Symantec™ Network Access Control 5.1.7 Linux Agent User Guide

Symantec Network Access Control 5.1.7 Linux Agent User Guide

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

Documentation version 5.1.7 MR7

Legal Notice

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

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014

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 feature and function. The Technical Support group also authors content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's maintenance offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- A telephone and web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers automatic software upgrade protection
- Global support that is available 24 hours a day, 7 days a week
- Advanced features, including Account Management Services

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

www.symantec.com/techsupp/

Contacting Technical Support

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

www.symantec.com/techsupp/

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

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

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

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

Licensing and registration

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

www.symantec.com/techsupp/

Customer service

Customer service information is available at the following URL:

www.symantec.com/techsupp/

Customer Service is available to assist with the following types of issues:

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

Maintenance agreement resources

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

- Asia-Pacific and Japan: contractsadmin@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:

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

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

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

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

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

www.symantec.com

Select your country or language from the site index.

Contents

Technical Support

Chapter 1 System Requirements

Chapter 2 Configuring the Symantec Policy Manager to manage the Linux Agent

Index

Chapter 1

System Requirements

This chapter includes the following topics:

- Supported Linux Platforms

Supported Linux Platforms

The following Linux platforms are supported in this release:

- Red Hat Linux Enterprise Linux 3 Update 0 to 8 (x86_32 and x86_64)
- Red Hat Linux Enterprise Linux 4 Update 0 to 4 (x86_32 and x86_64)
- Fedora Core 6 initial release (x86_32 and x86_64)
- SuSE Linux Enterprise Server 10 initial release (x86_32 and x86_64)

Chapter 2

Configuring the Symantec Policy Manager to manage the Linux Agent

This chapter includes the following topics:

About this documentation

This addendum supplements the documentation for Symantec Enterprise Protection 5.1. That documentation is included with this release in PDF format, and is fully valid. Only changes from that documentation appear in this addendum. This addendum explains how to configure the Symantec Policy Manager to work with the Linux agent.

Overview

This documentation describes how to install and use Symantec Network Access Control Enforcement Agent for Linux, one of the components of Symantec Enterprise Protection suite of products.

The Symantec Network Access Control Enforcement Agent for Linux (Linux agent) is security software that runs on your Linux system and ensures that your computer complies with the policies set in Policy Manager by your administrator.

The Linux Agent has the job of monitoring your computer to ensure that it is secure and alerting you if your system requires updates. The Agent runs periodic checks to verify that your computer complies with security policies.

To protect the enterprise network, your computer may be blocked from connecting to the network if your security software is not up to date. Policy Manager and the Linux agent work in conjunction with the Symantec Policy Manager, communicating with and receiving security instructions from the Symantec Policy Manager server.

Your system administrator has defined the security policies that the Symantec Policy Manager distributes to a variety of agents, such as Windows agents, Mac agents, Linux agents, and XP Embedded agents, across the enterprise network. The Policy Manager serves as a centralized point of control over all agents. It enables system administrators to define and distribute security policies, collect logs, and maintain the integrity of the corporate network. It deploys security policies to the Linux Agent, sends out updated intrusion detection signatures, and handles security issues for the enterprise.

Linux agents' policies are automatically updated when it connects to the Symantec Policy Manager, repeatedly and periodically while connected. As an integral part of enterprise security, Linux agent also keeps track of attempted violations of security policies, and transfers this information in logs to the Symantec Policy Manager.

Note: Linux agent only supports Policy Manager 5.1.7 or higher releases.

Enforcer and Linux Agent may also interact with the Symantec Enforcer, if one is installed in your network. The Enforcer ensures that all computers connecting to the network paths it protects are running the Agent and have the proper security policy implemented.

Note: Linux agent supports Symantec Enforcer 5.x only.

For LAN Enforcer mode, the Linux agent currently supports transparent mode only.

Key features of Linux Agent 1.0 support

The new SNAC Enforcement Agent features available in this release for Linux 1.0 are as follows:

- Ongoing communication between the Linux agent and the Symantec Policy Manager server allow ongoing downloads of the newest polices and up-to-date uploads of essential Agent and server information. This constant checking between the Agent and Policy Manager is called the heartbeat. The heartbeat is set in the Policy Manager. If a new policy is defined for the group to which an Agent belongs, it receives that new policy at the next heartbeat. Updated policies are delivered as part of the Agent profile.

