Symantec™ Server Management Suite 8.1 powered by Altiris™ technology User Guide

Symantec™ Server Management Suite 8.1 powered by Altiris™ technology 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 website at the following URL:

support.symantec.com

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:

support.symantec.com

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

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

- Product release level
- Hardware information

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

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

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

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

Support agreement resources

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

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

Contents

Chapter 1

Introducing Server Management Suite

This chapter includes the following topics:

About this Guide

Server Management Suite provides an integrated set of tools for managing servers on a common platform. This User Guide describes the following Symantec components and solutions:

- Altiris Deployment Solution
- Altiris Inventory Solution
- Altiris Inventory Pack for Servers
- Altiris Patch Management Solution for Windows
- Altiris Patch Management Solution for Linux
- Altiris Patch Management Solution for Mac
- Altiris Software Management Solution
- Symantec Virtual Machine Management
- Altiris Monitor Solution for Servers

- Altiris Monitor Pack for Servers
- Workflow Solution
- Altiris IT Analytics Solution

Each solution builds on another, without putting additional demands on the architecture. Each solution also leverages the information that is collected by the previous solution. This capability is enabled through the use of the CMDB, a single repository of data, logic, and automated processes, including access rights.

This guide takes you through all aspects of managing Windows servers, from the moment the hardware is received, through configuration management, patching, software management, and server health monitoring, to process automation (workflow) and integration by centralized management.

About Server Management Suite

Server Management Suite combines the essential tools that help you manage your physical and virtual servers, reduce service interruptions, and increase uptime.

Server Management Suite incorporates a variety of features that let you automate configuration, stage tasks, and create policies to manage your servers. Graphical reports let you quickly identify the health of your environment, pinpoint problems, and analyze trends. Expanded support for virtual technologies simplifies the management of multiple operating system environments.

Server Management Suite is a collection of solutions that run on the Symantec Management Platform that provides the following key features:

- Discovery and inventory
  The suite automatically identifies the devices that are found in your network, and collects inventory data across your environment. Multi-platform support consolidates the discovery data of all Windows, UNIX, and Linux assets within an integrated console. You can easily assess security vulnerabilities, prepare for software audits, and more accurately determine hardware availability and needs.
- Provisioning
  The suite lets you improve the consistency and increase the quality of server configurations. It delivers deployment capabilities that include image-based or scripted operating system installation and continuous provisioning. The suite helps you implement the standardized configurations and provides the tools for migration.
- Software distribution and patch management

The suite lets you control server configurations through its software management capabilities. Automated policies for software and patch management help you keep the servers standardized and secure. You can modify similar configurations on multiple servers simultaneously. You can distribute applications, and security updates to target systems.

- Proactive monitoring and alerting
  The suite helps you monitor the critical components of your network. You can increase the network uptime with the remediation tasks that are configured before the critical events occur. You can organize your servers into vital groups and quickly ascertain the current health of the whole network. The monitoring capabilities provide a summarized view of each single-server performance over time.

See "Components of Server Management Suite" on page 14.

See "Where to get more information" on page 20.

Components of Server Management Suite

Server Management Suite is a collection of solutions that run on the Symantec Management Platform. These solutions let you discover, inventory, monitor, and provision servers from a central console - the Symantec Management Console.

See "About Server Management Suite" on page 13.

Table 1-1 Components of Server Management Suite

Component	Description	Link to User Guide
Symantec Management Platform	Symantec Management Platform provides a set of services that IT-related solutions can leverage. By leveraging these services, the solutions that are built on the platform can focus on their unique tasks. They also can take advantage of the more general services that the platform provides. The platform services also provide a high degree of consistency between the solutions, so that users do not need to learn multiple product interfaces. Symantec Management Platform provides the following services: ■ Role-based security ■ Client communications and management ■ Execution of scheduled or event-triggered tasks and policies ■ Package deployment and installation ■ Reporting ■ Centralized management through a single, common interface Symantec Management Platform includes the following components: ■ Configuration Management Database (CMDB) ■ Notification Server ■ Symantec Management Console ■ Symantec Management Agent for Windows ■ Symantec Management Agent for UNIX, Linux, and Mac ■ Network Discovery ■ Software Management Framework	DOC9469

