log-on
normal 82

M
mab command
database add 258
database clean 259
database download 260
database upload 260
disable 260
enable 261
ldap disable 261
ldap enable 262
ldap host 262
ldap password 262
ldap port 263
show 264
mab ldap commands 261
MAC address
trusted host 363
management console. See console Enforcer log 412
management server. See Symantec Endpoint Protection Manager legacy 344
management server list 93
message
Enforcer 401
messages
    Enforcer
        displaying 403
        modifying 403
monitor command 208, 264
    refresh 265
    show 265
    show blocked-hosts 265
    show connected-guests 266
    show connected-users 268

N
 Network Access Control Scanner
    and Integrated Enforcer 362
    Integrated Enforcer for Microsoft DHCP
        Servers 305
Network Access Control Scanners
    and Integrated Enforcer 344
network interface card
    configure command 251
    DHCP Enforcer appliance 75
    Gateway Enforcer appliance 75
network interface cards
    shutdown command 250
NIC. See network interface card
non-compliance message 105
    sending from DHCP Enforcer appliance 135
non-Windows client
    Gateway Enforcer appliance 47
non-Windows server
    Gateway Enforcer appliance 47
normal
    log on 82
ntp command
    disable 251
    enable 251
    server string 251

O
 on-demand authentication ad command 272
    ad domain 273
    disable 272
    enable 273
on-demand authentication command 271
    disable 274
    enable 274
on-demand authentication local-db command 275
    add 275
    (continued)
    disable 275
    enable 276
on-demand banner command 277
on-demand client-group command 277
on-demand command 271
on-demand dot1x certificate command 278
    import 279
    remove 280
on-demand dot1x command 278
on-demand dot1x show certificate command
    show 281
operating system requirement 333

P
 password
    default 78
    encryption 177
    replacement 78
password command 208, 235
password protection
    client 403
    Enforcers 403
ping command 208, 235
planning
    Integrated Enforcer for Alcatel-Lucent VitalQIP
        DHCP Servers 329
        See also Integrated Lucent Enforcer
    Integrated Enforcer for Microsoft DHCP
        Servers 313
    Integrated Enforcer for Microsoft Network
        Access Protection 373
policy enforcement 300
policy serial number 134
policy serial number check
    and Gateway Enforcer 104
policy serial number checking 361
profile serial number 129

Q
 quarantin 136
    and Integrated Enforcer 344, 347, 356
    DHCP Enforcer appliance 52
    DHCP server 56, 72
    Integrated Enforcer for Microsoft DHCP
        Servers 305
    user-class ID 248
RADIUS server 300
  and LAN Enforcer 156
  friendly name 159
  host integrity policy 148
  LAN Enforcer appliance 148
  shared secret 161
reauthentication 192
reboot command 208, 236
redirect command 252
redirection
  of HTTP requests 106
Redundant Managers 299
reimaging
  Enforcer appliance 70
remediation 32
Remote access 86
remote access server (RAS
  Gateway Enforcer appliance 45
report
  compliance 407
  Enforcer 407
  Site Status 407
  System 407
  Top Enforcers That Generate Errors 407
requirement
  hardware for Integrated Enforcer for
    Alcatel-Lucent VitalQIP DHCP Servers 333
  operating system for Integrated Lucent
    Enforcer 333
retention of log
  Enforcer 412
route command 252

S
security policy
  Cisco NAC 300
  compliance 305, 344
  DHCP 300
  LAN 300
  non-Symantec 300
  self enforcement 300
  serial number updates 361
  Universal Enforcement API 300
server protection
  Gateway Enforcer appliance 46
  shared secret 161
  editing 177
show command 208, 236, 253
  advanced 248
  capture 236
  configure 236
  console 236, 255
  debug 257
  status 236
  update 236
  version 236
shutdown command 208, 236
spm command 253
start command 208, 238
stop command 208, 238
subnet addressing 78
  Integrated Enforcer 344
secure 305
superuser
  log on 82
switch model 164
switch policy 175
  conditions and actions 184
Symantec Endpoint Protection Manager
  and DHCP Enforcer appliance 122
  and Gateway Enforcer 93
  and Integrated Enforcer 315, 344
  communication with Enforcer 31, 299
  configure SPM command 253
  host integrity 30
  Integrated Enforcer for Microsoft DHCP
    Servers 305
  LAN Enforcer appliance configuration 147
  trusted IP address 113
Symantec Enforcement client 396
Symantec Integrated NAP Enforcer
  configuring on NAP Enforcer console 382
  connecting to management server 382
  encrypted password 384
  group name 385
  hardware requirements 374
  HTTP communication protocol 386
  HTTP protocol 384
  HTTPS protocol 384
  installing 377
  operating system requirement 375
  removing from management server list 384
System
  report 407
traceroute command 208, 238
Traffic log
  Gateway Enforcer appliance 410
transparent mode 149
  authentication 36
troubleshooting 203, 293
trusted host
  client without authentication 142
  configuration 363
  device without authentication 142
  server without authentication 142
trusted network 305, 344
trusted vendors 353
unique identification checking 356
unique identifier (UID) 31
  Enforcer authentication for client 31
Universal Enforcement API 38
update command 208, 238
VLAN
  wireless access points 149
VLAN switch
  and LAN Enforcer 153
  LAN Enforcer appliance 163
VPN
  Gateway Enforcer appliance 46
vpn 203
wireless access points (WAP)
  Gateway Enforcer appliance 46
wireless access term (WAP)
  Gateway Enforcer appliance 43
wireless protocols 149, 179