  Note: Communication between the Linux agents and the Symantec Policy Manager server are based on HTTP protocol only in this release.

- The Auto-Location switching features allow the Linux agent to switch its location automatically or manually based on the conditions defined with the Symantec Policy Manager. The Agent can be customized by the Policy Manager to automatically recognize the environment, or location, in which it is working, and immediately switch to the security policy that has been created for that location. Each Agent can be configured to have a variety of locations predefined, each location providing an appropriate security policy.
- Host Integrity features allow the Linux agent to check its Host Integrity to make sure its environment is secure. Each Agent can be required to have certain applications running (virus protection, for example) and to be blocked from network access until that application is up to date and running on the Agent computer. The Agent can then be automatically routed to the appropriate location for downloading and installing the updates that are needed. Those updates can include operating system patches and completely separate programs.

- Enforcement features allow the Linux agent to communicate with Symantec Enforcer. Linux Agent can also be deployed in conjunction with 5.x Enforcer, which adds an additional protective layer of security that ensures that all computers connecting to the network paths it protects are running the Agent and have the proper security policy implemented.
- Graphical user interface features in the Symantec Policy Manager display necessary Linux agent information. The Linux agent has a user-friendly interface providing useful information, such as connection status and Host Integrity check results.
- Install and Uninstall features allow the user to install and uninstall the Linux agent by exporting zip files from the Symantec Policy Manager containing either an RPM package or shell scripts.

Configuring the Symantec Policy Manager

After you install the Symantec Policy Manager and restart your computer, the Symantec Server Configuration Wizard launches. You see the Symantec Server Configuration panel.

Note: If the wizard does not launch, select Start>Programs>Symantec Policy Manager>Server Configuration Assistant to launch the wizard. The Symantec Server Configuration panel appears.

Use the Server Configuration Wizard to:

- Configure the Policy Manager
- Create a new site or add the server to an existing site
- Create a Linux agent log database

To configure the Symantec Policy Manager

1. Read the welcome message on the Symantec Server Configuration panel and click **Next**.
2. In the Server Information panel, accept the defaults for server name, server port, and server root or specify alternate values. Click **Next**.
3. If you are installing the first Policy Manager on this site, select **Install a new Site** and click **Next**.
4. If you are installing an additional Policy Manager on this site, select **Add this server** to an existing site and click **Next**.

5 In the **Site Information** panel, type the site name and then browse and select the license file.

6 Type a value in the **Preshared Secret** field. Make a note of the Preshared Secret value so that you can use it later to register Enforcer and configure other software features. Click **Next**.

7 In the **Database Server Choice** panel, select **Embedded Database** and click **Next**.

8 In the

In the Linux Database Server Information panel, type a password. Make a note of your password for future use. Click **Next**.

9 Wait until the Configuration Completed panel appears. In the **Configuration Completed** panel, check **Start Symantec Policy Manager** and **Start Management Console**. Click **Finish**.

10 In the Symantec Policy Management Console, log in for the first time as **admin**and type the password as **admin**. Leave the domain blank. Because you are installing on your local host, the wizard automatically fills in your server name. Click **Login**.

11 Reset your password.

Deploying and installing a Linux Agent to the client

This portion of the documentation assumes that you have deployed agents to other types of clients and are familiar with the process. This documentation describes how to export an installation package from Symantec Policy Manager and use it to deploy a Linux agent to the client.

Note: Before deploying and installing a Linux agent to the client, first set up each group's policies from the Symantec Policy Manager and then export a default package containing configured security policies.

To export a Policy Manager installation package

1 Open the Client Manager tab of the Symantec Policy Management Console.

2 From the tree in the left pane of the tab, click **Client Manager**>**Agent Packages**>**Current Packages**.

3 From **Current Agent Packages**, select **Symantec Enforcement Agent for Linux 5.1.7-xxx**.

4. Right-click the name of the agent package and then click **Export package** on the context menu.
5. From the **Export Package** panel, select a directory into which to export the package.
6. Select an Operating System (**Linux OS**) type.
7. Choose an export package format: **RPM** or **Normal** (shell script).
8. Click **Export a default package without security policies** and specify a Symantec Policy Manager List.
9. Click **OK**.
10. Click **Close** on the Exporting Package panel.
11. Copy the package to the target client for installation by `rpm` package or shell script.