Table 1-1 Components of Server Management Suite *(continued)*

Component	Description	Link to User Guide
Deployment Solution	Deployment Solution helps to reduce the cost of deploying and managing servers, desktops, and notebooks from a centralized location in your environment. It offers operating system deployment, configuration, personality migration of computers, and software deployment across different hardware platforms and operating systems. Deployment Solution provides integrated, disk imaging, and personality migration from the Symantec Management Console. Using Symantec Ghost™, you can perform initial computer deployment using standard images and migrate user data and application settings to new computers. For the Deployment Solution release notes, see the link at the following URL: http://www.symantec.com/docs/DOC9583	DOC9496
ITMS Management Views	ITMS Management Views replace the default console views for computers and software that existed in Symantec Management Platform version 7.0. For tasks and policies, the Management views add drag-and-drop functionality. In addition, you can now search the tree rather than drilling down to find specific tasks or policies. The Management views are incorporated into the existing console. For more information, see the *IT Management Suite Administration Guide*.	DOC9469

Table 1-1 Components of Server Management Suite *(continued)*

Component	Description	Link to User Guide
Inventory Solution	Inventory Solution lets you gather inventory data about the computers, users, operating systems, and installed software applications in your environment. You can collect inventory data from the computers that run Windows, UNIX, Linux, and Mac. After you gather inventory data, you can analyze it using predefined or custom reports. For example, you can gather information for all the Symantec Endpoint Protection Windows and Mac clients that are installed on managed and unmanaged computers in your environment. Then you can view the gathered data in the Resource Manager or in the **Computers** Management view, in the **SEP Agent** summary flipbook.	DOC9616
Inventory Pack for Servers	Inventory Pack for Servers gathers server-based inventory data from servers that run Windows, UNIX, and Linux. It runs on top of Inventory Solution and uses the same Inventory plug-ins, tasks, and wizards.	DOC9616
Inventory for Network Devices	Inventory for Network Devices gathers inventory data from the devices that are not managed through the Symantec Management Agent. You can gather inventory on the devices that are already discovered and exist as resources in the CMDB.	DOC9605
Monitor Solution for Servers	Monitor Solution for Servers lets you monitor various aspects of computer operating systems, applications, and devices. These aspects can include events, processes, and performance. This ability helps you ensure that your servers and your devices work and reduces the costs of server and network monitoring.	DOC9587
Monitor Pack for Servers	Monitor Pack for Servers works with the Monitor Solution core components of the Symantec Management Platform. It lets you monitor operating system performance, services, and events of your Windows, UNIX, and Linux server environment.	DOC9587

Table 1-1 Components of Server Management Suite *(continued)*

Component	Description	Link to User Guide
Patch Management Solution	Patch Management Solution for Linux lets you scan Red Hat and Novell Linux computers for security vulnerabilities. The solution then reports on the findings and lets you automate the download and distribution of needed errata, or software updates. The solution downloads the required patches and provides wizards to help you deploy them. Patch Management Solution for Mac lets you scan Mac computers for the updates that they require. The solution then reports on the findings and lets you automate the downloading and distribution of needed updates. You can distribute all or some of the updates. Patch Management Solution for Windows lets you scan Windows computers for the updates that they require, and view the results of the scan. The system lets you automate the download and distribution of software updates. You can create filters of the computers and apply the patch to the computers that need it.	■ Patch Management Solution for Linux: DOC9606 ■ Patch Management Solution for Mac: DOC9607 ■ Patch Management Solution for Windows: DOC9608
Real-Time System Manager	Real-Time System Manager provides you detailed real-time information about a managed computer, and lets you remotely perform different administrative tasks in real time. Real-Time System Manager also lets you run some of the management tasks on a collection of computers. You can run the tasks immediately, or on a schedule.	DOC9304

Table 1-1 Components of Server Management Suite *(continued)*

Component	Description	Link to User Guide
Software Management Solution	Software Management Solution provides intelligent and bandwidth-sensitive distribution and management of software from a central web console. It leverages the Software Catalog and Software Library to ensure that the required software gets installed, remains installed, and runs without interference from other software. Software Management Solution supports software virtualization technology, which lets you install software into a virtual layer on the client computer. Software Management Solution also lets users directly download and install approved software or request other software.	DOC9609
Virtual Machine Management	Virtual Machine Management helps you to view virtual resource information in your network and perform management tasks on those virtual resources. You can create virtual environments of servers, storage devices, and network resources on a single physical server. Each virtual environment is isolated and functions independently from the physical server and from the other virtual environments. Virtualization enhances the efficiency and productivity of the hardware resources and helps to reduce administrative costs.	DOC9627

