Altiris Symantec™ Endpoint Protection Integration Component 7.1 SP2 User Guide

Altiris Symantec™ Endpoint Protection Integration Component 7.1 SP2 User Guide

Legal Notice

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 support offerings, you can visit our Web site at the following URL:

www.symantec.com/business/support/

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

Contacting Technical Support

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

www.symantec.com/business/support/

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

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

- Product release level

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

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

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

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

Contents

Chapter 1

Introducing Symantec Endpoint Protection Integration Component

This chapter includes the following topics:

About Endpoint Protection Integration Component

The Symantec Endpoint Protection Integration Component combines Symantec Endpoint Protection with your other Symantec Management Platform solutions. You can inventory computers, update patches, deliver software, and deploy new computers. You can also back up and restore your systems and data, manage DLP agents, manage Symantec Endpoint Protection clients. You can do this work from a single, Web-based Symantec Management Console.

You can perform common Symantec Endpoint Protection client management operations from the Symantec Management Console.

See "What you can do with Symantec Endpoint Protection Integration Component" on page 11.

What's new in Endpoint Protection Integration Component 7.1 SP2

In the 7.1 SP2 release of Endpoint Protection Integration Component, the following features are introduced:

- Symantec Management Platform 7.1 SP2 support:
  The Endpoint Protection Integration Component 7.1 SP2 release supports Symantec Management Platform 7.1 SP2 on the Windows Server 2008 R2 SP1 64-bit operating system.
- Inventory and migration support:
  The Endpoint Protection Integration Component 7.1SP2 release supports inventory and migration support for the following antivirus releases:
  - Symantec Endpoint Protection 11.0.6300.803
  - Symantec Endpoint Protection 11.0.7072.1031
  - Symantec Endpoint Protection 12.0.1001.95
  - Symantec Endpoint Protection 12.1.671.4971
  - Symantec Endpoint Protection 12.1.825.23

System requirements

Endpoint Protection Integration Component requires the following software to be installed:

- Symantec Management Platform 7.1SP2.
  When you install Endpoint Protection Integration Component using Symantec Installation Manager, the Symantec Management Platform is installed automatically.
- Symantec-Real Time Console Infrastructure 7.1 SP2.

The operating systems that are supported by the Symantec Management Platform are also supported by Endpoint Protection Integration Component.

For more information, see the product support matrix at the following URL:
http://www.symantec.com/docs/HOWTO9965

What you can do with Symantec Endpoint Protection Integration Component

Symantec Endpoint Protection Integration Component lets you perform common Symantec Endpoint Protection client management operations from the Symantec Management Console.

Specifically, Symantec Endpoint Protection Integration Component lets you perform the following tasks:

- Run an Antivirus Inventory.
  See "Running an antivirus inventory" on page 22.
- View summaries of the antivirus software that is installed in your environment.
  See "Viewing summaries of the antivirus versions that are installed in your environment" on page 41.
- Uninstall antivirus software remotely.
  See "Uninstalling antivirus software remotely" on page 31.
- Create Symantec Endpoint Protection client installation packages.
  See "Creating Symantec Endpoint Protection client installation packages" on page 22.
- Install Symantec Endpoint Protection clients remotely.
  See "Installing Symantec Endpoint Protection clients remotely" on page 30.
- View computers on which Symantec Endpoint Protection client rollouts are successful.
  See "Viewing computers on which the Symantec Endpoint Protection client rollout is successful" on page 42.
- View computers on which Symantec Endpoint Protection client rollout has failed.
  See "Viewing computers on which the Symantec Endpoint Protection client rollout is successful" on page 42.
- Repair Symantec Endpoint Protection clients.
  See "Repairing Symantec Endpoint Protection clients" on page 33.
- Repair and reboot remote client computers using SERT
  See "Using the remote SERT boot and repair task" on page 35.
- Perform power-sensitive malware scanning
  See "Using power sensitive malware scanning" on page 34.
- Migrate computers to the latest Symantec Endpoint Protection client.

See "Migrating computers to the latest Symantec Endpoint Protection client" on page 23.

- Update the content of Symantec Endpoint Protection clients.
  See "Updating the content of Symantec Endpoint Protection clients" on page 33.
- View computers on which Tamper Protection is detected and enabled.
  See "Viewing computers on which Tamper Protection is detected and enabled" on page 42.
- Run Quick Scans for viruses and security risks.
  See "Running a Quick Scan for viruses and security risks" on page 32.
- Run Full Scans for viruses and security risks.
  See "Running a full scan for viruses and security risks" on page 25.
- View your unmanaged computers that are discovered.
  See "Viewing your unmanaged computers that are discovered" on page 43.
- View the status of Symantec Management Agent installations.
  See "Viewing the status of Symantec Management Agent installations" on page 41.

See "About Endpoint Protection Integration Component" on page 9.

See "Getting started with Symantec Endpoint Protection Management" on page 17.