To install the Linux Agent package on the client computer

1. If your system administrator has not already installed the software on your computer, you have probably been given instructions on where to find the Agent software and how to install it yourself. If not, begin by unzipping the package.

   Note: The Linux agent is designed to start automatically when you turn on your computer.

   Unzip a NORMAL package (shell script) with the following command:

   Unzip slea-5.1.7-xxxx.zippack .zip

   OR

   Unzip an RPM package with the following command:

   Unzip slea-5.1.7-xxxx.rpmpack.zip

2. To install by RPM, enter:

   #rpm –ivh slea-5.1.7-xxxx.i386.rpm

   OR

   To install by shell script, enter:

   #chmod a+x install.sh

   #./install.sh

3. Please look through EULA carefully, and type **yes** to proceed.

   The Linux agent default directory is `/opt/slea`, and it is not possible to change this during the installation. The Linux agent GUI (`smcgui`) taskbar icon should display after the installation if the server has started.

   The red dot will turn to **green** if the connection with Policy Manager is OK.

To view connection information:

- Enter:

  #cat /opt/slea/status

To start or stop the Linux agent service (`smcservice`)

- Enter:

  #service smcservice start

  or

  #service smcservice stop.

To start the Linux agent GUI (`smcgui`)

- Enter:

  Redhat: "Applications" >> **"Internet"** >> **"Symantec Enforcement Agent"**;**SuSE: "More Applications"** >> **"Symantec Enforcement Agent"**;

Uninstalling the Linux Agent

This section describes how to uninstall the Linux agent software.

To uninstall the Linux Agent software

- To uninstall by **rpm**: enter

  #rpm –e slea

  or

  To uninstall by **Normal** (shell script): enter

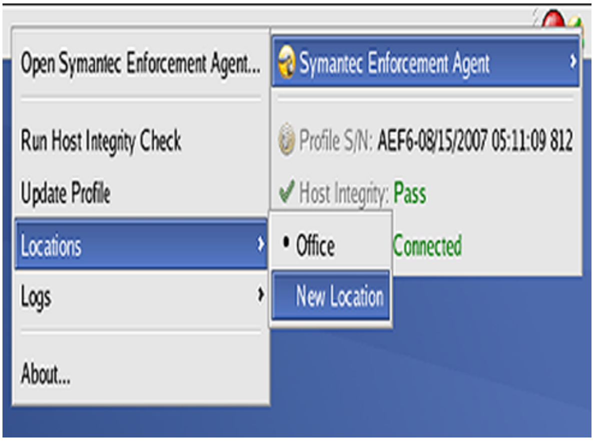
  #/opt/slea/uninstall.sh

Switching Linux Agent locations

To switch configured locations manually

1 Click the Linux Agent taskbar icon

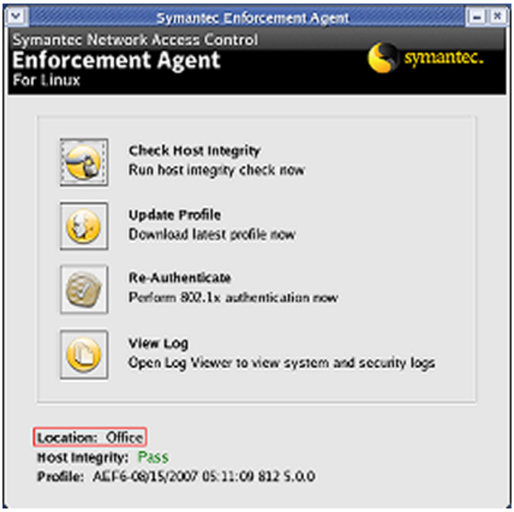
2 Click **Locations**



3 Click to select a pre-configured alternate location by name.

To view configured locations

- Open the main Linux agent console to view the currently configured location for the client.