Table 1-1 Components of Server Management Suite *(continued)*

Component	Description	Link to User Guide
Symantec Workflow Solution	Symantec Workflow is a security process development framework that you can use to create both automated business processes and security processes. These processes provide for increased repeatability, control, and accountability while reducing overall workload. The Symantec Workflow framework also lets you create Workflow processes that integrate Symantec tools into your organization's unique business processes. Once deployed, Symantec Workflow processes can respond automatically to environmental variables. Symantec Workflow processes can also allow for human interface points when a process calls for someone to make a decision with accountability. For the Symantec Workflow Solution release notes, see the link at the following URL: http://www.symantec.com/docs/DOC9624	DOC9625
Topology viewer	Topology viewer is a Web Part on the **Server Management Portal** page that provides a network topology diagram of the SNMP-enabled devices that are found in your network.	N/A
Server Resource Manager Home page	The **Server Resource Manager Home** page consolidates the most relevant inventory and monitoring data of a server resource into a single view.	N/A

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: https://www.symantec.com/products/products-az Open your product's support page, and then under **Common Topics**, click **Release Notes**.

Table 1-2 Documentation resources *(continued)*

Document	Description	Location
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: https://www.symantec.com/products/products-az Open your product's support page, and then under **Common Topics**, click **Documentation**.
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: ■ Click the page and then press the F1 key. ■ Use 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.	Knowledge Base
Cloud Unified Help System	All available IT Management Suite and solution guides are accessible from this Symantec Unified Help System that is launched on cloud.	Unified Help System

Table 1-3 Symantec product information resources *(continued)*

Resource	Description	Location
Symantec Connect	An online resource that contains forums, articles, blogs, downloads, events, videos, groups, and ideas for users of Symantec products.	The links to various groups on Connect are as follows: ■ Deployment and Imaging ■ Discovery and Inventory ■ ITMS Administrator ■ Mac Management ■ Monitor Solution and Server Health ■ Patch Management ■ Reporting ■ ServiceDesk and Workflow ■ Software Management ■ Server Management ■ Workspace Virtualization and Streaming

Chapter 2

Setting up Windows computers

This chapter includes the following topics:

Creating and Deploying a Windows disk image

When you perform the **Create Image** task with **Disk Image** as the option, a Symantec Management Platform package is created for the captured disk image. The Disk image is stored on the Deployment share of the site server on which the Package Service runs. Each image is stored in a separate folder and has a GUID. Information about the image is also stored in the CMDB as an image resource. You can use this package to distribute the image to other Package Servers

To view the disk image packages navigate to **Settings > All Settings > Deployment and Migration > Disk Images** menu.

To view the disk image packages navigate to **Settings > All Settings > Deployment > Disk Images** menu.

Symantec recommends that you run the **Prepare for Image capture** task before you create the disk images. For Windows disk images, use the Sysprep utility that prepares the computer for creating the disk image that can be deployed on multiple computers. You can create a Windows disk image and deploy a Windows disk image only when the computer is in the PXE environment or the automation environment

The following tables list the process of creating a Windows image of a client computer and deploying a Windows image on a client computer:

- Creating a Windows image of a client computer
  See Table 2-1 on page 24.
- Deploying a Windows image on a client computer
  See Table 2-2 on page 26.

Following are the steps that you must follow to create an image of a Windows client computer:

Table 2-1 Process for creating an image of a Windows client computer

Step	Action	Description
Step 1	Launch the Console	Launch the Symantec Management Console. You can launch the console either from the Start menu of the Notification Server computer or from any computer of the network. To access the console from a different computer, you must type the following: http://<IP address of NS>/altiris/console
Step 2	Prepare a reference computer for imaging.	Prepare the reference computer that contains the core software and settings that you want to be replicated on other computers. For Windows XP and Windows 2003, install the Sysprep files on the reference computer. Copy the `support\tools\deploy.cab` file from your Windows XP installation disk or service pack. See "Configuring the Sysprep imaging" on page 39.
Step 3	Create a client job for the deployment tasks in the console	To create a client job, right-click on the **Deployment and Migration** folder and select **New > Client Job** menu. By default, a job of the name **New Client Job** is created that you can rename appropriately. Navigate to the **Manage > Jobs and Tasks** menu of the console and create a client job for the **Deployment and Migration** folder. To create a client job, right-click on the **Deployment and Migration** folder and select **New > Client Job** menu. By default, a job of the name **New Client Job** is created that you can rename appropriately.