Components of Symantec Endpoint Protection Integration Component

This section describes the components that Symantec Endpoint Protection Integration Component works with.

Table 1-1 Components of Symantec Endpoint Protection Integration Component

Component	Description
Symantec Management Platform with SQL Server database	Symantec Management Platform installs and manages the Symantec Management Agent on client computers, and it manages your Configuration Management Database.
Symantec Management Console	The Symantec Management Console is the interface for the Symantec Management Platform and is automatically installed with the platform.

Table 1-1 Components of Symantec Endpoint Protection Integration Component *(continued)*

Component	Description
Symantec Endpoint Protection Integration Component	Symantec Endpoint Protection Integration Component lets you perform common Symantec Endpoint Protection client management tasks from the Symantec Management Console.
Task Server	Symantec Endpoint Protection Integration Component uses Task Server for task sequencing and automation of its tasks. Task Server is automatically installed with the Symantec Management Platform.
Symantec Management Agent (installed on client computers)	To use the Symantec Management Platform with Windows client computers, you must install the Symantec Management Agent on them. To run Symantec Endpoint Protection tasks from the Symantec Management Console, the client computers must have the Symantec Management Agent installed. Following the installation of the Symantec Management Platform, you can install the agent on your client computers.
Symantec Endpoint Protection client (installed on client computers)	The Symantec Endpoint Protection client software is installed on client computers. It lets Symantec Endpoint Protection Manager secure your environment. You can manage the Symantec Endpoint Protection client from the Symantec Management Console by installing Symantec Endpoint Protection Integration Component.
Client Task Agent and Script Task Agent (installed on client computers)	The Symantec Management Platform includes Task Server to run management tasks in sequence. Symantec Endpoint Protection Integration Component requires that two Task Server agents are installed on your client computers. Following the installation of Symantec Endpoint Protection Integration Component, you must install the Client Task Agent and the Script Task Agent on your client computers.

See "Getting started with Symantec Endpoint Protection Management" on page 17.

About Endpoint Protection Integration Component resource filters

The Symantec Management Platform lets you organize your computer resources into groups. These groups are called resource filters.

Computer resources are automatically organized into filters. Symantec Endpoint Protection Integration Component automatically adds each client computer to its applicable filter.

For more information, see topics about resource filters in the *Symantec Management Platform User Guide*.

Where to get more information

Use the following documentation resources to learn about and use this product.

Table 1-2 Documentation resources

Document	Description	Location
Release Notes	Information about new features and important issues.	The **Supported Products A-Z** page, which is available at the following URL: http://www.symantec.com/business/support/index?page=products Open your product's support page, and then under **Common Topics**, click **Release Notes**.
User Guide	Information about how to use this product, including detailed technical information and instructions for performing common tasks.	■ The Documentation Library, which is available in the Symantec Management Console on the **Help** menu. ■ The **Supported Products A-Z** page, which is available at the following URL: http://www.symantec.com/business/support/index?page=products Open your product's support page, and then under **Common Topics**, click **Documentation**.

Table 1-2 Documentation resources *(continued)*

Document	Description	Location
Help	Information about how to use this product, including detailed technical information and instructions for performing common tasks. Help is available at the solution level and at the suite level. This information is available in HTML help format.	The Documentation Library, which is available in the Symantec Management Console on the **Help** menu. Context-sensitive help is available for most screens in the Symantec Management Console. You can open context-sensitive help in the following ways: ■ The F1 key when the page is active. ■ The Context command, which is available in the Symantec Management Console on the **Help** menu.

In addition to the product documentation, you can use the following resources to learn about Symantec products.

Table 1-3 Symantec product information resources

Resource	Description	Location
SymWISE Support Knowledgebase	Articles, incidents, and issues about Symantec products.	http://www.symantec.com/business/theme.jsp?themeid=support-knowledgebase
Symantec Connect	An online resource that contains forums, articles, blogs, downloads, events, videos, groups, and ideas for users of Symantec products.	http://www.symantec.com/connect/endpoint-management

Chapter 2

Getting Started with Symantec Endpoint Protection Integration Component

This chapter includes the following topics:

Getting started with Symantec Endpoint Protection Management

Symantec Endpoint Protection Management includes a Quick Start tool to help you get started. The quick start tool is located on the Symantec Endpoint Protection Management portal page.

See "About Endpoint Protection Integration Component" on page 9.

To get started with Symantec Endpoint Protection Management

1. In the Symantec Management Console, on the **Home** menu, click **Symantec Endpoint Protection Management**.
2. Using the Quick Start page, complete the following steps:

Table 2-1 Process for getting started with Symantec Endpoint Protection Management

Step	Action	Description
Step 1	Import Microsoft Active Directory.	Before you can manage computers, you must complete the following tasks: ■ Discover the computers on your network. ■ Create resources for them in the CMDB. This process is called discovery and lets you discover the computers on which you can install the Symantec Management Agent and various solution agent/plug-ins. You can import all computers that are registered in your Microsoft Active Directory. You can choose to import only a subset of your computers that match the criteria you specify. You can also discover Windows computers with resource discovery . For more information, see topics about discovering Windows computers in the *Symantec Management Platform User Guide*.

