Implementation Guide for Symantec™ Network Access Control Enforcement

For Symantec Network Access Control and Symantec Network Access Control Starter Edition

Implementation Guide for Symantec Network Access Control Enforcement

Documentation version 11.00.06.00.00

Legal Notice

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.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

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

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

www.symantec.com/business/support/

Contacting Technical Support

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

www.symantec.com/business/support/

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

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

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

- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals

Support agreement resources

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

Asia-Pacific and Japan	customercare_apac@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

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:

Managed Services	Managed 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.
Education Services	Education 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/business/services/

Select your country or language from the site index.

Contents

Chapter 10 Configuring the Symantec Gateway Enforcer appliance from the Symantec Endpoint Protection Manager 127

Chapter 11 Planning for the installation of the DHCP Enforcer appliance 161

Chapter 12 Configuring the DHCP Enforcer appliance on the Symantec Endpoint Protection Manager 173

Appendix A Enforcer appliance command-line interface 365

Section 1

Managing network security with Symantec Network Access Control

Introducing Symantec Network Access Control

This chapter includes the following topics:

About Symantec Network Access Control

When enforcement controls are not in place, your organization's data is vulnerable to intended loss or inadvertent loss. Recovering the data can result in down time and the financial losses that are associated with lost productivity.

To prevent these losses, Symantec Network Access Control controls on site and remote access to corporate network resources. Symantec Network Access Control provides a complete end-to-end network access control solution.

Symantec Network Access Control provides two types of enforcement:

- Host-based self enforcement allows client computers to obtain and run the software they need to automatically remediate compliance failures. When the client computer is remediated, it can safely access the network. Host-based self enforcement does not use a Symantec Enforcer to check client integrity.
  See "About Host Integrity remediation" on page 63.
- Network-based enforcement using the Symantec Enforcer appliances and integrated software Enforcers let you control network access. Network-based

enforcement can authenticate clients to permit access only to those clients that meet your security policy.

The security policy on an endpoint is comprised of multiple individual policies, for firewall, for antivirus, for Host Integrity, and so on. Ultimately, that collection of policies becomes a numbered policy on the endpoint computer. This numbered policy is communicated to the Enforcer and checked with the Symantec Endpoint Protection Manager to determine if that the endpoint is up to date.

See "About the different types of Symantec Network Access Control enforcement" on page 26.

See "Deploying Symantec Network Access Control" on page 46.

Additionally, if your deployment includes a Gateway or DHCP Enforcer appliance, you can allow guests without compliant software to access your network temporarily. These Enforcers enable guest access by installing On-Demand clients on guest computers and dissolving them when guests log off.

See "Components of Symantec Network Access Control" on page 27.

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

About the different types of Symantec Network Access Control enforcement

Symantec Network Access Control provides different methods of enforcement to control access to your network. The product documentation describes all enforcement methods; however, you are entitled to use only the enforcement methods that your software license allows.

Table 1-1 Types of enforcement

Enforcement type	Description
Self enforcement	Self enforcement enables you to check the compliance of an endpoint with security policies and take appropriate action. Self enforcement is done entirely by the client computer. Available in all versions of Symantec NAC. Self enforcement is part of Host Integrity. See "How self enforcement works" on page 35.

Table 1-1 Types of enforcement *(continued)*

Enforcement type	Description
Gateway enforcement	Gateway enforcement provides a hardware appliance that stands between protected assets and the external network. Requires an Enforcer appliance. See About the LAN Enforcer appliance installation on page 93.
Guest access	Guest access provides on-demand access to clients that are not running Symantec Endpoint Protection or Symantec Network Access Control client software. Works with both Windows and Mac clients. Requires an Enforcer appliance. See "About the Symantec Network Access Control On-Demand Clients" on page 344.

See "Deploying Symantec Network Access Control" on page 46.

Components of Symantec Network Access Control

The following lists the Symantec Network Access Control components.

Table 1-2 Product components

Component	Description
Symantec Endpoint Protection Manager	Symantec Endpoint Protection Manager centrally manages the client computers that connect to your company's network. Symantec Endpoint Protection Manager includes the following software: ■ The console software coordinates and manages security policies and client computers. See "About working with Host Integrity policies" on page 52. ■ The server software provides secure communication to and from the client computers and the console.

Table 1-2 Product components *(continued)*

Component	Description
Database	The database that stores security policies and events. The database is installed on the computer that hosts Symantec Endpoint Protection Manager. Symantec Network Access Control comes with an embedded database, but you can also use an SQL database. See "Setting up user authentication with a local on-board database" on page 349.
Symantec Network Access Control client	The Symantec Network Access Control client enforces network compliance protection on the client computers by using Host Integrity checks and self-enforcement capabilities. The client reports its Host Integrity compliance status to a Symantec Enforcer. For more information, see the *Client Guide for Symantec Endpoint Protection and Symantec Network Access Control.*
LiveUpdate Server	The LiveUpdate Server has the ability to distribute definitions, signatures, and product updates to client computers by using LiveUpdate policies.
LiveUpdate Settings policies	LiveUpdate Settings policies specify the computers that clients connect to for content updates and the schedule for checking for updates. For Symantec Network Access Control, these updates consist of updates to Host Integrity policy templates.
Symantec Network Access Control Integrated Enforcers (optional)	These software Enforcers ensure that the clients that try to connect to the network comply with configured security policies. Symantec Network Access Control includes Integrated Enforcers for Microsoft DHCP servers and Microsoft Network Access Protection. See "How an Integrated Enforcer for Microsoft DHCP Servers works" on page 43. See "How an Integrated Enforcer for Microsoft Network Access Protection works" on page 44.

Table 1-2 Product components *(continued)*

Component	Description
Symantec Network Access Control Enforcer appliances (optional)	The Symantec Enforcer appliance is a hardware appliance that restricts non-compliant computers from the network. You can restrict non-compliant computers to specific network segments for remediation and you can completely prohibit access to non-compliant computers. Symantec Network Access Control includes Gateway, DHCP, and LAN Enforcer appliance images to copy to the appliance hardware. These images include the hardened Linux operating system and the Enforcer appliance software. See "How the Gateway Enforcer appliance works" on page 39. See "How the DHCP Enforcer appliance works" on page 40. See "How the LAN Enforcer appliance works" on page 41.
On-Demand clients for Windows and Macintosh (optional)	On-Demand clients are the temporary clients that you provide to users when they are unauthorized to access your network because they do not have the software that is compliant with your security policy. See "About the Symantec Network Access Control On-Demand Clients" on page 344.

Key features of Symantec Network Access Control

You can use Symantec Network Access Control to:

- Securely control access to corporate networks.
- Discover and evaluate client computer compliance status.
- Enforce your organization's client computer security policies.
- Provide the appropriate network access.
- Provide the appropriate remediation capabilities if needed.
- Continually monitor client computers for changes in compliance status.
- Easily integrate with all existing network infrastructure regardless of how client computers connect to the network.

See "Components of Symantec Network Access Control" on page 27.

See "About the different types of Symantec Network Access Control enforcement" on page 26.

See “Deploying Symantec Network Access Control” on page 46.

Chapter 2

Working with Symantec Network Access Control

This chapter includes the following topics:

- What you can do with Symantec Enforcer appliances
- What you can do with Symantec Integrated Enforcers
- What you can do with On-Demand Clients
- How Symantec Network Access Control works
- Deploying Symantec Network Access Control

What you can do with Symantec 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 up enforcement on the client computers that connect to the network with an 802.1x-aware switch or a wireless access point.

An Enforcer appliance performs host authentication rather than user-level authentication. It ensures that the client computers that try to connect to an enterprise network comply with the security policy of that enterprise. You can configure specific security policies on the Symantec Endpoint Protection Manager.

If the client does not comply with the security policies, the Enforcer appliance can take the following actions:

- Block access to the network.

- Allow access to limited resources only.
- Allow access when the client is non-compliant, and log that action.

The 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 41.

See “Planning for the installation of a LAN Enforcer appliance” on page 197.

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 40.

See “Installation planning for a DHCP Enforcer appliance” on page 161.

If you have employees who work remotely and connect through a VPN, you can use the Gateway Enforcer appliance for those clients.

You can also use the Gateway Enforcer appliance if a wireless access point is not 802.1x-enabled.

See “How the Gateway Enforcer appliance works” on page 39.

See “Installation planning for a Gateway Enforcer appliance” on page 113.

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

See “Failover planning for Gateway Enforcer appliances” on page 121.

See “Failover planning for DHCP Enforcer appliances” on page 168.

See “Failover planning for LAN Enforcer appliances” on page 201.

If you want to implement high availability for LAN Enforcer appliances, you must install multiple LAN Enforcer appliances and an 802.1x-aware switch. High availability is accomplished through the addition of an 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, the remaining Enforcer appliances authenticate the client before the client can connect to the network.

What you can do with Symantec Integrated Enforcers

The optional Symantec Network Access Control Integrated Enforcers are Enforcers provided as software components. You can configure them to ensure that the clients that try to connect to the network comply with your organization's configured security policies.

- Use the Symantec Network Access Control Integrated Enforcer for DHCP Servers to ensure that a Microsoft DHCP Server's clients comply with security policies.
- Use the Symantec Network Access Control Integrated Enforcer for Microsoft Network Access Protection to ensure that clients comply with Microsoft client health policies.

You can perform the following key tasks with the Integrated Enforcers:

- Ensure that client computers attempting to connect to the network comply with the security policies you set on the Symantec Endpoint Protection Manager.
- Configure a connection to a Symantec Endpoint Protection Manager.
- Start and stop the Enforcer service.
- View the connection status.
- View Security and System logs on the Symantec Endpoint Protection Manager.

See “How an Integrated Enforcer for Microsoft DHCP Servers works” on page 43.

See “How an Integrated Enforcer for Microsoft Network Access Protection works” on page 44.

What you can do with On-Demand Clients

When users cannot connect to your network because they lack the required compliance software, you can provide them with On-Demand clients. When an On-Demand client is installed, it authenticates the user and ensures that the computer passes a compliance check before it accesses the network. On-Demand clients stay in effect until the guest logs off. They are available for both Windows and Macintosh guest computers.

On-Demand clients protect your network's sensitive business information from data loss. With an On-Demand client:

- Guests and remote staff can connect to your network through Web-enabled applications without introducing the spyware, keyloggers, and other malware that can infect your network.
- You can encrypt data from non-corporate assets and later delete it securely.
- You can prevent exposure from the browser-related information that is left in cache or temporary files.

The provisioning process requires:

- A Gateway or DHCP Enforcer configured to provide On-Demand clients.
- An On-Demand client download and installation on guest computers

See "Enabling Symantec Network Access Control On-Demand clients to temporarily connect to a network" on page 347.

See "Setting up authentication on the Gateway or DHCP Enforcer console for Symantec Network Access Control On-Demand clients" on page 349.

How Symantec Network Access Control works

Symantec Network Access Control works by:

1. Discovering all attempts to access your network.
2. Checking that all client computers that access your network meet your security policy requirements.
3. For the client computers that do not meet requirements:
    - Remediating by downloading, installing, and running the software you require.
    - Allowing limited access.
    - Allowing complete access and log all network access attempts.
4. Monitoring and reporting on Enforcers, system traffic, and compliance status.

See "How self enforcement works" on page 35.

See "How the Gateway Enforcer appliance works" on page 39.

See "How the DHCP Enforcer appliance works" on page 40.

See "How the LAN Enforcer appliance works" on page 41.

See "How an Integrated Enforcer for Microsoft DHCP Servers works" on page 43.

See "How an Integrated Enforcer for Microsoft Network Access Protection works" on page 44.

See "How the On-Demand Client works" on page 45.

How self enforcement works

During the Host Integrity check, the client follows the requirements that are set in the Host Integrity policy. It examines active applications, date and size of a file, and other parameters. If these meet the Host Integrity policy's requirements, the client can access the network. If it does not, the client automatically generates a detailed message entry in the Security log for all failed requirements.

If the client computer cannot meet the requirements, the client can be set to silently connect to a remediation server. From there it can download and install the required software. The software can include a software patch, a hotfix, an update to virus definitions, and so on. The client can give the user a choice to download immediately or postpone a download. The computer cannot connect to the enterprise network until the software is installed. You can also configure the Enforcer to allow the client computer to connect even if it fails requirements.

The client can also detect whether or not an antivirus application is out of date. If an antivirus application is older than what a system administrator has specified, the client can be prevented from connecting to the enterprise network. Before it can connect, the client needs an up-to-date version of the antivirus application.

The Host Integrity policy includes the settings that determine how often the client runs a Host Integrity check on the client computer. The client computer can connect to the network through a Symantec Enforcer. You can set up the Host Integrity policy so that the client runs the Host Integrity check only when the Enforcer prompts the client. The Enforcer can verify the following: the client is running, the client's policy is up to date, and the Host Integrity check is passed before it allows access to the network.

See "What you can do with Host Integrity policies" on page 52.

Every time a client receives a new security policy, it immediately runs another Host Integrity check.

The client can be set up to automatically download and install the latest predefined or customized Host Integrity policies from the Symantec Endpoint Protection Manager. If the client cannot connect to the console, the On-Demand client gets the Host Integrity policy from the Enforcer appliance when first downloaded. After that it gets the Host Integrity policy from the Symantec Endpoint Protection Manager.

You can consider some of the following examples when you set up the requirements for Host Integrity enforcement:

- The client runs up-to-date antivirus software.
- The Host Integrity check is done only when the client tries to connect to the network through an Enforcer.
- The check triggers the actions that take place silently on the client.

You can also use an Enforcer to enforce these policies. The Enforcer is either a software application or an optional hardware appliance that mediates the connectivity of the client to the network. Most of the following examples show the use of an Enforcer.

The Enforcer can be configured to automatically do the following:

- Verify that a client has been installed on a user's computer.
- Prompt a client to retrieve updated security policies, if available.
- Prompts the client to run the Host Integrity check.

The client first verifies that the latest antivirus software is installed and runs it. If it has been installed but is not running, the client silently starts the antivirus application. If it is not installed, the client downloads the software from a URL that is specified in the Host Integrity requirement. Then the client installs and starts the software.

Next, the client verifies that the antivirus signature files are current. If the antivirus files are not current, the client silently retrieves and installs the updated antivirus files.

The client runs the Host Integrity check again and passes. The Enforcer receives the results and grants the client access to the enterprise network. In this example, the following requirements must be met:

- The file server that is used for Host Integrity updates has the latest files installed.

  The client obtains updated applications from the file server. You can set up one or more remediation servers that are connected to the enterprise network. From the remediation servers, users can copy or automatically download the required patches and hotfixes for any required application.

  If a remediation server fails, then Host Integrity remediation also fails. If the client tries to connect through an Enforcer, the Enforcer blocks the client if Host Integrity fails. If the client is connected to Symantec Endpoint Protection Manager, you can set the console to pass the Host Integrity check even though the check fails. In this case, the Enforcer can block the client. Information about the failed Host Integrity check is recorded in the client's Security log.
- The management server must be configured so that updates of the security policy are automatically sent to any computer that runs the client.

If the Enforcer blocks the client, the client tries to recover. The Host Integrity policy is set up to update files before it allows the client to connect to the network. The user is then notified that an update needs to be provided. A progress indicator for the update follows the update.

See "Adding Host Integrity requirements" on page 57.

How the Symantec Network Access Control Enforcer appliances work with Host Integrity policies

The security policies that all Enforcer appliances direct Symantec Network Access Control or Symantec Endpoint Protection clients to run 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

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

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.

See "How the Gateway Enforcer appliance works" on page 39.

See "How the DHCP Enforcer appliance works" on page 40.

See "How the LAN Enforcer appliance works" on page 41.

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 Globally Unique Identifier (GUID). The Enforcer appliance sends the GUID to the management server and receives an accept response or a reject response.

If an Enforcer appliance is configured to authenticate the GUID, it can retrieve information from the management server. The Enforcer appliance can then determine if the client profile has been updated with the latest security policies. If the client information changes on the management server, the management server can send the information to the Enforcer appliance. The Enforcer appliance can again perform host authentication on the client.

See “Changing Gateway Enforcer appliance configuration settings on a management server” on page 128.

See “Changing DHCP Enforcer appliance configuration settings on a management server” on page 174.

See “Changing LAN Enforcer configuration settings on a Symantec Endpoint Protection Manager Console” on page 206.

Communication between the Enforcer appliance and clients

The communication between the Enforcer appliance and a client begins when the client tries to connect to the network. The Enforcer appliance can detect whether a client is running. If a client is running, the Enforcer begins the authentication process with the client. The client responds by running a Host Integrity check and by sending the results, along with its profile information, to the Enforcer.

The client also sends its Globally Unique Identifier (GUID), which the Enforcer passes on to the 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 or Gateway Enforcer appliance allows the client to connect, it continues to communicate with the client at regular predefined intervals. This communication enables the Enforcer appliance to continue to authenticate the client. For the LAN Enforcer appliance, the 802.1x switch handles this periodic authentication. For example, the 802.1 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.

See "Creating and testing a Host Integrity policy" on page 53.

How the Gateway Enforcer appliance works

Gateway Enforcer appliances perform one-way checking. They check the clients that try to connect through the Gateway Enforcer appliance's external NIC to the organization's network.

A Gateway Enforcer appliance uses the following processes to check client computers and determine if they can access the network:

- The Gateway Enforcer appliance checks for client information and verifies that the client has passed the Host Integrity check.
  See "How the Symantec Network Access Control Enforcer appliances work with Host Integrity policies" on page 37.
- If the client satisfies the requirements for access, the Gateway Enforcer appliance connects it to the network.
- If a client does not satisfy the requirements for access, you can set up the Gateway Enforcer appliance to perform the following actions:
  - Monitor and log certain events.
  - Block users if the Host Integrity check failed.
  - Display a pop-up message on the client.
  - Provide the client with limited access to the network to allow the use of network resources for remediation.
    To provide limited access, you redirect client HTTP requests to a Web server with remediation information. For example, this Web server can include instructions on where to obtain remediation software. Or, it can allow the client to download the Symantec Network Access Control client software.
  - Allow the client to access the network even though it has failed the Host Integrity check.

The Gateway Enforcer appliance has the following optional configuration capabilities:

- Allows the client computers with trusted IP addresses to access the network immediately.
  You can configure which client IP addresses to check and which IP addresses are trusted. Clients with trusted IP addresses are granted access without additional authentication.
- Allows the computers that do not run Windows to access the network.
  In this case, the Gateway Enforcer appliance functions as a bridge instead of a router. As soon as a client is authenticated, the Gateway Enforcer appliance forwards packets to allow the client to have access to the network.

See About the LAN Enforcer appliance installation on page 93.

See "What you can do with Symantec Enforcer appliances" on page 31.

See "About installing an Enforcer appliance" on page 95.

How the DHCP Enforcer appliance works

The DHCP Enforcer appliance protects the network by managing the IP addresses that are used for accessing the network. Clients waiting for authentication and those that fail the authentication receive an IP address configuration. This IP address configuration limits them to short-term access to a restricted quarantine server. Clients that pass authentication receive an IP address configuration that grants full access to the normal DHCP server.

A DHCP Enforcer appliance uses the following process to check client computers and determine if they can access the production network:

- The client computer sends a request for a DHCP IP address that allows it to access the DHCP server network.
- A switch or a router routes the DHCP IP address request to the DHCP Enforcer appliance.
- The DHCP Enforcer forwards a request to a DHCP quarantine server to provide access.
- The DHCP quarantine server assigns the client a temporary quarantine server IP address
  See "Setting up an automatic quarantine for a client that fails authentication" on page 193.
- The Enforcer directs the client to perform a Host Integrity check and report back on its results. Clients that do not pass the check may be directed to a remediation server so that they can obtain the software they need to pass.

See “How the Symantec Network Access Control Enforcer appliances work with Host Integrity policies” on page 37.

- If the client satisfies the security policy requirements:
    - The Enforcer releases the quarantine server IP address.
    - The Enforcer routes the client's request to provide access to the production network.
    - The client accesses the production network.
- If the client does not satisfy the security policy requirements, the DHCP Enforcer appliance renews the lease on the quarantine server IP address. The quarantine server allows access to a remediation server. The client can then make use of remediation resources (such as links compliance software downloads) so it can successfully access to the production network.

The DHCP Enforcer appliance has the following optional configuration capabilities:

- You can use separate computers or the same computer for the normal and quarantine DHCP servers. In both cases you need to set up a remediation server that the client can access from the quarantine server.
  See “Where to place DHCP Enforcer appliances in a network” on page 162.
- You can allow non-Windows client computers to access the production DHCP server.
  See “Protection of non-Windows clients with DHCP enforcement” on page 165.

See “What you can do with Symantec Enforcer appliances” on page 31.

How the LAN Enforcer appliance works

The LAN Enforcer appliance gives you the option of 802.1x EAP (Extensible Authentication Protocol) authentication along with the client performing a Host Integrity check.

Note: For details on EAP, refer to the IETF’s RFC 2284 at http://www.ietf.org/rfc/rfc2284.txt. For additional details on IEEE Standard 802.1x, refer to the text of the standard at http://www.ieee802.org/1/files/public/MIBs/802-1x-2001-mib.txt.

You can deploy the LAN Enforcer using one of the following modes:

- Transparent mode: Checks if the client is compliant with Host Integrity security policy but it does not check the user name and password. Transparent mode does not use a RADIUS server.

- Full 802.1x mode: Authenticates the user's credentials (user name and password) in addition to having the client check for host authentication. Non-compliant clients are routed to a guest VLAN that your organization has set up for client security remediation. Full 802.1x authentication requires a RADIUS server, an 802.1x-capable switch or wireless access point, and supplicant (client) software.

In transparent mode, a LAN Enforcer appliance uses the following methods to process client computer requests to access the network:

- The client computer connects and sends logon, host authentication compliance, and policy data through EAP.
- The switch or wireless access point forwards the client computer data to the LAN Enforcer appliance.
- The LAN Enforcer appliance verifies that the client has passed a Host Integrity check.
  See “How the Symantec Network Access Control Enforcer appliances work with Host Integrity policies” on page 37.
- If the client passes the Host Integrity check, the Enforcer opens a part of the switch and allows full network access.
- If the client fails the Host Integrity check, the Enforcer assigns the client to quarantine VLAN where it can access remediation resources.

In full 802.1x mode, a LAN Enforcer appliance does the following to process client computer requests to access the network:

- The client computer connects and sends logon, host authentication compliance, and policy data through EAP.
- The supplicant on the client computer asks the user for their user name and password.
- The switch forwards the user name and password to the LAN Enforcer.
- The LAN Enforcer forwards the user name and password to the RADIUS server.
- The RADIUS server generates an EAP challenge (user name and password).
- The LAN Enforcer receives the EAP challenge and adds the Host Integrity check.
- The LAN Enforcer verifies that the client has passed the Host Integrity check.
- The LAN Enforcer checks the Host Integrity results and forwards them to the RADIUS server.
- The RADIUS server performs EAP authentication and sends the result to the LAN Enforcer.

- The LAN Enforcer receives the authentication result and forwards it and the action to take to the switch.
- If the client passes the EAP and Host Integrity challenges, the switch allows network access.
- If the client does not pass the challenges, the switch routes it to an alternate VLAN where it can access remediation resources.

The LAN Enforcer appliance has the following additional optional configuration capabilities. You can:

- Use a switch or wireless access point to direct the client to a remediation VLAN. (Recommended)
- Configure the possible failure responses depending on whether you use EAP authentication or Host Integrity checking.
- Connect multiple LAN Enforcer appliances to one switch for LAN Enforcer failover,
- Configure multiple RADIUS servers for RADIUS server failover.

See “What you can do with Symantec Enforcer appliances” on page 31.

How an Integrated Enforcer for Microsoft DHCP Servers works

The Integrated Enforcer for Microsoft DHCP Servers checks for Symantec Endpoint Protection or Symantec Network Access Control client installations on the DHCP clients that the DHCP server manages. It then enforces policies for those clients as configured on the Symantec Endpoint Protection Manager.

The Integrated Enforcer for Microsoft DHCP Servers also authenticates the client for:

- The existence of an agent.
- A Globally Unique Identifier (GUID).
- Host Integrity compliance
- The profile version of each configured policy.

The Integrated Enforcer for Microsoft DHCP Servers is a software component that interacts with the Microsoft DHCP Server. Although both must be installed on the same computer, the Integrated Enforcer for Microsoft DHCP Servers is not dependent on the DHCP server. When the Integrated Enforcer for Microsoft DHCP Servers resides on the same computer as the DHCP Server, it eliminates the need for additional hardware.

Note: Stopping the DHCP server does not stop the Integrated Enforcer for Microsoft DHCP Servers. Stopping the Integrated Enforcer for Microsoft DHCP Servers does not stop the DHCP server.

You use the Symantec Endpoint Protection Manager to configure the 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 for 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)?

  Is the GUID a 128-bit hexadecimal number? This number is assigned to a client computer that runs the Symantec Endpoint Protection client or the Symantec Network Access Control client. The management server generates a GUID when the client initially connects.
- Does the client comply with the latest Host Integrity policy that the administrator has set up on the console of the Symantec Endpoint Protection Manager?
- Has the client received the latest security policy?

If the Integrated Enforcer for Microsoft DHCP Servers cannot authenticate the client, it provides access to a quarantined area. The quarantine area provides limited network resources to the client. The quarantine area is configured on the same computer as the Integrated Enforcer for Microsoft DHCP Servers and the Microsoft DHCP server.

You can also set up access to a remediation server. The remediation server provides clients with links to software that allows them to become security compliant.

See "About the Symantec Network Access Control Integrated Enforcer for Microsoft DHCP Servers" on page 281.

How an Integrated Enforcer for Microsoft Network Access Protection works

The Integrated Enforcer for Microsoft Network Access Protection works by allowing you to extend the capabilities of Microsoft Network Access Protection (NAP), including:

- Checking for adherence to endpoint security policies. Connecting clients can use the same polices or different policies.
- Controlling guest access.
- Authenticating end users

When a Network Policy Server (NPS) is configured as a NAP policy server, it evaluates statements of health (SoH) sent by NAP-capable clients. If the clients are healthy they can connect to the network.

You can configure NAP policies on NPS that allow client computers to update their configuration to become compliant with your organization’s security policy.

See “About the Symantec Network Access Control Integrated Enforcer for Microsoft Network Access Protection” on page 282.

How the On-Demand Client works

The On-Demand Client checks your computer for compliance if you try to connect your computer to a protected network as a guest. If the client computer meets all requirements, a connection between the client computer and the Symantec Endpoint Protection Manager is automatically established. The client can then access the protected network.

Therefore the compliant client computer can perform any task that the administrator has 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 user needs to remediate all noncompliant requirements on the client computer by downloading the remediation files as set up by the administrator. Until the remediation is complete, the client cannot access the protected network as a guest.

Your computer must pass or fail a Compliance Status Check when it tries to connect to a company's protected network. Therefore the access status to a company's protected network is as follows:

- Allowed—You can connect to the network as a guest if your computer passes the Compliance Status Check and authenticates your credentials.
- Not Allowed—If your computer fails the Compliance Status Check or fails to authenticate your credentials, you cannot connect to the network as a guest. You must then take further actions to resolve this issue.

See “Enabling Symantec Network Access Control On-Demand clients to temporarily connect to a network” on page 347.

Deploying Symantec Network Access Control

The best approach for deploying Symantec Network Access Control is to do it in phases. This approach allows your organization to evolve an implementation that fits your needs. You build on each previous phase instead of completely redoing your entire security infrastructure to make changes or enhancements.

Table 2-1 Phases for deploying Symantec Network Access Control

Phase	Action	Description
Phase 1	Install Symantec Network Access Control clients and use Symantec Endpoint Protection Manager to configure Host Integrity policies.	You can control access for the laptops, desktops, and servers your organization manages with self-enforcement. With self-enforcement, computers can obtain the software they need to comply with your security policy. See "How self enforcement works" on page 35. See "Creating and testing a Host Integrity policy" on page 53.

Table 2-1 Phases for deploying Symantec Network Access Control *(continued)*

Phase	Action	Description
Phase 2	Install and configure a Gateway Enforcer appliance.	For partial network protection, control wired and wireless access to the network for managed and unmanaged clients and for guest computers. Managed clients are those that running the Symantec Network Access Control client. Unmanaged clients are those that: ■ Are not running Symantec Network Access Control client software. ■ Are running Symantec Network Access Control client software, but do not have the latest policy updates. Guest clients are the laptops, desktops, and servers that do not meet your security requirements for items such as installed software and secure passwords. These are devices owned by guests such as contractors, consultants, and partners. You can allow these guest clients to safely and temporarily connect to your network with On-Demand clients. See “About installing an Enforcer appliance” on page 95. See “Installing an Enforcer appliance” on page 96. See “How the Gateway Enforcer appliance works” on page 39. See “How the On-Demand Client works” on page 45.

Table 2-1 Phases for deploying Symantec Network Access Control *(continued)*

Phase	Action	Description
Phase 3	Install and configure a LAN Enforcer appliance or a DHCP Enforcer appliance	For complete network protection, you can control WAN access for client computers and guest computers. ■ For managed clients, use a LAN Enforcer appliance or a DHCP Enforcer appliance. ■ For unmanaged clients, use the LAN, DHCP, or Gateway Enforcer appliances. See "About installing an Enforcer appliance" on page 95. See "Installing an Enforcer appliance" on page 96. See "How the LAN Enforcer appliance works" on page 41. See "How the DHCP Enforcer appliance works" on page 40.

See "About the different types of Symantec Network Access Control enforcement" on page 26.

Section 2

Configuring Host Integrity to ensure endpoint compliance

Chapter 3

Configuring Host Integrity

This chapter includes the following topics:

- What you can do with Host Integrity policies
- About working with Host Integrity policies
- Creating and testing a Host Integrity policy
- About Host Integrity requirements
- Adding Host Integrity requirements
- Enabling and disabling Host Integrity requirements
- Changing the sequence of Host Integrity requirements
- Adding a Host Integrity requirement from a template
- About settings for Host Integrity checks
- Allowing the Host Integrity check to pass if a requirement fails
- Configuring notifications for Host Integrity checks
- About Host Integrity remediation
- Specifying the amount of time the client waits to remediate
- Allowing users to postpone or cancel Host Integrity remediation
- Hiding remediation if users have not logged on

What you can do with Host Integrity policies

Use Host Integrity policies to make sure that the client computers that access your network meet your organization's security policy. For example, you can use Host Integrity policies to ensure that client computers:

- Are running antivirus and antispyware applications. If they do not, allow them to remediate by downloading and installing the required antivirus and antispyware applications.
- Have the latest virus definitions. If they do not, automatically download virus definition updates.
- Have the latest patches and service packs. If they do not, allow them to remediate by downloading and installing the required patch or service pack.
- Use strong passwords and change them as frequently as required.
- Have backup software installed. If they do not, allow them to remediate by downloading and installing the required backup software.
- Have the software that lets you perform remote installations. If they do not, allow them to remediate by downloading and installing the required remote installation software.

See “Creating and testing a Host Integrity policy” on page 53.

About working with Host Integrity policies

You create and edit Host Integrity Policies similarly to how you create and modify other types of policies. You can assign, withdraw, replace, copy, export, import, or delete a Host Integrity Policy.

You typically assign a policy to multiple groups in your security network. You can create a non-shared, location-specific policy if you have specific requirements for a particular location.

To work with Host Integrity Policies, you must be familiar with the basics of policy configuration as explained in the *Administration Guide for Symantec Endpoint Protection and Symantec Network Access Control.*

See “How self enforcement works” on page 35.

About the Quarantine Policy

The Quarantine Policy is a policy for the Symantec Network Access Control client that runs the Host Integrity check. If the Host Integrity Policy requirements are not met, the client tries remediation. If remediation fails, the client automatically switches to a Quarantine Policy. A Quarantine Policy can be an Antivirus and Antispyware Policy, Firewall Policy, Intrusion Prevention Policy, LiveUpdate Policy, or Application and Device Control Policy. You can set up and assign a Quarantine Policy to a location.

See "Setting up an automatic quarantine for a client that fails authentication" on page 193.

See "Configuring automatic quarantine" on page 299.

Creating and testing a Host Integrity policy

The Host Integrity policy is the foundation of Symantec Network Access Control. The policy that you create for this test is for demonstration purposes only. The policy detects the existence of an operating system and, when detected, generates a FAIL event. Normally, you would generate FAIL events for other reasons.

See "What you can do with Host Integrity policies" on page 52.

You can then test the Host Integrity policy from the Symantec Endpoint Protection Manager Console.

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

To create a Host Integrity policy

1. In the console, click **Policies**.
2. Under **View Policies**, click and select **Host Integrity**.
3. In the right pane, if a Host Integrity policy is highlighted in yellow, deselect the policy.
4. Under **Tasks**, click **Add a Host Integrity Policy**.
5. In the **Overview** pane, in the Policy Name box, type a name for the policy.
6. Click **Requirements**.
7. In the **Requirements** pane, check **Always do Host Integrity checking**, and then click **Add**.
8. In the **Add Requirement** dialog box, in the Type drop-down menu, click **Custom Requirement**, and then click **OK**.

9 In the **Custom Requirement** window, in the **Name** box, type a name for the Custom Requirement.

10 Under **Customized Requirement Script**, right-click **Insert Statements Below**, and then click **Add > IF .. THEN**.

11 In the right pane, in the **Select a condition** drop-down menu, click **Utility: Operating System is**.

12 Under Operating system, check one or more operating systems that your client computers run.

13 Under **Customized Requirement Script**, right-click **THEN //Insert statements here**, and then click **Add > Function > Utility: Show message dialog**.

14 In the **Caption** of the message box, type a name to appear in the message title.

15 In the **Test of the message** box, type the text that you want the message to display.

16 To display information about the settings customize the message, click **Help**.

17 In the left pane, under **Customized Requirement Script**, click **PASS**.

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

19 In the **Host Integrity** window, click **OK**.

20 In the **Assign Policy prompt,** click **Yes**.

21 In the **Host Integrity Policy** dialog box, check the groups to which you want to assign the policy.

22 Click **Assign**.

23 In the **Assign Host Integrity policy prompt**, click **Yes**.

To test a Host Integrity policy

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

2 In the right pane, click the **Clients** tab.

3 In the left pane, under **View**, click and highlight the group that contains the client computers to which you applied the Host Integrity policy.

4 Under **Tasks**, click **Run Command on Group > Update Content**.

5 Log on to a client computer that runs Symantec Network Access Control and note the message box that appears.

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

See “How self enforcement works” on page 35.