Table 2-1 Process for creating an image of a Windows client computer *(continued)*

Step	Action	Description
Step 3	Create a client job for the deployment tasks in the console	To create a client job, right-click on the **Deployment** folder and select **New > Client Job** menu. By default, a job of the name **New Client Job** is created that you can rename appropriately. Navigate to the **Manage > Jobs and Tasks** menu of the console and create a client job for the **Deployment** folder. To create a client job, right-click on the **Deployment** folder and select **New > Client Job** menu. By default, a job of the name **New Client Job** is created that you can rename appropriately.
Step 4	Execute the **Prepare for Image capture** task	Run the **Prepare for Image capture** task if you want to perform Sysprep imaging and use the **Include DeployAnywhere for hardware independent imaging** option for the **Deploy Image** task. The **Prepare for Image capture** task ensures that the captured image does not contain any hardware-dependent data. You can then deploy a hardware independent image on other computers. **Note:** If you deploy a disk image using the **Include DeployAnywhere for hardware independent imaging** option and you have not performed the **Prepare for Image capture** task, the client computer image gets corrupted. See "Configuring the Sysprep imaging" on page 39. See "Preparing to capture an image" on page 39.

Table 2-1 Process for creating an image of a Windows client computer *(continued)*

Step	Action	Description
Step 5	Create an image of the client computer	Run the **Create Image** task to create the disk image of the reference computer. You can either run the task immediately by using the **Quick Run** option of the task that you have saved or you can schedule the task to run later on the reference computer. See "Creating a Windows image" on page 41.

Following are the steps that you must follow to deploy a Windows image on a client computer:

Table 2-2 Process for deploying an image of a Windows client computer

Step	Action	Description
Step 1	Launch the Console	Launch the Symantec Management Console. You can launch the console either from the Start menu of the Notification Server computer or from any computer of the network. To access the console from a different computer, you must type the following: http://<IP address of NS>/altiris/console
Step 2	Boot the client computer to Automation environment	Boot the client computer to Automation environment using the **Boot To** task.
Step 3	Create a client job for the deployment tasks in the console	To create a client job, right-click on the **Deployment and Migration** folder and select **New > Client Job** menu. By default, a job of the name **New Client Job** is created that you can rename appropriately. Navigate to the **Manage > Jobs and Tasks** menu of the console and create a client job for the **Deployment and Migration** folder. To create a client job, right-click on the **Deployment and Migration** folder and select **New > Client Job** menu. By default, a job of the name **New Client Job** is created that you can rename appropriately.

Table 2-2 Process for deploying an image of a Windows client computer *(continued)*

Step	Action	Description
Step 3	Create a client job for the deployment tasks in the console	To create a client job, right-click on the **Deployment**folder and select **New > Client Job** menu. By default, a job of the name **New Client Job** is created that you can rename appropriately. Navigate to the **Manage > Jobs and Tasks** menu of the console and create a client job for the **Deployment**folder. To create a client job, right-click on the **Deployment** folder and select **New > Client Job** menu. By default, a job of the name **New Client Job** is created that you can rename appropriately.
Step 4	Deploy the image on the client computer	Create a **Deploy Image** task for the target client computers. You can specify the Sysprep-enabled image that you captured to be deployed on the target client computers. You can either execute the task immediately by using the **Quick Run** option of the task that you have saved or you can schedule the task to be executed later on the reference computer. See "Creating a Deploy Image task" on page 44.
Step 5	Boot the client computer to Production environment	Boot the client computer to production environment using the **Boot To** task.

See "Configuring the Sysprep imaging" on page 39.

Preparing unknown computers to boot with WinPE image

After an unknown computer is added to a network, Deployment Solution boots the computer in the preboot environment using a PXE image. You can configure the unknown computer to boot in the preboot environment before you install the Windows operating system (OS) on the computer. The computer boots in the preboot environment with a PXE image.

For Windows, a PXE image is created using the preboot configuration files, WinPE that Deployment Solution supports,the PECTAgent, and the Deployment plug-in for Windows. The Deployment Plug-in is required for the execution of deployment tasks on the client computer.

The following process addresses how you must configure the settings to boot an unknown computer in the WinPE environment. After the computer boots in the preboot environment, the communication with Notification Server is established and the computer is registered as a managed computer.