Table 2-1 Process for getting started with Symantec Endpoint Protection Management *(continued)*

Step	Action	Description
Step 2	Install the Symantec Management Agent.	The Symantec Management Agent is the software that is installed on a computer to enable the Notification Server computer to monitor and manage it. To manage your computers with the Symantec Management Platform, you must first install the Symantec Management Agent on them. For more information, see topics about installing the Symantec Management Agent in the *Symantec Management Platform User Guide*.
Step 3	Run antivirus inventory.	The antivirus inventory task checks your managed computers for the known types of antivirus software. Antivirus inventory also retrieves information about computers with tamper protection enabled. Antivirus inventory can also retrieve details about the version of Symantec Endpoint Protection virus definitions. See "Running an antivirus inventory" on page 22.
Step 4	Configure Endpoint Protection packages.	Before you can remotely migrate and install the Symantec Endpoint Protection client on your managed computers, you must first configure the installation package. You must configure the installation package locally on the Notification Server computer. See "Creating Symantec Endpoint Protection client installation packages" on page 22.

Table 2-1 Process for getting started with Symantec Endpoint Protection Management *(continued)*

Step	Action	Description
Step 5	Run migration job.	The migration job uninstalls any existing antivirus software, and then it installs a new Symantec Endpoint Protection client on the computers that you specify. See "Migrating computers to the latest Symantec Endpoint Protection client" on page 23.
Step 6	View computers on which the Symantec Endpoint Protection client rollout task has failed.	You can view a list of the computers that the Symantec Endpoint Protection client rollout task has failed to run on. See "Viewing computers on which the Symantec Endpoint Protection client rollout task has failed" on page 25.
Step 7	Run Full Scan Task.	You can run a full scan for viruses and security risks on the computers that you specify. See "Running a full scan for viruses and security risks" on page 25.

See "About Endpoint Protection Integration Component" on page 9.

See "Components of Symantec Endpoint Protection Integration Component" on page 12.

About Antivirus Inventory

Symantec Endpoint Protection Integration Component lets you deploy and manage your Symantec Endpoint Protection clients from the Symantec Management Console. Symantec Endpoint Protection Integration Component includes a feature called Antivirus Inventory. When Antivirus Inventory is run, it searches for common types of antivirus software. If a recognized type of antivirus is located on a managed computer, this data is stored for reporting purposes. This data is also reflected in the Antivirus Version Summary pie-chart and the Antivirus Summary report on the Symantec Endpoint Protection Home page.

Antivirus Inventory can also identify computers with tamper protection enabled. If the feature tamper protection is enabled on a computer, the computer is

displayed in the following report: **Computers on which tamper protection is detected and enabled**.

See "Viewing computers on which Tamper Protection is detected and enabled" on page 42.

If computers have a recognized type of antivirus, the antivirus software is first removed before your Symantec Endpoint Protection client package is installed. This functionality occurs if you apply the following tasks:

- **Migrate computers to latest Symantec Endpoint Protection client**.
- **Install Symantec Endpoint Protection client**.
- **Uninstall antivirus**.

See "Migrating computers to the latest Symantec Endpoint Protection client" on page 23.

See "Installing Symantec Endpoint Protection clients remotely" on page 30.

See "Uninstalling antivirus software remotely" on page 31.

Symantec Endpoint Protection Integration Component can remove the following software from your managed computers:

- *CA Anti-Virus for Enterprise*
- *CA eTrust Threat Management Agent*
- *ESET*
- *F-Secure Anti-Virus for Windows Servers*
- *Kaspersky Antivirus*
- *Trend MICRO OfficeScan*
- *McAfee Virus Scan Enterprise*
- *McAfee Virus Scan Enterprise*
- *Sophos Anti-Virus*
- *Sophos Endpoint Security and Control*
- *Symantec Anti Virus*
- *Symantec Endpoint Protection*
- *Symantec Endpoint Protection Small Business Enterprise Edition*

See "Running an antivirus inventory" on page 22.

Running an antivirus inventory

You can run an inventory of the antivirus software that is installed on your managed computers. Running an antivirus inventory can help you to determine which groups of computers may be vulnerable. You can then migrate these computers to have the latest version of Symantec Endpoint Protection client installed.

See "About Antivirus Inventory" on page 20.

You can create an inventory by scheduling the antivirus inventory task to run on the groups of computers that you specify. The inventory information is displayed in the **Antivirus Version summary** Web part after you run the antivirus inventory task.

Running the antivirus inventory on a regular basis is a good practice to continue tracking the installed version of Symantec Endpoint Protection. This practice help you identify computers in your environment that need to be migrated.