About Host Integrity requirements

When you plan Host Integrity requirements, you must consider the following issues:

- What software (applications, files, patches, and so on) do you want to require for enterprise security?
- What occurs if a requirement is not met? For example:
  - The client can connect to a server and restore the software to meet the requirement.
  - The Host Integrity check can pass even though the requirement fails.
  - The Host Integrity check can fail and network access can be blocked.
  - A message can notify the user what to do next.

Consider the following areas in more detail:

- Which antivirus applications, antispyware applications, firewall applications, patches, or updates are required on every user’s computer when it connects to the network? You usually create a separate requirement for each type of software. Predefined Host Integrity requirements let you easily set up these commonly used requirements.
- You can give users the right to select which firewall, antispyware, or antivirus applications they want to run on their computers. The predefined requirements let you specify either a specific application or an entire list of supported applications as acceptable. You can create a custom requirement that includes the applications that are acceptable in your company.
- How to handle restoring the user’s computer to meet the requirements? Normally, you need to set up a remediation server with the required software. When you configure the requirement, you must specify the URL from which the client can download and install the required software.
- Some patches require a user to restart the computer. Updates are completed in a specific order so that all updates are applied before a user has to restart. As part of the Host Integrity policy, you can set the order in which requirements are checked and the remediation is tried.
- You should also consider what occurs if a requirement fails and cannot be restored. For each requirement, you have the choice to allow the Host Integrity check to pass even though that requirement fails. As part of the general Host Integrity policy, you also can configure messages. The client displays these

messages to the user if the Host Integrity check fails or if it passes after previous failure. You may want to plan additional instructions for the user in these messages. In addition, you can set up a quarantine policy to activate if Host Integrity fails.

- You can simplify the management of required applications by including similar applications in one custom requirement. For example, you can include Internet browsers such as the Internet Explorer and Firefox in one requirement.
- As part of a custom requirement, you can specify whether to allow the Host Integrity check to pass if the requirement fails. When you plan how many conditions to check for in one script, remember that this setting applies to the custom requirement script as a whole. This aspect of the setting may affect whether you want to create several small custom requirements or a longer one that includes multiple steps.

You may find it helpful to set up a spreadsheet that represents your company's Host Integrity enforcement requirements.

The Host Integrity policy includes the following requirement types:

- Predefined requirements cover the most common types of Host Integrity checks and let you choose from the following types:
    - Antivirus requirement
    - Antispyware requirement
    - Firewall requirement
    - Patch requirement
    - Service pack requirement

  See "Adding Host Integrity requirements" on page 57.
- Custom requirements, which you define by using the Custom Requirement Editor.
  See "Writing a custom requirement script" on page 79.
- Host Integrity requirement templates, which are updated as part of the Symantec Enterprise Protection LiveUpdate.
  See the *Administration Guide for Symantec Endpoint Protection and Symantec Network Access Control* for more information on LiveUpdate.
  See "Adding a Host Integrity requirement from a template" on page 59.

When you add a new requirement, you can select one of the predefined requirement types. A dialog box is then displayed with the set of predefined settings that you can configure. If the predefined settings do not meet your needs, you can create a custom requirement.

You can also change the position of requirements. The position of a requirement determines the order in which it is executed.

See "Changing the sequence of Host Integrity requirements" on page 59.

Adding Host Integrity requirements

A Host Integrity policy sets the requirements for firewalls, antivirus, antispyware, patches, service packs, or other required applications on client computers.

Each Host Integrity policy includes requirements and general settings. The requirements specify the following items:

- What conditions to check
- What actions (such as downloads and installs) the client takes in response to the condition

When you specify Host Integrity requirements, you can choose from the following types: predefined, custom, or template requirements. Template requirements are available through the Host Integrity policy LiveUpdate service. You can copy and paste and export and import requirements between policies.

General settings enable you to configure when and how often the client runs a Host Integrity check, remediation options, and notifications.

You can create a new shared or non-shared Host Integrity policy. After you create a new policy, you can add a predefined requirement, a custom requirement, or both.

See "About Host Integrity requirements" on page 55.

To add a Host Integrity requirement

1. In the console, open a Host Integrity policy.
2. On the **Host Integrity Policy** page, click **Requirements**.

3 On the **Requirements** page, select when the Host Integrity checks should run on the client from one of the following options:

Always do Host Integrity checking	This choice is the default. A Host Integrity check is always performed in this location at the frequency interval you specify.
Only do Host Integrity checking through the Gateway or DHCP Enforcer	A Host Integrity check is performed in this location only when the client is authenticated through a Gateway Enforcer or a DHCP Enforcer.
Only do Host Integrity checking when connected to the management server	A Host Integrity check is performed in this location only when the client is connected to a management server.
Never do Host Integrity checking	A Host Integrity check is never performed in this location.

4 Click **Add**.

5 In the **Add Requirement** dialog box, select one of the following requirement types:

- Antivirus requirement
- Antispyware requirement
- Firewall requirement
- Patch requirement
- Service pack requirement
- Custom requirement

6 Click **OK**.

7 Configure the settings for the requirement.

See “About Host Integrity requirements” on page 55.

8 On the Advanced Settings page, configure settings for Host Integrity checks, remediation, and notifications.

For more information, click **Help**.

See “About settings for Host Integrity checks” on page 60.

9 When you are done with the configuration of the policy, click **OK**.

10 Assign the policy to groups or locations.

Enabling and disabling Host Integrity requirements

When you create requirements for a Host Integrity policy, you can create requirements for future use. You must disable them from being used until they are needed. You can disable a requirement temporarily while you test your Host Integrity policy.

To enable and disable Host Integrity requirements

1. In the console, open a Host Integrity policy.
2. On the **Host Integrity Policy** page, click **Requirements**.
3. On the **Requirements** page, select a requirement, and then do one of the following tasks:
   - To enable a requirement, check the **Enable** check box for the selected requirement.
   - To disable a requirement, uncheck the **Enable** check box for the selected requirement.
4. When you are done with the configuration of the policy, click **OK**.

See "What you can do with Host Integrity policies" on page 52.

Changing the sequence of Host Integrity requirements

You can change the position of requirements. When you change the position, you determine the order in which they are executed. The position can be important when you download the software that requires a restart after installation. You set the order to ensure that the requirements that require a restart for remediation are performed last.

To change the sequence of Host Integrity requirements

1. In the console, open a Host Integrity policy.
2. On the Host Integrity page, click **Requirements**.
3. On the **Requirements** page, select the requirement that you want to move, and then click **Move Up** or **Move Down**.
4. When you are done with the configuration of the policy, click **OK**.

See "Adding Host Integrity requirements" on page 57.

Adding a Host Integrity requirement from a template

The online subscription service provides Host Integrity templates.

You can import the latest templates and use them while you develop custom requirements for a Host Integrity policy. You can select as many or as few requirements as you want. You can select the requirement by using them as is or by modifying them as needed for your environment.

If your subscription is expired, the requirements that you already imported still can be used. However, the latest updates are no longer available to import.

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

See "About Host Integrity requirements" on page 55.

To add a Host Integrity requirement from a template

1. In the console, open a Host Integrity policy.
2. On the **Host Integrity** page, click **Requirements**.
3. On the **Requirements** page, click **Template**.
4. In the **Host Integrity Online Updating** dialog box, expand Templates, and then select a template category.
5. Next to each template you want to add, click **Add**.
6. Click **Import**.
7. When you are done with the configuration of the policy, click **OK**.

About settings for Host Integrity checks

When you set up Host Integrity policies, you can select from a number of settings. The settings relate to how the Host Integrity check is carried out and how the results are handled.

See "How self enforcement works" on page 35.

If you change a Host integrity policy, it is downloaded to the client at the next heartbeat. The client then runs a Host Integrity check.

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

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

Table 3-1 displays the settings for Host Integrity checks.

Table 3-1 Host Integrity checking settings

Setting	Description
Check Host Integrity every	Specifies the frequency of Host Integrity checks.
Keep check results for	Sets the duration for maintaining Host Integrity results. You can set the amount of time that a client retains the result of a previous Host Integrity check. The client maintains the result even if the user takes an action that would normally result in a new Host Integrity check. For example, the user may download new software or change a location.
Continue to check requirements after one fails	Specifies that the client continues to check the requirements even if one requirement fails. The client does stop the Host Integrity check until the failed requirement is restored. The client checks the Host Integrity requirements in the order that is specified in the Host Integrity policy. If you enable this setting, the Host Integrity check fails, but you can try other remediation actions, if required. You can allow the Host Integrity check to pass even if a requirement fails. This setting is found on the **Requirements** dialog box for each requirement type. You apply the setting separately for each requirement.

Allowing the Host Integrity check to pass if a requirement fails

In addition to enabling or disabling a requirement on your Host Integrity policy to determine whether or not the client runs the requirement script, you can have the client run the requirement script and log the results but ignore the results. You can let the Host Integrity check pass whether or not the requirement fails. A requirement can pass even if the requirement condition is not met.

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

If you enable the setting to allow the Host Integrity check to pass even if the requirement fails, the following message appears in the client window when the event occurs:

```
Host Integrity failed but reported as pass
```

To allow the Host Integrity check to pass if a requirement fails

1. In the console, open a Host Integrity Policy.
2. On the **Host Integrity** page, click **Requirements**.
3. On the **Requirements** page, click **Add**, add a predefined requirement or a custom requirement, and then click **OK**.
4. On the dialog box for the requirement, check **Allow the Host Integrity check to pass even if this requirement fails**.
5. Click **OK**.
6. When you finished with the configuration of this policy, click **OK**.

See “Adding Host Integrity requirements” on page 57.

Configuring notifications for Host Integrity checks

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

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

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

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

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

See “Allowing users to postpone or cancel Host Integrity remediation” on page 65.

To configure notifications for Host Integrity checks

1. In the console, open a Host Integrity policy.
2. On the **Host Integrity** page, click **Advanced Settings**.
3. On the **Advanced Settings** page, under **Notifications**, to show detailed requirement information, check **Show verbose Host Integrity Logging**.

   The lower right-hand pane of the client's Security log displays complete information about a Host Integrity requirement.
4. Check any of the following options:
   - **Display a notification message when a Host Integrity check fails**.
   - **Display a notification message when a Host Integrity check passes after previously fails**.
5. To add a custom message, click **Set Additional Text**, type up to 512 characters of additional text, and then click **OK**.
6. To display either of the notifications even if the user has not yet logged on, uncheck **User must log on before applications and Host Integrity notifications appear**.
7. When you are finished with the configuration of this policy, click **OK**.

About Host Integrity remediation

If the client Host Integrity check shows that the Host Integrity requirements are not met, the client can try to restore the necessary files to meet the requirements The client computer then needs to pass the Host Integrity check. The client downloads, installs files, or runs required applications. When you set up Host Integrity Policies, you can specify what happens during the remediation process. You can specify not only where the client goes to download remediation files but also how the remediation process is implemented.

You can allow the user to cancel software being downloaded. You can also set the number of times the user can postpone a download and for how long. The settings apply to all types of requirements in the policy except those on which you have disabled remediation cancellation. Users can cancel predefined requirements only.

See “About remediating applications and files for Host Integrity” on page 64.

About remediating applications and files for Host Integrity

When you set up remediation for a requirement, you specify the location of an installation package or files to be downloaded and installed.

See "About Host Integrity remediation" on page 63.

When you specify the location of the installation package or file to be downloaded, you can use any of the following formats:

UNC	\\servername\sharename\dirname\filename UNC restore does not work if Network Neighborhood browsing is disabled on the target client. Be certain that Network Neighborhood browsing has not been disabled if you use UNC paths for remediation.
FTP	FTP://ftp.ourftp.ourcompany.com/folder/filename
HTTP	HTTP://www.ourwww.ourcompany.com/folder/filename

Installation packages or files are always downloaded to the temporary directory. Any relative path refers to this directory. The temporary directory is defined in the TMP environment variable if it exists, or in the TEMP environment variable if that exists. The default directory is in the Windows directory.

For file execution, the current working directory is always set to the Windows temporary directory. Environment variables are substituted before execution. The Windows directory path replaces the command %windir%.

You can use %1 (the default) to execute the file you specified in the Download URL field. The `%1` variable represents the last downloaded file.

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

Host Integrity remediation and Enforcer settings

When you set up Host Integrity requirements, you can specify that if the Host Integrity requirements are not met, the client should update the client computer with whatever is required by connecting to a remediation server. If you apply such requirements to clients that connect to the network through an Enforcer, you must ensure that the client, while blocked from regular network access, can access the remediation server. Otherwise, the client does not restore Host Integrity and the client continues to fail the Host Integrity requirement.

How you accomplish this task depends on the type of Enforcer. The following list offers a few examples:

- For the Gateway Enforcer, you can configure the Gateway Enforcer to recognize the remediation server as a trusted internal IP address.
- For the DHCP Enforcer, you set up the quarantine network configuration on the DHCP server to allow access to the remediation server.
- For a LAN Enforcer, if you use a switch with dynamic VLAN capability, you can set up a VLAN with access to the remediation server.

See "About Host Integrity remediation" on page 63.

Specifying the amount of time the client waits to remediate

You can specify the amount of time the client waits before it tries to install and start the remediation download again. Regardless of the time that you specify, whenever a new Host Integrity check is initiated, the client tries to remediate the client computer again.

To specify the amount of time the client waits to remediate

1. In the console, open a Host Integrity Policy.
2. On the **Host Integrity Policy** page, click **Requirements**.
3. On the **Requirements** page, click **Add**, add a predefined requirement, and then click **OK**.
4. On the dialog box for each predefined requirement, check **Install** *requirement name* **if it has not been installed on the client**.
5. Check **Download Installation Package**.

   For the Antivirus requirement, check **Download the installation package**.
6. Check **Specify wait time before attempting the download again if the download fails**.
7. Specify the amount of time to wait by the minutes, hours, or days.
8. When you are done with the configuration of the policy, click **OK**.

See "About Host Integrity remediation" on page 63.

Allowing users to postpone or cancel Host Integrity remediation

If a requirement specifies a remediation action, you can allow the user to cancel the remediation. Or, you can allow the user to postpone the remediation to a more convenient time. Examples of remediation actions include the installation of an application or an update of a signature file. You can set a limit on how many times a remediation can be canceled and how long the user can postpone it. The limits you set determine the selections available to the user on the message window that the client displays when remediation is needed. You can also add text to the message window.

The minimum and the maximum time settings determine the range of choices available on the message window. The message window displays to a user when a requirement fails. The range appears as a list next to the Remind me later icon on the message.

If the user selects a shorter time for postponement than the Host Integrity check frequency, the user selection is overridden. The message window does not appear again until the client runs another Host Integrity check. If the user has chosen to be reminded in 5 minutes, but the Host Integrity check runs every 30 minutes, the remediation message window does not appear until 30 minutes have passed. To avoid confusion for the user, you may want to synchronize the minimum time setting with the Host Integrity check frequency setting.

If the user postpones remediation, the client logs the event. The Host Integrity is shown as failed since the requirement is not met. The user can manually run a new Host Integrity check at any time from the client user interface.

If the user has postponed a remediation action and in the interim the client receives an updated policy, the amount of time available for remediation is reset to the specified maximum.

To allow users to postpone Host Integrity remediation

1. In the console, open a Host Integrity policy.
2. On the **Host Integrity Policy** page, click **Advanced Settings**.
3. On the **Advanced Settings** page, under **Remediation Dialog Options**, set a minimum time limit and the maximum time limit that a user can postpone the remediation.
4. Type the maximum number of times that the user can cancel the remediation.
5. To add a custom message on the client computer, click **Set Additional Text**.

   The message you type is displayed on the client remediation window if the user clicks the **Details** option. If you specify no additional text, the default window text is repeated in the Details area when the user clicks Details.
6. In the **Enter Additional Text** dialog box, type a custom message up to 512 characters, and then click **OK**.
7. When you are done with the configuration of the policy, click **OK**.

To allow users to cancel Host Integrity remediation

1. In the console, open a Host Integrity policy.
2. On the **Host Integrity Policy** page, click **Requirements**.
3. On the **Requirements** page, click **Add**, add a predefined requirement, and then click **OK**.
4. On the dialog box for each predefined requirement, check **Install** *requirement name* **if it has not been installed on the client**.
5. Check **Download Installation Package**.

   For the Antivirus requirement, check **Download the installation package**.
6. Check **Allow the user to cancel the download for Host Integrity remediation**.
7. When you are done with the configuration of the policy, click **OK**.

See "About Host Integrity remediation" on page 63.

Hiding remediation if users have not logged on

By default, Host Integrity remediation runs whether or not the user is logged on. The client can remediate the client computer with operating system updates or necessary security software at any time. However, when the remediation runs either a local application or a downloaded application, users can run the application even if they have not logged on. For example, an installation package might launch Internet Explorer, from which users can run either the command prompt or another application. For security purposes, you may not want any applications or notifications to appear until after the user logs on to the client.

You can work around this issue when you write a custom requirement that uses the Run a program function. The Run a program function launches a program that uses the logged on user context.

See "Running a program" on page 86.

To hide remediation if users have not logged on

1. In the console, open a Host Integrity policy.
2. On the **Host Integrity** page, click **Advanced Settings**.
3. On the **Advanced Settings** page, under **Notifications**, verify that **User must log before applications and Host Integrity notifications appear** is checked.
4. When you are finished with the configuration of this policy, click **OK**.

Chapter 4

Adding custom requirements

This chapter includes the following topics:

About custom requirements

Custom requirements check a client computer for any number of administrator-selected or defined criteria. You can write custom requirements to remediate any identified compliancy issues.

You can create a complex or a simple requirement script by using predefined selections and fields.

The fields and lists that are available in the predefined requirement dialog boxes are available when you create custom requirements. However, custom requirements give you more flexibility. In custom requirements, you can add the applications that are not included in the predefined lists of applications. You can create subsets of predefined lists by adding each application individually.

See “About conditions” on page 70.

See “About functions” on page 76.

See “About custom requirement logic” on page 77.

About conditions

Conditions are the checks that may be performed within a custom requirement script to detect compliancy issues.

You can chose from the following categories of conditions:

- Antivirus checks
  See “About antivirus conditions” on page 71.
- Antispyware checks
  See “About antispyware conditions” on page 71.
- Firewall checks
  See “About firewall conditions” on page 72.
- File checks and operation
  See “About file conditions” on page 72.
- Registry checks and operations
  See “About registry conditions” on page 75.
- Utilities

You can specify conditions as present or absent (NOT). You can include multiple condition statements by using AND or OR keywords.

About antivirus conditions

In a custom requirement, you can specify antivirus applications and signature file information to check as part of your IF-THEN condition statement.

You can check for the following conditions:

- Antivirus is installed
- Antivirus is running
- Antivirus signature file is up to date

When you check applications and signature files as part of a custom requirement, you specify the same information as when you create a predefined requirement. The option names may differ slightly.

If you select **Any Antivirus Product**, any of the applications in the drop-down list meet the requirement. You can include a subset of applications by selecting each by using the OR keyword.

When you specify the signature file information, you can select one or both options for checking that the signature file is up to date. If you select both, the following conditions must be satisfied to meet the requirement:

- Select **Check signature file is less than** and enter a number of days. A file that is dated before the number of days you specify is out of date.
- Select **Check signature file date is** and select before, after, equal to, or not equal to, and specify a date (mm/dd/yyyy). Optionally, specify an hour and minute; the default is 00:00. The file's last modified date determines the signature file age.

See "Adding Host Integrity requirements" on page 57.

About antispyware conditions

For a custom Host Integrity requirement, you can specify Antispyware applications and signature file information to check as part of your IF THEN condition statement.

You can check for the following conditions:

- Antispyware is installed
- Antispyware is active
- Antispyware signature file is up to date

When you check applications and signature files as part of a custom requirement, you can specify the same information as when you create a predefined requirement. The option names may differ slightly.

If you select **Any Antispyware Product**, any of the applications in the drop-down list meet the requirement.

When you specify the signature file information, you can select one or both options for checking that the signature file is up to date. If you select both options, both of the following conditions must be satisfied to meet the requirement:

- Select **Check signature file** is less than and enter a number of days.
  A file that is dated before the number of days you specify is out of date.
- Select **Check signature file date is** and select before, after, equal to, or not equal to, and specify a date (mm/dd/yyyy). Optionally, specify an hour and minute; the default is 00:00. The file's last modified date determines the signature file age.

See "Adding Host Integrity requirements" on page 57.

About firewall conditions

For a custom Host Integrity requirement, you can specify firewall applications to check as part of your IF-THEN condition statement.

You can check for the following conditions:

- Firewall is installed
- Firewall is running

If you want to select any of the applications in the drop-down list, you can select **Any Firewall Product**. You can include a subset of applications by selecting each using the OR keyword.

See "Adding Host Integrity requirements" on page 57.

About file conditions

For a custom Host Integrity requirement, you can check an application or a file as part of your IF-THEN condition statement.

You can specify the following options to check file information in a custom Host Integrity requirement:

File: Compare file age to	Specify a number of days or weeks and select greater than or less than.
File: Compare file date to	Specify a date in the format mm/dd/yyyy. Optionally, specify an hour and minute. The default time is 00:00. You can select equal to, not equal to, before, or after.

File: Compare file size to	Specify the number of bytes. You can select equal to, not equal, less than, or greater than.
File: Compare file version to	Specify a file version in the format x.x.x.x, where x represents a decimal number from 0 to 65535. You can select equal to, not equal, less than, or greater than.
File: File exists	Specify the name of the file to be checked for.
File: File fingerprint equals	Normally you get this information by selecting an application using **Search for Applications**.
Specify a hexadecimal number (up to 32 digits)	When you select an option, additional fields appear on the dialog. For each option you specify the file name and path and you enter the additional information that is required.
File: File Download complete	You can download a file from a location that you specify to a directory that you specify. If authentication is required to access a file location by HTTP, you can specify the user name and password.

You can use system variables, registry values, or a combination of them to specify the file name and path. When you select one of the file options, the dialog shows examples of ways to enter the file name and path.

You can locate the applications that have been recorded by using the Search for Applications feature. When you specify file options in the custom requirement script, the **Search for Applications** option provides access to the same search tool as the **Search for Applications** tool. You can browse the groups that are defined in the management server to filter applications, enter a search query, and export the results to a file.

To search using system environment variables or registry values:

To use the system environment variable	To specify the file named cmd.exe located under the directory that is specified in the WINDIR environment variable, type the following command: `%WINDIR%\cmd.exe`
To use the registry value	To read the value `HKEY_LOCAL_MACHINE\Software\Symantec\\AppPath` as the path of the file sem.exe, type the following command: `#HKEY_LOCAL_MACHINE\Software\Symantec\AppPath#\sem.exe`

To use the combined registry and system environment variable	Use the following example to use the combined registry value and system environment variable: `%SYSTEMDIR%\#HKEY_LOCAL_MACHINE\Software\Symantec\AppPath#`.

See "Adding Host Integrity requirements" on page 57.

About operating system conditions

For a custom Host Integrity requirement, you can specify operating system information to check as part of your IF-THEN condition statement. When you select an option, additional fields appear on the dialog.

Utility: Operating system is	Specify an operating system. When you want to update a patch, you need to select the exact versions that require that patch. You can use the OR keyword to specify more than one operating system.
Utility: Operating system language is	The function detects the language version of the client's operating system. If the language version is not listed in the **Custom Requirement** dialog, you can add languages by typing their identifiers in the **Language Identifiers** field. To add multiple identifiers, use a comma to separate each ID such as 0405,0813. See the Language Identifiers table for the list of identifiers.
Patch: Compare current service pack with specified version	Type the number of the service pack that you want to check for, such as 1a. The number is limited to two characters. You can check for the following conditions: equal to, not equal to, less than, or greater than. A number that is followed by a letter is considered greater than the number alone; for example, service pack number 6a is considered greater than 6. Be sure to apply patches one at a time.
Patch: Patch is installed	Type the patch name that you want to check for. For example: KB12345. You can type only numbers and letters in this field.

Be sure to match the patch name or service pack number with the correct version of the operating system. If you specify an operating system that does not match the patch or the service pack, the requirement fails.

See "Adding Host Integrity requirements" on page 57.

About registry conditions

For a custom Host Integrity requirement, you can specify Windows registry settings to check as part of your IF-THEN condition statement. You can also specify ways to change registry values. Only HKEY_LOCAL_MACHINE, HKEY_CLASSES_ROOT, and HKEY_CURRENT_CONFIG are supported registry settings.

The following selections are available for checking registry settings:

Registry: Registry key exists	Specify a registry key name to check whether it exists.
Registry: Registry value equals	Specify a registry key name and a value name and specify what data to compare the value against.
Registry: Registry value exists	Specify a registry key name to check if it has the specified value name.
Registry: Set registry value	Specify a value to assign for the specified key; if the key does not exist, it creates the key. This selection replaces an existing value, whether or not it is of the same type. If the existing value is a DWORD value but you specify a string value, it replaces the DWORD with the string value.
Registry: Increment registry DWORD value	Specify a DWORD value. This selection lets you perform counts, such as allowing an unpatched computer to meet the requirement no more than n times.

When you specify registry keys, remember the following considerations:

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

When you specify registry values, remember the following considerations:

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

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

The following are examples of registry values:

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

See “Adding Host Integrity requirements” on page 57.

About functions

You use functions to define the actions that are performed when a conditional expression is evaluated as true or false.

A custom requirement condition can check for the installation of a particular antivirus product, but it cannot be configured to install the product as a remediation action. When you write custom requirements, you must explicitly define the remediation actions to be performed by using function statements.

Functions appear within THEN and ELSE statements, or may appear at the end of a custom requirement script. To achieve a desired remediation result, you may need to specify multiple functions. Each function performs a very specific task, such as to download a file or to execute a file. You do not define individual functions to provide specific remediation actions, such as to install a specific antivirus product. To download a specific antivirus product, you must use the general download function.

Table 4-1 displays the following functions in a custom requirement script:

Table 4-1 Custom requirement functions

Function	Description
Download a file	Downloads a file that is referenced by a URL or UNC to the client computer. If a URL is used, both HTTP and FTP are supported.

Table 4-1 Custom requirement functions *(continued)*

Function	Description
Set registry value Increment registry DWORD value	Creates and then sets or increments a Windows registry value within a specified registry key.
Log message	Specifies a custom message to be added to the client Security log and the registry.
Run a program	Executes a program that is already resident on the client computer. You can specify the program to run whether or not the user is logged on.
Run a script	Runs a custom script on the client computer. You can use the built-in text editor to create the script contents. The script may be a batch file, an INI file, or any executable format Windows recognizes. Additionally, the script may contain only parameters to be provided to another program.
Set Timestamp	Stamps a specified file on the client computer with the current time and date.
Show message dialog	Displays a message dialog window on the client computer with an OK option. A default timeout may be specified.
Wait	Pauses the execution of the custom requirement script for a specified period.

See “Adding Host Integrity requirements” on page 57.

About custom requirement logic

You write the custom requirements by using the script-like logic. The rules use IF..THEN..ELSE logic from a list of predefined conditions and actions.

See “About the RETURN statement” on page 78.

See “About the IF, THEN, and ENDIF statement” on page 78.

See “About the ELSE statement” on page 78.

See “About the NOT keyword” on page 78.

See “About AND, OR keywords” on page 79.

About the RETURN statement

You can add a RETURN statement to specify the overall Host Integrity result of the requirement. The RETURN statement includes the PASS keyword and the FAIL keyword. All custom requirements must include a RETURN statement at the end.

Unlike a predefined requirement, a custom requirement must explicitly specify the result of the Host Integrity check. In some cases, the evaluation of a set of conditions as being true should be interpreted as the custom requirement passing Host Integrity evaluation. In other cases, you may want the same evaluation to be interpreted as failing Host Integrity evaluation.

See “Adding Host Integrity requirements” on page 57.

About the IF, THEN, and ENDIF statement

You can define the primary logic structure of a custom requirement by one or more IF, THEN, and ENDIF statements. An IF, THEN, and ENDIF statement:

- Defines a structure in which specific conditions are checked (IF).
- The actions that are taken when those conditions are evaluated as being true (THEN).

You can nest IF, THEN, and ENDIF statements to form more complex custom requirements. You must nest the IF, THEN, and ENDIF statements whenever one condition must be true before another condition can be evaluated.

See “Adding an IF THEN statement” on page 81.

About the ELSE statement

An IF, THEN, and ENDIF statement is a set of conditions and actions that are executed when the conditions are evaluated as being true. In many cases, you may need to specify one or more actions to be taken to perform a desired remediation action. You may add an ELSE statement to identify the actions to be taken whenever the specified conditions are evaluated as being false.

See “Adding an ELSE statement” on page 81.

About the NOT keyword

You can use the NOT keyword to reverse the logical evaluation of a particular condition. After a condition has been added to the custom requirement script, right-click the condition and select Toggle NOT to reverse the logical of the condition. The use of the NOT keyword does not change the overall true and false evaluation of the IF statement. It reverses only the true and the false state of a particular condition.

See "Adding Host Integrity requirements" on page 57.

About AND, OR keywords

You can specify multiple conditions within an IF, THEN, or ENDIF statement; however, additional keywords must be added to the statement. Within any IF statement, you can add the AND OR keywords to logically associate multiple conditions. The logical association of the conditions directly affects the overall true or false evaluation of the IF statement. If you use the AND keyword in an IF statement, all the conditions in the IF statement must be evaluated as true for the IF statement to be true. If you use the OR keyword, only one of the conditions in the IF statement must be evaluated for the IF statement to be true.

When you specify multiple conditions, you must interpret the logical association of the conditions to anticipate what the correct true or false evaluation should be. The custom requirement script does not display the expression with a parenthesis format, but with nested keywords and nodes. The first expression always begins with the first condition specified, and continues as long as the same logical operator keyword is used. For example, you can use the OR keyword to associate three different conditions. As long as you use the OR keyword, all the conditions are contained within the same logical expression.

See "Adding Host Integrity requirements" on page 57.

Writing a custom requirement script

To build a custom requirement, you add one or more IF..THEN.. statements to a script. When you run the script, the Host Integrity check looks for the condition that is listed under the IF node. Depending upon the condition, the action that is listed under the THEN node is executed. The result (pass or fail) is returned.

The script displays a tree structure in the left pane and a drop-down list of conditions or functions in the right pane.

As part of a custom requirement, you can specify whether to allow the Host Integrity check to pass if the requirement fails. When you plan how many different conditions to check for in one script, remember that this setting applies to the entire custom requirement script. This choice may affect whether you want to create several small custom requirements or a longer one that includes multiple steps.

To write a custom requirement script

1. Add a custom requirement.

   See "Adding Host Integrity requirements" on page 57.

2. In the **Custom Requirement** dialog box, type a name for the requirement.

   The requirement name can appear on the client computer. The name notifies the user whether the requirement has passed or the requirement has failed or prompts the user to download the software.

3. To add a condition, under **Customized Requirement Script**, click **Add**, and then click **IF..THEN..**.

4. With the highlight on the empty condition under the IF node, in the right pane, select a condition.

   The Host Integrity check looks for the condition on the client computer.

5. Under the **Select a condition** drop-down list, specify the additional information that is required.

6. Under **Customized Requirement Script,** click THEN, and then click **Add**.

   The THEN statement provides the action that should be taken if the condition is true.

7. Click any of the following options:

   - IF.. THEN
     Use a nested IF.. THEN.. statement to provide additional conditions and actions.
     See "Adding an IF THEN statement" on page 81.

   - Function
     Use a function to define a remediation action.
     See "About functions" on page 76.

   - Return
     Use a return statement to specify whether the results of the evaluation of the condition passes or fails. Every custom requirement must end with a pass or fail statement.

   - Comment
     Use a comment to explain the functionality of the conditions, functions, or statements that you are adding.
     See "Adding a comment" on page 82.

8. In the right-hand pane, define the criteria that you added.

   For more information on these options, click **Help**.

9 To add more nested statements, conditions, or functions, under **Customized Requirement Script**, right-click the node, and then click **Add**.

10 Repeat steps 7 to 9 as needed.

11 To allow the Host Integrity check to pass no matter what the result, check **Allow the Host Integrity check to pass even if this requirement fails**.

12 When you are done with the configuration of the requirement, click **OK**.

Adding an IF THEN statement

Add an IF..THEN statement to a custom script to define conditions to check and actions to take if the condition is evaluated as true.

To add an IF THEN statement

1 Write a custom requirement script.

See "Writing a custom requirement script" on page 79.

2 Under **Customized Requirement Script**, select one of the following:

- To add the first IF THEN statement, select the top node.
- To add an IF THEN statement at the same level as an existing one, select **END IF**.
- To add a nested IF THEN statement, select the line under which you want to add it.

3 Click **Add**.

4 Click **IF..THEN**.

Switching between the IF statement and the IF NOT statement

You may need to change between checking for the presence or absence of a condition.

To change between the IF statement and the IF NOT statement

1 Write a custom requirement script.

See "Writing a custom requirement script" on page 79.

2 Right-click the condition, and then click **Toggle NOT**.

Adding an ELSE statement

You may add an ELSE statement to identify the actions to be taken whenever the specified conditions are evaluated as being false.

To add an ELSE statement

1 Write a custom requirement script.

See "Writing a custom requirement script" on page 79.

2 Under **Customized Requirement Scrip**t, click **THEN**.

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

Adding a comment

For informational purposes, you can choose to add a comment to a statement.

To add a comment

1 Write a custom requirement script.

See "Writing a custom requirement script" on page 79.

2 Under **Customized Requirement Script**, select any statement that you have already added, and then click **Add**.

3 Click **Comment**.

4 Click **//Insert statements here**, and in the right-hand pane, in the **Comment** text field, enter your comments.

Copying and pasting IF statements, conditions, functions, and comments

You can copy and paste statements or entire IF THEN nodes within or between custom requirements. You may want to copy and paste these elements if you want to move them to another part of the script or to repeat the functionality.

To copy and paste an IF statement

1 Write a custom requirement script.

See "Writing a custom requirement script" on page 79.

2 Under **Customized Requirement Script**, right-click the script element, and then click **Copy**.

3 Right-click an empty statement line, and then click **Paste**

Deleting a statement, condition, or function

You can delete statements, conditions, or functions at any time. If there is only one condition statement under an IF node, deleting it deletes the entire IF THEN statement.

To delete a statement, condition, or function

1. Write a custom requirement script.

   See "Writing a custom requirement script" on page 79.

2. Under **Customized Requirement Script**, select the requirement element that you want to delete.

3. Click **Delete**.

4. If you are asked to confirm the deletion, click **Yes**.

Displaying a message dialog box

You can specify a function or a condition in the custom Host Integrity requirement that creates a message that the client displays to the user. The function or the condition returns true if the user clicks OK or Yes. Otherwise it returns false.