Symantec Enforcement Agent
Symantec Network Access Control
Enforcement Agent
For Linux
symantec.
Check Host Integrity
Run host integrity check now
Update Profile
Download latest profile now
Re-Authenticate
Perform 802.1x authentication now
View Log
Open Log Viewer to view system and security logs

Location: Office
Host Integrity: Pass
Profile: AEF6-08/15/2007 05:11:09 812 5.0.0

To view Agent information

1. On the Symantec Policy Management console, click the Client Manager tab and select the group to which the Linux agent belongs.
2. Right click the name of the Linux agent in the right pane, then click **Properties** on the popup menu.

   The agent’s information is displayed.

Configuring Linux Agent communication modes

There are two types of connection modes between the Symantec Policy Manager server and the Linux agent: PUSH mode and PULL mode.

In PUSH mode the Agent communicates with the Symantec Policy Manager server normally with a stable HTTP connection until the Agent is stopped or the Agent could no longer communicate with the server. After changes are made on the Symantec Policy Manager server, those changes are "pulled" to the Linux agent and the agent then receives a new profile from the server.

In PULL mode the Agent sends a specified request to the Symantec Policy Manager server periodically, and based on the request, the server will send a response back to the agent, after which the Agent fetches the newest profile from the Symantec

Policy Manager server. After all the related profiles are received, the connection is closed. The Agent then periodically reconnects to the Symantec Policy Manager server to check if any changes have been made to the profile. If nothing has been updated, the Agent closes the connection again. If the check indicates that some change to the profile on the server has taken place, the Agent requests the index profile to check what the changes are and then fetches the newest related profiles from the Symantec Policy Manager server. After the Agent has received all the profiles, this connection is again closed.

Note: refer to `Symantec Policy Manager Administration Guide` for more information.

Communication between the Symantec Policy manager and the Linux agent include the following types of updates:

- Update of the Linux agent's HI policy
- Update of the Linux agent's group settings
- Update of the configured Linux agent location settings
- Update of the XML-formatted Sylink registration file
- Update of the communication mode: PUSH or PULL
- Update of the Symantec Policy Manager server information
- Update of the Log settings

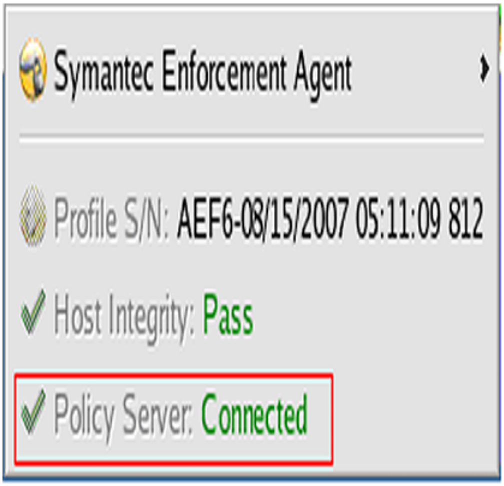
To configure a Linux Agent communication mode

1. On Policy Manager, select the Policies tab, and click **Linux Agent group** to edit.
2. Click **Communication**, then select **PULL** or **PUSH** mode.

To check connection status

- Click the Linux a gent icon in the taskbar to display the Policy Server connection status.

  Server connection status between the Linux agent and the Symantec Policy Manager is monitored as either "Connected" or "Disconnected".



Symantec Enforcement Agent

Profile S/N: AEF6-08/15/2007 05:11:09 812

Host Integrity: Pass

Policy Server: Connected

To download the latest profile manually

- Download the latest profile manually in two different ways:

  Click the Linux Agent taskbar icon, then click the **Update Profile** menu:

  OR

  Open the main console window of the Agent, and click the **Update Profile** button:

To display the Linux Agent Profile Format and Serial Information

- View the profile format number and serial number display at the bottom of the Linux agent main console:

Configuring Linux Agent Log Settings

The Linux agent posts System log and Security logs to the Symantec Policy Manager using HTTP.