To run an antivirus inventory

1. In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**.
2. In the left pane, click **Jobs and Tasks > System Jobs and Tasks > Symantec Endpoint Protection Management > Antivirus inventory**.
3. On the **Antivirus inventory** page, Click **New Schedule** to schedule the task and to define the computers that you want to run the antivirus inventory task on.

   For more information, see topics about using tasks in the *Symantec Management Platform User Guide*.
4. On the **New Schedule** page, click **Schedule**.

   The status of your task is displayed under **Task Status**.

See "Getting started with Symantec Endpoint Protection Management" on page 17.

See "Types of tasks for Symantec Endpoint Protection Integration Component" on page 28.

Creating Symantec Endpoint Protection client installation packages

You must create a Symantec Endpoint Protection client package before you can install and migrate Symantec Endpoint Protection clients from the Symantec Management Console. You must upload the Symantec Endpoint Protection client

SETUP.EXE file into the Symantec Management Platform. The Symantec Management Platform creates a software package that you can roll out using Software Management Framework packaging features.

For more information, see topics about configuring packages in the *Symantec Management Platform User Guide*.

See "Getting started with Symantec Endpoint Protection Management" on page 17.

Note: This task must be performed locally on your Notification Server computer.

To create a Symantec Endpoint Protection client package

1. In the Symantec Management Console, on the **Settings** menu, click **All Settings**.
2. In the left pane, click **Settings > Software > Symantec Endpoint Protection > Client Package Configuration**.
3. On the **Client Package Configuration** page, under **Symantec Endpoint Protection Packages**, click **New**.
4. On the **Create Symantec Endpoint Protection Client Package** page, complete the following options:

Symantec Endpoint Protection Package Type	The type of computers that you intend the package to run on; either 32-bit or 64-bit.
Package Name	The name of the installation package. The package name must be a valid Windows folder name because a folder is created on the Notification Server computer using this name.
Symantec Endpoint Protection Setup File	The location of the Symantec Endpoint Protection client SETUP.EXE file. The SETUP.EXE file must be stored locally on the Notification Server computer.

5. Click **OK**.

Migrating computers to the latest Symantec Endpoint Protection client

You can migrate your managed computers to the latest version of Symantec Endpoint Protection client. To accomplish this goal you run an antivirus software

migration job. The migration job stages the new installer on the client computers, it then uninstalls existing antivirus software. The job then installs a new Symantec Endpoint Protection client on the computers that you specify.

See "Types of tasks for Symantec Endpoint Protection Integration Component" on page 28.

Note: You must create at least one Symantec Endpoint Protection client software package before you can use this job.

See "Creating Symantec Endpoint Protection client installation packages" on page 22.

To migrate computers to the latest Symantec Endpoint Protection client

1. In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**.
2. In the left pane, click **Jobs and Tasks > System Jobs and Tasks > Symantec Endpoint Protection Management**, right-click, and then click **New > Job or Task**.
3. On the **Create New Task** page, in the left pane, click **Symantec Endpoint Protection Management > Migrate computers to latest Symantec Endpoint Protection Client**.
4. On the **Create New Task** page, in the right pane, complete the following options:

Name	Name of the job.
Description	Description of the job.
Package	The software package that contains the Symantec Endpoint Protection client SETUP.EXE file.
Restart After Old Antivirus Uninstall	Forces the target computers to restart after the previous antivirus version is removed. See "Creating Symantec Endpoint Protection client installation packages" on page 22.
Restart After Endpoint Protection Install	Forces the target computers to restart after the Symantec Endpoint Protection client is installed.

5 Click **Ok**.

6 In the left pane, click **Jobs and Tasks > System Jobs and Tasks > Symantec Endpoint Protection Managment**, and then click your job.

7 In the right pane, click **New Schedule** to schedule the task and to define the computers that you want to run the antivirus inventory task on.

For more information, see topics about using tasks in the *Symantec Management Platform User Guide*.

8 On the **New Schedule** page, click **Schedule**.

The status of your job is displayed under **Task Status**.

See "Getting started with Symantec Endpoint Protection Management" on page 17.

Viewing computers on which the Symantec Endpoint Protection client rollout task has failed

You can view reports on the computers that the Symantec Endpoint Protection client rollout task has failed to run on.

To view computers on which the Symantec Endpoint Protection client rollout task has failed

1 In the Symantec Management Console, on the **Reports** menu, click **All Reports**.

2 In the left pane, click **Reports > Symantec Endpoint Protection Management > Computers on which Symantec Endpoint Protection Client rollout task has failed**.

3 On the **Computers on which Symantec Endpoint Protection Client rollout task has failed** page, in the right pane, view the report.

For more information, see topics about using reports in the *Symantec Management Platform User Guide*.

See "Symantec Endpoint Protection Integration Component reports" on page 40.

See "Getting started with Symantec Endpoint Protection Management" on page 17.

Running a full scan for viruses and security risks

You can use the Symantec Management Platform to remotely run full scans for viruses and security risks on the computers that you specify.

See "Types of tasks for Symantec Endpoint Protection Integration Component" on page 28.