To display a message dialog box

1. Write a custom requirement script.

   See "Writing a custom requirement script" on page 79.

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

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

4. Click **Utility: Show message dialog**.

   To insert a condition, select **IF...Then**, and then select the appropriate branch. Then select **Utility: Message dialog return value equals**.

5. Type a caption for the message box, up to 64 characters.

6. Type the text for the message box up, to 480 characters.

7. Select one of the following icons to display: Information, Question, Warning, or Error.

   Both the icon and the text appear.

8. Select the set of options that appear in the dialog box:

   - OK
   - OK and Cancel
   - Yes and No

9. Select the default option for each set of options.
10. To close the message box and return a default value after a certain time with no user interaction, check **Action to take to dismiss message box after maximum waiting time**, and specify the wait time.

    The time value must be greater than 0.

Downloading a file

For a custom requirement, you can specify that a file is downloaded to the client computer.

To download a file

1. Write a custom requirement script.

   See "Writing a custom requirement script" on page 79.
2. In the **Custom Requirement** dialog box, under **Customized Requirement Script**, select the node where you want to add the function.
3. Click **Add**, and then click **Function**.
4. Click **File: Download a file**.
5. Enter the URL location that the file is downloaded from, and the folder on the client computer you want the file to be downloaded to.

   You can specify the location by a URL or a UNC. If you use a URL, both HTTP and FTP are supported.

   If you choose HTTP, check **Authentication required for HTTP only**. Enter the user name and password for the authentication
6. Check **Show the download process dialog** so that the users can watch the file as the file gets downloaded to the client computer.
7. If you want the user to be able to cancel the file download, check **Allow the user to cancel Host Integrity for this requirement**.

   Users may lose work if the file is downloaded at the wrong time.

Setting a registry value

For a custom requirement, you can set a Windows registry value to a specific value. The Set registry value function creates the value if it does not already exist.

To set a registry value

1 Write a custom requirement script.

  See “Writing a custom requirement script” on page 79.

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

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

4 Click **Registry: Set registry value**. The registry value contains the value name and type to be checked.

5 Enter the registry key in the **Registry key** field.

6 Enter a value name to be checked in the **Value name** field.

7 Under **Specify Type and Data**, choose one of the following value and content types:

  - DWORD value
  - String value
  - Binary value

Incrementing a registry DWORD value

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

To increment the registry DWORD value

1 Write a custom requirement script.

  See “Writing a custom requirement script” on page 79.

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

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

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

4 Enter the registry key to check in the **Registry key** field.

5 Enter a value name to be checked in the **Value name** field.

Generating a log message

In the custom Host Integrity requirement, you can specify a function to log a message about an action. This function inserts the specified message string into the client Security log. The message appears in the details area of the Security log.

To generate a log message

1. Write a custom requirement script.

   See "Writing a custom requirement script" on page 79.

2. In the **Custom Requirement** dialog box, under **Customized Requirement Script**, select the node where you want to add the function.
3. Click **Add**, and then click **Function**.
4. Click **Utility: Log message**.
5. In the **Severity Type** drop-down list, select one of the following log severity types: Information, Major, Minor, or Critical.
6. Type a message up to 512 characters long.

Running a program

For a custom Host Integrity requirement, you can specify a function to have the client launch a program.

To run a program

1. Write a custom requirement script.

   See "Writing a custom requirement script" on page 79.

2. In the **Custom Requirement** dialog box, under **Customized Requirement Script**, select the node where you want to add the function.
3. Click **Add**, and then click **Function**.
4. Click **Utility: Run a program**.
5. In the **Execute the command** text field, type the command to execute the script.

   Environment variables are substituted before execution. For example, `%windir%` replaces the Windows directory path. You can use the `%1` variable to execute the last downloaded file.

6. Under **Run a Program**, select one of the following options:
   - in system context

- in logged-in user context

  The Execute command must include the whole file path, thus showing who the logged-in user is. If no user is logged in, the result fails.

7. To specify the amount of time to allow the execute command to complete, select one of the following options:
   - Do not wait

     The action returns true if the execution is successful but it does not wait until the execution is completed.
   - Wait until execution completes
   - Enter maximum time

     Enter a time in seconds. If the Execute command does not complete in the specified time, the file execution is terminated.
8. Optionally, uncheck **Show new process window** if you do not want to see a window that shows the requirement running the program.

Running a script

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

To run a script

1. Write a custom requirement script.

   See "Writing a custom requirement script" on page 79.
2. In the **Custom Requirement** dialog box, under **Customized Requirement Script**, select the node where you want to add the function.
3. Click **Add**, and then click **Function**.
4. Click **Utility: Run a script**.
5. Enter a file name for the script, such as myscript.js.
6. Type the content of the script.
7. In the **Execute the command** text field, type the command to execute the script.

   Use %F to specify the script file name. The script executes in system context.
8. To specify the amount of time to allow the execute command to complete, select one of the following options:
   - Do not wait

The action returns true if the execution is successful but it does not wait until the execution is completed.

- Wait until execution completes
- Enter maximum time
  Enter a time in seconds. If the Execute command does not complete in the specified time, the file execution is terminated.

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

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

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

Setting the timestamp of a file

In the custom Host Integrity requirement, you can specify the Set Timestamp function to create a Windows registry setting to store the current date and time. You can then use the Check Timestamp condition to find out if a specified amount of time has passed since that timestamp was created.

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

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

To set the timestamp of a file

1 Write a custom requirement script.

See "Writing a custom requirement script" on page 79.

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

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

4 Click **Utility: Set Timestamp**.

5 Type a name up to 256 characters long for the registry setting that stores the date and the time information.

To compare the current time to the stored time value

1. Write a custom requirement script.

   See "Writing a custom requirement script" on page 79.

2. In the **Custom Requirement** dialog box, under **Customized Requirement Script**, select the node where you want to add the condition.
3. Click **Add**, and then click **IF..THEN..**.
4. Click **Utility: Check Timestamp**.
5. Type the name you entered for the saved time registry setting.
6. Specify an amount of time in minutes, hours, days, or weeks.

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

Specifying a wait time for the custom requirement script

In the custom Host Integrity requirement, you can specify a function that causes the custom requirement script to wait for a specified length of time before it runs.

To specify a wait time for the script

1. Write a custom requirement script.

   See "Writing a custom requirement script" on page 79.

2. In the **Custom Requirement** dialog box, under **Customized Requirement Script**, select the node where you want to add the function.
3. Click **Add**, and then click **Function**.
4. Click **Utility: Wait**.
5. Type the number of seconds to wait.

Section 3

Controlling network access with Symantec Network Access Control Enforcer appliances

Chapter 5

Introducing the Symantec Network Access Control Enforcer appliances

This chapter includes the following topics:

- About the Symantec Network Access Control Enforcer appliances
- Support for third-party enforcement solutions

About the Symantec Network Access Control Enforcer appliances

Symantec Enforcer appliances are the optional network components that work with the Symantec Network Access Control-enabled clients and the Symantec Network Access Control clients.

Symantec Network Access Control comes with the following Linux-based Enforcer images which you install on the Symantec Enforcer appliances:

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

Additionally, all Windows-based Symantec Enforcers work with managed clients to protect your network. These clients include the Symantec Endpoint Protection client and the Symantec Network Access Control client.

See "Installing an Enforcer appliance" on page 96.

See "Installation planning for a Gateway Enforcer appliance" on page 113.

See “Installation planning for a DHCP Enforcer appliance” on page 161.

See “Installing an Enforcer appliance” on page 96.

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.

Chapter 6

Installing all types of Enforcer appliances

This chapter includes the following topics:

About installing an Enforcer appliance

You select the type of Enforcer appliance that you want to use during the installation process. Before you start to install any of the Enforcer appliances:

- Familiarize yourself with the locations of the components in your network.
- Locate the Symantec Network Access Control Enforcer installation Disc 2.
  This disc contains the software for the all types of Symantec Network Access Control Enforcer appliances.
- Identify the host name that you want to assign to the Enforcer appliance. The default host name is Enforcer. You may want to change this name to make it easier to identify each Enforcer appliance in a network.
- Identify the IP addresses of the network interface cards (NICs) on the Enforcer appliance.

- Identify the IP address, host name, or domain ID of the Domain Name Server (DNS) if applicable. Only DNS servers can resolve host names.

  If you want the Enforcer appliance to connect to a Symantec Endpoint Protection Manager by using a host name, it needs to connect to a DNS server.

  You can configure the IP address of the DNS server during the installation. However, you can use the configure DNS command to change the IP address of a DNS server from the Enforcer console with the Configure DNS command.

See "Installing an Enforcer appliance" on page 96.

Installing an Enforcer appliance

Table 6-1 lists the steps to install all types of Enforcer appliances.

Table 6-1 Installation summary for an Enforcer appliance

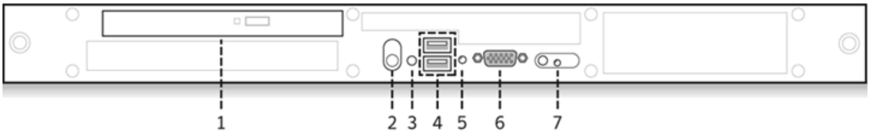
Step	Action	Description
Step 1	Learn where to place Enforcers in your network.	Enforcers need to be placed in specific locations on your network to ensure that all endpoints comply with your security policy. See "Installation planning for a Gateway Enforcer appliance" on page 113. See "Where to place DHCP Enforcer appliances in a network" on page 162. See "Where to place LAN Enforcer appliances" on page 198.
Step 2	Set up the appliance.	Connect the Enforcer appliance to your network. See "About installing an Enforcer appliance" on page 95. See "About the Enforcer appliance indicators and controls" on page 97. See "Setting up an Enforcer appliance" on page 98.
Step 3	Configure the appliance.	Log on and configure the Enforcer appliance from the Enforcer command line. See "Logging on to an Enforcer appliance" on page 100. See "Configuring an Enforcer appliance" on page 100.

About the Enforcer appliance indicators and controls

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

Figure 6-1 shows the controls, indicators, and connectors that are located behind the optional bezel on the front panel.

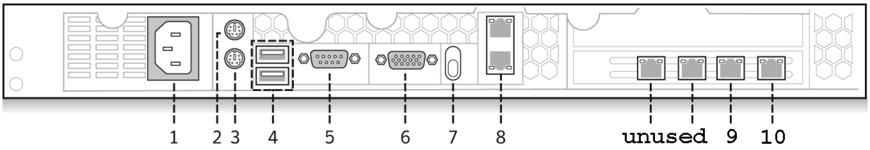
Figure 6-1 Enforcer appliance front panel



1	DVD-ROM drive
2	Power switch
3	Reset icon
4	USB ports
5	Hard drive light
6	Monitor
7	Reserved; do not use

Figure 6-2 shows the back panel of the system.

Figure 6-2 Enforcer appliance back panel (Failopen model shown)



1	Power cord connector
2	Mouse connector
3	Keyboard connector
4	USB ports
5	Serial port

6	Monitor
7	Reserved; do not use
8	Reserved network ports; do not use
9	eth0 network port
10	eth1 network port

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.

See “Installing an Enforcer appliance” on page 96.

See “Setting up an Enforcer appliance” on page 98.

Setting up an Enforcer appliance

Set up the Enforcer appliance hardware by connecting it to your network, switching it on, and logging on at the command line.

See “Installing an Enforcer appliance” on page 96.

See “About the Enforcer appliance indicators and controls” on page 97.

To set up an Enforcer appliance

1. Unpack the Enforcer appliance.
2. Mount the Enforcer appliance in a rack, or place it on a level surface.

   See the rack mounting instructions that are included with the Enforcer appliance.
3. Plug it into an electrical outlet.
4. Connect the Enforcer appliance by using one of the following methods:
   - Connect another computer to the Enforcer appliance by using a serial port.
     Use a null modem cable with a DB9 connector (female). You must use terminal software, such as HyperTerminal, CRT, or NetTerm, to access the Enforcer console. Set your terminal software to 9600 bps, data bits 8, no parity, 1 stop bit, no flow control.

- Connect a keyboard and VGA monitor directly to the Enforcer appliance.

5 Connect the Ethernet cables to the network interface ports as follows:

Gateway Enforcer appliance	Connect two Ethernet cables. One cable connects to the eth0 port (internal NIC). The other cable connects to the eth1 port (external NIC) on the rear of the Enforcer appliance. The internal NIC connects to the protected network and the Symantec Endpoint Protection Manager. The external NIC connects to the endpoints.
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 protected network and the Symantec Endpoint Protection Manager. The external NIC connects to the endpoints.
LAN Enforcer appliance	Connect one Ethernet cable to the eth0 port on the rear of the Enforcer appliance. This cable connects to the internal network. The internal network connects to an 802.1x-enabled switch and to any additional 802.1x-enabled switches in your network.

6 Switch on the power.

The Enforcer appliance starts.

7 Press **Enter** twice.

8 At the logon prompt, log on as follows:

Console Login: **root**

Password: **symantec**

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

See “Logging on to an Enforcer appliance” on page 100.

See “Configuring an Enforcer appliance” on page 100.

Logging on to an Enforcer appliance

When you turn on or restart the Enforcer appliance, the logon prompt for the Enforcer appliance console appears:

```
Enforcer Login
```

The following levels of access are available:

Superuser	Access to all commands
Normal	Access only to the `clear`, `exit`, `help`, and `show` commands for each level of the command hierarchy

---

Note: The Enforcer appliance automatically logs users off after 90 seconds of inactivity.

See "Setting up an Enforcer appliance" on page 98.

To log on to an Enforcer appliance with access to all commands

1. On the command line, log on to an Enforcer appliance with access to all commands by typing the following command:

   ```
   root
   ```

2. Type the password that you created during the initial installation.

   The default password is symantec

   The console command prompt for root is Enforcer#

To log on to an Enforcer appliance with limited access to commands

1. If you want to log on to an Enforcer appliance with limited access to commands, type the following command on the command line:

   ```
   admin
   ```

2. Type the password on the command line.

   The default password is `symantec`

   The console command prompt for admin is `Enforcer$`

See "Configuring an Enforcer appliance" on page 100.

Configuring an Enforcer appliance

Configure the appliance from the Enforcer command-line interface.

See "About the Enforcer appliance CLI command hierarchy" on page 365.

See "Logging on to an Enforcer appliance" on page 100.

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
   [G] Gateway  [D] DHCP  [L] LAN
   ```

   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 the 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 374.

   where *hostname* is the new host name for the Enforcer appliance.

   Be sure to register the host name of the Enforcer appliance on the Domain Name Server itself.

3. Type the following command to confirm the new host name of the Enforcer appliance:

   ```
   show hostname
   ```

4. Type the IP address of the DNS server and press **Enter**.

5 Type the new root password at the prompt by first typing the following command:

password

Old password: *new password*

You must change the root password that you used to log on to the Enforcer appliance. Remote access is not enabled until you change the password. The new password must be at least nine characters long, and contain one lowercase letter, one uppercase letter, one digit, and one symbol.

6 Type the new admin password.

7 Set the time zone by following these prompts.

```
Set the time zone
Current time zone is [+0000]. Change it? [Y/n]
If you click 'Y', follow the steps below:
1) Select a continent or ocean
2) Select a country
3) Select one of the time zone regions
4) Set the date and time
Enable the NTP feature [Y/n]
Set the NTP server:
Note: We set up the NTP server as an IP address
```

8 Set the date and time.

9 Configure the network settings and complete the installation, following the Enforcer prompts.

```
Enter network settings

Configure eth0:
Note: Input new settings.
IP address []:
Subnet mask []:
Set Gateway? [Y/n]
   Gateway IP[]:

   Apply all settings [Y/N]:
```

Chapter 7

Upgrading and migrating all types of Enforcer appliance images

This chapter includes the following topics:

- About upgrading and migrating Enforcer appliance images
- Determining the current version of an Enforcer appliance image
- Upgrading the Enforcer appliance image
- Migrating the Enforcer appliance image
- Reimaging an Enforcer appliance image

About upgrading and migrating Enforcer appliance images

Determine the version of the Enforcer appliance software before you plan to update, migrate, or reimage any of the Enforcer appliance software.

See "Determining the current version of an Enforcer appliance image" on page 104.

You may need to upgrade the image of an Enforcer appliance to the current version if you want to connect to the most current version of Symantec Endpoint Protection Manager. The upgrade enables you to take advantage of the new features that the Symantec Network Access Control Enforcer appliance provides. The Enforcer appliances works with Symantec Endpoint Protection Manager 11.0 and all subsequent release updates.

You can select any of the following methods to upgrade the Enforcer appliance image:

- Upgrade the current Enforcer appliance image.
  See "Upgrading the Enforcer appliance image" on page 104.
- Migrate from your current Enforcer appliance image to the latest Enforcer appliance image.
  See "Migrating the Enforcer appliance image" on page 105.
- Install a different Enforcer appliance image over a previous Enforcer appliance image.
  See "Reimaging an Enforcer appliance image" on page 105.

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 is v11.0.6. If you have a version that precedes v11.0.6, you should try to upgrade or migrate.

For example, when you check the version of a DHCP Enforcer appliance image, the output may appear as follows:

```
Symantec Network Access Control Enforcer - v11.0.6
build XXXX, 2010-11-29,19:09
DHCP Enforcer mode
```

To check the current version of an Enforcer appliance image, type the following command on the command-line interface of an Enforcer appliance:**show version**

See "Show" on page 376.

Upgrading the Enforcer appliance image

You can use the following method to update an Enforcer appliance image to the latest version.

To upgrade the Enforcer appliance image from 11.0, 11.0.2000, 11.0.3000 to 11.0.6000

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
   ```

See “Update” on page 378.

Migrating the Enforcer appliance image

You can use any of the following methods to update an Enforcer appliance image to the latest image:

- Migrate the Enforcer appliance image from 5.1.x to 11.0.6000 with a USB (Universal Serial Bus) disk.
- Migrate the Enforcer appliance image from 5.1.x to 11.0.6000 from a TFTP server.

To migrate the Enforcer appliance image from 5.1.x to 11.0.6.000 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 378.

To migrate the Enforcer appliance image from 5.1.x to 11.0.6000 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 378.
3. Select **Y** when you are prompted to launch the new image.
4. Select **1** to restart the Enforcer appliance after you apply a new image.

   Do not launch the new image without restarting the Enforcer appliance.
5. Log on to the Enforcer appliance.
6. See “Logging on to an Enforcer appliance” on page 100.

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 disc 2, 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.

To reimage an Enforcer appliance

1. Insert product disc 2 in the disc 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 hard disc instead of the product disc. To reimage, you must restart from the disc.
4. Install and configure the Enforcer appliance.

   See “About installing an Enforcer appliance” on page 95.

Chapter 8

Performing basic tasks on the console of all types of Enforcer appliances

This chapter includes the following topics:

About performing basic tasks on the console of an Enforcer appliance

You must have already configured the following parameters during the installation of the Enforcer appliance:

- Host name of the Enforcer appliance
- Group name of the Enforcer appliance group of which a particular Enforcer appliance is a member
- IP addresses of the internal and the external network interface cards (NICs)
- IP address of the DNS server, if applicable

- IP address of the NTP server, if applicable

However, you must still configure a connection between an Enforcer appliance and a Symantec Endpoint Protection Manager. You execute the spm command on the console of the Enforcer appliance to configure this connection. You cannot proceed to use an Enforcer appliance unless you complete this task.

See "Configuring a connection between an Enforcer appliance and a Symantec Endpoint Protection Manager" on page 108.

After initially installing and configuring an Enforcer appliance, you can perform administrative tasks from the Enforcer appliance console or Symantec Endpoint Protection Manager. If you administer multiple Enforcer appliances, it is convenient to administer them all from one centralized location

All Enforcer appliances also have a command-line interface (CLI) from which you can execute commands to change any number of parameters.

See "About the Enforcer appliance CLI command hierarchy" on page 365.

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 the external NICs on the Enforcer appliance.

See "About installing an Enforcer appliance" on page 95.

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

- IP address of the Symantec Endpoint Protection Manager
  Check with the administrator of the server on which the Symantec Endpoint Protection Manager has been installed to obtain the IP address.
- Enforcer group name to which you want to assign the Enforcer appliance
  After you finish configuring the Enforcer group name for the Enforcer appliance, the group name automatically registers on the Symantec Endpoint Protection Manager.
- Port number on the Symantec Endpoint Protection Manager that is used to communicate with the Enforcer appliance
  The default port number is 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 "Configuring SPM" on page 109.

   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 111.
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. This client is also known as a managed client.

   To allow guests (unmanaged client computers) to automatically download Symantec Network Access Control On-Demand Clients, 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 347.

Configuring 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.
http <port-number>	Enables you to specify the HTTP protocol and the port number to communicate with the Symantec Endpoint Protection Manager. The default protocol is HTTP. The default port number for the HTTP protocol is 80.
https <port-number>	Enables you to specify the HTTPS protocol and the port number to communicate with the Symantec Endpoint Protection Manager. You should only use this command if the Symantec Endpoint Protection Manager has been set up to use the HTTPS protocol. The default port number for the HTTPS protocol is 443.
key <key-name>	Enables you to specify the encrypted password that is required if the Symantec Endpoint Protection Manager has been installed with one.

The following example describes configuring an Enforcer appliance to communicate with the Symantec Endpoint Protection Manager at IP address 192.168.0.64 in an Enforcer group called CorpAppliance. It uses the HTTP protocol on port 80 with an encrypted password of “security.”

```
configure spm ip 192.168.0.64 group CorpAppliance http 80 key security
```

See “CLI command hierarchy” on page 366.

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 100.