The following log options and settings can be configured using the Symantec Policy Manager server:

- Choose if the log created by the Agent should be uploaded to the Symantec Policy Manager server
- Set the size of each log
- Set the time the log should be saved in the Symantec Policy Manager server

When the Linux agent is running on the client computer, the System log created by the agent is uploaded to the Symantec Policy Manager server at every heartbeat. The uploading of the Security logs to the Symantec Policy Manager is enabled by the log setting of SyLink file. When the Linux agent is running on the client computer, the Security log created by the agent is also uploaded to the Symantec Policy Manager server at every heartbeat.

The System log includes the following contents:

- The Linux Agent version and the current network status
- The status of the Agent: running, stopped, or terminated
- Contact requests from the Agent to the Symantec Policy Manager server
- Whether the Linux agent Host Integrity check is enabled or disabled
- The location to which the Linux agent has been switched
- Whether or not the Agent could download the newest profile from the Symantec Policy Manager server or not

The Security log includes the following contents:

- Whether the Linux agent's Host Integrity checks have passed or failed
- Whether the system logs were uploaded to the Symantec Policy Manager server
- Whether uploading the system log to the log setting of the SyLink file is enabled
- Whether the Linux agent was able to successfully build a connection to the Symantec Policy Manager server

Additionally, agent information can be set to upload to the Symantec Policy Manager server at every heartbeat as well.

Agent information uploads to the Symantec Policy Manager server include the following contents:

- Version of the Linux agent
- Build number of the Linux agent
- Profile serial number of the Linux agent
- Profile format number of the Linux agent
- Signature file serial number of the Linux agent

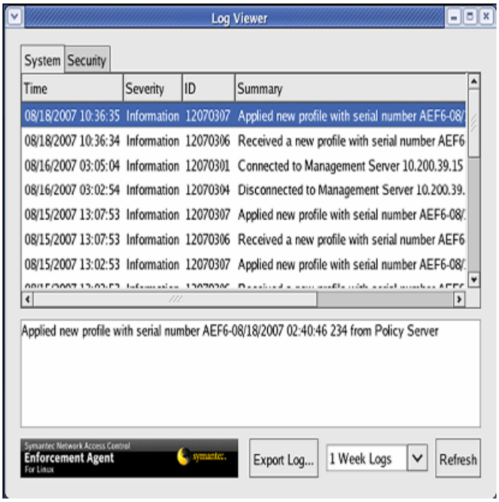
- OS information specific to where the Linux agent is installed on the client

To view log files

The Linux agent supports System and Security log viewing. There are two ways to view logs:

◆ View the Linux Agent logs from the Symantec Policy Manager by selecting the **Monitoring** tab, and select **Log Viewer**.

Select the Log type by clicking on the **System** or **Security** tab in the Log Viewer, set the length of log monitoring to be included in the log (example, **1 Week** worth of log information), then click **Refresh**. Click **Export Log** to obtain a copy of the log.



Time	Severity	ID	Summary
08/18/2007 10:36:35	Information	12070307	Applied new profile with serial number AEF6-08/
08/18/2007 10:36:34	Information	12070306	Received a new profile with serial number AEF6
08/16/2007 03:05:04	Information	12070301	Connected to Management Server 10.200.39.15
08/16/2007 03:02:54	Information	12070304	Disconnected to Management Server 10.200.39.
08/15/2007 13:07:53	Information	12070307	Applied new profile with serial number AEF6-08/
08/15/2007 13:07:53	Information	12070306	Received a new profile with serial number AEF6
08/15/2007 13:02:53	Information	12070307	Applied new profile with serial number AEF6-08/

Applied new profile with serial number AEF6-08/18/2007 02:40:46 234 from Policy Server

OR

Click the Linux Agent taskbar icon and select **Logs** > **System Log**, or **Logs** > **Security Log** from the popup menu:

To edit Linux Agent log settings

1. On the Policies tab, select the group to which the Linux agent belongs, then click the **Log Settings** link and select whether the log created by the Agent should be uploaded to the Symantec Policy Manager server.
2. Set the Maximum Size of each log.

Configuring Linux Agent Auto-location switching

Auto-location allows the Linux agent to switch between configured locations such as office, home and remote locations, automatically or manually, as configured in the Symantec Policy Manager.

Note: Manual location switching of the agent assumes that the client machine meets the requirements of the selected location.