To run a full scan for viruses and security risks

1. In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**.
2. In the left pane, click **Jobs and Tasks > System Jobs and Tasks > Symantec Endpoint Protection Management > Full scan for viruses and security risks**.
3. In the right pane, click **New Schedule** to schedule the task and to define the computers on which you want to run the antivirus inventory task.

   For more information, see topics about Using Tasks in the *Symantec Management Platform User Guide*.
4. On the **New Schedule** page, click **Schedule**.

   The status of your task is displayed under **Task Status**.

See "Getting started with Symantec Endpoint Protection Management" on page 17.

Chapter 3

Completing jobs and tasks with Symantec Endpoint Protection Integration Component

This chapter includes the following topics:

About tasks for Endpoint Protection Integration Component

Symantec Endpoint Protection Integration Component provides several predefined tasks that you can use to manage your Symantec Endpoint Protection clients. You can execute these tasks on the groups of computers that you organize with filters.

For more information, see topics about task management in the *Symantec Management Platform User Guide*.

Symantec Endpoint Protection Integration Component includes the following tasks:

- Antivirus inventory.
- Full Scan of viruses and security risks.
- Install Symantec Endpoint Protection client.
- Migrate computers to latest Symantec Endpoint Protection client.
- Quick Scan of viruses and security risks.
- Power sensitive malware scanning.
- Using the remote SERT boot and repair task
- Repair Symantec Endpoint Protection client.
- Uninstall antivirus.
- Update content of Symantec Endpoint Protection client.

See "Types of tasks for Symantec Endpoint Protection Integration Component" on page 28.

Types of tasks for Symantec Endpoint Protection Integration Component

Symantec Endpoint Protection Integration Component includes several tasks. You can use tasks to manage your Symantec Endpoint Protection clients and to protect your environment against viruses and security risks.

For more information see topics about task management in the *Symantec Management Platform User Guide*.

Table 3-1 Tasks of Symantec Endpoint Protection Integration Component

Task	Description
Antivirus inventory	Creates an inventory of the antivirus software that is installed on the computers that you specify. See "Running an antivirus inventory" on page 22.
Full Scan of viruses and security risks	Runs a full scan for viruses and security risks on the computers that you specify. See "Running a full scan for viruses and security risks" on page 25.
Install Symantec Endpoint Protection client	Installs a new Symantec Endpoint Protection client on the computers that you specify See "Installing Symantec Endpoint Protection clients remotely" on page 30.
Migrate computers to latest Symantec Endpoint Protection client	Stages a new Symantec Endpoint Protection client , then uninstalls the previous antivirus software. The task then installs a new Symantec Endpoint Protection client on the computers that you specify. See "Migrating computers to the latest Symantec Endpoint Protection client" on page 23.
Power sensitive malware scanning	This power sensitive malware scanning job lets you turn on one or multiple systems with Wake-on-LAN and Intel vPro technologies. You can then update the content of Symantec Endpoint Protection clients and run a scan for viruses and security risks. The computers are then turned off after these tasks are completed. See "Using power sensitive malware scanning" on page 34.
Quick scan of viruses and security risks	Runs a Quick Scan for viruses and security risks on the computers that you specify. See "Running a Quick Scan for viruses and security risks" on page 32.

Table 3-1 Tasks of Symantec Endpoint Protection Integration Component *(continued)*

Task	Description
Remote SERT boot and repair	This task lets you boot a remote Intel AMT enabled client computer. The bootable image contains the Symantec Endpoint Recovery Tool (SERT) to repair the client computer. See "Using the remote SERT boot and repair task" on page 35.
Repair Symantec Endpoint Protection client	Repairs the Symantec Endpoint Protection client on the computers that you specify. See "Repairing Symantec Endpoint Protection clients" on page 33.
Uninstall antivirus	Uninstalls any existing antivirus software on the computers that you specify. See "Uninstalling antivirus software remotely" on page 31.
Update content of Symantec Endpoint Protection client	Updates the Symantec Endpoint Protection client content on the computers that you specify. See "Updating the content of Symantec Endpoint Protection clients" on page 33.

See "About tasks for Endpoint Protection Integration Component" on page 28.

Installing Symantec Endpoint Protection clients remotely

You can use the Symantec Management Platform to remotely install new Symantec Endpoint Protection clients on the computers that you specify.

You can also use this task to roll out Symantec Endpoint Protection updated files.

Note: You must create at least one Symantec Endpoint Protection client software package before you can use this task.

See "Creating Symantec Endpoint Protection client installation packages" on page 22.

To install the Symantec Endpoint Protection client remotely

1. In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**.
2. In the left pane, click **Jobs and Tasks > System Jobs and Tasks > Symantec Endpoint Protection Management**, right-click, and click **New > Job or Task**.
3. On the **Create New Task** page, in the left pane, click **Symantec Endpoint Protection Management > Install Symantec Endpoint Protection Client**.
4. On the **Create New Task** page, in the right pane, complete the following options:

Option	Description
Name	The name of the package.
Package	The software package that contains the Symantec Endpoint Protection client SETUP.EXE file. See "Creating Symantec Endpoint Protection client installation packages" on page 22.