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
Policy ID:                 24/03/2010  21:31:55
```

Remote access to an Enforcer appliance

To securely communicate with the Enforcer for command-line access, use one of the following methods:

- Networked KVM switch or similar device
- SSH client which supports SSH v2 Terminal Console server
- Serial cable

See “Setting up an Enforcer appliance” on page 98.

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 and logs” on page 272.

Chapter 9

Planning for the installation of the Gateway Enforcer appliance

This chapter includes the following topics:

- Installation planning for a Gateway Enforcer appliance
- Gateway Enforcer appliance NIC settings
- Failover planning for Gateway Enforcer appliances
- Fail-open planning for a Gateway Enforcer appliance

Installation planning for a Gateway Enforcer appliance

A Gateway Enforcer appliance is generally used inline as a secure policy-enforcing bridge to protect a corporate network from external intruders. Before you install a Gateway Enforcer appliance, you need to think about locating it appropriately on the network. Gateway Enforcer appliances can be placed throughout the enterprise to ensure that all endpoints comply with the security policy.

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

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

General placement:

- See “Where to place a Gateway Enforcer appliance” on page 114.
- See “Guidelines for IP addresses on a Gateway Enforcer appliance” on page 117.
- See “About two Gateway Enforcer appliances in a series” on page 117.

Specific areas of the network:

- See “Protection of VPN access through a Gateway Enforcer appliance” on page 118.
- See “Protection of wireless access points through a Gateway Enforcer appliance” on page 118.
- See “Protection of servers through a Gateway Enforcer appliance” on page 118.
- See “Protection of non-Windows servers and clients through a Gateway Enforcer appliance” on page 119.
- See “Requirements for allowing non-Windows clients without authentication” on page 120.

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 117.

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

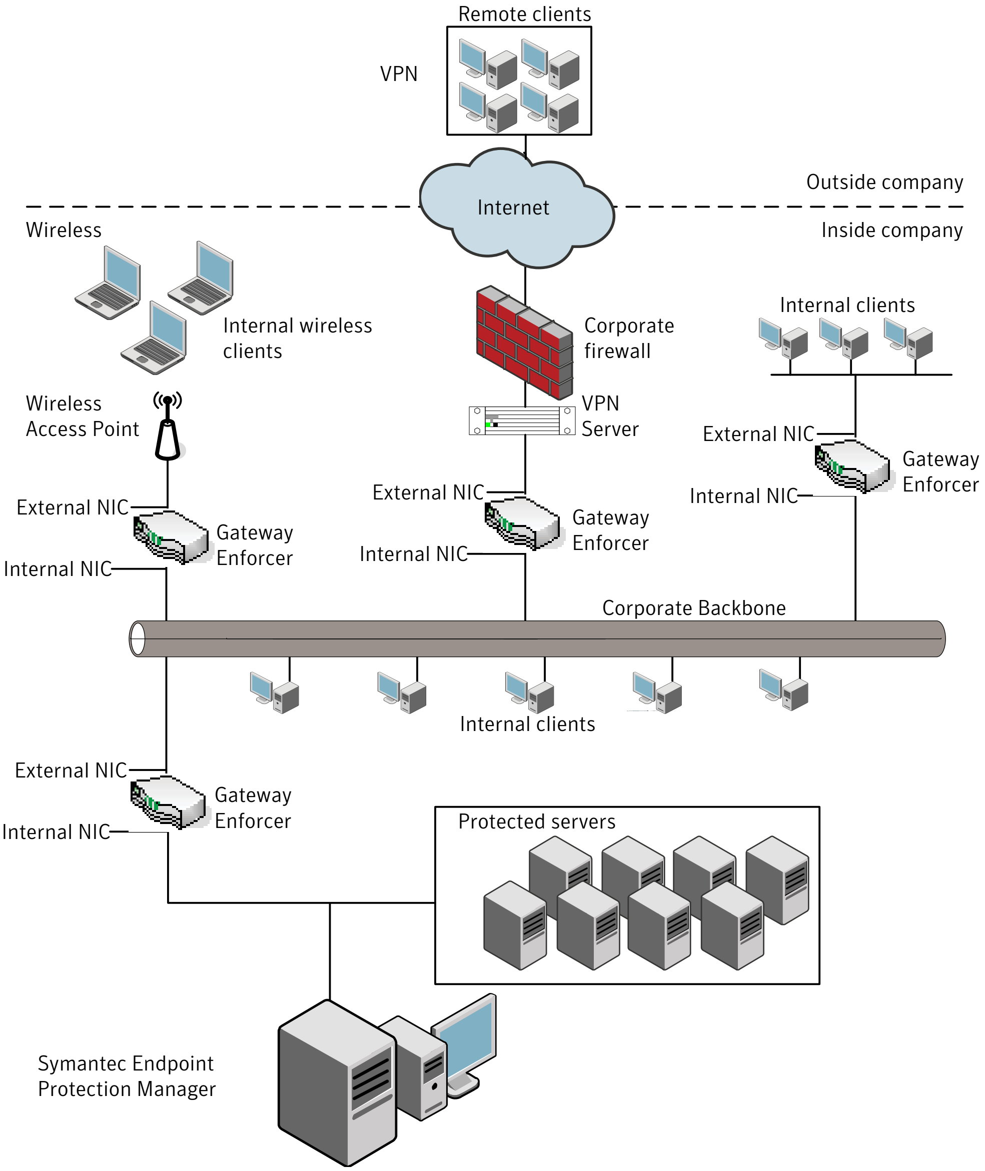
VPN	Between virtual private network (VPN) concentrators and the corporate network
Wireless Access Point (WAP)	Between a wireless access point and the corporate network
Servers	In front of corporate servers

Larger organizations may require a Gateway Enforcer appliance to protect every network entry point. Gateway Enforcers are typically located in different subnets. In most cases, you can integrate Gateway Enforcer appliances into a corporate network without having to make hardware configuration changes.

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 the servers that contain sensitive information. Gateway Enforcer appliances must use two network interface cards (NICs).

Figure 9-1 provides an example of where you can place Gateway Enforcer appliances in the overall network configuration.

Figure 9-1 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 up to connect to a corporate network. RAS dial-up clients are configured similarly to wireless and VPN clients. The external NIC connects to the RAS server and the internal NIC connects to the network.

Guidelines for IP addresses on a Gateway Enforcer appliance

Follow these guidelines when you set up the internal NIC address for a Gateway Enforcer appliance:

- A Gateway Enforcer appliance's internal NIC must be able to communicate with a Symantec Endpoint Protection Manager. By default, the internal NIC must face a Symantec Endpoint Protection Manager.
- Clients must be able to communicate with the Gateway Enforcer appliance's internal IP address. The VPN server or wireless AP can be in a different subnet. This works if the clients can 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 generates a bogus external NIC address, based on the internal NIC address. You do not need to configure this address again if you install another Gateway Enforcer.

See "Setting up an Enforcer appliance" on page 98.

About two Gateway Enforcer appliances in a series

If a network supports two Gateway Enforcer appliances in a series so that a client connects to the network through more than one Gateway Enforcer appliance, you must specify the Enforcer appliance that is closest to the Symantec Endpoint Protection Manager as a trusted internal IP address of the other Gateway Enforcer appliance. Otherwise a 5-minute delay can occur before the client can connect to the network.

This delay can occur when the client runs a Host Integrity check that fails. As part of Host Integrity remediation, the client downloads the required software updates. Then the client runs the Host Integrity check again. At that point the Host Integrity check passes, but network access is delayed.

See the *Administration Guide for Symantec Endpoint Protection and Symantec Network Access Control* for information about trusted internal IP addresses.

See “Adding a trusted internal IP address for clients on a management server” on page 154.

Protection of VPN access through a Gateway Enforcer appliance

The protection of VPN access is the first and the 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.

See “Where to place a Gateway Enforcer appliance” on page 114.

See “Setting up an Enforcer appliance” on page 98.

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.

See “Where to place a Gateway Enforcer appliance” on page 114.

See “Setting up an Enforcer appliance” on page 98.

Protection of servers through a Gateway Enforcer appliance

Gateway Enforcer appliances can protect the corporate servers that hold sensitive information in the corporate network. An organization may place important data on the servers that may be located in a locked computer room. Only system administrators may have access to the locked computer room.

The Gateway Enforcer appliance acts like an additional lock on the door. It does so by allowing only the users that meet its criteria to access the protected servers. Servers locate the internal NIC in this setup. However, users who try to gain access must pass through the external NIC.

To safeguard these servers, you can limit access only to clients with designated IP addresses and you can set up strict Host Integrity rules. For example, you can configure a Gateway Enforcer appliance to protect servers in a network. A Gateway Enforcer appliance can be located between clients on a corporate LAN and the servers that it safeguards. The external NIC points to the corporate LAN inside the company and the internal NIC points toward the protected servers. This configuration prevents unauthorized users or clients from gaining access to the servers.

See "Where to place a Gateway Enforcer appliance" on page 114.

See "Setting up an Enforcer appliance" on page 98.

Protection of non-Windows servers and clients through a Gateway Enforcer appliance

You can install the servers and the clients on an operating system other than Microsoft Windows. However, the Gateway Enforcer appliance cannot authenticate any servers and clients that do not run on a computer that does not support Microsoft Windows.

If an organization includes servers and clients with operating systems on which the client software is not installed, you must decide which of the following methods to use:

- Implement support through a Gateway Enforcer appliance.
- See "Implementation of non-Windows support through a Gateway Enforcer appliance" on page 119.
- Implement support without a Gateway Enforcer appliance.
  See "Implementation of non-Windows without a Gateway Enforcer appliance" on page 119.

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.

See "Where to place a Gateway Enforcer appliance" on page 114.

See "Setting up an Enforcer appliance" on page 98.

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.

See "Where to place a Gateway Enforcer appliance" on page 114.

See "Setting up an Enforcer appliance" on page 98.

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 121.

When a client tries to access the network through a Gateway Enforcer appliance, the Enforcer appliance first checks whether the client software has been installed on the client computer. If the client 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.

The Gateway Enforcer appliance correctly detects the Windows operating system if the Windows client meets the following requirements:

- The Client for Microsoft Networks option must be installed and enabled on the client.
  See the Windows documentation.

- The UDP port 137 must be open on the client. It must be accessible by the Gateway Enforcer.

If a Windows client fails to meet these requirements, the Gateway Enforcer appliance may interpret the Windows client to be a non-Windows client. Therefore the Gateway Enforcer appliance can allow the non-Windows client to connect to the network without authentication.

See "Allowing non-Windows clients to connect to a network without authentication" on page 143.

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.

See "Allowing non-Windows clients to connect to a network without authentication" on page 143.

Gateway Enforcer appliance NIC settings

The network interface cards (NICs) on a Gateway Enforcer appliance are configured by default so that eth0 is used for the internal NIC. The internal NIC must connect to the Symantec Endpoint Protection Manager.

You can use the configure interface-role command if you need to change which NIC is external and which is internal.

See "Top-level commands" on page 372.

Failover planning for Gateway Enforcer appliances

An enterprise can support two Gateway Enforcer appliances that are configured to continue operations when one of the Gateway Enforcer appliances fails. If a Gateway Enforcer appliance fails in a network that is not configured for failover, then network access at that location is automatically blocked. If a Gateway Enforcer appliance fails in a network that does not provide for failover, the clients can no longer connect to the network. The clients continue to be blocked from connecting to the network until the problem with the Gateway Enforcer appliance is corrected.

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

See "Setting up Gateway Enforcer appliances for failover" on page 125.

How failover works with Gateway Enforcer appliances in the network

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

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

- When the first Gateway Enforcer appliance is started, it runs in standby mode. While in standby mode, it queries the network to determine whether another Gateway Enforcer appliance runs. It sends out three queries to search for another Gateway Enforcer. Therefore it can take a few minutes to change its status to Online.
- If the first Gateway Enforcer appliance does not detect another Gateway Enforcer appliance, the first Gateway Enforcer appliance becomes the active Gateway Enforcer appliance.
- While the active Gateway Enforcer appliance runs, it broadcasts failover packets on both the internal and the external networks. It continues to broadcast the failover packets.
- As soon as the second Gateway Enforcer appliance is started, it runs in standby mode. It queries the network to determine whether another Gateway Enforcer appliance runs.
- The second Gateway Enforcer appliance then detects the active Gateway Enforcer appliance that is running and therefore remains in standby mode.
- If the active Gateway Enforcer appliance fails, it stops to broadcast failover packets. The standby Gateway Enforcer appliance no longer detects an active Gateway Enforcer appliance. Therefore it now becomes the active Gateway Enforcer appliance that handles network connections and security at this location.

- If you start the other Gateway Enforcer appliance, it remains the standby Gateway Enforcer appliance because it detects that another Gateway Enforcer appliance is active.

See “Setting up Gateway Enforcer appliances for failover” on page 125.

Where to place Gateway Enforcer appliances for failover in a network with one or more VLANs

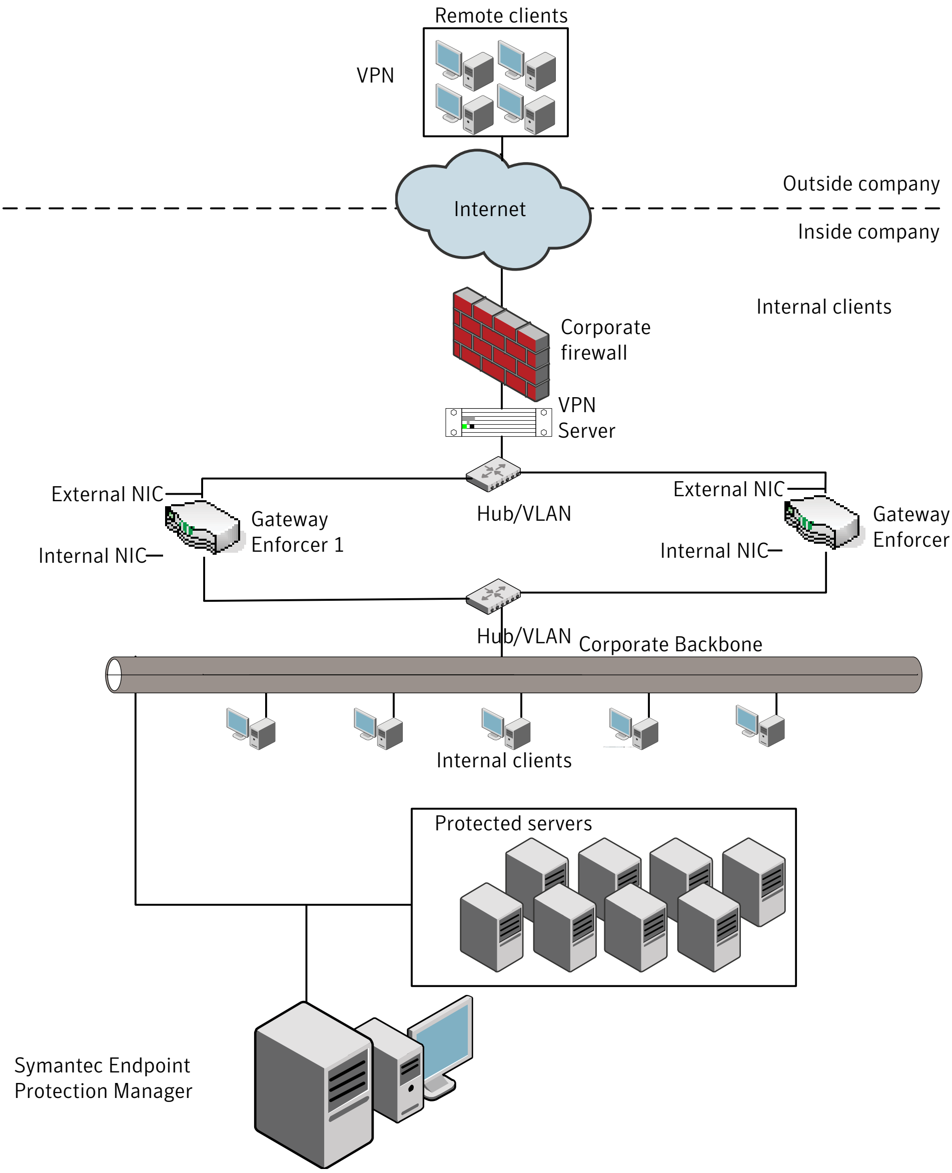
You set up a Gateway Enforcer appliance for failover by its physical location and by the configuration that you perform on the Symantec Endpoint Protection Manager. If you use a hub that supports multiple VLANs, you can use only one VLAN unless you integrate an 802.1q-aware switch instead of a hub.

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 9-2 shows how to set up two Gateway Enforcer appliances for failover to protect network access at a VPN concentrator.

Figure 9-2 Placement of two Gateway Enforcer appliances



See “Setting up Gateway Enforcer appliances for failover” on page 125.

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 122.

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 123.

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 117.

Fail-open planning for a Gateway Enforcer appliance

Fail-open is available for Gateway Enforcer appliance models with a fail-open NIC. Fail-open is an alternative to failover that provides network availability when the Enforcer service is not available.

See "Installing an Enforcer appliance" on page 96.

Chapter 10

Configuring the Symantec Gateway Enforcer appliance from the Symantec Endpoint Protection Manager

This chapter includes the following topics:

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 "Setting up an Enforcer appliance" on page 98.
- Configure the Symantec Gateway Enforcer appliance on the local Gateway Enforcer console during the installation.
  See "Configuring an Enforcer appliance" on page 100.

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

When you install a Gateway Enforcer appliance, a number of default settings and ports are automatically set up. The default settings for the Gateway Enforcer appliance on the Symantec Endpoint Protection Manager allow all clients to connect to the network if the client passes the Host Integrity check. The Gateway Enforcer appliance acts as a bridge. Therefore you can complete the process of setting up the Gateway Enforcer appliance and deploying clients without blocking access to the network.

However, you need to change the default settings on Symantec Endpoint Protection Manager to limit which clients are allowed access without authentication. Optionally, there are other Enforcer default settings for the Gateway Enforcer appliance that you may want to customize before you start enforcement.

Changing Gateway Enforcer appliance configuration settings 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 **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. Select the Gateway Enforcer appliance for which the configuration settings must be changed.

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

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

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

General	Settings for the Enforcer group description and management server list. See "Using general settings" on page 131.
Authentication	Settings for a variety of parameters that affect the client authentication process. If a matching address is still not found, the Gateway Enforcer appliance begins the authentication session and sends the challenge packet. See "Using authentication settings" on page 134.
Auth Range	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. See "Authentication range settings" on page 148.
Advanced	Settings for authentication timeout parameters and Gateway Enforcer appliance message timeouts. Settings for MAC addresses for the trusted hosts that the Gateway Enforcer appliance allows to connect without authentication (optional). Settings for DNS Spoofing and Local Authentication. Settings for protocols to be allowed without blocking clients. See "Using advanced Gateway Enforcer appliance settings" on page 158.
Log Settings	Settings for enabling logging of Server logs, Client Activity logs, and specifying log file parameters. See "About Enforcer reports and logs" on page 272. See "Configuring Enforcer log settings" on page 273.

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 131.

See "Adding or editing the description of a Gateway Enforcer appliance" on page 132.

You cannot add or edit the name of a Gateway Enforcer appliance group in the Symantec Endpoint Protection Manager. You cannot add or edit the IP address or host name of a Gateway Enforcer appliance in the Symantec Endpoint Protection Manager. 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 132.

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 133.

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.

See "About configuring the Symantec Gateway Enforcer appliance on the Symantec Endpoint Protection Manager Console" on page 128.

See "Using general settings" on page 131.

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

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

5. In the **Settings** dialog box, on the **Basic Settings** tab, add or edit a description for the Gateway Enforcer appliance group in the **Description** field.
6. Click **OK**.

Adding or editing the description of a Gateway Enforcer appliance

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

See "Using general settings" on page 131.

See "About configuring the Symantec Gateway Enforcer appliance on the Symantec Endpoint Protection Manager Console" on page 128.

To add or edit the description of a Gateway Enforcer appliance

1. In the Symantec Endpoint Protection Manager Console, click **Admin**.
2. Click **Servers**.
3. Under **View Servers**, select and expand the Gateway Enforcer appliance group whose description you want to add or edit.
4. Select the Gateway Enforcer appliance 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 Gateway Enforcer appliance in the Description field.
7. Click **OK**.

Adding or editing the IP address or host name of a Gateway Enforcer appliance

You can change the IP address or host name of a Gateway Enforcer appliance on the Gateway Enforcer console only during the installation. If you want to change the IP address or host name of a Gateway Enforcer appliance at a later time, you can do so on a Gateway Enforcer console.

See "About the Enforcer appliance CLI command hierarchy" on page 365.

See "About configuring the Symantec Gateway Enforcer appliance on the Symantec Endpoint Protection Manager Console" on page 128.

See "Using general settings" on page 131.

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, management servers, 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 a Gateway Enforcer connects. It also specifies to which Symantec Endpoint Protection 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 management servers at that site are automatically added to the default management server list.

A default management server list includes the management server's IP addresses or host names to which 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.

See “About configuring the Symantec Gateway Enforcer appliance on the Symantec Endpoint Protection Manager Console” on page 128.

See “Using general settings” on page 131.

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

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

3 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.

4 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 Gateway Enforcer appliance to use.

6 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 Gateway Enforcer appliance authentication session. When you apply these changes, they are automatically sent to the selected Gateway Enforcer appliance during the next heartbeat.

See “Authentication settings” on page 134.

Authentication settings

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

Table 10-1 provides more information about the options on the **Authentication** tab.

Table 10-1 Authentication configuration settings for a Gateway Enforcer appliance

Option	Description
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 139.
Time between packets in authentication session (seconds)	The time in seconds between each challenge packet that the Enforcer sends. The default value is 3 seconds. The range is 3 through 10. See "Specifying the frequency of challenge packets to be sent to clients" on page 140.
Time rejected client will be blocked (seconds)	The amount of time in seconds for which a client is blocked after it fails authentication. The default setting is 30 seconds. The range is 10 through 300 seconds. See "Specifying the time period for which a client is blocked after it fails authentication" on page 141.
Time authenticated client will be allowed (seconds)	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 142.

Table 10-1 Authentication configuration settings for a Gateway Enforcer appliance *(continued)*

Option	Description
Allow all clients, but continue to log which clients are not authenticated	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 142.
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 143.
Check the Policy Serial Number on Client before allowing Client into network	If this option is enabled, the Gateway Enforcer appliance verifies that the client has received the latest security policies from the management server. If the policy serial number is not the latest, the Gateway Enforcer notifies the client to update its security policy. The client then forwards the Gateway request to receive a quarantine network configuration. If this option is not enabled and if the Host Integrity check succeeds, the Gateway Enforcer appliance forwards the Gateway request to receive a normal network configuration. The Gateway Enforcer forwards the request even if the client does not have the latest security policy. The default setting is not enabled. See "Having the Gateway Enforcer appliance check the policy serial number on a client" on page 144.

Table 10-1 Authentication configuration settings for a Gateway Enforcer appliance *(continued)*

Option	Description
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 145.
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 147.
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 147.
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 147.

About authentication sessions on a Gateway Enforcer appliance

When a client tries to access the internal network, the Gateway Enforcer establishes an authentication session with it. An authentication session is a set of challenge packets that are sent from a Gateway Enforcer appliance to a client.

During an authentication session, the Gateway Enforcer appliance sends a challenge packet to the client at a specified frequency. The default setting is every three seconds. It keeps sending packets until it receives a response from the client, or until it has sent out the maximum number of packets specified. The default number is 10 packages.

If the client responds and passes authentication, the Gateway Enforcer appliance allows it access to the internal network for a specified number of seconds. The default is 30 seconds. The Gateway Enforcer appliance starts a new authentication session during which the client must respond to retain the connection to the internal network. The Gateway Enforcer appliance disconnects the clients that do not respond or are rejected because they fail authentication.

If the client does not respond or fails authentication, the Gateway Enforcer appliance blocks it for a specified number of seconds. The default is 30 seconds. If another client tries to log on using that same IP address, it has to be reauthenticated.

You can configure the authentication session for each Gateway Enforcer appliance on the management server.

See “Changing Gateway Enforcer appliance configuration settings on a management server” on page 128.

See “Authentication settings” on page 134.

About client authentication on a Gateway Enforcer appliance

The Gateway Enforcer appliance authenticates remote clients before it allows access to the network. Client authentication in the Gateway Enforcer performs the following functions:

- Determines whether to authenticate the client or allow it without authentication

  You can specify individual clients or ranges of IP addresses to trust or to authenticate on the **Auth Range** tab.
- Carries out the authentication session

  You configure the settings for the authentication session on the **Authentication** tab.

Each Gateway Enforcer maintains the following lists of trusted IP addresses that are allowed to connect to the network through the Gateway Enforcer:

- A static list
  The trusted external IP addresses that are configured for the Enforcer on the **Auth Range** tab.
- A dynamic list
  The additional trusted IP addresses that are added and dropped as clients are authenticated, allowed to connect to the network, and finally disconnected.

When traffic arrives from a new client, the Gateway Enforcer appliance determines whether this client is included in the list of trusted client IP addresses. If the client has a trusted IP address, it is allowed on the network with no further authentication.

If the client lacks a trusted IP address, the Gateway Enforcer appliance checks if the trusted IP address is within the client IP 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.

See “Authentication settings” on page 134.

Specifying the maximum number of challenge packets during an authentication session

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

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

- The Gateway Enforcer appliance receives a response from the client.

- The Gateway Enforcer appliance has sent the specified maximum number of packets.

The default setting is 10 packets for the maximum number of challenge packets for an authentication session. The range is from 2 through 100 packets.

See “Using authentication settings” on page 134.

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

1. In the Symantec Endpoint Protection Manager Console, click **Admin**.
2. Click **Servers**.
3. 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. 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. Click **OK**.

Specifying the frequency of challenge packets to be sent to clients

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

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

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

The default setting is every 3 seconds. The range is 3 through 10 seconds.

See “Using authentication settings” on page 134.

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

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

3. 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. Under **Tasks**, click **Edit Group Parameters**.
5. In the **Settings** dialog box, on the **Authentication** tab, under **Authentication Parameters**, type the maximum number of challenge packets that you want the Gateway Enforcer appliance to keep sending to a client during an authentication session in the **Time between packets in authentication session** field.

   The default setting is 3 seconds. The range is from 3 through 10 seconds.

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

Specifying the time period for which a client is blocked after it fails authentication

You can specify the amount of time for which a client is blocked after it fails authentication.

The default setting is 30 seconds. The range is 10 through 300 seconds.

See "Using authentication settings" on page 134.

To specify the time period for which a client is blocked after it fails authentication

1. In the Symantec Endpoint Protection Manager Console, click **Admin**.
2. Click **Servers**.
3. 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. Under **Tasks**, click **Edit Group Properties**.
5. In the **Settings** dialog box, on the **Authentication** tab, under **Authentication Parameters**, type the number of seconds for the amount of time for which a client is blocked after it fails authentication in the **Time rejected client will be blocked (seconds)** field.
6. Click **OK**.

Specifying the time period for which a client is allowed to retain its network connection without reauthentication

You can specify the amount of time in seconds for which a client is allowed to retain its network connection without reauthentication.

The default setting is 30 seconds. The range is 10 through 300 seconds.

See "Using authentication settings" on page 134.

To specify the time period for which a client is allowed to retain its network connection without reauthentication

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

See "Using authentication settings" on page 134.

To allow all clients with continued logging of non-authenticated clients

1. In the Symantec Endpoint Protection Manager Console, click **Admin**.
2. Click **Servers**.
3. 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. 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 **Authentications** tab, click **OK**.

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

The Gateway Enforcer appliance cannot authenticate a client that is running a non-Windows operating system. Therefore non-Windows clients cannot connect to the network unless you specifically allow them to connect to the network without authentication.

The default setting is not enabled.

You can use one of the following methods to enable the clients that support a non-Windows platform to connect to the network:

- Specify each non-Windows client as a trusted host.
- Allow all clients with non-Windows operating systems.

The Gateway Enforcer appliance detects the operating system of the client and authenticates Windows clients. However, it does not allow non-Windows clients to connect to the Gateway Enforcer appliance without authentication.

If you need to have non-Windows clients connect to the network, then you must configure additional settings on the Symantec Endpoint Protection Manager Console.

See "Requirements for allowing non-Windows clients without authentication" on page 120.

See "Using authentication settings" on page 134.

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 Gateway Enforcer appliance for which you want to allow all non-Windows clients to connect to a network.
4. Under **Tasks**, click **Edit Group Properties**.
5. In the **Settings** dialog box, on the **Authentication** tab, check **Allow all clients with non-Windows operating systems**.

   The default setting is not enabled.
6. Click **OK**.

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:

- Retrieves the policy serial number from the Symantec Endpoint Protection Manager.
- Compares the policy serial number with the one that it receives from the client.
- If the policy serial numbers match, the Gateway Enforcer appliance has validated that the client is running an up-to-date security policy.

The default value for this setting is not enabled.

The following guidelines apply:

- If the **Check the Policy Serial Number on Client before allowing Client into network** option is checked, a client must have the latest security policy before it can connect to the network through the Gateway Enforcer appliance. If the client does not have the latest security policy, the client is notified to download the latest policy. The Gateway Enforcer appliance then forwards its Gateway request to receive a quarantine network configuration.
- If the **Check the Policy Serial Number on Client before allowing Client into network** option is not checked and the Host Integrity check is successful, a client can connect to the network. The client can connect through the Gateway Enforcer appliance even if its security policy is not up-to-date.

See “Using authentication settings” on page 134.

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. 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 a user that they cannot connect to the network. The message typically tells the user that a client cannot connect to the network because it does not run the Symantec Network Access Control client.

Most administrators type a brief statement of the need to run the Symantec Endpoint Protection client or the Symantec Network Access Control client. The message may include information about a download site where users can download the required client software. You can also provide a contact telephone number and other relevant information.

This setting is enabled by default. It applies only to clients that do not run the Symantec Endpoint Protection client or the Symantec Network Access Control client.

As soon as you complete this task, the pop-up message appears on the client if the Windows Messenger service is running on the client.

See "Using authentication settings" on page 134.

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

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

   You can select any of the following time periods:

   - Once
     The default value is Once.
   - Every 30 seconds
   - Every minute
   - Every 2 minutes
   - Every 5 minutes
   - Every 10 minutes
8. Type the message that you want to appear in the text box.

   The maximum number of characters is 125. This number includes spaces and punctuation.

   The default message is:

   ```
   You are blocked from accessing the network because you
   do not have the Symantec Client running. You will need to
   install it.
   ```
9. Click **OK**.
10. In the **Settings** dialog box, on the **Authentication** tab, click **OK**.

Redirecting HTTP requests to a Web page

The Gateway Enforcer appliance has an option to redirect HTTP requests to an internal Web server if the client tries to access an internal Web site through a browser and a client is not running on the client. If you do not specify a URL, the Gateway Enforcer appliance pop-up message appears as the HTML body for the first HTML page. You may want to connect users to a Web page that you set up. Clients can download Remediation software from this Web site. The Gateway Enforcer appliance can redirect the HTTP GET request to a URL that you specify.

This setting is enabled by default.

For example, you can redirect a request to a Web server from which the client can download the client software, patches, or up to date versions of applications.

See "Using authentication settings" on page 134.

To redirect HTTP requests to a Web page

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

   This also uses the Gateway Enforcer pop-up message as the HTML body for the first HTML page it sends back to the client.
7. In the **Gateway Settings** dialog box, on the **Authentication** tab, click **OK**.

Authentication range settings

You can configure the following settings:

- Client IP addresses that the Gateway Enforcer appliance authenticate
  See "Adding client IP address ranges to the list of addresses that require authentication" on page 152.
- External IP addresses that the Gateway Enforcer appliance does not authenticate
  See "Specifying trusted external IP addresses" on page 155.
- Internal IP address to which the Gateway Enforcer allows access
  See "Adding a trusted internal IP address for clients on a management server" on page 154.

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 blacklist. You can specify the client IP addresses that tell the Gateway Enforcer appliance to only check specific IP addresses to see if they are running the client and meet required security policies. If a client is not on the Client IP list, then it functions as if it had been assigned a trusted IP address.

In contrast to the Client IP 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.

See "Adding client IP address ranges to the list of addresses that require authentication" on page 152.

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

See "Adding client IP address ranges to the list of addresses that require authentication" on page 152.

Allowing 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.

See "Adding client IP address ranges to the list of addresses that require authentication" on page 152.

Authentication of a subset of clients

You may want to use client IP addresses to have a Gateway Enforcer appliance authenticate a limited subset of clients at a company.

You can have the Gateway Enforcer appliance check only those clients that connect through one subnet if you have already installed the clients on all of the computers. Other clients accessing the corporate network at that location are allowed to pass through without authentication. As the client is installed on other clients, you can add their addresses to the Client IP range or use a different authentication strategy.

See "Adding client IP address ranges to the list of addresses that require authentication" on page 152.

About trusted IP addresses

You work with the following types of trusted IP addresses on a Gateway Enforcer:

- Trusted external IP addresses
  A trusted external IP address is the IP address of an external computer that is allowed to access the corporate network without running the client.
  See "Specifying trusted external IP addresses" on page 155.
- Trusted internal IP addresses
  A trusted internal IP address is the IP address of a computer within the corporate network that any client can access from the outside.
  See "Adding a trusted internal IP address for clients on a management server" on page 154.

You can add trusted IP addresses of both types on the Symantec Endpoint Protection Manager Console. Traffic to the console is always allowed from the Gateway Enforcer appliance.

Trusted external IP addresses

One of the primary duties of a Gateway Enforcer appliance is to check that all computers that try to access the network are running the client. Some computers may not be running the Windows operating system or may not be running the client.

For example, VPN and wireless servers do not typically run the client. In addition, a network setup may include the devices that normally access the network and run an operating system other than Windows. If these computers need to bypass a Gateway Enforcer appliance, you need to make sure that the Gateway Enforcer appliance knows about them. You can accomplish this objective by creating a range of trusted external IP addresses. In addition, you must also assign an IP address from that IP address range to a client.

See "Specifying trusted external IP addresses" on page 155.

Trusted internal IP addresses

A trusted internal IP address represents the IP address of a computer inside the corporate network that external clients can access from the outside. You can make certain internal IP addresses into trusted internal IP addresses.

When you specify trusted internal IP addresses, clients can get to that IP address from outside the corporate network whether or not:

- The client software has been installed on the client computer
- The client complies with a security policy

Trusted internal IP addresses are the internal IP addresses that you want users outside the company to be able to access.

Examples of the internal addresses that you may want to specify as trusted IP addresses are as follows:

- An update server
- A file server that contains antivirus signature files
- A server that is used for remediation
- A DNS server or a WINS server that is required to resolve domain or host names

When a client tries to access the internal network and does not get authenticated by the Gateway Enforcer appliance, the client can be placed in quarantine when:

- The client is not running the client software on the client computer
- The Host Integrity check failed
- The client does not have an up-to-date policy

The client is still allowed to access certain IP addresses; these are the trusted internal IP addresses.

For example, the concept of trusted internal IP addresses may have an external client that needs to access the corporate network to get the client or other needed software. The Gateway Enforcer appliance allows the external client to get to a computer that is on the list of trusted internal IP addresses.

See "Adding a trusted internal IP address for clients on a management server" on page 154.

Adding client IP address ranges to the list of addresses that require authentication

You can specify those clients with IP addresses to which the Gateway Enforcer appliance authenticates.

You want to be aware of the following issues:

- You must check the **Enable** option that is located next to the IP address or range if you want that address to be authenticated. If you want to temporarily disable authentication of an address or range, uncheck **Enable**.
- If you type an invalid IP address, you receive an error message when you try to add it to the Client IP list.

See "When to use client IP ranges" on page 149.

To restrict a client's network access despite authentication

1. In the Symantec Endpoint Protection Manager Console, click **Admin**.
2. Click **Servers**.
3. Under **View Servers**, select and expand the Gateway Enforcer appliance groups.
4. 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 address and an end address of a range, or an IP address plus subnet mask.

10 Click **OK**.

The address information you typed is added to the Client IP Range table, with the **Enable** option selected.

11 Continue to click **Add** and specify any other IP addresses or ranges of addresses that you want the Gateway Enforcer to authenticate.

12 Click **OK**.

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

You may need to edit client IP address ranges that you want to be authenticated.

See "When to use client IP ranges" on page 149.

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 Click **Servers**.

3 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 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.

See "When to use client IP ranges" on page 149.

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. Click **Servers**.