The following configurable switching options are supported for the Linux agent in the Symantec Policy Management console:

- Agent IP Address
  This option allows the auto-location switch to occur based on the IP address of the Agent machine. In the Symantec Policy Management console, set IP address in the auto-location policy.
  Three types of IP addresses can be configured:
  a) One single IP address
  b) One IP range
  c) One subnet.
  These options can be combined in the auto-location policy. The following actions are supported:
  a) If the IP address the Agent machine matches any of IP address/ IP range/ Subnet values set in the condition
  b) If all the IP addresses of the Agent machine matches the IP address/ IP range/ Subnet set in the policy condition
  c) If none of the IP addresses of the Agent machine match any of IP address/ IP range/ Subnet values set in the condition

- Gateway Address
  This switch option allows the auto-location switching to occur based on the Gateway Address of the Agent machine. Configure the Gateway Address in the auto-location policy using four optional types of addressing options:
  a) One single IP address
  b) One IP range
  c) One subnet.
  These types can be combined in the auto-location policy.
  The following actions are supported:
  a) If the Gateway Address of the Agent machine matches any of IP address, IP range, or Subnet value set in the condition
  or

b) If none of the Gateway Addresses of the Agent machine matches any of IP address, IP range, or Subnet values set in the condition.

- DNS Server IP Address

  This switch option allows the auto-location switch to occur based on the DNS IP address of the Agent computer.

  Three types of DNS addresses can be configured:

  a) One single IP address

  b) One IP range

  c) One subnet

  These types can be combined in the auto-location policy.

  The following actions are also supported:

  a) If the DNS address the Agent machine uses matches any of IP address/ IP range/ Subnet set in the condition

  b) If all the DNS addresses of the Agent machine match the IP address/ IP range/ Subnet set in the condition

  c) If none of the DNS addresses of the Agent machine matches any of IP address/ IP range/ Subnet set in the condition

- Policy Manager Connection

  This option allows auto-location switching to occur by configuration of the Policy Manager Connection. Policy Manager Connection supports the following switching configurations:

  a) Switch to a specified location when the Linux agent connects to the Symantec Policy Manager

  b) Switch to a specified location when the Linux agent does not connect to the Symantec Policy Manager

- DHCP Server Address

  This option allows auto-location switching to occur based on the DHCP Server IP Address of the Linux agent machine. Four types of addresses can be configured:

  a) One single IP address

  b) One IP range

  c) One subnet

  These types can be combined in the auto-location policy.

  The following actions are also supported:

  a) If the DHCP server Address of the Agent machine matches any of IP address, IP range, or Subnet values set in the condition

  or

  b) If none of the DHCP server Addresses of the Agent machine matches any of IP address, IP range, or Subnet values set in the condition.

- Network Connection

  This option allows auto-location switching to occur based on how the Agent builds a network connection with the Symantec Policy Manager. The supported network connection options include:

  a) Any network connection type

  b) Ethernet network connection

  c) Wireless network connection

  The following actions can also be configured supported:

  a) The Linux agent performs the auto-location switching after the network connection type of the Agent computer matches the network connection type configured in the switch policy

  or

  b) The Linux agent performs the auto-location switching after the network connection type of the Agent computer does not match the network connection type in the switch policy.

- DNS Lookup

  This option allows auto-location switching to occur based on whether the specified IP Address is resolved from the Hostname of the Agent machine and matches the IP Address set in the auto-location policy.

  There the following configurations must be set for this switch option:

  a) The hostname of the Linux agent computer

  b) The IP address of the Linux agent computer

  The following actions are supported:

  a) The Agent performs the auto-location switching if the IP address resolved by the Linux agent computer's hostname matches the IP Address configured in the policy

  b) The Agent performs the auto-location switching if the IP address resolved by the Linux agent computer's hostname does not match the IP Address configured in the policy.

- Remote Device Communication

  This option allows auto-location switching to occur based on the communication status between the Linux agent and the Symantec Policy Manager server. There are two auto-location actions supported:

  a) The Linux agent performs the auto-location switching if the Agent can ping a a specified host normally

  b) The Agent performs the auto-location switching if the Agent cannot ping a specified host normally.