5. Click **OK**.
6. In the left pane, click **Jobs and Tasks > System Jobs and Tasks > Symantec Endpoint Protection Managment**, and then click your task.
7. In the right pane, click **New Schedule** to schedule the task and to define the computers that you want to run the antivirus inventory task on.

   For more information, see topics about Using Tasks in the *Symantec Management Platform User Guide*.
8. In the **New Schedule** page, click **Schedule**.

   The status of your task is displayed under **Task Status**.

See "Types of tasks for Symantec Endpoint Protection Integration Component" on page 28.

Uninstalling antivirus software remotely

You can use the Symantec Management Platform to uninstall existing antivirus software on the computers that you specify.

To uninstall antivirus software remotely

1. In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**.
2. In the left pane, click **Jobs and Tasks > System Jobs and Tasks > Symantec Endpoint Protection Management**, right-click, and click **New > Job or Task**.
3. On the **Create New Task** page, in the left pane, click **Symantec Endpoint Protection Management > Uninstall Antivirus**.
4. On the **Create New Task** page, name the task.
5. Click **OK**.
6. In the left pane, click **Jobs and Tasks > System Jobs and Tasks > Symantec Endpoint Protection Managment**, and then click your task.
7. In the right pane, click **New Schedule** to schedule the task and to define the computers that you want to run the antivirus inventory task on.

   For more information, see topics about using tasks in the *Symantec Management Platform User Guide*.
8. In the **New Schedule** page, click **Schedule**.

   The status of your task is displayed under **Task Status**.

See "Types of tasks for Symantec Endpoint Protection Integration Component" on page 28.

Running a Quick Scan for viruses and security risks

You can use the Symantec Management Platform to remotely run quick scans for viruses and security risks on the computers that you specify.

See "Types of tasks for Symantec Endpoint Protection Integration Component" on page 28.

To run a Quick Scan for viruses security risks

1. In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**.
2. In the left pane, click **Jobs and Tasks > System Jobs and Tasks > Symantec Endpoint Protection Management > Quick scan for viruses and security risks**.

3 In the right pane, click **New Schedule** to schedule the task and to define the computers that you want to run the antivirus inventory task on.

For more information, see topics about using tasks in the *Symantec Management Platform User Guide*.

4 On the **New Schedule** page, click **Schedule**.

The status of your task is displayed under **Task Status**.

Repairing Symantec Endpoint Protection clients

You can use the Symantec Management Platform to remotely repair the Symantec Endpoint Protection client on the computers that you specify.

To repair Symantec Endpoint Protection clients

1 In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**.

2 In the left pane, click **Jobs and Tasks > System Jobs and Tasks > Symantec Endpoint Protection Management > Repair Symantec Endpoint Protection Client**.

3 In the right pane, click **New Schedule** to schedule the task and to define the computers that you want to run the antivirus inventory task on.

For more information, see topics about using tasks in the *Symantec Management Platform User Guide*.

4 On the **New Schedule** page, click **Schedule**.

The status of your task is displayed under **Task Status**.

See "Types of tasks for Symantec Endpoint Protection Integration Component" on page 28.

Updating the content of Symantec Endpoint Protection clients

You can use the Symantec Management Platform to remotely update the Symantec Endpoint Protection client content on the computers that you specify. When the content is updated, the Symantec Endpoint Protection client is forced to update from the source for which it is configured: either Symantec Endpoint Protection Manager or the Internet.

To update the content of Symantec Endpoint Protection clients

1. In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**.
2. In the left pane, click **Jobs and Tasks > System Jobs and Tasks > Symantec Endpoint Protection Management > Update Content of Symantec Endpoint Protection Management Client**.
3. In the right pane, click **New Schedule** to schedule the task and to define the computers that you want to run the antivirus inventory task on.

   For more information, see topics about using tasks in the *Symantec Management Platform User Guide*.
4. On the **New Schedule** page, click **Schedule**.

   The status of your task is displayed under **Task Status**.

See "Types of tasks for Symantec Endpoint Protection Integration Component" on page 28.

Using power sensitive malware scanning

This power sensitive malware scanning job lets you turn on one or multiple systems with Wake-on-LAN and Intel vPro technologies. You can then update the content of Symantec Endpoint Protection clients and run a scan for viruses and security risks. The computers are then turned off after these tasks are completed.

See "Types of tasks for Symantec Endpoint Protection Integration Component" on page 28.

To use power sensitive malware scanning

1. In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**.
2. In the left pane, click **Jobs and Tasks > System Jobs and Tasks > Symantec Endpoint Protection Management**.
3. Right-click **Symantec Endpoint Protection Management**, then click **New > Task**.
4. On the **Create New Task** page, in the left pane, click **Symantec Endpoint Protection Management > Power Sensitive Malware Scanning**.