3. 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. 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 appliances. If a client first fails a Host Integrity check and then passes it, you may have up to a 5-minute delay before a client can connect to the network.

See "About trusted IP addresses" on page 150.

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. 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. 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.

See "About trusted IP addresses" on page 150.

To specify trusted external IP addresses

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

See "About trusted IP addresses" on page 150.

To edit a trusted internal or external IP address

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

2 Click **Servers**.

3 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 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, remove the IP address from the Trusted Internal IP Address table.

See "About trusted IP addresses" on page 150.

To remove a trusted internal IP or trusted external IP address

1. In the Symantec Endpoint Protection Manager Console, click **Admin**.
2. Click **Servers**.
3. 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. 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 instances of the Symantec Endpoint Protection Manager.

  If a matching address is still not located, the Gateway Enforcer appliance begins the authentication session and sends the challenge packet.

See “Specifying trusted external IP addresses” on page 155.

See “Adding client IP address ranges to the list of addresses that require authentication” on page 152.

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 158.
- Allow legacy clients
  See “Allowing a legacy client to connect to the network with a Gateway Enforcer appliance” on page 159.
- Enable local authentication
  See “Enabling local authentication on a Gateway Enforcer appliance” on page 160.

When you apply the settings, the changes that have been made are sent to the selected Gateway Enforcer appliance during the next heartbeat.

Specifying packet types and protocols

You can specify that the Gateway Enforcer appliance allows certain packet types to pass through without requiring a client to run or require authentication.

See “Using advanced Gateway Enforcer appliance settings” on page 158.

To specify packet types and protocols

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

See “Using advanced Gateway Enforcer appliance settings” on page 158.

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. Click **Servers**.
3. Under **View Servers**, select and expand the group of Gateway Enforcers appliances.
4. Under **Tasks**, click **Edit Group Properties**.
5. In the Settings dialog box, on the **Advanced** tab, check **Allow legacy clients**.
6. Click **OK**.

Enabling local authentication on a Gateway Enforcer appliance

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

See “Using advanced Gateway Enforcer appliance settings” on page 158.

To enable local authentication on a Gateway Enforcer appliance

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

Chapter 11

Planning for the installation of the DHCP Enforcer appliance

This chapter includes the following topics:

- Installation planning for a DHCP Enforcer appliance
- DHCP Enforcer appliance NIC settings
- Failover planning for DHCP Enforcer appliances
- Fail-open planning for a DHCP Enforcer appliance

Installation planning for a DHCP Enforcer appliance

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.

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

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 162.
- See “DHCP Enforcer appliance IP addresses” on page 164.
- See “Protection of non-Windows clients with DHCP enforcement” on page 165.
- See “About the DHCP server” on page 166.

Where to place DHCP Enforcer appliances in a network

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.

See “Setting up an Enforcer appliance” on page 98.

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.

See “Configuring an Enforcer appliance” on page 100.

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.

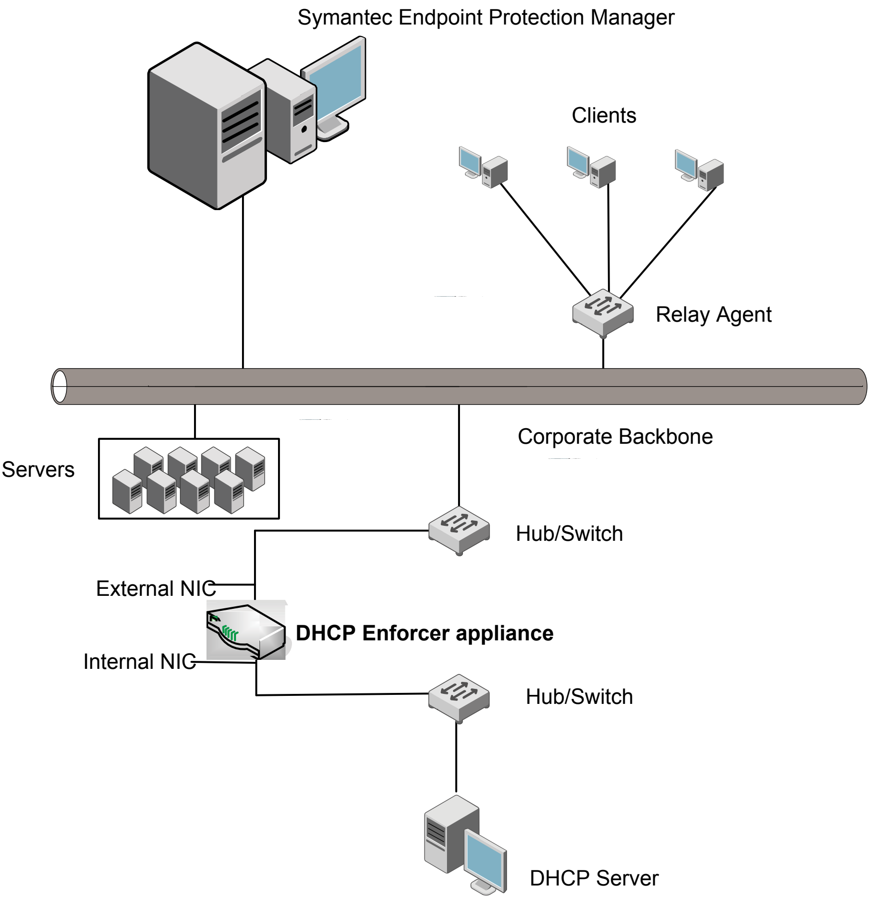
You also must set up a remediation server so that the clients that receive quarantine configurations can connect with the remediation server. Optionally, the Symantec Endpoint Protection Manager can run on the same computer as the remediation server. Neither the Symantec Endpoint Protection Manager nor 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 11-1 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.

Figure 11-1 Placement of a DHCP Enforcer appliance



DHCP Enforcer appliance IP addresses

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

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 Enforcer appliances in a failover configuration:
  - The IP address of the internal NIC on each DHCP Enforcer appliance must be different.
  - The IP address of the external NIC on each DHCP Enforcer appliance must be different.
  - Clients must be able to communicate with the internal IP address of both the active DHCP Enforcer appliance and the standby 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.

See "Installing an Enforcer appliance" on page 96.

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.

See "Installing an Enforcer appliance" on page 96.

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 succeeds, 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.

See “Installing an Enforcer appliance” on page 96.

Normal and quarantine DHCP servers on one DHCP server

You can use the same server for both the normal DHCP server and the quarantine DHCP server. The best practice is to use two servers.

If you want to use one DHCP server as both the normal and quarantine DHCP server, you must 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, 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.

See “Enabling separate normal and quarantine DHCP servers” on page 190.

DHCP Enforcer appliance NIC settings

The network interface cards (NICs) on a Gateway Enforcer appliance or a DHCP Enforcer appliance are 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 “About the Enforcer appliance CLI command hierarchy” on page 365.

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 “About installing an Enforcer appliance” on page 95.

Failover planning for DHCP Enforcer appliances

You 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.

See "Where to place DHCP Enforcer appliances for failover in a network with only one or multiple VLANs" on page 169.

See "Setting up DHCP Enforcer appliances for failover" on page 170.

How failover works with DHCP Enforcer appliances in the network

The operational DHCP Enforcer appliance 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 starts, 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.

See “Setting up DHCP Enforcer appliances for failover” on page 170.

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

Set up a DHCP Enforcer appliance for failover by its physical location and by configuring 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.

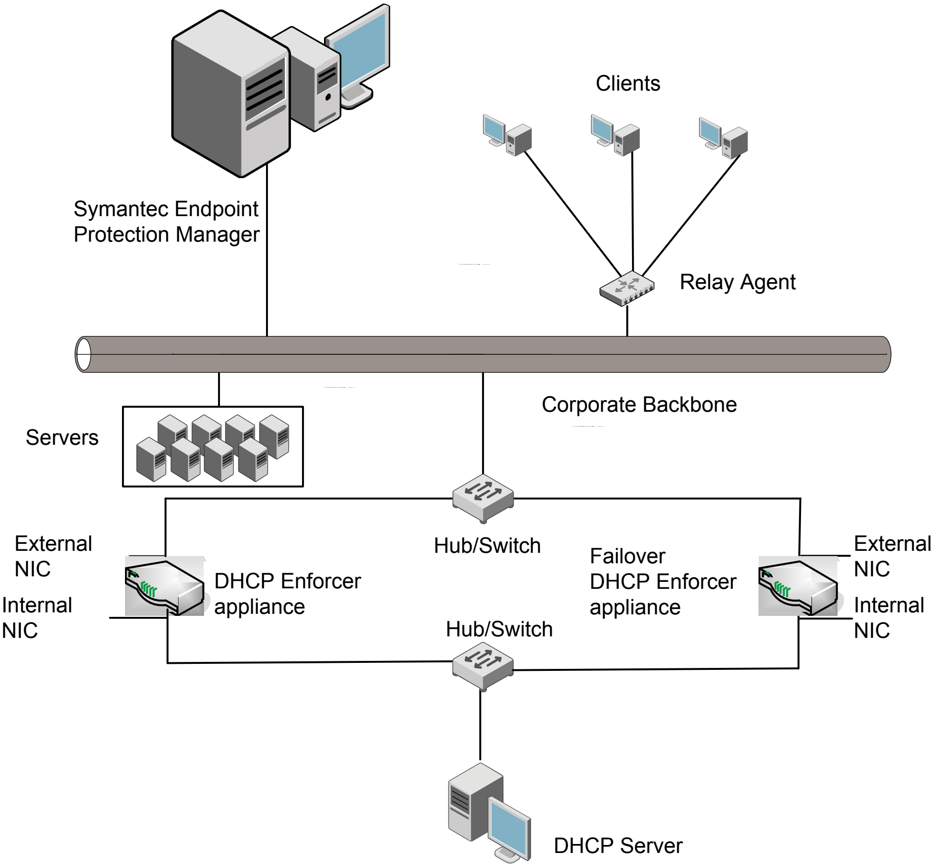
A DHCP Enforcer appliance for failover must be set up on the same network segment. A router or gateway cannot be installed between the two DHCP Enforcer appliances. A router or gateway does not forward the failover packet. The internal NICs must both connect to the internal network through the same switch 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.

See “Setting up DHCP Enforcer appliances for failover” on page 170.

Figure 11-2 shows how to set up two DHCP Enforcer appliances for failover to protect network access at a VPN concentrator.

Figure 11-2 Placement of two DHCP Enforcer appliances



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 168.

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 169.

2. Set up the external NICs and the 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 164.

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.

Fail-open planning for a DHCP Enforcer appliance

Fail-open is available for DHCP Enforcer appliance models with a fail-open NIC. Fail-open is an alternative to failover that provides network availability when the Enforcer service is not available.

See “Installing an Enforcer appliance” on page 96.

Chapter 12

Configuring the DHCP Enforcer appliance on the Symantec Endpoint Protection Manager

This chapter includes the following topics:

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 "Setting up an Enforcer appliance" on page 98.
- Configure the Symantec DHCP Enforcer appliance on the Enforcer console during the installation.
  See "Configuring an Enforcer appliance" on page 100.

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. Click **Servers**.
3. 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 Select the DHCP Enforcer appliance whose configuration settings need to be changed.

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

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

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

General	Settings for the description of the DHCP Enforcer appliance group and management server list. See "Adding or editing the name, description, or IP address of a DHCP Enforcer" on page 176.
Authentication	Settings for a variety of parameters that affect the client authentication process. See "Using authentication settings" on page 179.
DHCP Servers	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 188.
Advanced	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 "About advanced DHCP Enforcer appliance settings" on page 192.
Log settings	Settings for enabling logging of Server logs, Client Activity logs, and specifying log file parameters. See "About Enforcer reports and logs" on page 272. See "Configuring Enforcer log settings" on page 273.

Adding or editing the name, description, or IP address of a DHCP Enforcer

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 176.

See "Adding or editing the description of an Enforcer group with a DHCP Enforcer" on page 176.

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 177.

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 178.

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.

All Enforcers in a group share the same configuration settings.

See "About changing a group name" on page 266.

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.

See "About configuring the Symantec DHCP Enforcer appliance on the Symantec Endpoint Protection Manager Console" on page 174.

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. Click **Servers**.
3. Under **View Servers,** select and expand the Enforcer group whose description you want to add or edit.
4. Under **Tasks**, click **Edit Group Properties**.
5. In the **Settings** dialog box, on the **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 "About configuring the Symantec DHCP Enforcer appliance on the Symantec Endpoint Protection Manager Console" on page 174.

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.

See "About configuring the Symantec DHCP Enforcer appliance on the Symantec Endpoint Protection Manager Console" on page 174.

To add or edit the description of a DHCP Enforcer

1. In the Symantec Endpoint Protection Manager Console, click **Admin**.
2. Click **Servers**.
3. Under **View Servers**, select and expand the Enforcer group that includes the DHCP Enforcer whose description you want to add or edit.
4. Select the DHCP 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 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, management servers, 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 a DHCP Enforcer connects. It also specifies to which Symantec Endpoint Protection 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 management servers at that site are automatically added to the default management server list.

A default management server list includes the management server's IP addresses or host names to which 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.

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 "Adding or editing the name, description, or IP address of a DHCP Enforcer" on page 176.

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. Click **Servers**.
3. 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. 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 authentication settings for a DHCP Enforcer

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

Table 12-1 provides more information about the options on the **Authentication** tab.

Table 12-1 Authentication configuration settings for a DHCP Enforcer

Option	Description
Maximum number of packets per authentication session	The maximum number of challenge packets that the DHCP 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 182.
Time between packets in authentication session	The time (in seconds) between each challenge packet that the Enforcer sends. The default value is 3. See "Specifying the frequency of challenge packets to be sent to clients" on page 183.

Table 12-1 Authentication configuration settings for a DHCP Enforcer *(continued)*

Option	Description
Allow all clients, but continue to log which clients are not authenticated	If this option is enabled, the Enforcer authenticates all users by checking that they are running a client. 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 184.
Allow all clients with non-Windows operating systems	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 185.
Check Policy Serial Number on Client before allowing Client into network	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 186.

Table 12-1 Authentication configuration settings for a DHCP Enforcer *(continued)*

Option	Description
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 DHCP Enforcer appliance to a client about non-compliance" on page 187.

About authentication sessions on a DHCP Enforcer appliance

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:

- The Globally Unique Identifier (GUID)
- Its current Profile Serial Number
- The results of the Host Integrity check

The DHCP Enforcer appliance verifies the client GUID 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 161.

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.

See "About authentication sessions on a DHCP Enforcer appliance" on page 181.

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

1. In the Symantec Endpoint Protection Manager Console, click **Admin**.
2. Click **Servers**.
3. 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.
4. Under **Tasks**, click **Edit Group Properties**.
5. On the **Authentication** tab, under **Authentication Parameters**, type the maximum number of challenge packets to be allowed during an authentication session in the field **Maximum number of packets per authentication session**.

   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 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.

See "About authentication sessions on a DHCP Enforcer appliance" on page 181.

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

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

3 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 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.

See “About authentication sessions on a DHCP Enforcer appliance” on page 181.

To allow all clients with continued logging of non-authenticated clients

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

2 Click **Servers**.

3 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 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 servers without authentication.

See “About authentication sessions on a DHCP Enforcer appliance” on page 181.

To allow non-Windows clients to connect to a network without authentication

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

2 Click **Servers**.

3 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 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.

See "About authentication sessions on a DHCP Enforcer appliance" on page 181.

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. 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 if the Windows Messenger service is running on the client.

See “About authentication sessions on a DHCP Enforcer appliance” on page 181.

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. Under **View Servers**, select and expand the group of Enforcers.
4. Under **Tasks**, click **Edit Group Properties**.
5. In the **Settings** dialog box, on the **Authentication** tab, check **Enable pop-up message on 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 d**ialog 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.

See "Adding a normal DHCP server" on page 190.

See "Adding a quarantine DHCP server" on page 191.

See "Enabling separate normal and quarantine DHCP servers" on page 190.

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 190.

See “Adding a quarantine DHCP server” on page 191.

See “Enabling separate normal and quarantine DHCP servers” on page 190.

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 189.

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 190.

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.

See “About using DHCP servers settings” on page 188.

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. Under **View Servers**, select and expand the group of Enforcers.
4. 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 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.

See "About using DHCP servers settings" on page 188.

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. Under **View Servers**, select and expand the group of Enforcers.
4. Under **Tasks**, click **Edit Group Properties**.
5. In the **Settings** dialog box, on the **DHCP Servers** tab, uncheck **Enable User Class ID**.
6. 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.

See "About using DHCP servers settings" on page 188.

To add a normal DHCP server

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. 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.

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 first forwards DHCP requests to the DHCP server that has the highest priority. The DHCP server then forwards the DHCP requests to the others.

10 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.

See “About using DHCP servers settings” on page 188.

To add a quarantine DHCP server

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

5 In the **Settings** dialog box, on the **DHCP Servers** tab, under **Quarantine DHCP Server**s, 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 t**ab, click **OK**.

About 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 193.
- DHCP message timeout
  See "To specify a DHCP Enforcer appliance's wait period before it grants a client access to the network" on page 194.
- 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 194.
- Enabling DNS spoofing
  See "Preventing DNS spoofing" on page 195.
- Allowing legacy clients
  See "Allowing a legacy client to connect to the network with a DHCP Enforcer appliance" on page 196.
- Enabling local authentication

See “Enabling local authentication on the DHCP Enforcer appliance” on page 196.

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 specified interval, the client is kept in quarantine.

See “About configuring the Symantec DHCP Enforcer appliance on the Symantec Endpoint Protection Manager Console” on page 174.

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. Under **View Servers,** select and expand the group of Enforcers.
4. Select the DHCP Enforcer appliance for which you want to set the configuration setting.
5. 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

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.

See “About configuring the Symantec DHCP Enforcer appliance on the Symantec Endpoint Protection Manager Console” on page 174.

To specify a DHCP Enforcer appliance's wait period before it 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. Under **View Servers**, select and expand the group of Enforcers.
4. Select the DHCP Enforcer appliance for which you want to set the configuration setting.
5. 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. Examples include a non-Windows server or a device such as a printer. 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.

See "About configuring the Symantec DHCP Enforcer appliance on the Symantec Endpoint Protection Manager Console" on page 174.

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

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

7 Click **OK**.

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

The MAC address or addresses that you added now appear in the **Settings** dialog box in the **MAC Address** area.

9 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.

See “About configuring the Symantec DHCP Enforcer appliance on the Symantec Endpoint Protection Manager Console” on page 174.

To prevent DNS spoofing

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

5 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 with 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 with any of the IP addresses that you have specified.

6 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 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.

See "About configuring the Symantec DHCP Enforcer appliance on the Symantec Endpoint Protection Manager Console" on page 174.

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. Under **View Servers**, select and expand the group of DHCP Enforcers appliances.
4. Under **Tasks**, click **Edit Group Properties**.
5. In the **Settings** dialog box, on the **Advanced** tab, check **Allow legacy clients**.
6. Click **OK**.

Enabling local authentication on 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.

See "About configuring the Symantec DHCP Enforcer appliance on the Symantec Endpoint Protection Manager Console" on page 174.

To enable local authentication on the DHCP Enforcer appliance

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

Chapter 13

Installation planning for the LAN Enforcer appliance

This chapter includes the following topics:

- Planning for the installation of a LAN Enforcer appliance
- Failover planning for LAN Enforcer appliances

Planning for the installation of a LAN Enforcer appliance

The LAN Enforcer appliance can perform host authentication and act as a pseudo-RADIUS server (even without a RADIUS server). The Enforcement client acts as an 802.1x supplicant. It responds to the switch's Extensible Authentication Protocol (EAP) challenge with the Host Integrity status and policy number information. The RADIUS server IP address is set to 0 in this case, and no traditional EAP user authentication takes place. The LAN Enforcer appliance checks Host Integrity. It can allow, block, or dynamically assign a VLAN, based on the results of the Host Integrity check.

Another configuration is also available. You can use a LAN Enforcer appliance with a RADIUS server to enforce 802.1x EAP authentication internally in a corporate network. If a LAN Enforcer appliance is used in this configuration, you need to position it so that it can communicate with the RADIUS server.

If your switch supports dynamic VLAN switching, additional VLANs can be configured on the switch and accessed through the LAN Enforcer appliance. The switch can dynamically put the client into a VLAN that is based on the reply from the LAN Enforcer appliance. You may want to add VLANs for quarantine and remediation.

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

See "Where to place LAN Enforcer appliances" on page 198.

Where to place LAN Enforcer appliances

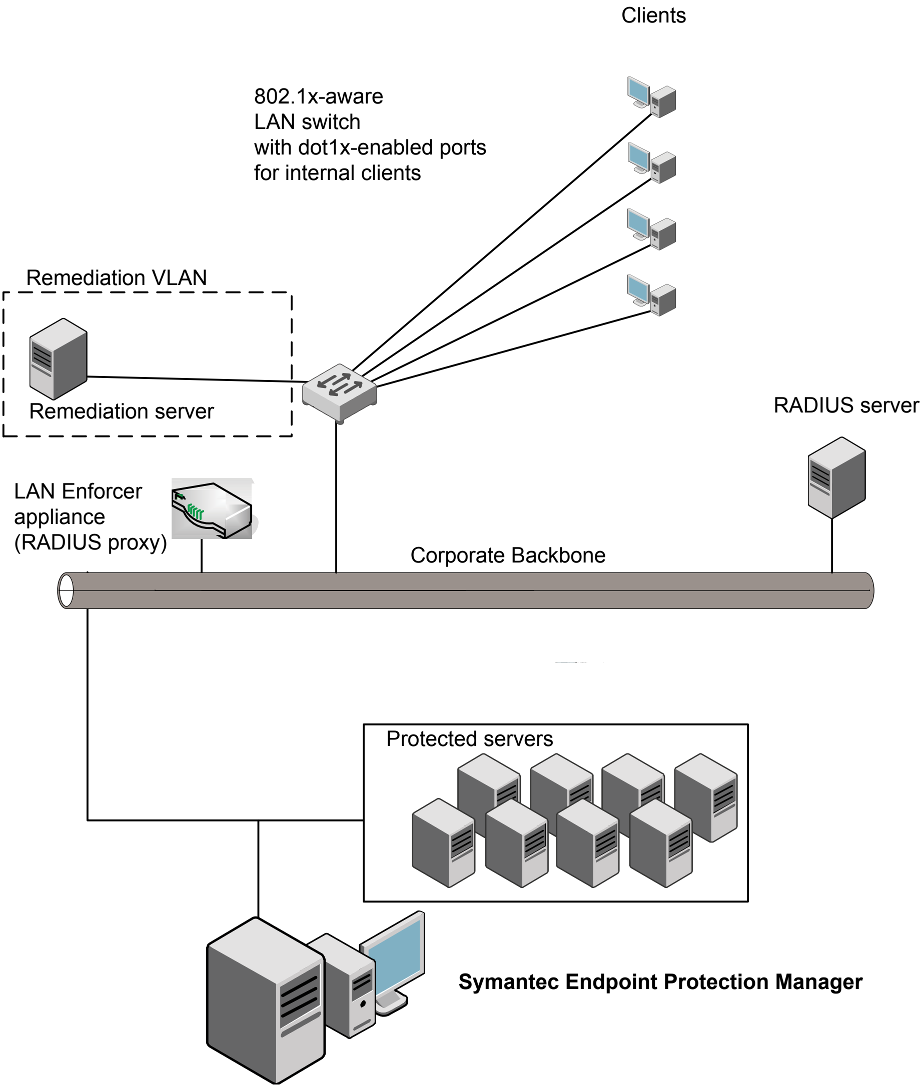
A LAN Enforcer appliance acts as a RADIUS proxy. Administrators typically use a LAN Enforcer appliance with a RADIUS server to enforce 802.1x Extensible Authentication Protocol (EAP) authentication in a corporate network. If you use a LAN Enforcer appliance in this configuration, the LAN Enforcer appliance must be able to communicate with the RADIUS server.

For example, you can connect a LAN Enforcer appliance to an 802.1x-aware LAN switch on an internal VLAN with a Symantec Endpoint Protection Manager, RADIUS server, and clients. A computer that does not have the client software cannot connect to the network. However, the client is directed to a remediation server from which it can obtain the software that it needs to become compliant.

See "Setting up an Enforcer appliance" on page 98.

Figure 13-1 shows an example of where you can place a LAN Enforcer appliance in the overall internal network configuration.

Figure 13-1 Placement of LAN Enforcer appliances



If a switch supports dynamic VLAN switching, additional VLANs can be configured on the 802.1x-aware switch and accessed through the LAN Enforcer appliance. The 802.1x-aware switch can dynamically put the client into a VLAN after it receives a reply from the RADIUS server. Some 802.1x-aware switches also include a default VLAN or guest VLAN feature. If a client has no 802.1x supplicant, the 802.1x-aware switch can put the client into a default VLAN.

You can install the LAN Enforcer appliance so that you can enable EAP authentication throughout the network with the equipment that is already deployed. LAN Enforcer appliances can work with existing RADIUS Servers, 802.1x supplicants, and 802.1x-aware switches. They perform the computer level authentication. It makes sure that the client complies with security policies.

For example, it checks that antivirus software has been updated with the latest signature file updates and the required software patches. The 802.1x supplicant and the RADIUS server perform the user-level authentication. It authenticates the clients who try to connect to the network are the ones who they claim to be.

Alternatively, a LAN Enforcer appliance can also work in transparent mode, removing the need for a RADIUS server. In transparent mode, the client passes Host Integrity information to the 802.1x-aware switch in response to the EAP challenge. The switch then forwards that information to the LAN Enforcer. A LAN Enforcer appliance then sends authentication results back to the 802.1x-aware switch. The information that the LAN Enforcer appliance sends is based on the Host Integrity validation results. Therefore the LAN Enforcer appliance requires no communication with a RADIUS server.

The following configurations are available for a LAN Enforcer appliance:

- 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, specify the same group Enforcer name on the Enforcer console.

If you use a RADIUS server in your network, provide for RADIUS server failover by configuring the LAN Enforcer appliance to connect to multiple RADIUS servers. If all the RADIUS servers that are configured for that LAN Enforcer appliance become disabled, the switch assumes that the LAN Enforcer appliance is disabled. Therefore, the 802.1x-aware switch connects to a different LAN Enforcer appliance that provides additional failover support.

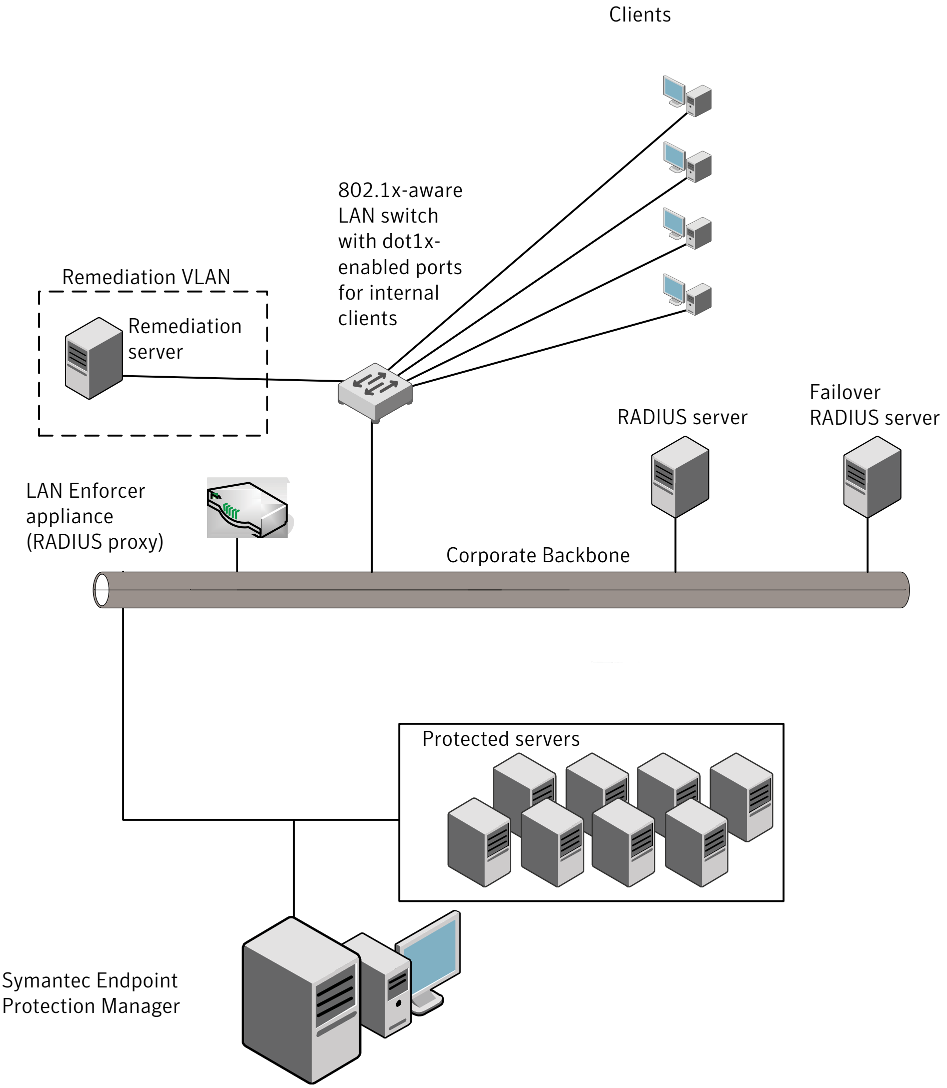
See “Configuring an Enforcer appliance” on page 100.

Where to place LAN Enforcer appliances for failover in a network

Figure 13-2 describes how to provide failover for LAN Enforcer appliances.

See “Failover planning for LAN Enforcer appliances” on page 201.

Figure 13-2 Placement of two LAN Enforcer appliances


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

Chapter 14

Configuring the LAN Enforcer appliance on the Symantec Endpoint Protection Manager

This chapter includes the following topics:

About configuring the Symantec LAN Enforcer on the Symantec Endpoint Protection Manager Console

You can add or edit the configuration settings for the LAN Enforcer in the Symantec Endpoint Protection Manager Console. The Symantec Endpoint Protection Manager is also referred to as the management server.

Before you can proceed, you must complete the following tasks:

- Install the software for the Symantec Endpoint Protection Manager on a computer.
  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.
  See "Setting up an Enforcer appliance" on page 98.
- Configure the Symantec LAN Enforcer appliance on the local LAN Enforcer console during the installation.
  See "Changing LAN Enforcer configuration settings on a Symantec Endpoint Protection Manager Console" on page 206.

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 205.

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 network includes a wireless LAN Enforcer appliance with 802.1x.
- Wireless clients run a supplicant that supports one of these protocols.
- The wireless AP supports one of these protocols.

For wireless connections, the authenticator is the logical LAN port on the wireless AP.

You configure a wireless AP for 802.1x and for switches in the same way. You include wireless APs to the LAN Enforcer settings as part of a switch profile. Wherever an instruction or part of the user interface refers to a switch, use the comparable wireless AP terminology. For example, if you are instructed to select a switch model, select the wireless AP model. If the vendor of the wireless AP is listed, select it for the model. If the vendor is not listed, choose **Others**.

The configuration for wireless AP for 802.1x and for switches include the following differences:

- Only basic configuration is supported.
  The transparent mode is not supported.
- There can also be differences in support for VLANs, depending on the wireless AP.
  Some dynamic VLAN switches may require you to configure the AP with multiple service set identifiers (SSIDs). Each SSID is associated with a VLAN.
  See the documentation that comes with the dynamic VLAN switch.

Based on the wireless AP model that you use, you may want to use one of the following access control options instead of a VLAN:

Access control lists (ACLs)	Some wireless APs support ACLs that enable the network administrator to define policies for network traffic management. You can use the generic option on the LAN Enforcer by selecting the vendor name of the wireless AP. As an alternative, you can select **Others** for the 802.1x-aware switch model (if it is not listed). The generic option sends a generic attribute tag with the VLAN ID or name in it to the access point. You can then customize the access point. Now the access point can read the generic attribute tag for the VLAN ID and match it with the WAP's ACL ID. You can use the Switch Action table as an ACL Action table. Additional configuration on the wireless AP or AP controller may be required. For example, you may need to map the RADIUS tag that is sent to the wireless AP on the AP controller. See the wireless AP documentation for details.
MAC level 802.1x	You can plug the wireless AP into a switch that supports MAC level 802.1x. For this implementation, you must disable 802.1x on the wireless AP. You can only use it on the switch. The switch then authenticates the wireless clients by recognizing the new MAC addresses. After it authenticates a MAC address, it puts that MAC address on the specified VLAN instead of the whole port. Every new MAC address has to be authenticated. This option is not as secure. However, this option enables you to use the VLAN switching capability.

See "Changing LAN Enforcer configuration settings on a Symantec Endpoint Protection Manager Console" on page 206.

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. Click **Servers**.

3. 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. Select the LAN Enforcer appliance whose configuration settings need to be changed.

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

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

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

General	This tab provides the following LAN Enforcer settings: ■ Group name for LAN Enforcer appliances ■ Listening port ■ Description for the LAN Enforcer appliance group ■ Selection of the management server list that the LAN Enforcer uses See “Using general settings” on page 208.
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 212.
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 219.

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 244.
Log settings	Settings for enabling logging of Server logs, Client Activity logs, and specifying log file parameters. See "About Enforcer reports and logs" on page 272. See "Configuring Enforcer log settings" on page 273.

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 210.

See "Adding or editing the description of a LAN Enforcer" on page 210.

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

See "Specifying a listening port for communication between a VLAN switch and a LAN Enforcer" on page 209.

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 209.

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 210.

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 211.

Adding or editing the name of a LAN Enforcer appliance group with a LAN Enforcer

You cannot add or edit the name of a LAN Enforcer appliance group of which a LAN Enforcer appliance is a member. You perform these tasks on the Enforcer console during the installation. If you later want to change the name of a LAN Enforcer appliance group, you can do so on the Enforcer console.

All Enforcers in a group share the same configuration settings.

See “Using general settings” on page 208.

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

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

- The listing port that is used for communication between the VLAN switch and the LAN Enforcer.
  The VLAN switch sends the RADIUS packet to the UDP port.
- The listening port that is used for communication between the LAN Enforcer and a RADIUS server.
  You specify this port when you specify a RADIUS server.

If the RADIUS server is installed on the management server, it should not be configured to use port 1812. The RADIUS servers are configured to use port 1812 as the default setting. Because the management server also uses port 1812 to communicate with the LAN Enforcer, there is a conflict.

See “Using general settings” on page 208.

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

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

2 Click **Servers**.

3 Under **View Servers**, select the Enforcer group.

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

5. In the **LAN Enforcer Setting**s 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. 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.

See "Using general settings" on page 208.

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. Click **Servers**.
3. Under **View Servers**, select and expand the Enforcer group whose description you want to add or edit.
4. Under **Tasks**, click **Edit Group Properties**.
5. In the **Settings** dialog box, on the **Basic Settings** tab, add or edit a description for the Enforcer group in the **Description** field.
6. Click **OK**.

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

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

See "Using general settings" on page 208.

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.

See “Using general settings” on page 208.

To add or edit the description of a LAN Enforcer

1. In the Symantec Endpoint Protection Manager Console, click **Admin**.
2. Click **Servers**.
3. Under **View Servers**, select and expand the Enforcer group that includes the LAN Enforcer whose description you want to add or edit.
4. Select the LAN Enforcer whose description you want to add or edit.
5. Under **Tasks**, click **Edit Enforcer Properties**.
6. In the **Enforcer Properties** dialog box, add or edit a description for the LAN Enforcer in the **Description** field.
7. Click **OK**.

Connecting the LAN Enforcer to 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, management servers, 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 a LAN Enforcer connects. It also specifies to which Symantec Endpoint Protection Manager a LAN Enforcer connects in case of a management server's failure.

A default management server list is automatically created for each site during the initial installation. All available management servers at that site are automatically added to the default management server list.

A default management server list includes the management server's IP addresses or host names to which 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.

See “Using general settings” on page 208.

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. Click **Servers**.
3. 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. 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. 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. 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 213.

See "Editing the name of a RADIUS server group" on page 214.

See "Deleting the name of a RADIUS server group" on page 218.

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 213.

See "Editing the friendly name of a RADIUS server" on page 215.

See "Editing the host name or IP address of a RADIUS server" on page 216.

See "Editing the authentication port number of a RADIUS server" on page 216.

See "Editing the shared secret of a RADIUS server" on page 217.

See "Deleting a RADIUS server" on page 218.

Adding a RADIUS server group name and RADIUS server

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

See "Using RADIUS server group settings" on page 212.

To add a RADIUS server group name and RADIUS server

1. In the Symantec Endpoint Protection Manager Console, click **Admin**.
2. Click **Servers**.
3. Under **View Servers**, select the Enforcer group.
4. Under **Tasks**, click **Edit Group Properties**.
5. In the **LAN Enforcer Settings** dialog box, on the **RADIUS Server Group** tab, click **Add**.

   The name of the RADIUS server group and the IP address of an existing RADIUS server appear in the table.
6. In the **Add RADIUS Server Group** dialog box, type the name of the RADIUS server group in the **Group** text box.

   The name of the RADIUS server group, the host name or IP address of an existing RADIUS server, and the port number of the RADIUS server appear in the table.
7. Click **Add**.

8 In the **Add RADIUS Server** dialog box, type the following:

In the field: Friendly name of RADIUS server	Type a name that easily identifies the name of the RADIUS server when it appears on the list of servers for that group.
In the field: Hostname or IP address	Type the hostname or IP address of the RADIUS server.
In the field: Authentication port	Type the network port on the RADIUS server where the LAN Enforcer sends the authentication packet from the client. The default setting is 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 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.

See "Using RADIUS server group settings" on page 212.

To edit the name of a RADIUS server group

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

2 Click **Servers**.

3. Under **View Servers**, select the Enforcer group of which the LAN Enforcer is a member.
4. Under **Tasks**, click **Edit Group Properties**.
5. In the **LAN Enforcer Settings** dialog box, on the **RADIUS Server Group** tab, click the RADIUS server group whose name you want to change.
6. Click **Edit**.
7. In the **Add RADIUS Server** dialog box, edit the name of the RADIUS server group in the **Group name** field.
8. Click **OK**.
9. In the **LAN Enforcer Settings** dialog box, on the **RADIUS Server Group** tab, click **OK**.

Editing the friendly name of a RADIUS server

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

See "Using RADIUS server group settings" on page 212.

To edit the friendly name of a RADIUS server

1. In the Symantec Endpoint Protection Manager Console, click **Admin**.
2. Click **Servers**.
3. Under **View Servers**, select the Enforcer group of which the LAN Enforcer is a member.
4. Under **Tasks**, click **Edit Group Properties**.
5. In the **LAN Enforcer Settings** dialog box, on the **RADIUS Server Group** tab, click the RADIUS server group that includes the RADIUS server whose friendly name you want to change.
6. Click **Edit**.
7. In the **Add a RADIUS Server** dialog box, edit the friendly name of the RADIUS server in the **Friendly name of RADIUS server** field.
8. Click **OK**.
9. In the **LAN Enforcer Settings** dialog box, on the **RADIUS Server Group** tab, click **OK**.

Editing the host name or IP address of a RADIUS server

You can change the host name or IP address of the RADIUS server at any time if circumstances change.

See "Using RADIUS server group settings" on page 212.

To edit the host name or IP address of a RADIUS server

1. In the Symantec Endpoint Protection Manager Console, click **Admin**.
2. Click **Servers**.
3. Under **View Servers**, select the Enforcer group of which the LAN Enforcer is a member.
4. Under **Tasks**, click **Edit Group Properties**.
5. In the **LAN Enforcer Settings** dialog box, on the **RADIUS Server Group** tab, click the RADIUS server group that includes the RADIUS server whose host name or IP address you want to change.
6. Click **Edit**.
7. In the **Add a RADIUS Server** dialog box, edit the host name or IP address of the RADIUS server in the **Hostname or IP Address** field.
8. Click **OK**.
9. In the **LAN Enforcer Settings** dialog box, on the **RADIUS Server Group** tab, click **OK**.

Editing the authentication port number of a RADIUS server

You can change the authentication port number of the RADIUS server at any time if circumstances change.

See "Using RADIUS server group settings" on page 212.

To edit the authentication port number of a RADIUS server

1. In the Symantec Endpoint Protection Manager Console, click **Admin**.
2. Click **Servers**.
3. Under **View Servers**, select the Enforcer group of which the LAN Enforcer is a member.