  The configurable Location-detection timer must be set for remote device communication to occur. When the Linux agent is running, location detecting and location switching take place automatically according to location-detection timer settings.

The location-detection timer alerts the Agent to perform the location-detection, and if it detects a change in a configured Gateway Address, DHCP Server IP address, DNS IP Address, Network connection type, DNS name lookup, or Remote Device communication configuration, the auto-location switching occurs based on the settings in the auto-location profile.

Note: For manual location switching, the Agent location must support switching of the location manually. If changes to a configured Gateway Address, DHCP Server IP address, DNS IP Address, Network connection type, DNS name lookup, or Remote Device communication configuration are detected, the location to which the Agent is to be switched can be performed manually.

To set location-detection to enable the Agent to switch locations automatically

1. In the Policies Tab, select the group to which the agent belongs, then click **Add Location**.
2. Click **Edit** to define conditions and set the location-detection timer; the, default location-detection timer value is 30 seconds.

To set location-detection to switch Agent locations manually

- If the client machine meets the requirements of a given location, then you can switch the Agent to this location manually.

Configuring Linux Agent Host Integrity policies

The Host Integrity feature performs protective checks of the Linux agent computer's system settings, security settings, and application installations against the configured policies you specify in the Symantec Policy Manager settings.

To view Host Integrity check results

- View your Linux agent Host Integrity check result(s) in either of two ways:

  Click on the **Linux Agent taskbar icon**

  OR

  Open the Linux Agent main console:

Antivirus enforcement

The Host Integrity feature includes AntiVirus enforcement. Configure this Host Integrity option to check whether Symantec Antivirus for Linux or another antivirus program is installed and running on the Agent machine. The supported antivirus types are:

a) Any supported AntiVirus application

b) Symantec AntiVirus Corporation Edition

The Host Integrity feature also supports the installation of a supported antivirus application if it has not yet been installed on the Linux agent computer. A predefined URL from which to download the software is provided, or an execute command is issued, depending on your configuration.

The option to start an antivirus program if it is not running on the Linux agent is also provided, as well as support for antivirus signature file checking and updating. Additionally, the option to allow the Host Integrity check to pass even if a specified requirement fails is also available.

To add an antivirus policy to a Linux agent location

1. From the Policies tab of the Symantec Policy Management Console, select **Host Integrity Policies** from left pane, and click **Add a Policy**.
2. In the Requirements tab, enter a policy name, and select **Linux** as the OS type.
3. Click the **Add** button and enter a requirement name, then select the Type as **AntiVirus enforcement**.
4. In the Requirements dialog, select **Symantec AntiVirus Corporation Edition** (other antivirus programs are not supported at this time). Click **OK**.
5. Customize the settings as needed.

Firewall enforcement

Configure this Host Integrity option to check whether the Linux firewall iptables are installed and running on the Linux agent machine. The supported types include:

a) Any supported Firewall Application "iptables"

b) Only check whether firewall is running

c) Allow HI check to pass even if this requirement fails

To add a Linux firewall enforcement policy to a Linux agent location

1. On the Symantec Policy Manager **Policies** tab, select **Host Integrity Policies** from the left pane.
2. Click **Add a Policy**.
3. In the Requirements tab, enter a policy name, and select the OS type as **Linux**.
4. Click **Add** and enter a requirement name, then select Type as **Firewall enforcement**.
5. In the Requirement dialog, select **iptables** and customize the settings as required.

Custom Host Integrity checking

The supported custom configuration options for Host Integrity checking include:

- AntiVirus: AntiVirus is installed
- AntiVirus: AntiVirus is running
- AntiVirus: AntiVirus signature file is up to date
- File: File exists
- File: File fingerprint equals
- File: Compare file size to
- File: Compare file date to
- File: Compare file age to
- Firewall: Firewall is running
- Utility: Operating system is specified
- Utility: Process is running
- Utility: Service is running
- Utility: Operating system language is specified
- Functions: Utility: Wait
- Utility: Run a program
- Utility: Run a script
- File: Download a file
- Utility: Set Timestamp

Note: Supported OS platforms for Linux Custom Host Integrity checks are as follows: SuSE Linux Enterprise Server 10; Fedora Core 6; Red Hat Enterprise Linux 3; Red Hat Enterprise Linux 4. The supported script for Linux Custom Host Integrity checks is shell script. The Linux Custom Host Integrity environment variables comply with Linux conventions, e.g., `$HOME`.