5 On the **Create New Task** page, in the right pane, complete the following options:

Name	Enter a name for the task.
Update content of Symantec Endpoint Protection clients	Enable this option if you need to update content, for example virus definition files.
Select scan type	Choose the malware scan type that you need the task to run.
Select power management technology	Select **Intel vPro** if your client computers are Intel vPro computers with AMT enabled. Select **Wake-on-LAN** if your client computers are Wake-on-LAN enabled. You can select **Both** if your targeted computers contain a combination of both technologies.

6 Click **OK**.

7 In the left pane, click **Jobs and Tasks > System Jobs and Tasks > Symantec Endpoint Protection Management**, and then click your task.

8 In the right pane, click **New Schedule** to schedule the task. On this page, configure the connection profile.

See "Configuring a connection profile for Endpoint Protection Integration Component tasks" on page 37.

9 On **New Schedule** page, select the targeted computers that you want to roll out the job.

10 Click on **schedule** to run a task.

11 In the **Task Management** page, you can view the status of the scheduled task.

Using the remote SERT boot and repair task

This task lets you boot a remote Intel AMT enabled client computer. The bootable image contains the Symantec Endpoint Recovery Tool (SERT) to repair the client computer. Use a remote control tool like Symantec pcAnywhere installed on the server computer. You can use pcAnywhere's Thost.exe running in the SERT ISO. This task first redirects to the boot-capable win-PE image with SERT and boots the client computer using this image. The task works irrespective of the power state of the Intel vPro computer. You can then repair the client computer using SERT tool by using remote control software.

For this task to work, you must have an Intel vPro managed computer with Symantec Management Agent installed on it. The AMT (Active Management Technology) protocol and the IDE Redirection feature must be enabled. These steps can be done when you provision the Intel computer.

For information about setting up AMT see:
http://www.fic.com.tw/product/AMT_Procedure.pdf

See "Types of tasks for Symantec Endpoint Protection Integration Component" on page 28.

To use the remote SERT boot and repair task

1. In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**.
2. In the left pane, click **Jobs and Tasks > System Jobs and Tasks > Symantec Endpoint Protection Management**, right-click, and then click **New > Task**.
3. On the **Create New Task** page, in the left pane, click **Symantec Endpoint Protection Management > Remote SERT Boot Task**.
4. On the Create New Task page, in the right pane, complete the following options:

Performe Boot From	Boot option : select **CD Image** if you boot from an ISO image. Use CD with ISO image only. DVD boot is not supported.
Browse	If you select the boot option, **CD Image**, then browse to the location where your ISO image is stored. If you select **CD/DVD** drive option then this option is disabled. The task automatically receives the boot location.

5. Click **OK**.
6. In the left pane, click **Jobs and Tasks > System Jobs and Tasks > Symantec Endpoint Protection Management**, and then click your newly created task.
7. In the right pane, click **New Schedule** to schedule the task. Select the computers that you want to run the Remote SERT Boot task on.
8. On the **New Schedule** page, configure a connection profile .

   See "Configuring a connection profile for Endpoint Protection Integration Component tasks" on page 37.
9. Click **Schedule** to run the task.
10. The status of your task is displayed under **Task Status**.

See "What you can do with Symantec Endpoint Protection Integration Component" on page 11.

Configuring a connection profile for Endpoint Protection Integration Component tasks

When you set up the power sensitive malware scanning task and the remote SERT boot task you must specify or create a connection profile. Use this topic to create and configure a connection profile.

To configure a connection profile for the power sensitive malware scanning task

1. When you schedule a task on the **New Schedule** page, you must click **Select Connection Profile**.

   See "Using power sensitive malware scanning" on page 34.

   See "Using the remote SERT boot and repair task" on page 35.

2. Select **Default Connection Profile**.
3. Do one of the following:
   - If you have already created and configured a connection profile, select it and click **OK**.
   - If you have not configured a connection profile, click **Edit** to configure and existing profile.
   - Click **Add Settings** to add a new connection profile. You must specify a name for the connection profile.
4. In the **Connection Profile** window, enable the AMT protocol.
5. Click **Add** to add new AMT credentials.
6. Select **AMT Credentials** from the **Credential Type** drop-down menu .
7. Enter your AMT user name and password. This password must match the password that was configured for AMT provisioning.
8. Click **OK**.
9. Select the name of your credential.
10. Select your new connection profile.

See "Types of tasks for Symantec Endpoint Protection Integration Component" on page 28.

Chapter 4

Viewing Symantec Endpoint Protection Integration Component Reports

This chapter includes the following topics:

About reports for Endpoint Protection Integration Component

The Symantec Management Platform collects up-to-date environmental information about your client computers. You can view this information in reports. Symantec Endpoint Protection Integration Component provides several reports that give you information on infected and at risk computers. You can also view reports about your Symantec Endpoint Protection clients.