4. Under **Tasks**, click **Edit Group Properties**.
5. In the **LAN Enforcer Settings** dialog box, on the **RADIUS Server Group** tab, click the RADIUS server group that includes the RADIUS server whose authentication port number you want to change.

6. Click **Edit**.
7. In the **Add a RADIUS Server** dialog box, edit the authentication port number of the RADIUS server in the **Authentication port** field.
8. Click **OK**.
9. In the **LAN Enforcer Settings** dialog box, on the **RADIUS Server Group** tab, click **OK**.

Editing the shared secret of a RADIUS server

You can change the shared secret of the RADIUS server at any time if circumstances change.

See "Using RADIUS server group settings" on page 212.

To edit the shared secret of a RADIUS server

1. In the Symantec Endpoint Protection Manager Console, click **Admin**.
2. Click **Servers**.
3. Under **View Servers**, select the Enforcer group of which the LAN Enforcer is a member.
4. Under **Tasks**, click **Edit Group Properties**.
5. In the **LAN Enforcer Settings** dialog box, on the **RADIUS Server Group** tab, click the RADIUS server group that includes the RADIUS server whose shared secret you want to change.
6. In the **LAN Enforcer Settings** dialog box, on the **RADIUS Server Group** tab, click **Edit**.
7. In the **Add a RADIUS Server** dialog box, edit the shared secret of the RADIUS server in the **Shared secret** field.

   The shared secret is used for encrypted communication between the RADIUS server and the LAN Enforcer. The shared secret between a RADIUS server and a LAN Enforcer can be different from the shared secret between an 802.1x-aware switch and a LAN Enforcer. The shared secret is case sensitive.
8. Edit the shared secret of the RADIUS server in the **Confirm shared secret** field.
9. Click **OK**.
10. In the **LAN Enforcer Settings** dialog box, on the **RADIUS Server Group** tab, click **OK**.

Deleting the name of a RADIUS server group

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

See "Using RADIUS server group settings" on page 212.

To delete the name of a RADIUS server group

1. In the Symantec Endpoint Protection Manager Console, click **Admin**.
2. Click **Servers**.
3. Under **View Servers**, select the Enforcer group of which the LAN Enforcer is a member.
4. Under **Tasks**, click **Edit Group Properties**.
5. In the **LAN Enforcer Settings** dialog box, on the **RADIUS Server Group** tab, click the RADIUS server group whose name you want to delete.
6. Click **Remove**.
7. 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.

See "Using RADIUS server group settings" on page 212.

To delete a RADIUS server

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

9 Click **OK**.

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

Using switch settings

You configure a switch policy when you specify LAN Enforcer settings for switches. A switch policy is a collection of settings that is applied to a group of switches of the same manufacturer or model. The only information that you need to enter separately for individual switches is the IP address of the switch.

See "Adding an 802.1x switch policy for a LAN Enforcer appliance with a wizard" on page 224.

See "Editing basic information about the switch policy and 802.1x-aware switch" on page 231.

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 224.

See "Editing basic information about the switch policy and 802.1x-aware switch" on page 231.

You need to specify the following information for the set of 802.1x-aware switches to which the switch policy applies:

- A friendly switch name of your choice

- IP address, IP range, or subnet

See "Adding an 802.1x switch policy for a LAN Enforcer appliance with a wizard" on page 224.

See "Editing information about the 802.1x-aware switch" on page 236.

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 224.

See "Editing VLAN information for the switch policy" on page 237.

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 224.

About the support for attributes of switch models

When you configure the LAN Enforcer appliance, you specify the model of the 802.1x-aware switch. Different 802.1x-aware switches look for different attributes to determine which client can access the VLAN. Some switches identify VLANs by VLAN ID and others by VLAN Name. Some devices have limited or no VLAN support.

The LAN Enforcer appliance forwards attributes from the RADIUS server to the switch. If necessary, however, it modifies or appends the VLAN attribute based on the switch type by using supported values. If a conflict exists between the vendor-specific attribute information that the RADIUS server sends and the vendor-specific VLAN attribute information that the LAN Enforcer uses, the LAN Enforcer removes the vendor-specific information that the RADIUS server sends.

The LAN Enforcer then replaces that information with the information that appears in Table 14-1.

If you want to keep the attributes from the RADIUS server, you can select an action called **Open Port**. With this action, the LAN Enforcer forwards all attributes from the RADIUS server to the 802.1x-aware switch without any modifications.

The 802.1x-aware switch model can use VLAN ID or VLAN Name to perform dynamic VLAN assignments. Specify both the VLAN ID and VLAN name when you provide VLAN information for the LAN Enforcer, with the exception of the Aruba switch.

See "Changing LAN Enforcer configuration settings on a Symantec Endpoint Protection Manager Console" on page 206.

Table 14-1 describes the 802.1x-aware switch models and attributes.

Table 14-1 Support for attributes of switch models

Switch model	Attributes added by LAN Enforcer	Comments
Airespace Wireless Controller	The vendor code is 14179. The vendor-assigned attribute number is 5. The attribute format is "string."	VLAN Name is used. Name is case sensitive.
Alcatel	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.	VLAN ID is used.
Aruba	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.	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.

Table 14-1 Support for attributes of switch models *(continued)*

Switch model	Attributes added by LAN Enforcer	Comments
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 three 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 14-1 Support for attributes of switch models *(continued)*

Switch model	Attributes added by LAN Enforcer	Comments
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 the Enterasys switch. The name is case sensitive.

Extreme	Vendor Specific (#26) Vendor ID is 1916 for Extreme. VLAN Name is added after the Vendor ID. All vendor-specific attributes from RADIUS server with an ID of 1916 are removed in case of conflict.	VLAN Name is used. The name is case sensitive.

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

You can add multiple 802.1x-aware switches for use with a LAN Enforcer appliance as part of a switch policy. You must enter the information that is needed to configure the LAN Enforcer appliance interaction with the switch.

See “Using switch settings” on page 219.

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**.
2. Click **Servers**.
3. Under **View Servers**, select the Enforcer group.
4. Under **Tasks**, click **Edit Group Properties**.
5. In the **LAN Enforcer Settings** dialog box, on the **Switch** tab, click **Add**.
6. In the **Welcome to the Switch Policy Configuration Wizard** panel of the **Switch Policy Configuration Wizard,** click **Next**.
7. In the **Basic Information** panel of the **Switch Policy Configuration Wizard**, complete the following tasks:

Switch policy name	Type a name of your choice that identifies the switch policy. For example, you can use the manufacturer's name and model as the name for the switch policy name.

Switch model	The LAN Enforcer uses the switch model to determine the vendor-specific RADIUS server attribute. Select one of the following 802.1x-aware models from the list of supported switches: - Other If your model is not listed, select **Other** to use a generic RADIUS server attribute. - 3Com - Alcatel switch - Cisco Catalyst Series - Enterasys 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 **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 it.
Encrypted password or Shared secret	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.
Confirm encrypted password or shared secret	You must type the encrypted password or shared secret again.
RADIUS server group	If you use the LAN Enforcer appliance with a RADIUS server, you must select the RADIUS server group from the available RADIUS server group list.

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 this option to allow the LAN Enforcer appliance to forward the RADIUS packets that contain other authentication protocols besides EAP. Other protocols include Challenge Handshake Authentication Protocol (CHAP) and PAP. The default setting is enabled.

8. In the **Basic Information** panel of the **Switch Policy Configuration Wizard**, click **Next**.
9. In the **Switch List** panel of the **Switch Policy Configuration Wizard**, click **Add**.

10 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 th**e 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.

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

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

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

14 In the **Add VLAN** dialog box, complete the following tasks:

VLAN ID	Type an integer that can range from 1 to 4094 in the VLAN ID field. The VLAN ID must be the same as the one that is configured on the 802.1x-aware switch except for the Aruba switch. If you plan to add VLAN information about an Aruba switch, you may want to configure VLAN and role information differently than you have for other 802.1x switches. See "Configuring VLAN and role information on the 802.1x-aware Aruba switch" on page 239.
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 239.
Send customized RADIUS attributes to switch	Check **Send customized RADIUS attributes to switch** if you want the LAN Enforcer to send a customized RADIUS attribute to the 802.1x-aware switch. An attribute can be an access control list (ACL). See "About the support for attributes of switch models" on page 220.
Customized attributes in hex format	Type the RADIUS attribute in hex format. The length must be even.

When you specify a switch policy for a LAN Enforcer, you use the **VLAN** tab to add the VLAN information for each VLAN that is configured on the switch. You want the switch policy to be available for use by the LAN Enforcer as an action. The best practice is to specify at least one remediation VLAN.

15 Click **OK**.

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

17 In the **Switch Action Configuration** panel of the **Switch Policy Configuration Wizard**, click **Add**.

18 In the **Add Switch Action** dialog box, complete the following tasks:

Host Authentication	Click any of the following conditions: - Passed - Failed - Unavailable - Ignore Result A typical situation in which a Host Integrity check becomes unavailable would be the result of a client not running. If you set Host Authentication to Unavailable, you must also set Policy Check to Unavailable.
User Authentication	Click any of the following conditions: - Passed The client has passed user authentication. - Failed The client has not passed user authentication. - Unavailable The user authentication result is always unavailable if user authentication is not performed in transparent mode. If you use the LAN Enforcer in transparent mode, you must create an action for the Unavailable condition. If you use the basic configuration, you may also want to configure an action for the user authentication as an error condition. For example, an 802.1x supplicant uses an incorrect user authentication method or the RADIUS server fails in the middle of the authentication transaction. The user authentication's Unavailable condition may also occur on some RADIUS servers if the user name does not exist in the RADIUS database. For example, this problem may occur with Microsoft IAS. Therefore you may want to test the condition of a missing user name with your RADIUS server. You may want to see whether it matches the Failed or Unavailable user authentication conditions. - Ignore Result A typical situation in which a Host Integrity check becomes unavailable would be the result of a client not running. If you set Policy Check to Unavailable, you must also set Host Authentication to Unavailable.

Policy Check	Click any of the following conditions: ■ Passed The client has passed the Policy Check. ■ Failed The client has not passed the Policy Check. ■ Unavailable The Unavailable result for the policy may occur under the following conditions: ■ If the client has an invalid identifier, then the LAN Enforcer cannot obtain any policy information from the management server. This problem can occur if the management server that deployed the client policy is no longer available. ■ If the client is first exported and installed before it connects to the management server and receives its policy. ■ Ignore Result
Action	You can select the following actions that the 802.1x-aware switch performs when the conditions are met: ■ Open Port The 802.1x-aware switch allows network access on the default VLAN to which the port is normally assigned. It also allows network access on the VLAN that is specified in an attribute that is sent from the RADIUS server. Therefore the support of users having VLAN access is based on user ID and user role. The default action is Open Port. ■ Switch to VLAN-*test* Allows access to the specified VLAN. The VLANs that are available to select are the ones that you configured previously. ■ Close Port Deny network access on the default or RADIUS-specified VLAN. On some switch models, depending on the switch configuration, the port is assigned to a guest VLAN. For the Aruba switch, you can restrict access according to a specified role as well as a specified VLAN. The restrictions depend on how you configured the VLAN information for the switch policy.

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

20 In the **Switch Action Configuration** panel of the **Switch Policy Configuration Wizard**, in the **Switch Action** table, click the switch action policy whose priority you want to change.

The LAN Enforcer checks the authentication results against the entries in the switch action table in the order from top to bottom of the table. After it finds a matching set of conditions, it instructs the 802.1x-aware switch to apply that action. You can change the sequence in which actions are applied by changing the order in which they are listed in the table.

21 Click **Move Up** or **Move Down**.

22 Click **Next**.

23 In the **Complete the Switch Policy Configuration** panel of the **Switch Policy Configuration Wizard**, click **Finish**.

Editing basic information about the switch policy and 802.1x-aware switch

You can change the following parameters about the switch policy and the 802.1x-aware switch:

- Switch policy name
  See "Editing the name of a switch policy" on page 231.
- Switch model
  See "Selecting a different switch model for the switch policy" on page 232.
- Shared secret
  See "Editing an encrypted password or shared secret" on page 233.
- RADIUS server group
  See "Selecting a different RADIUS server group" on page 234.
- Reauthentication time period
  See "Editing the reauthentication period" on page 234.
- Forwarding protocols besides EAP
  See "Enabling protocols other than EAP" on page 235.

Editing the name of a switch policy

You can edit the name of the switch policy at any time if circumstances change.

See "Switch settings" on page 219.

To edit the name of a switch policy

1. In the Symantec Endpoint Protection Manager Console, click **Admin**.
2. Click **Servers**.
3. Under **View Servers**, select the Enforcer group.
4. Under **Tasks**, click **Edit Group Properties**.
5. In the **LAN Enforcer Settings** dialog box, on the **Switch** tab in the **Switch Policy** table, click the switch policy that you want to change.
6. Click **Edit**.
7. In the **Edit Switch Policy for *name of switch policy*** dialog box, on the **Basic Information** tab, edit the name of the switch policy in the **Switch policy name** field.
8. Click **OK**.
9. In the **LAN Enforcer Settings** dialog box, on the **Switch** tab, click **OK**.

Selecting a different switch model for the switch policy

You can select a different switch model for the switch policy at any time if circumstances change.

See “Switch settings” on page 219.

To select a different switch model for the switch policy

1. In the Symantec Endpoint Protection Manager Console, click **Admin**.
2. Click **Servers**.
3. Under **View Servers**, select the Enforcer group.
4. Under **Tasks**, click **Edit Group Properties**.
5. In the **LAN Enforcer Settings** dialog box, on the **Switch** tab in the **Switch Policy** table, click the switch policy whose switch mode you want to change.
6. Click **Edit**.
7. In the **Edit Switch Policy for *name of switch policy*** dialog box, on the **Basic Information** tab, select a different switch model from the following Switch model list:
   - Other
     If your model is not listed, select **Other** to use a generic RADIUS server attribute.
   - 3Com

- Alcatel switch
- Cisco Catalyst Series
- Enterasys 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 it.

8 Click **OK**.

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

Editing an encrypted password or shared secret

You can edit the shared secret at any time if circumstances change.

See "Switch settings" on page 219.

To edit an encrypted password or shared secret

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

2 Click **Servers**.

3 Under **View Servers**, select the Enforcer group.

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

5 In the **LAN Enforcer Settings** dialog box, on the **Switch** tab in the **Switch Policy** table, click the switch policy whose shared secret you want to change.

6 Click **Edit**.

7 In the **Edit Switch Policy for *name of switch policy*** dialog box, on the **Basic Information** tab, edit the name of the shared secret in the **Shared secret** field.

8 Edit the name of the shared secret in the **Confirm shared secret** field.

9 Click **OK**.

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

Selecting a different RADIUS server group

You can select a different RADIUS server group at any time if circumstances change.

See "Switch settings" on page 219.

To select a different RADIUS server group

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

2 Click **Servers**.

3 Under **View Servers**, select the Enforcer group.

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

5 In the **LAN Enforcer Settings** dialog box, on the **Switch** tab in the **Switch Policy** table, click the switch policy whose shared secret you want to change.

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

7 In the **Edit Switch Policy for *name of switch policy*** dialog box, on the **Basic Information** tab, select a different RADIUS server group from the RADIUS server group list.

   You must have added more than one RADIUS server group before you can select a different RADIUS server group.

8 Click **OK**.

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

Editing the reauthentication period

You can edit the reauthentication period at any time if circumstances change.

You must specify the amount of time in seconds during which the client must be reauthenticated. Otherwise the client is removed from the list of connected clients and disconnected from the network.

You should set the reauthentication period to be at least double the amount of time of the reauthentication interval on the switch.

For example, if the reauthentication interval on the switch is 30 seconds, the LAN Enforcer reauthentication period should be at least 60 seconds. Otherwise the

LAN Enforcer assumes that the client is timed out. Therefore the client does not release and renew its IP address.

The default setting is 30 seconds.

See "Switch settings" on page 219.

To edit the reauthentication period

1. In the Symantec Endpoint Protection Manager Console, click **Admin**.
2. Click **Servers**.
3. Under **View Servers**, select the Enforcer group.
4. Click **Edit Group Properties**.
5. In the **LAN Enforcer Settings** dialog box, on the **Switch** tab in the **Switch Policy** table, click the switch policy that you want to change.
6. Click **Edit**.
7. In the **Edit Switch Policy for *name of switch policy*** dialog box, on the **Basic Information** tab, edit the reauthentication period in the Reauthentication period in seconds field.
8. Click **OK**.
9. In the **LAN Enforcer Settings** dialog box, on the **Switch** tab, click **OK**.

Enabling protocols other than EAP

You can make the selections that allow the LAN Enforcer to forward the RADIUS packets that contain other authentication protocols besides EAP.

Other protocols include:

- Challenge Handshake Authentication Protocol (CHAP)
- PAP

The default setting is enabled.

See "Switch settings" on page 219.

To enable protocols other than EAP

1. In the Symantec Endpoint Protection Manager Console, click **Admin**.
2. Click **Servers**.
3. Under **View Servers**, select the Enforcer group.
4. Click **Edit Group Properties**.
5. In the **LAN Enforcer Settings** dialog box, on the **Switch** tab in the **Switch Policy** table, click the switch policy that you want to change.

6. In the **LAN Enforcer Settings** dialog box, on the **Switch** tab in the Switch Policy table, click **Edit**.
7. In the **Edit Switch Policy for *name of switch policy*** dialog box, on the **Basic Information** tab, check **Enable protocols besides EAP**.

   You can have the following protocols forwarded:

   - Challenge Handshake Authentication Protocol (CHAP)
   - PAP
8. Click **OK**.
9. In the **LAN Enforcer Settings** dialog box, on the **Switch** tab, click **OK**.

Editing information about the 802.1x-aware switch

You can change the following parameters about the 802.1x-aware switch:

- Change of IP address, host name, or subnet for an 802.1x-aware switch
  See "Editing the IP address, host name, or subnet of an 802.1x-aware switch" on page 236.
- Removal of an 802.1x-aware switch from switch list
  See "Deleting an 802.1x-aware switch from the switch list" on page 237.

Editing the IP address, host name, or subnet of an 802.1x-aware switch

You can change the IP address, hostname, or subnet of an 802.1x-aware switch at any time if circumstances require it.

See "About the support for attributes of switch models" on page 220.

To edit the IP address, hostname, and subnet of an 802.1x-aware switch

1. In the Symantec Endpoint Protection Manager Console, click **Admin**.
2. Click **Servers**.
3. Under **View Servers**, select the Enforcer group.
4. Under **Tasks**, click **Edit Group Properties**.
5. In the **LAN Enforcer Settings** dialog box, on the **Switch** tab in the **Switch Policy** table, click the switch policy that you want to change.
6. Click **Edit**.
7. In the **Edit Switch Policy for *name of switch policy*** dialog box, on the **Switch Address** tab, check **Edit All**.

8 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*

9 Click **OK**.

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

Deleting an 802.1x-aware switch from the switch list

You can delete an 802.1x-aware switch from the switch list at any time if circumstances require it.

See “About the support for attributes of switch models” on page 220.

To delete an 802.1x-aware switch

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

2 Click **Servers**.

3 Under **View Servers**, select the Enforcer group.

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

5 In the **LAN Enforcer Settings** dialog box, on the **Switch** tab in the **Switch Policy** table, click the 802.1x-aware switch that you want to delete from the switch list.

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

7 Click **OK**.

Editing VLAN information for the switch policy

You can change the following parameters about VLANs on the 802.1x-aware switch:

- Change the VLAN ID and VLAN name of an 802.1x-aware switch
  See “Editing the VLAN ID and VLAN name of an 802.1x-aware switch” on page 238.
- 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 239.

- Removal of VLANs on an 802.1x-aware switch

  See "Deleting the VLANs on an 802.1x-aware switch" on page 239.

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

You can change the VLAN ID and VLAN name of an 802.1x-aware switch at any time if circumstances require it.

Some switches, such as the Cisco switch, have a guest VLAN feature. The guest VLAN is normally used if EAP user authentication fails. If EAP authentication fails, the switch connects the client to the guest VLAN automatically.

If you use the LAN Enforcer for VLAN switching, it is recommended that you do not use the reserved guest VLAN when you set up VLANs and actions on the LAN Enforcer. Otherwise the 802.1x supplicant may respond as if EAP authentication failed.

When setting up VLANs, make sure that all of them can communicate with the management server.

See "Switch settings" on page 219.

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

1. In the Symantec Endpoint Protection Manager Console, click **Admin**.
2. Click **Servers**.
3. Under **View Servers**, select the Enforcer group.
4. Under **Tasks**, click **Edit Group Properties**.
5. In the **LAN Enforcer Settings** dialog box, on the **Switch** tab in the **Switch Policy** table, click the switch policy whose VLAN information you want to change.
6. Click **Edit**.
7. In the **Edit Switch Policy for *name of switch policy*** dialog box, on the **Switch Address** tab, select the VLAN that you want to edit.
8. On the **VLAN** tab, check **Edit**.
9. In the **Edit VLAN** dialog box, edit the VLAN ID in the **VLAN ID** field.

10 Edit the VLAN name in the **VLAN name** field.

   If you plan to edit VLAN information about an Aruba switch, you may want to configure VLAN and role information somewhat differently than you have for other 802.1x switches.

   See "Configuring VLAN and role information on the 802.1x-aware Aruba switch" on page 239.

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

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

Deleting the VLANs on an 802.1x-aware switch

You can delete the VLANs on an 802.1x-aware switch at any time if circumstances require it.

See "Switch settings" on page 219.

To delete the VLANs on an 802.1x-aware switch

1. In the Symantec Endpoint Protection Manager Console, click **Admin**.
2. click **Servers**.
3. Under **View Servers**, select the Enforcer group.
4. Under **Tasks**, click **Edit Group Properties**.
5. In the **LAN Enforcer Settings** dialog box, on the **Switch** tab in the **Switch Policy** table, click the switch policy whose VLAN information you want to delete.
6. Click **Edit**.
7. In the **Edit Switch Policy for *name of switch policy*** dialog box, on the **Switch Address** tab, select the VLAN that you want to delete.
8. On the **VLAN** tab, check **Remove**.
9. Click **OK**.
10. In the **LAN Enforcer Settings** dialog box, on the **Switch** tab, click **OK**.

Configuring VLAN and role information on the 802.1x-aware Aruba switch

If you use an Aruba switch, you can leave the VLAN ID or the VLAN name field blank. However, for other switches, you must enter information in both fields. For the Aruba switch, you can use these fields to specify either a VLAN or a role or both as follows:

- To specify a VLAN, enter the VLAN ID in the VLAN ID field.
- To specify a role, enter the role name in the VLAN name field.

For the Aruba switch you can also use this dialog box to set up separate switch actions for multiple roles on one VLAN or multiple VLANS for one role.

See “Switch settings” on page 219.

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 241.
- 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 242.
- Select different actions
  See “Selecting different actions” on page 243.

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

When configuring switch policies, note the following:

- The Switch Action table must contain at least one entry.
- If you do not select an action for a particular combination of results, the default action, Open Port, is performed.
- To specify a default action for any possible combination of results, select Ignore Result for all three results.
- When you add the actions to the table, you can edit any cell by clicking on the right corner of a column and row to display a drop-down list.

- Some switches, such as the Cisco switch, have a guest VLAN feature. The guest VLAN is normally intended to be used if user authentication fails. In other words, if user authentication fails, the switch connects the client to the guest VLAN automatically.

  If you use the LAN Enforcer for VLAN switching, it is recommended that you do not use the reserved guest VLAN when setting up VLANs and actions on the LAN Enforcer. Otherwise the 802.1x supplicant may respond as though user authentication failed.
- If you deploy clients and are not ready to implement the full capabilities of the LAN Enforcer, you can specify an action of allowing access to the internal network that is based on the condition Ignore Result for the Host Integrity check and Policy Check. If you want to disregard the user authentication results and allow network access regardless of the results, you can do so with the condition Ignore Result for User Authentication results.

See "Setting the order of condition checking" on page 241.

See "Selecting a different Host Authentication, User Authentication, or Policy Check condition" on page 242.

See "Selecting different actions" on page 243.

Setting the order of condition checking

You can change a different Host Authentication, User Authentication, or Policy Check condition for a switch policy at any time if circumstances require it.

You can add an entry to the Switch Action table for each of the possible combinations of authentication results.

When you set up the conditions to check for, remember that the only circumstance in which all three results can be Pass or Fail is in the basic configuration. In the basic configuration, the client runs both an 802.1x supplicant that provides information about user authentication and a client that provides information about Host Integrity and the Policy Serial Number.

If you run only an 802.1x supplicant without a client, the results for the Host Integrity check and Policy Check are always unavailable. If you run in transparent mode without a user authentication check, the user authentication result is always Unavailable.

The LAN Enforcer checks the authentication results against the entries in the table in the order from top to bottom of the table. After the LAN Enforcer finds a matching set of conditions, it instructs the 802.1x-aware switch to apply that action. You can change the sequence in which actions are applied by changing the order in which they are listed in the table.

If a LAN Enforcer cannot locate any entry that matches the current condition, a CLOSE PORT action is taken.

See "About issues with the switch policy, associated conditions, and actions" on page 240.

To set the order of condition checking

1. In the Symantec Endpoint Protection Manager Console, click **Admin**.
2. In the Admin page, click **Servers**.
3. Under **View Servers**, select the Enforcer group.
4. Under **Tasks**, click **Edit Group Properties**.
5. In the **LAN Enforcer Settings** dialog box, on the **Switch** tab in the **Switch Policy** table, click the switch policy whose order of conditions checking you want to change.
6. Click **Edit**.
7. In the **Edit Switch Policy for *name of switch policy*** dialog box, on the **Action** tab, select the switch policy whose order of conditions checking you want to change.
8. Click **Move Up** or **Move Down**.
9. Click **OK**.
10. In the **LAN Enforcer Settings** dialog box, on the **Switch** tab, click **OK**.

Selecting a different Host Authentication, User Authentication, or Policy Check condition

You can select a different Host Authentication, User Authentication, or Policy Check condition for a switch policy at any time if circumstances require it.

See "About issues with the switch policy, associated conditions, and actions" on page 240.

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

1. In the Symantec Endpoint Protection Manager Console, click **Admin**.
2. Click **Servers**.
3. Under **View Servers**, select the Enforcer group.
4. Under **Tasks**, click **Edit Group Properties**.

5 In the **LAN Enforcer Settings** dialog box, on the **Switch** tab in the **Switch Policy** table, click the switch policy whose authentication conditions you want to change.

6 Click **Edit**.

7 In the **Edit Switch Policy for *name of switch policy*** dialog box, on the **Action** tab, click any of the authentication conditions that you want to change in any of the following columns:

- Host authentication
- User authentication
- Policy check

8 Select any of the following actions that the 802.1x-aware switch needs to take when certain criteria are met:

- Host authentication result: Pass, Fail, Unavailable, or Ignore Result
- User authentication result: Pass, Fail, Unavailable, or Ignore Result
- Policy Check result: Pass, Fail, Unavailable, or Ignore Result

9 Click **OK**.

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

Selecting different actions

You can select the different actions that the 802.1x-aware switch can take when certain criteria are met:

See “About issues with the switch policy, associated conditions, and actions” on page 240.

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

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

2 Click **Servers**.

3 Under **View Servers**, select the Enforcer group.

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

5 In the **LAN Enforcer Settings** dialog box, on the **Switch** tab in the **Switch Policy** table, click the switch policy whose actions you want to change.

6 Click **Edit**.

7. On the **Action** tab, click any of the actions that you want to change in the **Action** column.
8. Select any of the following actions that the 802.1x-aware switch needs to take when certain criteria are met:
   - Open Port
     The 802.1x-aware switch allows network access on the default VLAN to which the port is normally assigned. It also allows network access on the VLAN that is specified in an attribute that is sent from the RADIUS server. Therefore the support of users having VLAN access is based on user ID and user role.
     The default action is Open Port.
   - Switch to VLAN-*test*
     Allows access to the specified VLAN. The VLANs that are available to select are the ones that you configured previously.
   - Close Port
     Deny network access on the default or RADIUS-specified VLAN. On some switch models, depending on the switch configuration, the port is assigned to a guest VLAN.
9. Click **OK**.
10. In the **LAN Enforcer Settings** dialog box, on the **Switch** tab, click **OK**.

Using advanced LAN Enforcer appliance settings

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

- Allow a legacy client.
  See "Allowing a legacy client to connect to the network with a LAN Enforcer appliance" on page 244.
- Enable local authentication.
  See "Enabling local authentication on the LAN Enforcer appliance" on page 245.

Allowing a legacy client to connect to the network with a LAN Enforcer appliance

You can enable a LAN Enforcer appliance to connect to 5.1.x legacy clients. If your network supports an 11.0.2 Symantec Endpoint Protection Manager, a Symantec LAN Enforcer appliance, and needs to support 5.1.x legacy clients, you can enable the support of 5.1.x legacy clients on the management server console so that the Symantec LAN Enforcer appliance does not block them.

See "Using advanced LAN Enforcer appliance settings" on page 244.

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. Click **Servers**.
3. Under **View Servers**, select and expand the group of LAN Enforcers appliances.
4. Under **Tasks**, click **Edit Group Properties**.
5. In the **Settings** dialog box, on the **Advanced** tab, check **Allow legacy clients**.
6. Click **OK**.

Enabling local authentication on the LAN Enforcer appliance

If a LAN Enforcer appliance loses its connection with the computer on which the Symantec Endpoint Protection Manager is installed, the LAN Enforcer appliance can authenticate a client locally.

See "Using advanced LAN Enforcer appliance settings" on page 244.

To enable local authentication on the LAN Enforcer appliance

1. In the Symantec Endpoint Protection Manager Console, click **Admin**.
2. 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 14-2 describes the types of options that you can configure for 802.1x authentication.

Table 14-2 802.1x authentication options

Option	Description
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.

Table 14-2 802.1x authentication options *(continued)*

Option	Description
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.
Built-in supplicant	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.

Warning: You must know whether your corporate network uses the RADIUS server as the authentication server. If you configure 802.1x authentication incorrectly, the connection to the network may break.

Note: To enable the user to configure 802.1x authentication on the client, you must set the client to client control.

See "How the LAN Enforcer appliance works" on page 41.

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 has occurred:

- The client computer failed the user authentication because users typed their user name or their password incorrectly.
- The client computer is in the wrong VLAN.
- The client computer does not obtain a network connection. A broken network connection usually happens because the switch between the client computer and the LAN Enforcer did not authenticate the user name and password.
- Users need to log on to a client computer that authenticated a previous user.
- The client computer failed the compliance check.

Users can reauthenticate the computer only if you configured the computer with a built-in supplicant. The right-click menu on the notification area icon of the client computer displays a Reauthentication command.

See “Using 802.1x authentication” on page 245.

Troubleshooting the Enforcer appliance

This chapter includes the following topics:

- About troubleshooting an Enforcer appliance
- Troubleshooting an Enforcer appliance
- About debug information transfer over the network
- Frequently asked questions for the Enforcer appliances
- Which antivirus software provides support for Host Integrity?
- Can Host Integrity policies be set at the group level or the global level?
- Can you create a custom Host Integrity message?
- What happens if Enforcer appliances cannot communicate with Symantec Endpoint Protection Manager?
- Is a RADIUS server required when a LAN Enforcer appliance runs in transparent mode?
- How does enforcement manage computers without clients?

About troubleshooting an Enforcer appliance

You may need to troubleshoot communication problems with between Enforcers and the Symantec Endpoint Protection Manager.

See "Frequently asked questions for the Enforcer appliances" on page 254.

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

See "Troubleshooting an Enforcer appliance" on page 252.

Troubleshooting an Enforcer appliance

Table 15-1 displays the possible problems and solutions you might have with an Enforcer appliance.

Table 15-1 Troubleshooting problems and solutions for an Enforcer appliance

Symptom	Solution
Enforcer root password is shown as invalid when set using the command-line interface	Limit passwords to 128-characters. Use another password of shorter length. See "Password" on page 374.
Time synchronization fails when installing a LAN Enforcer with NTP enabled and configured on Dell 850	The workaround to this hardware issue is to disable NTP and then enable it. See "Configuring an Enforcer appliance" on page 100.
Changing memory on the R200 causes hardware errors	The errors are due to hard coding of the IRQs. Remove the additional memory or reinstall the Enforcer after the hardware change. Our tests have shown that additional memory does not make an appreciable difference. See "Installing an Enforcer appliance" on page 96.
Some settings (Debug Level, Capture) return to default when the Enforcer is upgraded	A return to defaults can appear on upgrade, but does not appear thereafter. See "Upgrading the Enforcer appliance image" on page 104.

Table 15-1 Troubleshooting problems and solutions for an Enforcer appliance *(continued)*

Symptom	Solution
Problems appear when you are running SNMP with the Enforcer and HP OpenView	Resolve this problem by configuring HP OpenView: ■ Load the Symantec MIB file by selecting **Option > Load/unload MIB** ■ Using **Option > Event Configuration**, choose **OnDemandTraps (.1.3.6.1.4.1.393.588)**, and modify each trap as required. For example on **Event Message**, choose **Log and display in category**. Then select a category from the drop-down list. Set the **Event Log Message** as **$1**.

See "About troubleshooting an Enforcer appliance" on page 251.

About debug information transfer over the network

When problems occur on the Enforcer appliance, a debug log is created on the Enforcer (kernel.log). If you need to transfer debug information over the network, use one of the following debug commands to transfer the debug logs:

debug upload	To transfer one file to a tftp server

File transfer over the network requires a serial connection between a computer and the Enforcer appliance.

The following example represents a file-transfer output that the HyperTerminal performs:

```
<date>          <Time>     <File Name>
2008-08-01   16:32:26     user.log
2008-08-01   16:32:24     kernel.log
2008-08-01   14:30:03     ServerSylink[04-05-2010-14-30-03].xml
2008-08-01   14:29:59     ServerProfile[04-05-2010-14-29-59].xml
Enforcer(debug)# upload tftp 10.1.1.1 filename kernel.log
```

See "CLI command hierarchy" on page 366.

Frequently asked questions for the Enforcer appliances

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 254.
- See “Can Host Integrity policies be set at the group level or the global level?” on page 255.
- See “Can you create a custom Host Integrity message?” on page 255.
- See “What happens if Enforcer appliances cannot communicate with Symantec Endpoint Protection Manager?” on page 256.
- See “Is a RADIUS server required when a LAN Enforcer appliance runs in transparent mode?” on page 257.
- See “How does enforcement manage computers without clients?” on page 258.

Which antivirus software provides support for Host Integrity?

See “What you can do with Host Integrity policies” on page 52.

Symantec Network Access Control supports the following antivirus software:

- AhnLab V3 Internet Security 7.0 Platinum
- AVG AV 8.0
- AVG IS 8.0
- BitDefender IS 2008
- BitDefender TotalSecurity 2008
- CA Antivirus 2007, 2008, 2009
- CA Internet Security 2007, 2008, 2009
- CA eTrust Antivirus r8.1
- CA ez Antivirus r8.2
- Kaspersky Antivirus 7.0
- Kaspersky Internet Security 7.0
- McAfee VirusScan Enterprise 8.0i, 8.5i, 8.7i

- McAfee Internet Security 2006, 2007, 2008, 2009
- McAfee Total Protection 2009, 2010
- McAfee VirusScan Plus 2006, 2007, 2008, 2010
- Microsoft ForeFront
- Microsoft LiveOneCare
- Panda Antivirus+Firewall 2008
- Panda Antivirus 2007, 2008, 2009
- Panda Internet Security 2007, 2008
- Panda IS_Platinium 2006
- Panda Titanium 2006, 2007
- Sophos 5.x, 6.x, and 7.x
- Symantec Endpoint Protection, all versions
- Symantec AntiVirus
- Symantec Norton Internet Security 2006, 2007, 2008, 2009, 2010
- Symantec Norton 360 1.x, 2.x, and 3
- Trend Internet Security 2008, 2009
- Trend Pc-cillin 2006, 2007
- Trend OfficeScan 7.3, 8.0
- Trend Server Protector

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.

See “Creating and testing a Host Integrity policy” on page 53.

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.

See “Displaying a message dialog box” on page 83.

What happens if Enforcer appliances cannot communicate with Symantec Endpoint Protection Manager?

If you plan to use Enforcers with Symantec Endpoint Protection, we recommend that you have redundant management servers. If the Symantec Endpoint Protection Manager is unavailable, the Enforcer blocks the traffic from the clients.

Redundant management servers are preferable. The Enforcer sends a UDP packet on port 1812 by using the RADIUS protocol to the Symantec Endpoint Protection Manager to verify the GUID from the clients. If a firewall blocks this port or if a Symantec Endpoint Protection Manager is unavailable, then the clients are blocked.

An option on the Enforcer allows client access to the network when the Symantec Endpoint Protection Manager is unavailable. If this option is enabled and the Symantec Endpoint Protection Manager is unavailable, the GUID check and the profile checks are not performed. Only the Host Integrity check can be performed on the client when the Symantec Endpoint Protection Manager is unavailable.

You can use the advanced local-auth command to enable or disable the Enforcer’s authentication of a client.

See “Advanced local-auth” on page 256.

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:

Disable	Verifies the Agent with the Policy Manager. This blocks the Agent if it is unable to connect to a Policy Manager. The default setting for client authentication is Disable.

Enable	Disables Agent verification and performs Host Integrity validation only.

By default, the Gateway Enforcer appliance verifies the Globally Unique Identifier (GUID) of the client with the Symantec Endpoint Protection Manager. If the Gateway Enforcer is unable to connect with a Symantec Endpoint Protection Manager to verify the GUID, it blocks the client. Although it is not recommended as a troubleshooting step, you can stop the Gateway Enforcer appliance from verifying the GUID.

By default, the Gateway Enforcer appliance verifies the GUID. 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 GUID.

See “Communication between an Enforcer appliance and a Symantec Endpoint Protection Manager” on page 37.

Is a RADIUS server required when a LAN Enforcer appliance runs in transparent mode?

RADIUS server requirements depend on how the switch is configured and what you use the switch to authenticate.

The following are some items to watch out for:

- Switches that use RADIUS servers for more than the authentication of 802.1x users.

  For example, when you log on to the switch, you must type a user name and password. The RADIUS server typically performs authentication for this logon. When the LAN Enforcer appliance is installed, this authentication is sent to the LAN Enforcer appliance. If the authentication is sent to the LAN Enforcer appliance, you must configure the RADIUS server IP address in the LAN Enforcer appliance. You must configure the LAN Enforcer appliance to forward all non-EAP requests directly to the RADIUS server.
- Installation of a 802.1x supplicant on a client system. If an 802.1x supplicant exists on a client system, the LAN Enforcer appliance tries to authenticate with the RADIUS server. 802.1x authentication is enabled by default on Windows XP. If you enable your client to work in transparent mode, it does not automatically disable the built-in 802.1x supplicant. You must make sure that no 802.1x supplicant runs on any of your client computers.
- Configuration of the Enforcer to ignore the RADIUS request from any client computer that includes a third-party 802.1x supplicant. You can set up this

configuration by using an IP address of 0.0.0.0 for the RADIUS server. You can use this setup if you want to run a LAN Enforcer in transparent mode. Some clients can have an 802.1x supplicant. In this case, you can specify that the LAN Enforcer appliance does not send any traffic to a RADIUS server.

See "Using RADIUS server group settings" on page 212.

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. See "How self enforcement works" on page 35.
Gateway enforcement	In the networks that use gateway enforcement, the systems without clients cannot pass through the gateway. Where you place the Gateway Enforcer in the network is critical; it can block access to critical network resources to which other systems require access. You can make exceptions for trusted IP addresses so that they can pass through the gateway inbound or outbound without a client. Similarly, the gateway can also exempt non-Microsoft operating systems from enforcement. One network design can be to place non-critical servers on the same side of the gateway. This configuration simplifies the network design without seriously compromising security. See "How the Gateway Enforcer appliance works" on page 39.

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. See "How the DHCP Enforcer appliance works" on page 40.
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 has host NAC status. The switch configuration must handle the exceptions for systems without clients, rather than any Symantec configuration. You have several ways to set up this switch configuration. Methods vary depending on the type of switch and software version it runs. A typical method implements the concept of a guest VLAN. Systems without clients are assigned to a network that has a lower level of network connectivity. Another method involves basing the exceptions on MAC addresses. You can disable 802.1x on selected ports. However, to disable by selected ports allows anyone to connect by using the port, so it is not recommended. Many vendors have special provisions for the VoIP phones that can automatically move these devices to special voice VLANs. See "How the LAN Enforcer appliance works" on page 41.
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.

Section 4

Administering Enforcer appliances on the Symantec Endpoint Protection Manager

Chapter 16

Managing Enforcers on the Symantec Endpoint Protection Manager

This chapter includes the following topics:

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.

See "Configuring an Enforcer appliance" on page 100.

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 268.

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.

See "Setting up an Enforcer group name on the Symantec Integrated Enforcer for Microsoft Network Access Protection console" on page 332.

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.

See "Setting up an Enforcer group name on the Symantec Integrated Enforcer for Microsoft Network Access Protection console" on page 332.

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.

See "Failover planning for Gateway Enforcer appliances" on page 121.

See "Failover planning for DHCP Enforcer appliances" on page 168.

For LAN Enforcers, failover is handled through the switch rather than through the Enforcer so the automatic assignment to the same group does not occur. You can ensure that multiple LAN Enforcers share settings. Specify the same group name in the Enforcer local console on the console **Settings** dialog box.

See "Planning for the installation of a LAN Enforcer appliance" on page 197.

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.

See “How the console determines the Enforcer group name” on page 265.

About creating a new Enforcer group

Usually, you only need to create a new Enforcer group if you add an Enforcer that required different settings from the existing Enforcers.

You can create a new Enforcer group on the Enforcer local console by specifying the new name on the console **Settings** dialog box. The new group has the Enforcer default settings.

You can leave the group name field blank when you connect the new Enforcer from the local console. In that case, the console assigns the Enforcer to a new group. This group takes the name of the Enforcer computer and its default settings.

You can use the same method to move an Enforcer to another group. Specify the desired group name from the Enforcer local console. The Enforcer takes on the settings of the group to which it is moved.

See “Adding or editing the name of an Enforcer group with a DHCP Enforcer” on page 176.

See “Adding or editing the name of a LAN Enforcer appliance group with a LAN Enforcer” on page 209.

See “Adding or editing the name of an Enforcer group for Symantec Network Access Control Integrated Enforcer” on page 302.

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.

See “Displaying information about the Enforcer on the management console” on page 267.

Table 16-1 describes the type of information that you can view.

Table 16-1 Information about the Enforcer appliance on the management console

Field	Description
Name	Same as Hostname field.
Description	Brief description of the Enforcer. The description is the only information that you can be edit on the management console.
Version	Version of the Enforcer software that runs on the selected Enforcer computer.
Hostname	Name of the computer on which the Enforcer is installed.
Operating System	Operating system that is running on the computer on which the selected Enforcer is installed.
Online Status	Online: The service is running and is the primary active Enforcer. Offline: The service is stopped.
Failover Status	(Gateway and DHCP Enforcer only) Whether the Enforcer is active or on standby.
Internal IP	IP address of the internal network interface card.
External IP	(Gateway and DHCP Enforcer only) IP address of the external network interface card.
Internal MAC	The MAC address of the internal network interface card.
External MAC	(Gateway and DHCP Enforcer only) The MAC address of the external network interface card.
Internal NIC	Manufacturer and model of the internal network interface card.
External NIC	(Gateway and DHCP Enforcer only) Manufacturer and model of the external network interface card.

Displaying information about the Enforcer on the management console

You can display information about the Enforcer from a management console.

See "About the Enforcer information that appears on the Enforcer console" on page 266.

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 does 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:

- Message for the computers that are running a client
- Message for Windows computers that are not running a client (Gateway or DHCP Enforcer only)

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 without special configuration. The exception is some 802.1x authentication settings required for the LAN Enforcer.

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 release and renew the IP address. However, if the end user stops the client on the client computer, the Enforcer is unable to enforce the release and renew. To ensure that the Enforcer can continue to quarantine or 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**.

About Enforcer reports and logs

Enforcer reports and logs let you view Enforcer client activities and how the Enforcers flow through your system. For detailed information about the types reports and logs and how to view them, see Symantec Endpoint Protection Manager Help.

The **Reports** page on the Symantec Endpoint Protection Manager console provides both predefined reports and custom reports. You can view the predefined Quick Reports that contain information about Enforcers on the **Reports** page.

The following Enforcer reports are available:

- The System report that is called Top Enforcers That Generate Errors contains information about Enforcers that generated errors and warnings.
- The System report that is called Site Status contains information about Enforcer system, traffic, and packet log throughput.

- The Compliance reports contain information about the compliance status of clients.

Enforcer logs include the data that you can use to monitor and troubleshoot system activity:

The following types of Enforcer logs are available:

- Enforcer Server log. This log contains the information that is related to the functioning of an Enforcer.
- Enforcer Client log. This log contains information about interactions between an Enforcer and clients trying to connect to the network.
- Enforcer Traffic log (Gateway Enforcer only). This log records all traffic that enters through a Gateway Enforcer appliance's external adapter and leaves through the internal adapter.
- Enforcer Activity log. This log contains information about events such as when Enforcers start and when they connect to the Symantec Endpoint Protection Manager.

By default, Enforcer logs are stored on the same computer on which the Enforcer software is installed or on the Enforcer appliance itself. You can have the logs automatically sent from the Enforcer appliance or the computer on which you installed an Integrated Enforcer to the Symantec Endpoint Protection Manager Console. However, you must enable the sending of the logs on the Symantec Endpoint Protection Manager Console.

The log data is sent from the Enforcer to 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.

For detailed information about the types of reports and logs and how to view them, see Symantec Endpoint Protection Manager Help.

See “Configuring Enforcer log settings” on page 273.

Configuring Enforcer log settings

You can configure settings for Enforcer logs on the *Enforcer name* **Settings** dialog box on the **Logging** tab. The changes are sent to the selected Enforcer during the next heartbeat.

To configure Enforcer logs

1. In the Symantec Endpoint Protection Manager Console, click **Admin**.
2. Click **Servers**.
3. Under **View Servers**, select the Enforcer group for which you want to change log settings.
4. Under **Tasks**, click **Edit Group Properties**.
5. In the *Enforcer name* **Settings** dialog box, on the **Logging** tab, change any of the following:

Disable logging on the Symantec Endpoint Protection Manager Console	Uncheck **Enable logging** for each log that you want to disable.
Enable the sending of Enforcer logs from an Enforcer to the Symantec Endpoint Protection Manager	Check **Send the log to the management server**.
Set up the size and age of logs	In each of the **Maximum log file size** fields, specify that number of kilobytes of data to maintain in each log. In the **Log entry will expire after** field, specify the number of days that the entry remains in the database before it is removed. The range is 1 to 365 days.
Filter the Enforcer traffic log	Select one of the following filter options: ■ **All traffic** to log all traffic including that which is allowed and that which is dropped. ■ **Only blocked traffic** to log only the clients that the Enforcer blocks. ■ **Only allowed traffic** to log only the traffic that the Enforcer allows.

6. Click **OK**.

See “About Enforcer reports and logs” on page 272.

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. Click **Servers**.
3. Under **View Servers,** select the Enforcer group for which you want to disable Enforcer logging.
4. Under **Tasks**, click **Edit Group Properties**.
5. In the *Enforcer name* **Settings** dialog box, on the **Logging** tab, uncheck **Enable logging** for each log that you want to disable.
6. Click **OK**.

See “About Enforcer reports and logs” on page 272.

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. Click **Servers**.
3. 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. 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**.

See "About Enforcer reports and logs" on page 272.

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. Click **Servers**.
3. Under **View Servers**, select the Enforcer group for which you want to set the size and age of Enforcer logs.
4. 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.

   You can enter a size between 64 KB and 2 GB. The default setting is 512 KB.

6. In the **Log entry will expire after** field, specify the number of days that the entry remains in the database before it is removed.

   The range is 1 day to 365 days, with a default range of 30 days.

7. Click **OK**.

See "About Enforcer reports and logs" on page 272.

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. Click **Servers**.
3. Under **View Servers**, select the Enforcer group for which you want to filter Traffic logs.
4. 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:

All traffic	Logs all traffic, including that which is allowed and dropped
Only blocked traffic	Logs only the clients that the Enforcer blocks
Only allowed traffic	Logs only the traffic that the Enforcer allows

6. Click **OK**.

See “About Enforcer reports and logs” on page 272.

Section 5

Controlling network access with Symantec Network Access Control Integrated Enforcers

Chapter 17

Introducing the Symantec Integrated Enforcers

This chapter includes the following topics:

- About the Symantec Network Access Control Integrated Enforcer for Microsoft DHCP Servers
- About the Symantec Network Access Control Integrated Enforcer for Microsoft Network Access Protection

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

The Symantec Network Access Control Integrated Enforcer for Microsoft DHCP Servers works in concert with the Microsoft 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 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.

About the Symantec Network Access Control Integrated Enforcer for Microsoft Network Access Protection

The Integrated Enforcer for Microsoft Network Access Protection (NAP) works in concert with the Microsoft Windows Network Policy Server (NPS) on a Microsoft Windows Server 2008. The Symantec Integrated NAP Enforcer ensures that the clients that try to connect to the network comply with configured security policies.

NAP restricts access to networks by creating a controlled environment. It checks the security posture of a client before the client can connect to the enterprise network. If a client is noncompliant, NAP either corrects the security posture or limits access to endpoints that do not meet a company's security policy.

Network Access Protection is a client security health policy creation, enforcement, and remediation technology that is included in the Windows Server 2008 operating system. System administrators can create and automatically enforce security 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. When their configuration is updated and brought into compliance with a policy, clients have full network access. Depending on how you deploy NAP, noncompliant clients can be automatically updated so that users regain full network access without manually updating or reconfiguring their computers.

See “How an Integrated Enforcer for Microsoft Network Access Protection works” on page 44.

Chapter 18

Installing the Symantec Network Access Control Integrated Enforcer for Microsoft DHCP Servers

This chapter includes the following topics:

- Process for installing the Symantec Network Access Control Integrated Enforcer for Microsoft DHCP Servers
- Components for an Integrated Enforcer for Microsoft DHCP servers
- Placement requirements for an Integrated Enforcer for Microsoft DHCP Servers
- How to get started with the installation of an Integrated Enforcer for Microsoft DHCP servers
- Installing an Integrated Enforcer for Microsoft DHCP Servers

Process for installing the Symantec Network Access Control Integrated Enforcer for Microsoft DHCP Servers

Table 18-1 lists the steps to install the Symantec Network Access Control Integrated Enforcer for Microsoft DHCP servers.

Table 18-1 Installation summary for the Symantec Network Access Control Integrated Enforcer for Microsoft DHCP servers

Step	Action	Description
Step 1	Read the system requirements and the installation requirements.	Identifies the hardware, software, and Symantec Network Access Control components you need to obtain to run the Enforcer and helps you plan for its placement on your network. See "Components for an Integrated Enforcer for Microsoft DHCP servers" on page 284.
Step2	Install the Symantec Endpoint Protection Manager.	Installs the application that you use to support the Enforcer on your network.
Step 3	Install the Symantec Network Access Control Integrated Enforcer for Microsoft DHCP servers.	Installs the Symantec Network Access Control Integrated Enforcer for Microsoft DHCP servers components. See "Installing an Integrated Enforcer for Microsoft DHCP Servers" on page 288.

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.

Table 18-2 shows the components that are required for using the Integrated Enforcer for Microsoft DHCP servers:

Table 18-2 Components for Symantec Network Access Control Integrated Enforcer for Microsoft DHCP servers

Component	Description
Symantec Endpoint Protection Manager	Creates the security policies in a centralized location and assigns them to clients.

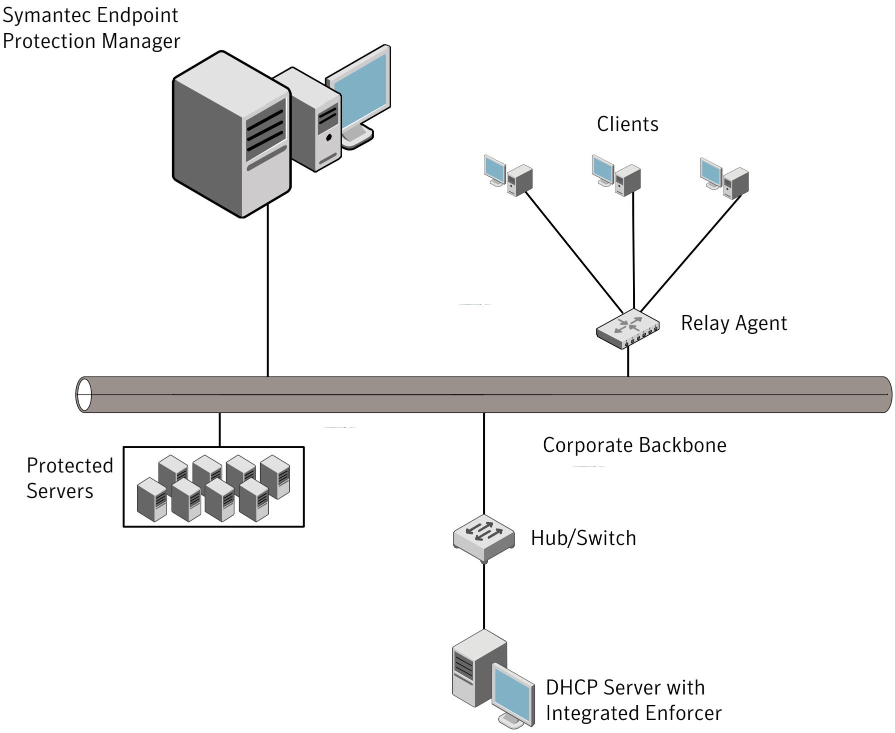
Table 18-2 Components for Symantec Network Access Control Integrated Enforcer for Microsoft DHCP servers *(continued)*

Component	Description
Symantec Network Access Control client	Protects end users with the security policies that the Integrated Enforcer for Microsoft DHCP servers provides.
Microsoft Windows DHCP server	Protects end users with the security policies that the Integrated Enforcer for Microsoft DHCP servers enforces. You must configure the DHCP Service on this server.
Integrated Enforcer for Microsoft DHCP servers (installed on the same computer as the DHCP service)	Authenticates clients and enforces security policies.

Placement requirements for an Integrated Enforcer for Microsoft DHCP Servers

Figure 18-1 illustrates how to place the Integrated Enforcer for Microsoft DHCP Servers, the Microsoft DHCP Server, and the Symantec Endpoint Protection Manager, as well as internal or remote clients in a network.

Figure 18-1 Placement of Symantec Network Access Control Integrated Enforcer for Microsoft DHCP Servers


Symantec Endpoint Protection Manager
Clients
Relay Agent
Corporate Backbone
Protected Servers
Hub/Switch
DHCP Server with Integrated Enforcer

How to get started with the installation of an Integrated Enforcer for Microsoft DHCP servers

The documentation describes how to install, configure, and use the Integrated Enforcer for Microsoft DHCP Servers. Perform the following tasks to get started:

Table 18-3 Process for installing an Integrated Enforcer for Microsoft DHCP servers

Step	Action	Description
Step 1	Locate the Symantec Network Access Control installation components.	Describes the components that are needed for the installation of an Integrated Enforcer for Microsoft DHCP servers. See "Components for an Integrated Enforcer for Microsoft DHCP servers" on page 284.
Step 2	Obtain the required hardware.	Lists the hardware requirements for an Integrated Enforcer for Microsoft DHCP servers.
Step 3	Obtain the required operating system.	Lists the operating system requirements that for an Integrated Enforcer for Microsoft DHCP servers.
Step 4	Place the Integrated Enforcer for Microsoft DHCP servers on your network.	Explains where to place an Integrated Enforcer for Microsoft DHCP servers in a network. See "Placement requirements for an Integrated Enforcer for Microsoft DHCP Servers" on page 285.
Step 5	Install an Integrated Enforcer for Microsoft DHCP server	Explains how to install an Integrated Enforcer for Microsoft DHCP servers. See "Installing an Integrated Enforcer for Microsoft DHCP Servers" on page 288.

Table 18-3 Process for installing an Integrated Enforcer for Microsoft DHCP servers *(continued)*

Step	Action	Description
Step 6	Configure the Integrated Enforcer for Microsoft DHCP servers	Explains how to configure the connections and settings of an Integrated Enforcer for Microsoft DHCP servers on an Enforcer console. See "About configuring Integrated Enforcers on an Enforcer appliance console" on page 294.

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 as a user in the administrators group.

Note: After installing the Microsoft DHCP server, you must configure the Integrated Enforcer for Microsoft DHCP servers. The Integrated Enforcer for Microsoft DHCP servers can then connect to the Symantec Endpoint Protection Manager.

To install the Integrated Enforcer for Microsoft DHCP Servers with a Wizard

1. Insert the installation disc 2.

   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 Network Access Control Integrated Enforcer can be installed based on the services running on the server.

7 In the **Ready to Install the Application** panel, click **Next**.

8 When 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 “Stopping and starting the Microsoft DHCP Server manually” on page 291.

9 Click **Finish**.

If you need to reinstall the Integrated Enforcer, you must first uninstall it.

See “Uninstalling the Symantec Network Access Control Integrated Enforcer for Microsoft DHCP servers” on page 290.

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`.

Uninstalling the Symantec Network Access Control Integrated Enforcer for Microsoft DHCP servers

You can uninstall the Symantec Network Access Control Integrated Enforcer for Microsoft DHCP servers from the Windows taskbar or the command line.

To uninstall the Integrated Enforcer for Microsoft DHCP Servers

1. On the Windows taskbar, click **Start > Control Panel > Add or Remove Programs**.
2. Click **Symantec 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	**`misexec.exe /qn /X <filename >`**The filename should be under Program Files\Common Files\Wise Installation Wizard.

Upgrading the Integrated Enforcer for Microsoft DHCP Servers

The following steps detail how to upgrade to a Symantec Network Access Control Integrated Enforcer for Microsoft DHCP Servers:

Table 18-4 Upgrade steps for the Integrated Enforcer for Microsoft DHCP Servers

Step	Action	Description
Step 1	Stop the Microsoft DHCP server.	Stop the DHCP service before upgrading the Integrated Enforcer for Microsoft DHCP Servers. See "Stopping and starting the Microsoft DHCP Server manually" on page 291.
Step 2	Uninstall the old version.	Uninstall the existing version of the Integrated Enforcer. See "Uninstalling the Symantec Network Access Control Integrated Enforcer for Microsoft DHCP servers" on page 290.
Step 3	Restart the DHCP service.	Restart the DHCP service before you install the new version of the Integrated Enforcer. See "Stopping and starting the Microsoft DHCP Server manually" on page 291.
Step 4	Install the new version.	Install the new version of the Integrated Enforcer. See "Installing an Integrated Enforcer for Microsoft DHCP Servers" on page 288.

Stopping and starting the Microsoft DHCP Server manually

Stop the Microsoft DHCP Server manually before upgrading to a new version of the Integrated Enforcer for Microsoft DHCP Servers. You then restart it after you complete the upgrade.

To stop and start the Microsoft DHCP Server manually

1. On the Windows taskbar, click **Start** > **Control Panel** > **Administrative Tools** > **Services**.
2. Right-click **DHCP Server** and click **Stop**.
3. Click **Start**.

Chapter 19

Configuring the Symantec Integrated Enforcers on the Enforcer console

This chapter includes the following topics:

- About configuring Integrated Enforcers on an Enforcer appliance console
- Establishing or changing communication between an Integrated Enforcer for Microsoft DHCP servers and a Symantec Endpoint Protection Manager
- Configuring automatic quarantine
- Configuring Symantec Network Access Control 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 Network Access Control Integrated Enforcer
- Configuring Symantec Network Access Control Integrated Enforcer authentication settings
- Configuring Symantec Network Access Control Integrated Enforcer advanced settings
- Stopping and starting communication services between an Integrated Enforcer and a management server
- Configuring a secure subnet mask

About configuring Integrated Enforcers on an Enforcer appliance console

After you complete the installation of a Symantec Network Access Control Integrated Enforcer, there are two stages of configuration. First, configure the settings on the Integrated Enforcer appliance console. Secondly, move to the Symantec Endpoint Protection Manager to make any desired changes to the configuration settings for the group that the Integrated Enforcer is part of.

Table 19-1 outlines these tasks.

Table 19-1 Enforcer console configuration summary

Step	Action	Description
Step 1	Establish a connection between the Integrated Enforcer for Microsoft DHCP Servers and a management server.	Use the management console of a Symantec Endpoint Protection Manager to configure the connection between the Integrated Enforcer for Microsoft DHCP Servers and a management server. See "Establishing or changing communication between an Integrated Enforcer for Microsoft DHCP servers and a Symantec Endpoint Protection Manager" on page 296.
Step 2	Set up the DHCP server with a quarantine configuration.	Use one of two methods to configure a quarantine user class for remediation. See "Configuring automatic quarantine" on page 299.
Step 3	Restart the DHCP service.	Manually stop and start the DHCP service on the DHCP server. See "Stopping and starting the Microsoft DHCP Server manually" on page 291.

Table 19-1 Enforcer console configuration summary *(continued)*

Step	Action	Description
Step 4	Optionally, change Integrated Enforcer basic settings.	Add or edit descriptions for an Integrated Enforcer or group of Integrated Enforcers, or for the Integrated Enforcer IP address or host names. See "Configuring Symantec Network Access Control Integrated Enforcer basic settings" on page 301.
Step 5	Connect the Integrated Enforcer to a Symantec Endpoint Protection Manager.	Connect the Integrated Enforcer to a server on which the Symantec Endpoint Protection Manager is installed. See "Connecting the Symantec Network Access Control Integrated Enforcer to a Symantec Endpoint Protection Manager" on page 303.
Step 6	As needed, update the connection to the Symantec Endpoint Protection Manager.	Update the connection to the Symantec Endpoint Protection server address and port information as required. See "Editing a Symantec Endpoint Protection Manager connection" on page 305.
Step 7	As needed, configure a trusted vendor list.	Configure a trusted vendor list for devices on your network such as printers or IP telephones. These are the devices that the Integrated Enforcer does not need to authenticate. See "Configuring a trusted vendor list" on page 305.
Step 8	Optionally, set where you want to view logs.	Set up logs for viewing on the Enforcer console or the Symantec Endpoint Protection Manager. See "Viewing Enforcer logs on an Enforcer console" on page 306. See "Configuring logs for the Symantec Network Access Control Integrated Enforcer" on page 306.

Table 19-1 Enforcer console configuration summary *(continued)*

Step	Action	Description
Step 9	Optionally, set authentication settings for your network.	Set up how you want to authenticate clients, servers, and devices. See "Specifying the maximum number of challenge packets during an authentication session" on page 310. See "Specifying the frequency of challenge packets to be sent to clients" on page 311. See "Allowing all clients with continued logging of non-authenticated clients" on page 311. See "Allowing non-Windows clients to connect to a network without authentication" on page 312. See "Enabling servers, clients, and devices to connect to the network as trusted hosts without authentication" on page 315.
Step 10	Optionally, validate that clients are running up-to-date policies.	Validate that clients have the most recent policies by comparing the policy serial number received from the client with the policy serial number in the Symantec Endpoint Protection Manager.

Establishing or changing communication between an Integrated Enforcer for Microsoft DHCP servers and a Symantec Endpoint Protection Manager

You must specify one or more management servers 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 the Integrated Enforcer console and Symantec Endpoint Protection Manager

1. On the Windows taskbar of the Integrated Enforcer computer, click **Start > Programs > Symantec Endpoint Protection > Symantec NAC Integrated Enforcer**.

   The Symantec Network Access Control Integrated Enforcer configuration console appears. This main page shows the connection status between the Integrated Enforcer and the Symantec Endpoint Protection Manager. A green light indicates that Integrated Enforcer is actively connected to the management server. A red light indicates that the connection is 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 resolves correctly with 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 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 Network Access Control Integrated Enforcer uses to connect to a Symantec Endpoint Protection Manager.

   The first time the Symantec Network Access Control 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 Network Access Control 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 for your connection.

   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 Network Access Control Integrated Enforcer to a default Enforcer group with default settings. The default group name is I-DHCP. However, a Symantec Network Access Control Integrated Enforcer for Microsoft NAP Servers and appliance-based enforcers must each be in a separate group.

   You can view the group settings from the Symantec Endpoint Protection Manager console on the **View Servers** page.

10 To specify the protocol that the Symantec Network Access Control Integrated Enforcer uses to communicate with the Symantec Endpoint Protection Manager, select **HTTP** or **HTTPS**.

You can only use the HTTPS protocol if the Symantec Endpoint Protection Manager is running Secure Sockets Layer (SSL).

If you select HTTPS and want to require verification of the management server's certificate with a trusted third-party certificate authority, check **Verify certificate when using HTTPs protocol**.

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 Network Access Control 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 Network Access Control Integrated Enforcer

1. On the Windows taskbar of the Integrated Enforcer computer, click **Start > Programs > Symantec Endpoint Protection > Symantec NAC Integrated Enforcer**.
2. In the left-hand panel, click **Symantec Integrated Enforcer > Configure > Automatic Quarantine Configuration**.
3. In the **Automatic Quarantine Configuration** page of the Integrated Enforcer, click **Add** to begin creating an IP address list.
4. Enter an allowed IP address and click **OK** to add the IP address to the list.
5. Click **Add** again to continue adding IP addresses to the list.
6. Modify the **IP Address** list by clicking **Edit, Remove, Remove all, Move Up**, or **Move down**.
7. When all IP Addresses are listed or modified, click **OK** at the bottom of the page to save your configurations.

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, including 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 **DHCP Standard 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 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.
10. Click **OK**.
11. Click **File > Exit**.

Configuring Symantec Network Access Control Integrated Enforcer basic settings

You can add or edit the description of a Symantec Network Access Control Integrated Enforcer or an Integrated Enforcer group in 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 Network Access Control Integrated Enforcer" on page 302.

See "Adding or editing the description of a Symantec Network Access Control Integrated Enforcer" on page 303.

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 Network Access Control Integrated Enforcer" on page 302.

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 Network Access Control Integrated Enforcer" on page 303.

You must connect the Integrated Enforcer to a Symantec Endpoint Protection Manager.

See "Connecting the Symantec Network Access Control Integrated Enforcer to a Symantec Endpoint Protection Manager" on page 303.

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

You can add or edit the name of an Enforcer group of which an Integrated Enforcer is a member. You perform these tasks on the Enforcer console during the installation. Later, if you want to change the name of an Enforcer group, you can do so on the Enforcer console.

See "Establishing or changing communication between an Integrated Enforcer for Microsoft DHCP servers and a Symantec Endpoint Protection Manager" on page 296.

All Enforcers in a group share the same configuration settings.

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

You can add or edit the description of an Enforcer group of which a Symantec Network Access Control Integrated Enforcer is a member. You can perform this task on the Symantec Endpoint Protection Manager console instead of the Integrated Enforcer console.

To add or edit the description of an Enforcer group with a Symantec Network Access Control Integrated Enforcer

1. In the Symantec Endpoint Protection Manager Console, click **Admin**.
2. Click **Servers**.
3. Under **View Servers**, select and expand the Enforcer group whose name you want to add or edit.
4. Under **Tasks**, click **Edit Group Properties**.
5. In the **Settings** dialog box, on the **General** tab, add or edit a description for the Enforcer group in the **Description** field.
6. Click **OK**.

Adding or editing the IP address or host name of a Symantec Network Access Control 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 Network Access Control Integrated Enforcer

You can add or edit the description of a Symantec Network Access Control Integrated Enforcer. You can perform this task on 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 Network Access Control Integrated Enforcer

1. In the Symantec Endpoint Protection Manager Console, click **Admin**.
2. 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 Network Access Control 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 management server includes a file that helps manage the traffic between clients, management servers, and optional Enforcers such as an Integrated Enforcer. This file is called a management server list.

The management server list specifies to which Symantec Endpoint Protection Manager an Integrated Enforcer connects. It also specifies to which Symantec Endpoint Protection an Integrated Enforcer connects in case of a management server's failure.

A default management server list is automatically created for each site during the initial installation. All available management servers at that site are automatically added to the default management server list.

A default management server list includes the management server's IP addresses or host names to which Integrated Enforcers can connect after the initial installation. You may want to create a custom management server list before you deploy any Enforcers. If you create a custom management server list, you can specify the priority in which an Integrated Enforcer can connect to management servers.

You can select the specific management server list that includes the IP addresses or host names of those management servers to which you want the Integrated Enforcer to connect. If there is only one management server at a site, then you can select the default management server list.

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 Network Access Control Integrated Enforcer to a Symantec Endpoint Protection Manager

1. In the Symantec Endpoint Protection Manager Console, click **Admin**.
2. 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.
4. Under **Tasks**, click **Edit Group Properties**.
5. In the **Settings** dialog box, on the **General** tab, under **Communication**, select the management server list that you want this Integrated Enforcer to use.
6. On the **General** tab, under **Communication**, click **Select**.

   You can view the IP addresses and host names of all available management servers, as well as the priorities that have been assigned to them.
7. In the **Management Server List** dialog box, click **Close**.
8. In the **General** dialog box, click **OK**.

Editing a Symantec Endpoint Protection Manager connection

You can update the Symantec Endpoint Protection Manager IP address and port information as required.

To edit a Symantec Endpoint Protection Manager connection

1. On the Windows taskbar of the Enforcer computer, click **Start > Programs > Symantec Endpoint Protection > Symantec Integrated Enforcer**
2. In the left-hand panel, expand Symantec Integrated Enforcer.
3. Expand **Configure**.
4. Click **Management Servers**.
5. In the **Management Servers** panel, click **Edit** 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 host name or a domain name, the Symantec Network Access Control Integrated Enforcer must connect to a Domain Name Server (DNS) server.
7. Click **OK**.

Configuring a trusted vendor list

Clients cannot be installed on some network devices such as printers or IP telephones. To allow for those cases, you can configure a trusted vendor list. If the name of the vendor is considered trusted, then the Symantec Network Access Control Integrated Enforcer will not authenticate the device. The devices will obtain normal IP addresses from the DHCP server.

To configure a trusted vendor list

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 > DHCP Trusted Vendors Configuration**.

3. To enable the trusted vendor list, check **Turn on Trusted Vendors**.

   When the **Turn on Trusted Vendors** box is checked, Host Integrity will not be enforced for DHCP traffic from the selected trusted vendors.

4. Select the vendors you want to establish as trusted vendors.
5. Click **Save**.

Viewing Enforcer logs on an Enforcer console

The Symantec Network Access Control Integrated Enforcer automatically logs messages in the Enforcer Client log and the Enforcer System log. These Enforcer logs are uploaded to the Symantec Endpoint Protection Manager. The client log provides information about client connections and communication with the Integrated Enforcer. The system log records information that relates to the Integrated Enforcer itself, such as instances of starting and stopping the Enforcer service.

In the Symantec Endpoint Protection Manager, you can enable and disable logging and set log file parameters for the Integrated Enforcer. All logs are enabled and sent to the Symantec Endpoint Protection Manager by default.

To view Enforcer logs on an Enforcer console

1. In the left pane, expand **Symantec NAC Integrated Enforcer**.
2. Expand **View Logs**, and click **System Log** or click **Client Log**.
3. To view any changes to the log since you last opened the log, click **Refresh**.
4. Click **OK**.

Configuring logs for the Symantec Network Access Control Integrated Enforcer

Logs for a Symantec Network Access Control Integrated Enforcer are stored on the same computer on which you installed the Symantec Network Access Control Integrated Enforcer. Enforcer logs are generated by default.

If you want to view Enforcer logs 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 Network Access Control Integrated Enforcer authentication settings

You can specify a number of authentication settings for an Integrated Enforcer authentication session. When you apply these changes, they are automatically sent to the selected Integrated Enforcer during the next heartbeat.

About using authentication settings

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

Table 19-2 provides more information about the options on the **Authentication** tab.

Table 19-2 Authentication configuration settings for a Symantec Network Access Control Integrated Enforcer

Option	Description
Maximum number of packets per authentication session	The maximum number of challenge packets that the Integrated Enforcer sends in each authentication session. The default number is 10. See "Specifying the maximum number of challenge packets during an authentication session" on page 310.
Time between packets in authentication session	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 311.

Table 19-2 Authentication configuration settings for a Symantec Network Access Control Integrated Enforcer *(continued)*

Option	Description
Allow all clients, but continue to log which clients are not authenticated	If this option is enabled, the Enforcer authenticates all users by checking that they are running a client. It then forwards the 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 311.
Allow all clients with non-Windows operating systems	If this option is enabled, the Integrated Enforcer checks for the operating system of the client. The Integrated Enforcer then allows all clients that do not run the Windows operating systems to receive a normal network configuration without being authenticated. If this option is not enabled, the clients receive a quarantine network configuration. The default setting is not enabled. See "Allowing non-Windows clients to connect to a network without authentication" on page 312.
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 succeeds, the Integrated Enforcer forwards the Integrated request to receive a normal network configuration. The Integrated Enforcer forwards the Integrated request even if the client does not have the latest security policy. The default setting is not enabled. See "Having the Symantec Network Access Control Integrated Enforcer check the Policy Serial Number on a client" on page 313.

Table 19-2 Authentication configuration settings for a Symantec Network Access Control Integrated Enforcer *(continued)*

Option	Description
Enable pop-up message on client if Client is not running	This option is displayed but currently unavailable for the Symantec Network Access Control Integrated Enforcer. See "Sending a message from a Symantec Network Access Control Integrated Enforcer to a client about non-compliance" on page 314.

About authentication sessions

When a client tries to access the internal network, the Symantec Network Access Control Integrated Enforcer first detects whether the client is running a 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:

- Globally Unique Identifier (GUID)
- Its current Profile Serial Number
- The results of the Host Integrity check

The Integrated Enforcer verifies the client GUID and the Policy Serial Number with 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 Network Access Control 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. 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.

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 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 to the Integrated Enforcer to keep sending to a client during an authentication session in the **Time between packets in authentication session** field.

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

Allowing all clients with continued logging of non-authenticated clients

It can take some time to deploy all the client software. You can configure the Integrated Enforcer to allow all clients to connect to the network until you have finished distributing the client package to all users. These users all connect to an 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. 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 to log non-authenticated clients.
4. 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**.
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. 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.
4. Under **Tasks**, click **Edit Group Properties**.
5. In the **Settings** dialog box, on the **Authentication** tab, check **Allow all clients with non-Windows operating systems**.
6. Click **OK**.

Having the Symantec Network Access Control Integrated Enforcer check the Policy Serial Number on a client

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 Network Access Control 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. Click **OK**.

Sending a message from a Symantec Network Access Control Integrated Enforcer to a client about non-compliance

Although this option is displayed, it is currently unavailable for Symantec Network Access Control Integrated Enforcer configuration.

Configuring Symantec Network Access Control Integrated Enforcer advanced settings

You can configure the following Integrated Enforcer advanced configuration settings:

- Timeout parameters, Authentication timeout, and DHCP message timeout
  Although these options are displayed, they are currently unavailable for Symantec Network Access Control Integrated Enforcer configuration.
- MAC addresses for the trusted hosts that the Integrated Enforcer allows to connect to the normal DHCP server without authentication
  See "Enabling servers, clients, and devices to connect to the network as trusted hosts without authentication" on page 315.
- Enabling local authentication
  See "Enabling local authentication on the Integrated Enforcer" on page 316.

When you apply any of these configuration settings, the changes are sent to the selected Symantec Network Access Control Integrated Enforcer during the next heartbeat.

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. 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, it always asks the management server to verify the client's GUID regardless of whether local authentication is enabled or disabled.

To enable local authentication on the Integrated Enforcer

1. In the Symantec Endpoint Protection Manager Console, click **Admin**.
2. 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 Network Access Control 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 Windows registry.

Stopping the Integrated Enforcer does not stop the DHCP server. If the Integrated Enforcer is stopped, the DHCP server functions as if no Enforcer was ever installed. If the DHCP server becomes unavailable, the Integrated Enforcer stops collecting the compliance status about new clients. However, it continues to communicate with existing clients and continues to log status changes. The DHCP server may become unavailable because of maintenance and other problems.

To stop and start the communication services between an Integrated Enforcer and a management server

1. Start the Symantec Network Access Control Integrated Enforcer.
2. Click **Symantec NAC Integrated Enforcer**.
3. Perform one or both of the following tasks:
   - In the Enforcer service group box, click **Stop**.
     This option stops the Enforcer service.
   - In the Management server communication service group box, click **Stop**.
     This option stops the Enforcer service that connects to the Symantec Endpoint Protection Manager.

If the status is set to Stopped, the service is not running.

4. To restart either service, click **Start**.

   If you turn off or restart the computer to which a Symantec Network Access Control Integrated Enforcer is connected, the Enforcer service restarts automatically when the computer restarts.

   If the server communication service is stopped and subsequently restarted, the Symantec Network Access Control Integrated Enforcer tries to connect to a Symantec Endpoint Protection Manager to which it last connected. If that Symantec Endpoint Protection Manager is unavailable, the Integrated Enforcer connects to the first management server that is listed in the management server list.

Configuring a secure subnet mask

The Integrated Enforcer Advanced Settings configuration page allows users to 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 Network Access Control Integrated Enforcer for Microsoft DHCP servers.

To connect to a legacy Symantec Endpoint Protection Manager

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.

Chapter 20

Installing the Symantec Network Access Control Integrated Enforcer for Microsoft Network Access Protection

This chapter includes the following topics:

Before you install the Symantec Integrated Enforcer for Network Access Protection

Before you install the Symantec Integrated Enforcer for Network Access Protection, you must have completed the following installation and configuration tasks:

- Installation of the Symantec Endpoint Protection Manager

Note: It is recommended that you install Symantec Endpoint Protection Manager before you install the Symantec Integrated Enforcer for Network Access Protection. The Symantec Endpoint Protection Manager must be installed before the Symantec Integrated Enforcer for Network Access Protection can work properly.

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

- Verification of hardware and software requirements for the computer on which you plan to install the following components:
  - DHCP Server service
  - Network Access Protection Server service
  - Domain Controller
  - Symantec Integrated Enforcer for Network Access Protection

  See "Components of a Symantec Integrated Enforcer for Network Access Protection" on page 323.

Process for installing the Symantec Network Access Control Integrated Enforcer for Microsoft Network Access Protection

Table 20-1 lists the steps to install the Symantec Network Access Control Integrated Enforcer for Microsoft Network Protection.

Table 20-1 Installation summary for the Symantec Network Access Control Integrated Enforcer for Microsoft Network Protection

Step	Action	Description
Step 1	Read the system requirements and the installation requirements.	Identifies the hardware, software, and Symantec Network Access Control components you need to obtain to run the Enforcer and plan its placement on your network. See "Hardware requirements for an Integrated Enforcer Microsoft Network Access Control" on page 322. See "Operating system requirements for an Integrated Enforcer for Microsoft Network Access Protection" on page 322. See "Components of a Symantec Integrated Enforcer for Network Access Protection" on page 323.
Step 2	Install the Symantec Endpoint Protection Manager.	Installs the application that you use to support the Enforcer on your network. For installation instructions, see the *Installation Guide for Symantec Endpoint Protection and Symantec Network Access Control.*
Step 3	Install the Symantec Network Access Control Integrated Enforcer for Microsoft Network Access Protection.	Installs the Symantec Network Access Control Integrated Enforcer for Microsoft Network Access Protection components. See "Installing the Integrated Enforcer for Microsoft Network Access Protection" on page 323.

System requirements for an Integrated Enforcer for Microsoft Network Access Protection

Before you begin installation of a Symantec Integrated Enforcer for Network Access Protection, you should review the system and the installation requirements. You should confirm that the computers you plan to use meet the requirements and are correctly configured.

Hardware requirements for an Integrated Enforcer Microsoft Network Access Control

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 an Integrated Enforcer for Microsoft Network Access Protection

The Symantec Integrated NAP Enforcer requires that the following operating system and services are installed:

- Windows 2008 server Standard Edition and Windows 2008 server Enterprise Edition
- 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

Components of a Symantec Integrated Enforcer for Network Access Protection

The Symantec Integrated Enforcer for Network Access Protection 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 Enforcer for Network Access Protection verifies that the clients comply with configured security policies before any clients can connect to a network.

The following required components must be installed before you can use the Symantec Integrated Enforcer for Network Access Protection:

Symantec Endpoint Protection Manager version 11.0.6	Required to create security policies in a centralized location and assign them to clients.
Windows 2008 server DHCP Server service as well as the Network Policy Server (NPS) service must also be installed on the same computer	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 Network Access Protection Integrated Enforcer.
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 Enforcer for Network Access Protection	Required to authenticate clients and enforce security policies.
Symantec Network Access Control client	Required installation of the Symantec Network Access Control client.

Installing the Integrated Enforcer for Microsoft Network Access Protection

You must install the Integrated Enforcer for Microsoft Network Access Protection 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.

To install the Integrated Enforcer for Microsoft Network Access Protection with the Installation Wizard

1. Insert the installation disc for Symantec Network Access Control into the DVD 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.
   - Click **Browse** to locate and select a destination folder, click **OK**, and 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 Endpoint Protection Manager > Symantec Integrated Enforcer**.

Uninstalling the Integrated Enforcer for Microsoft Network Access Protection

You can uninstall the Integrated Enforcer for Microsoft Network Access Protection from the Windows taskbar or the command line.

To uninstall the Integrated Enforcer for Microsoft Network Access Control from the Windows taskbar

1 On the Windows taskbar, click **Start > Control Panel > Add or Remove Programs**.

2 Click **Symantec Integrated Enforcer,** and then click **Remove**.

3 To respond the prompt about whether you want to remove the software, click **Yes**.

4 To respond the prompt about whether you want to restart the NAP server, do one of the following:

- 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 Integrated Enforcer for Microsoft Network Access Protection from the command line

1 Open a DOS command window.

2 At the command prompt, type: `MsiExec.exe /qn/X{A145EB45-0852-4E18-A9DC-9983A6AF2329}`

3 Restart the NAP server.

Stopping and starting the Network Access Protection server manually

Stop the Network Access Protection (NAP) server manually before upgrading to a new version of the Integrated Enforcer for Microsoft Network Access Control. You then restart it after you complete the upgrade.

To stop and start the NAP server manually

1. On the Windows taskbar, click **Start > Control Panel > Administrative Tools > Services**.
2. Click **NAP Server**.
3. Right-click, and then click **Stop**.
4. Click **Start**.

Chapter 21

Configuring the Symantec Network Access Control Integrated Enforcer for Microsoft Network Access Protection on an Enforcer console

This chapter includes the following topics:

About configuring a Symantec Integrated Enforcer for Microsoft Network Access Protection on an Enforcer console

After you complete the installation of the Symantec Integrated NAP Enforcer, you must perform the following tasks before the Symantec Integrated Enforcer for Microsoft Network Access Protection can become operational.

Table 21-1 Enforcer console configuration summary

Step	Action	Description
Step 1	Connect the Integrated Enforcer to at least one Symantec Endpoint Protection Manager.	Specify at least one Symantec Endpoint Protection Manager to which the Symantec Integrated Enforcer for Microsoft Network Access Protection can connect. You include the host name or IP address of 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 Enforcer for Microsoft Network Access Protection to a management server on an Enforcer console" on page 329.
Step 2	Encrypt communication between the Integrated Enforcer and the management server.	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 Enforcer for Microsoft Network Access Protection and a management server" on page 331.

Table 21-1 Enforcer console configuration summary *(continued)*

Step	Action	Description
Step 3	Name the Enforcer group.	Set up an Enforcer group name See "Setting up an Enforcer group name on the Symantec Integrated Enforcer for Microsoft Network Access Protection console" on page 332.
Step 4	Set up an HTTP communication protocol.	Establish HTTP communication between the Symantec Integrated Enforcer for Microsoft Network Access Protection and the Symantec Endpoint Protection Manager. See "Setting up an HTTP communication protocol on the Symantec Integrated Enforcer for Microsoft Network Access Protection console" on page 332.

Connecting a Symantec Integrated Enforcer for Microsoft Network Access Protection to a management server on an Enforcer console

You need to connect a Symantec Integrated Network Access Protection (NAP) 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

1. On the Windows taskbar of the Enforcer computer, click **Start > Programs > Symantec Endpoint Protection > Symantec Integrated NAP Enforcer**.

   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 8014 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 Enforcer for Microsoft Network Access Protection 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 Enforcer for Microsoft Network Access Protection 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 Enforcer for Microsoft Network Access Protection console

You need to establish a communication protocol between the Symantec Integrated Enforcer for Microsoft Network Access Protection and the Symantec Endpoint Protection Manager. Otherwise the communication between the Symantec Integrated Enforcer for Microsoft Network Access Protection 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 Enforcer for Microsoft Network Access Protection

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**.

Chapter 22

Configuring the Symantec Network Access Control Integrated Enforcer for Microsoft Network Access Protection on the Symantec Endpoint Protection Manager

This chapter includes the following topics:

About configuring the Symantec Integrated Enforcer for Microsoft Network Access Protection on the Symantec Endpoint Protection Manager

If you want to support the Symantec Integrated Enforcer for Microsoft Network Access Protection in a network environment, you must enable NAP enforcement on the Symantec Endpoint Protection Manager. Otherwise the Enforcer works incorrectly.

You also need to define one or more criteria for the Security Health Validator policy requirements. For example, you can verify whether or not the client's Security Health Validator policy is the latest one that has been installed on a client. If it is not the latest Security Health Validator policy, then the client is blocked and is therefore unable to connect to the network.

Table 22-1 Symantec Endpoint Protection Manager configuration summary

Step	Action	Description
Step 1	Enable Network Access Protection enforcement for clients.	Enable Network Access Protection enforcement for clients so that the Integrated Enforcer can run Security Health Validator policies. See "Enabling NAP enforcement for clients" on page 337.
Step 2	Optionally, verify that the Symantec Endpoint Protection Manager is managing the Symantec Network Access Control client or the Symantec Endpoint Protection client.	Set up a verification check to ensure that the management server manages the Symantec Network Access Control client or the Symantec Endpoint Protection client. See "Verifying that the management server manages the client" on page 338.
Step 3	Optionally, verify that the latest Security Health Validator polices are installed.	Verify that the Symantec Network Access Control client and the Symantec Endpoint Protection client have the latest Security Health Validator policies are installed See "Verifying Security Health Validator policies" on page 338.

Table 22-1 Symantec Endpoint Protection Manager configuration summary *(continued)*

Step	Action	Description
Step 4	Optionally, verify that clients pass the Host Integrity check.	Verify that clients are in compliance with the Host Integrity policy. See "Verifying that clients pass the Host Integrity check" on page 339.
Step 5	Optionally, configure logs for viewing on the Symantec Endpoint Protection Manager.	Enable the sending of log data to the Symantec Endpoint Protection Manager. See "Configuring logs for the Symantec Integrated Enforcer for Network Access Protection" on page 339.

Enabling NAP enforcement for clients

You must enable NAP (Network Access Protection) enforcement for Symantec Endpoint Protection and Symantec Network Access Control clients. If you do not enable NAP enforcement for clients, the Symantec Integrated Enforcer for Microsoft Network Access Protection cannot implement any Security Health Validator policies.

To enable NAP enforcement for clients

1. In 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.
3. On the **Policies** tab, click **General Settings**.
4. In the **Settings** dialog box, click **Security Settings**.
5. On the **Security Settings** tab, in the **Enforce Client** area, check **Enable NAP Enforcement**.

   The **Enable NAP Enforcement** setting is disabled by default.
6. Click **OK**.

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. Click **Servers**.
3. Under **View**, select the Enforcer group for which you want to verify that the management server manages the client.
4. Right-click the Enforcer group and select **Edit Properties**.
5. In the **Client Information area on the NAP Setting** tab in the **I-DHCP Settings** dialog box, check **Verify that the management server manages the client**.

   The **Verify that the management server manages the client** setting is disabled by default.
6. Click **OK**.

Verifying Security Health Validator policies

You can make sure that the Symantec Endpoint Protection and Symantec Network Access Control clients have the latest Security Health Validator policies installed.

To verify Security Health Validator policies

1. In the Symantec Endpoint Protection Manager Console, click **Admin**.
2. Click **Servers**.
3. Under **View,** select the group for which you want to set up Security Health Validator policies.
4. Right-click the Enforcer group and select **Edit Properties**.
5. In the **Client Information** area on the NAP Setting tab in the **I-DHCP Settings** dialog box, check **Verify that the Security Health Validator policy is current**.

   The **Verify that the Security Health Validator policy is current** setting is disabled by default.
6. Click **OK**.

Verifying that clients pass the Host Integrity check

You can set up a compliance check for clients on the Symantec Endpoint Protection Manager.

To verify that clients pass the Host Integrity check

1. In the Symantec Endpoint Protection Manager Console, click **Admin**.
2. Click **Servers**.
3. Under **View**, select the Enforcer group for which you want to verify that the client has passed the Host Integrity check.
4. Right-click the Enforcer group and select **Edit Properties**.
5. In the **Host Integrity Status** area on the **NAP Setting** tab in the **I-DHCP Settings** dialog box, check **Verify that the client passes the Host Integrity check**.

   The **Verify that the client passes the Host Integrity check setting** is disabled by default.
6. Click **OK**.

Configuring logs for the Symantec Integrated Enforcer for Network Access Protection

Logs for the Symantec Integrated Network Access Protection (NAP) Enforcer are stored on the same computer on which you installed the Symantec Integrated NAP Enforcer. Enforcer logs are generated by default.

If you want to view Enforcer logs 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

  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.

Section 6

Setting up guest access to the network with On-Demand clients

Chapter 23

Setting up temporary connections for Symantec Network Access Control On-Demand clients

This chapter includes the following topics:

About the 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, the Enforcer can install On-Demand clients on computers so that they are compliant. Once the Enforcer has installed an On-Demand client, it temporarily connects 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.

See "What you can do with On-Demand Clients" on page 33.

See "How the On-Demand Client works" on page 45.

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 product disc 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 product disc called CD1, the Symantec Endpoint Protection Manager software cannot install all of the required components.
- 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.

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.

- Checked the connection status between the Enforcer appliance and the management server on the console of the Enforcer appliance.

  See "Checking the communication status of an Enforcer appliance on the Enforcer console" on page 111.

  See "Show" on page 376.

- Enabled an HTTP redirect or DNS spoofing on the console of the Symantec Endpoint Protection Manager.

  The HTTP redirect or DNS spoofing is the IP address of the internal NIC (eth0) that is located on a Gateway or DHCP Enforcer appliance.

  See "Redirecting HTTP requests to a Web page" on page 147.

  See "Preventing DNS spoofing" on page 195.

  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.

- You must create the client group as a subgroup of the My Company group with Full Access rights.

  You add the client group on the Clients page as a subgroup of the My Company group on the Symantec Endpoint Protection Manager.

  Make sure that you write down the name of the Enforcer client group that manages Symantec Network Access Control On-Demand clients. If you do not create a separate group, then the Default group on the Symantec Endpoint Protection Manager takes over the management of the Symantec Network Access Control On-Demand clients.

- Created an optional separate location for an Enforcer client group on the Symantec Endpoint Protection Manager Console.

If you do not create a separate location for the group that manages the Symantec Network Access Control On-Demand or guest clients, then the default location is automatically assigned to the guest clients. The best practice is to create a separate location for the Enforcer client group on the Symantec Endpoint Protection Manager.

Location criteria help you define the criteria that can identify Symantec Network Access Control On-Demand or guest clients by its IP address, MAC address, host name, or other criteria. The best practice is to create a separate location to which all Symantec Network Access Control On-Demand or guest clients are automatically assigned if they want to connect to a network on a temporary basis without the correct credential.

You can add and assign a location to the Enforcer client group in the **Clients** page, under **Tasks**, on the Symantec Endpoint Protection Manager.

- Added and assigned an optional Host Integrity Policy to the Enforcer client group and location on the Symantec Endpoint Protection Manager Console.

  It is optional to add and assign a Host Integrity Policy to the Enforcer client group and location on the console of a Symantec Endpoint Protection Manager, but the best practice to specify the following criteria:

  - How frequently a host integrity check is run
  - Type of Host Integrity policy that you want to implement

  You can add and assign an optional Host Integrity Policy to an Enforcer client group and location in the **Policies** page, under **Tasks**, on the Symantec Endpoint Protection Manager.

- Enabled an optional pop-up message on the Symantec Endpoint Protection Manager Console.

- Obtain the domain ID number that is located on the Symantec Endpoint Protection Manager Console.

  You should have the domain ID handy because you may need to configure the domain ID on the Gateway or DCHP Enforcer with the on-demand spm-domain command.

  See “Enabling Symantec Network Access Control On-Demand clients to temporarily connect to a network” on page 347.

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

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 344.

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 347.

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 100.

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 344.

4. Type the following command:

   Enforcer (on-demand)# `client-group "My Company/`*`name of Enforcer client group`*`"`

   where:

   name of Enforcer client group represents the name of the Enforcer client group that you already set up in the Clients page under View Clients on the console of a Symantec Endpoint Protection Manager. You should have already set up this Enforcer client group as a subgroup to the My Company group with full access rights. If you have not set the Enforcer client group on the console of a Symantec Endpoint Protection Manager, the Enforcer registers to the Default group. The information about the Enforcer client group is automatically sent during the next heartbeat.

   You can now set up authentication for the Symantec Network Access Control On-Demand clients.

   See "Setting up authentication on the Gateway or DHCP Enforcer console for Symantec Network Access Control On-Demand clients" on page 349.

5. Type the following command:

   Enforcer (on-demand)#`enable`

Disabling Symantec Network Access Control On-Demand clients

If you want to stop allowing guest access, you can disable it.

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

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

   See "Logging on to an Enforcer appliance" on page 100.

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 with On-Demand clients by enabling one of the following for authentication.

- The local database that is on-board of the Gateway and DHCP Enforcer appliance
  See "Setting up user authentication with a local on-board database" on page 349.
- A Microsoft Windows Server 2003 Active Directory configured to manage the authentication of the end users with the Gateway and DHCP Enforcer appliances.
  See "Setting up user authentication with a Microsoft Windows 2003 Server Active Directory" on page 350.
- A RADIUS server configured to manage the authentication of the end users with the Gateway and DHCP Enforcer appliances.
  See "Setting up user authentication with a RADIUS server" on page 351.

Once you enable authentication, add user names and a password for each authenticated end user.

Setting up user authentication with a local on-board database

You can configure up to 1000 users in the local database on-board the Gateway or DHCP Enforcer appliance.

See "On-Demand authentication local-db commands" on page 358.

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 100.

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)# local-db add user name username
password password
```