To configure custom Host Integrity enforcement checks

1. On the Symantec Policy Management Console **Policies** tab, select **Host Integrity Policies** from the left pane, and click **Add a Policy**.
2. In the Requirements tab, enter a policy name, and select OS type as **Linux**.

3 Click **Add** button and enter a requirement name, then select the type as **Custom enforcement**.

4 Customize Host Integrity policies as required.

Linux Host integrity template support

You can add a Linux Host Integrity template to the Linux agent with the Symantec Policy Manager.

To add a Linux Host Integrity template

1 On the Symantec Policy Manager **Policies** tab, select **Host Integrity Policies** from the left pane, and click **Add a Policy**.

2 In the Requirements tab, enter a policy name, and select OS type as **Linux**.

3 Click the **Template** button and select the template desired. (If there is no existing template listed, you may customize one for yourself..)

Please refer to the *Symantec Policy Manager Administration Guide* for more information about creating custom templates.

Integrating the Linux Agent with Symantec Enforcer

LAN Enforcer

Linux agent communicates with both the switch and the LAN Enforcer to complete 802.1x authentication during Host Integrity checks, and/or also authenticates the user account information used to decide the set of resources the Linux agent computer has the right to access.

Linux agent supports the 802.1x protocol and works as an 802.1x supplicant with the following process:

- Accepts the Identity Request from the switch
- Sends the Identity Response to the switch
- Receives the EAP Challenge and the Host Integrity Challenge from the switch
- Send the EAP Response and Host Integrity Response to the switch
- Receives the `Auth` result from the switch

According to the `auth` result, the Agent receives the access rights according to the Response Result from the switch.

For more details, please refer to the *Symantec Policy Manager Administration Guide* and *Symantec Enforcer Installation and Administration Guide*.

Note: Linux Agent supports transparent mode in this release.

To set 802.1x authentication manually

- Click Re-Authenticate on the main Enforcement Agent console.

  This button is only available after 802.1x settings are enabled using the Symantec Policy Manager.

Gateway Enforcer

The Linux agent always communicates with the Symantec Policy Manager but it also connects to an internal network through the Gateway Enforcer by using authentication results (`Agent GUID, HI check, Profile SN`).

Usually, administrators set policies that grant access to the gateway according to the Host Integrity check results. These policies allow:

- Access to internal sites if Host Integrity check(s) Pass
- Always communicate with the Symantec Policy Manager server
- Re-direction to a specified remediation URL so the user can obtain resources that meet the requirements of Host Integrity if the Host Integrity check(s) Fail

Please refer to the *Symantec Policy Manager Administration Guide* and *Symantec Enforcer Installation and Administration Guide* for more information.

DHCP Enforcer

DHCP Enforcer controls the different access actions of a Linux agent computer by allocating to it the different IP addresses defined by different DHCP servers (Quarantine and Normal DHCP servers).

A Quarantine IP address allocated to an Agent is only used to perform authentication.

A Normal IP address allocated to an Agent is used to access the internal sites allowed.

The Linux agent receives the DHCP Enforcer’s IP address from the config profile and builds the connection to the DHCP Enforcer.

The Linux agent supports the following DHCP Enforcer functions:

- Receives the Quarantine address from the Quarantine DHCP server through the DHCP Enforcer.
- Sends the packet with Host Integrity check results to the DHCP Enforcer to perform the Authentication and receives the result from the DHCP Enforcer.

- If the Host Integrity check passes, the Agent releases the Quarantine address currently under instruction by the DHCP Enforcer, and receives the Normal IP address from the Normal DHCP Server through the DHCP Enforcer.
- If the Host Integrity check fails, the Agent keeps the Quarantine address and is re-directed to a specified remediation URL from which the related package is obtained, then installs these packages to meet the Host Integrity requirements.

For more details, please refer to the *Symantec Policy Manager Administration Guide* and *Symantec Enforcer Installation and Administration Guide*.

Note: The Linux agent currently works with 5.x Enforcer.

Index