For more information, see topics about using reports in the *Symantec Management Platform User Guide*.

See "Symantec Endpoint Protection Integration Component reports" on page 40.

Symantec Endpoint Protection Integration Component reports

You can view and manage your Symantec Endpoint Protection Integration Component data by using reports.

For more information, see topics about using reports in the *Symantec Management Platform User Guide*.

Table 4-1 Reports of Symantec Endpoint Protection Integration Component

Report	Description
Symantec Management Agent Installation Status	Lists the Agent installation status for the last week (by default). This list does not include agent pull install information. See "Viewing the status of Symantec Management Agent installations" on page 41.
Antivirus Version Summary	Lists the details about the versions of antivirus software that is installed in your environment. See "Viewing summaries of the antivirus versions that are installed in your environment" on page 41.
Computers on which Symantec Endpoint Protection Client rollout is successful	Lists the computers that the Symantec Endpoint Protection client rollout policy has been successfully run on. See "Viewing computers on which the Symantec Endpoint Protection client rollout is successful" on page 42.
Computers on which Symantec Endpoint Protection Client rollout task has failed	Lists the computers that the Symantec Endpoint Protection client rollout task has failed to run on. See "Viewing computers on which the Symantec Endpoint Protection client rollout task has failed" on page 25.

Table 4-1 Reports of Symantec Endpoint Protection Integration Component *(continued)*

Report	Description
Computers on which Tamper Protection is detected and enabled	Lists the details about the antivirus software that is installed on your computers with tamper protection. See "Viewing computers on which Tamper Protection is detected and enabled" on page 42.
Discovered computers that are unmanaged	Lists the computers that Symantec Management Platform has discovered, but that do not have the Symantec Management Agent installed on them. See "Viewing your unmanaged computers that are discovered" on page 43.

See "About reports for Endpoint Protection Integration Component" on page 39.

Viewing the status of Symantec Management Agent installations

You can view reports about the Agent installation status for the last week (by default). This list does not include agent pull install information.

To viewing the status of Symantec Management Agent installations

1. In the Symantec Management Console, on the **Reports** menu, click **All Reports**.
2. In the left pane, click **Reports > Notification Server Management > Agent > Agent Installation Status**.
3. On the **Agent Installation Status** page, in the right pane, view the report.

   For more information, see topics about using reports in the *Symantec Management Platform User Guide*.

See "Symantec Endpoint Protection Integration Component reports" on page 40.

Viewing summaries of the antivirus versions that are installed in your environment

You can view reports on the versions of antivirus software that are installed in your environment.

To view summaries of the antivirus versions that are installed in your environment

1. In the Symantec Management Console, on the **Reports** menu, click **All Reports**.
2. In the left pane, click **Reports > Symantec Endpoint Protection Management > Antivirus Version Summary**.
3. On the **Antivirus Version Summary** page, in the right pane, view the report.

   For more information, see topics about using reports in the *Symantec Management Platform User Guide*.

See "Symantec Endpoint Protection Integration Component reports" on page 40.

Viewing computers on which the Symantec Endpoint Protection client rollout is successful

You can view reports about the computers on which the Symantec Endpoint Protection client rollout policy has succeeded.

To view the status of your Symantec Endpoint Protection client installation jobs

1. In the Symantec Management Console, on the **Reports** menu, click **All Reports**.
2. In the left pane, click **Reports > Symantec Endpoint Protection Management > Computers on which Symantec Endpoint Protection Client rollout is successful**.
3. On the **Computers on which Symantec Endpoint Protection Client rollout is successful** page, in the right pane, view the report.

   For more information, see topics about using reports in the *Symantec Management Platform User Guide*.

See "Symantec Endpoint Protection Integration Component reports" on page 40.

Viewing computers on which Tamper Protection is detected and enabled

You can view reports about the antivirus software that is installed on your computers with tamper protection.

To view computers on which tamper protection is detected and enabled

1. In the Symantec Management Console, on the **Reports** menu, click **All Reports**.
2. In the left pane, click **Reports > Symantec Endpoint Protection Management > Computers on which tamper protection is detected and enabled**.
3. On the **Computers on which tamper protection is detected and enabled** page, in the right pane, view the report.

   For more information, see topics about using reports in the *Symantec Management Platform User Guide*.

See "Symantec Endpoint Protection Integration Component reports" on page 40.

Viewing your unmanaged computers that are discovered

You can view reports about the computers that Symantec Management Platform has discovered but that do not have the Symantec Management Agent installed on them.

To view your unmanaged computers that are discovered

1. In the Symantec Management Console, on the **Reports** menu, click **All Reports**.
2. In the left pane, click **Reports > Symantec Endpoint Protection Management > Discovered computers that are unmanged**.
3. On the **Discovered computers that are unmanged** page, in the right pane, view the report.

   For more information, see topics about using reports in the *Symantec Management Platform User Guide*.

See "Symantec Endpoint Protection Integration Component reports" on page 40.

Index