5 Type the following command:

```
Enforcer (authentication)# local-db enable
```

6 Type the following command:

```
Enforcer (authentication)# enable
```

Setting up user 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 355.

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 100.

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)# `ad domain` *`domain`* `name` *`alias name`*

5 Type the following command:

Enforcer (authentication)# `ad enable`

6 Type the following command:

Enforcer (authentication)# `enable`

Setting up user authentication with a RADIUS server

You can set up and configure one or more RADIUS servers for authentication. For example, you might want to have multiple RADIUS servers for load balancing.

See "On-demand authentication RADIUS server commands" on page 357.

To set up the On-Demand client for authentication with a RADIUS server

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

   See "Logging on to an Enforcer appliance" on page 100.

2. Type the following command:

   ```
   Enforcer# on-demand
   ```

3. Type the following command:

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

4. Type the following command:

   ```
   Enforcer (authentication)# radius add name alias name server
   RADIUS sever address secret shared secretauth_method auth method
   ```

   where:

   - *alias_name* represents the name displayed for the RADIUS authentication method listed in **Auth Server** in the logon dialog box.
   - *RADIUS server address* represents the RADIUS server and port. Port is an optional number between 1 and 65535. If you do not specify a port number the Enforcer uses a default of port 1812.
   - *shared secret* is the shared secret on the RADIUS server.
   - *auth method* is PAP, CHAP, MS-CHAP-V1, or MS-CHAP-V2.

5. Type the following command:

   ```
   Enforcer (authentication)# radius enable
   ```

6. `Enforcer (authentication#enable`

In addition to the RADIUS add name and RADIUS enable commands, you can run other RADIUS commands to manage the RADIUS server.

See "Setting up user authentication with a RADIUS server" on page 351.

Setting up the On-Demand client on Windows for authentication with the dot1x protocol

The Gateway and DHCP Enforcer appliances can connect to dot1.x-enable ports for internal clients.

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 the tftp server from which the Enforcer appliance can import the certificate by tftp.

   symantec is the password of the user certificate

   janedoe is the user name with which you log on the client.

   qa.pfx is the name of the user certificate.

   qa.cer is the name of the root certificate

Setting up the On-Demand client on Windows for authentication with the peap protocol

Gateway and DHCP Enforcer appliances can establish a connection with the peap protocol.

To set up the On-Demand client on Windows for authentication with the peap protocol

1. On the Enforcer console, type: `Enforcer#on-demand`
2. Type the following command: `Enforcer (on-demand)# dot1x`
3. Type the following command: `Enforcer (dot1x)# protocol peap`
4. Type the following command: `Enforcer (peap)# show protocol`

   Make sure that the peap server certificate is enabled; for example:

   ```
   PEAP Validate Server Certificate:       ENABLED
   PEAP Certificate Server:                DISABLED
   PEAP Certificate Server:                127.0.0.1
   PEAP Fast Reconnected:                  DISABLED
   ```

5. 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.

On-Demand authentication commands

Set up user authentication for Symantec Network Access Control On-Demand clients from the Gateway pr DHCP Enforcer appliance console.

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:

- The local database that is resident on a Gateway or a DHCP Enforcer appliance.
  You can choose to use the local on-board database to add user names and passwords for individual users.
- Active Directory server configured to work with the Gateway or DHCP Enforcer appliance.
  You must be able to connect to a Microsoft Windows Server 2003 Active Directory configured to work with a Gateway or DHCP appliance.
- RADIUS Server
  You must be able to connect to one or more RADIUS servers.

Table 23-1 provides information about the on-demand authentication command.

Table 23-1 On-demand authentication arguments

Command	Description
ad	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 355.
disable	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 357.
default	Sets the authentication methods (Active Directory, on-board local database, or RADIUS server) guest users can select when they log on. See "On-demand authentication default command" on page 354.
enable	Enables authentication of the Symantec Network Access Control On-Demand clients on the Gateway and DHCP Enforcer appliances. Once enabled, 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 356.
local-db	Enables authentication through the use of the on-board local database on the Gateway and DHCP Enforcer appliance. See "On-Demand authentication local-db commands" on page 358.
radius	Enables authentication through a RADIUS server. See "On-demand authentication RADIUS server commands" on page 357.
show	Lists the status information about the different options and arguments of the authentication command.
upload	Uploads authentication-related files to a server.

On-demand authentication default command

The on-demand authentication default command provides users with one or more authentication methods for logging on as guests. Configure Active Directory, local database, or one or more RADIUS server methods by using the on-demand default command. When more than one method has been configured, users select a method from the **Auth Server** drop-down list in the On-Demand client download **Welcome** screen.

The on-demand authentication default command uses the following syntax:

```
on-demand authentication default ad | radius | local-db index
```

Where:

ad, radius, and local-db represent the authentication method and index represents the index of the RADIUS server.

The following example describes how to specify the Active Directory and RADIUS server methods:

```
Enforcer# on-demand
Enforcer (on-demand)# authentication
Enforcer (authentication)# default ad | radius radiusAuthServerIndex
```

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 or a RADIUS server 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 100.

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 domain name |
  name alias name
```

where:

Active Directory Domain domain name	Represents the domain name of a Microsoft Windows Server 2003 Active Directory.
alias name	Represents the name that is displayed for the Active Directory authentication method listed in **Auth Server** in the **Log on** dialog box.

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 name symantec
```

where:

symantec.com represents the alias name displayed for Auth Server in the **Log on** dialog box.

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:

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

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 100.

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 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 100.

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 RADIUS server commands

To authenticate guest users with RADIUS servers, you must add a RADIUS server configuration on a Gateway Enforcer appliance or a DHCP Enforcer appliance. Once you add RADIUS servers, you can customize RADIUS attributes, or delete them.

See "Setting up user authentication with a RADIUS server" on page 351.

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 100.

On-demand authentication radius server add command

The on-demand radius authentication add command syntax adds a RADIUS server configuration to a Gateway Enforcer appliance or a DHCP Enforcer appliance. This command uses the following syntax:

```
on-demand authentication radius add name alias_name server
RADIUS server address secret shared secret
auth method
```

where:

alias_name	The name that is displayed for the RADIUS authentication method listed in **Auth Server** in the logon dialog box
RADIUS server address	The RADIUS server address and port in the format of IP:*port* or host:*port*. You can accept the default port of 1812 or specify a port number between 1 and 65535. The RADIUS server alias name.
shared secret	The shared secret on the RADIUS server.
auth_method	One of the following authentication methods: ■ PAP (Password Authentication Protocol) ■ CHAP (Challenge Handshake Authentication) ■ MS-CHAP-1 (Microsoft CHAP, version 1) ■ MS-CHAP-V2 (Microsoft CHAP, version 2)

The following examples describe how to add a RADIUS server:

```
Enforcer# on-demand
Enforcer (on-demand)# authentication
Enforcer (authentication)# radius add name guests server
   IP:1812 shared secret8d#>9fq4bV)H7%a3-zE13sW CHAP
```

On-Demand authentication local-db commands

Your enterprise can choose to 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 choose to 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 user authentication with a local on-board database" on page 349.

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 100.

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 following describes how to add to the local-db:

```
Enforcer# on-demand
Enforcer (on-demand)# authentication
Enforcer (authentication)# local-db add user jim
```

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 following example describes how to enable the local-db:

```
Enforcer# on-demand
Enforcer (on-demand)# authentication
Enforcer (authentication)# local-db enable
```

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 following example describes how to disable the local-db:

```
Enforcer# on-demand
Enforcer (on-demand)# authentication
Enforcer (authentication)# local-db disable
```

On-Demand authentication local-db username commands

The on-demand local-db authentication username commands let you add, delete, and edit user names:

```
local-db add username string password string
local-db delete username string
local-db edit username string password string
local-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
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
```

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 100.

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 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 23-2 Connection troubleshooting

Symptom	Solution
Firewall is blocking the client from working when the user downloads the agent through PPTP VPN, CheckPoint VPN, or Juniper VPN.	Several possible solutions: ■ Change firewall settings to unblock UDP port 39999. ■ Add a static route to the Enforcer's route table. For example: `route add IP netmask NM device eth0` where IP and NM are the IP address and netmask of the client's IP address pool. This pool is configured on the VPN by the administrator.
Download times are sometimes long.	The client sometimes sends traffic to VeriSign, making the download speed somewhat long. A workaround is let the admin add the VeriSign to the trusted IP list.
Host Integrity check is sometimes long the first time.	A long Host Integrity check 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 with the following: `cclientctl.exe`
Upgrading the Enforcer does not initially contain the manual installation package.	This problem is due to the size of the packages taken together. The workaround is to upgrade the Enforcer and import the Client Manual Install Package on Symantec Endpoint Protection Manager first, and then enable On-Demand functionality on the Enforcer. That adds the manual installation files.
The redirect URL on the Enforcer will overwrite a previous redirect URL on Symantec Endpoint Protection Manager.	The redirect URL overwrite problem only happens when the On-Demand feature is enabled on the Enforcer. This is expected behavior.
Vista clients sometimes do not receive an IP address from the DHCP server.	This problem is a timing issue. Change the DHCP timeout setting to 12 seconds or more.
A normal user can not install the agent if JRE is not installed.	The workaround is to ensure that JRE is installed. Otherwise only Admin users can install JRE..

Table 23-2 Connection troubleshooting *(continued)*

Symptom	Solution
Wireless service is disconnected when the On-Demand client is installed and quits and 802.1x authentication is used.	The user should restart the wireless connection.
Systems that are running Norton 360 v. 2.x have a problem receiving the client.	To solve this problem, follow the manual download link to download and install and install the client.
With Firefox, you cannot download the client and NP Plugin with only user rights.	Installation of the NP plugin requires Admin rights.
Manual installation sometimes fails.	To solve this problem, you may need to install Microsoft patch KB893803. This patch is included with the manual install, and should be installed before the client installation. Admin privileges are required.
802.1x authentication fails	The agent needs to install a driver to work. If the user needs 802.1x authentication on Windows Vista, the user needs to open the browser with the "Run as Administrator" method or turn off UAC to make sure that the agent works with Administrator privileges.
"Old version of ActiveX detected" message appears	You should delete the existing ActiveX by clicking **Tools -> Manage Add-ons -> Enable or Disable Add-ons -> Downloaded ActiveX Controls**, and deleting **HodaAgt class**.
Browser notifies the user , "can not display webpage," and the client cannot download successfully.	The client may already be running. As a security feature, you cannot download a new client inside of a running client session.
Firefox browser sometimes cannot download the client.	This problem happens when Firefox runs first. The first few Firefox restarts are required for it to finish its configuration. After that the On-Demand client should download.
Computers running Mac OS 10.4 sometimes do not authenticate properly due to a changing hostname.	This appears to be a problem with this version of the Mac OS. Version 10.5 and later does not have the problem. The workaround for version 10.4 is to set the hostname in `/etc/hostconfig/`.

Table 23-2 Connection troubleshooting *(continued)*

Symptom	Solution
Custom Host Integrity checks that rely upon the system variable %temp% do not work.	This is because of the transitory nature of %temp%. The workaround is to point to different locations.
Custom Host Integrity rules that point to Windows registry values do not work properly.	This is because of the transient nature of user sessions.
Installation of Panda Titanium 2007 or Panda Internet Security 2007 or 2008 software causes a message to appear, "Please wait while Windows configures Symantec Network Access Control."	Panda deletes a crucial Symantec Network Access Control file. It is automatically reinstalled, and you may safely take no action.

Appendix A

Enforcer appliance command-line interface

This appendix includes the following topics:

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 A-1 describes the hierarchy for the Enforcer commands.

Table A-1 Enforcer appliance CLI command hierarchy

Top-level commands	First sub-level commands	Second sub-level commands
capture	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: ■ clear ■ compress ■ exit ■ filter ■ help ■ show ■ start ■ upload ■ verbose	Not available.
clear	Not available.	Not available.
configure	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: ■ advanced ■ clear ■ dns ■ exit ■ help ■ interface ■ interface-role ■ ntp ■ redirect ■ route ■ show ■ spm	Only the advanced command has a set of sub-level commands.

Table A-1 Enforcer appliance CLI command hierarchy *(continued)*

Top-level commands	First sub-level commands	Second sub-level commands
console	baud-rate, clear, exit, help, show, ssh, and sshkey The clear, exit, help, and show commands are available to the admin logon and root (superuser).	Not available.
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 A-1 Enforcer appliance CLI command hierarchy *(continued)*

Top-level commands	First sub-level commands	Second sub-level commands
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	See each command for information about second sub-level commands.
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.

Table A-1 Enforcer appliance CLI command hierarchy *(continued)*

Top-level commands	First sub-level commands	Second sub-level commands
update	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 A-2 lists the CLI keyboard shortcuts and help.

Table A-2 CLI keyboard shortcuts and help

Keys or key combinations	Action
Tab key or ?	Pressing the tab key or typing ? can do the following: ■ List all available commands or all available options. ■ Completes the command or the option name. ■ Lists all possible commands or options that start with the letters that you typed. See "Getting help with CLI commands" on page 371.
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
```

Keys or key combinations	Action
Up-arrow key Down-arrow key	Restores the commands in the history buffer by moving up and down by index.
Left-arrow key Right-arrow key	Moves the cursor a character to the left and right.
Home and End keys	Moves the cursor to the beginning or end of the command line.
Backspace key	Deletes a character on the command line that is to the left of the cursor.
Delete key	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 A-3 shows the ways in which you can get help with CLI commands.

Table A-3 Getting help with CLI commands

What would you like to do?	Action
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 A-3 Getting help with CLI commands *(continued)*

What would you like to do?	Action
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`

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 for 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 **?** 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 |
 hostname| status | update | version }
```

where:

capture	Displays the packet capture settings such as protocol, filters, and compression.
configure	Shows the Enforcer network and the Symantec Endpoint Protection Manager configuration.
console	Shows the console configuration
status	Shows the Enforcer service detail status.
update	Shows the update available for installation from tftp or the CD-ROM or USB drive.
version	Shows the Enforcer version and copyright information.
date	Displays local time and UTC time.
debug	Displays the Enforcer debug configuration.
hostname	Displays 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, 2010-04-29,19:09
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 or the CD-ROM or USB drive.

The following is an example of the syntax for the update command:

```
Enforcer:# update
```

Index