You must perform the following steps to boot an unknown computer with the WinPE image:

Table 2-3 Booting an unknown computer with WinPE image

Step	Action	Description
Step 1	Launch the console	Launch the Symantec Management Console. You can launch the console either from the Start menu of the Notification Server computer or from any computer of the network. To access the console from a different computer, you must type the following: http://<IP address of NS>/altiris/console
Step 2	Install **Network Boot Service** on a site server	You must install the **Network Boot Service** (NBS) on a site server and also enable the policy before you configure the unknown client computer to boot in the preboot environment. See "Installing Network Boot Service on site server" on page 29.
Step 3	Create a WinPE image	You must create a WinPE image through the **Create Preboot Configurations** dialog box of the console. You must create a WinPE image through the **Manage Preboot Configurations** dialog box of the console. See "Creating preboot configuration for Windows" on page 30.
Step 4	Configure NBS settings for unknown computers	You must configure the NBS settings for the unknown client computer from the console. For the unknown computer, you configure the **NBS General Settings** that lets you select the image to boot the client computer with and also configure the boot menu. Besides, you can also configure the **NBS Global Setting** that lets you filter computers based on MAC address to which the NBS site server must or must not respond.

Table 2-3 Booting an unknown computer with WinPE image *(continued)*

Step	Action	Description
Step 5	(optional) Set up **Initial Deployment** job to execute tasks on the client computers	You can set up an **Initial Deployment** job for the Windows unknown client computer to execute the deployment tasks that you create. You can perform this step after you create the deployment tasks for the unknown client computer. The **Initial Deployment** job menu is displayed on the client computer after the computer boots to the preboot environment. You can select all or specific tasks from the menu and execute them on the client computer. See "Configuring the initial deployment settings" on page 47.
Step 6	Add the unknown computer to the network and wait for the client computer to boot to preboot environment	If you have added predefined computer entries through the console with no hardware identifier values, then the Windows unknown client computers boot in the preboot environment using the PXE image that was configured for predefined computers. You configure the PXE image for a predefined computer through the **NBS General Settings** dialog box. After the computer boots to the preboot environment, Deployment Solution provides an option to boot the unknown computer as a predefined computer.

See "Booting managed Windows computer with WinPE image" on page 37.

Installing Network Boot Service on site server

Network Boot Service (NBS) is a component of Deployment Solution that you install and run as a service on a site server. This service is independent of the presence of Task service or Package service on a site server and handles all communication with the Symantec Management Platform (SMP) for Deployment Solution. You must install the Microsoft XML Core Services 6.0 on the site server on which you install the NBS component. The NBS comprises of the PXE and BSDP service and the TFTP service that are installed on the site server after you roll out the NBS service through the SMP console.

After the NBS is installed, the status of the service is displayed as green and the service status is displayed as **Started**.

You must install and enable the Network Boot Service (NBS) service on the site server before you create preboot configuration and start configuration of NBS settings.

Note: If you want to install the Deployment Package server component and the NBS on the same site server, then you must install the Deployment Package Server component after installing the NBS on the site server.

To install NBS service on site server

1. In the Symantec Management Console, navigate to **Settings > Notification Server > Site Server settings** menu.
2. In the **Site Management** window, expand **Site Server** node in the tree.
3. On the **Site Servers** page, click **New** under the **Detailed Information** pane.
4. In the **Select Computers** dialog box, select the Windows computers that you want to configure as site server and click **OK**.
5. In the **Add/Remove services** dialog box, check the **Network Boot Service** option for the site servers that you select.

Creating preboot configuration for Windows

Deployment Solution lets you create Windows preboot environments. The preboot configuration is required to boot client computers in the preboot environment or the pre-OS state. Deployment Solution lets you create two types of preboot environments for Windows operating system such as PXE and automation.

The PXE environment lets you boot a client computer in the preboot environment using a PXE image over a network. A PXE image is saved on the site server on which the Network Boot Service (NBS) is installed. Deployment Solution lets you configure the WinPE image using the **Create Preboot Configurations** option of the console. Ensure that the NBS policy is enabled on the site server before you configure the WinPE image. If you configure a WinPE image before installing the NBS on a site server, then you have to recreate the environment. Every time a WinPE image is configured and saved, Notification Server (NS) distributes the image to all the NBS site servers of a network.

The PXE environment lets you boot a client computer in the preboot environment using a PXE image over a network. A PXE image is saved on the site server where the Network Boot Service (NBS) is installed. Deployment Solution lets you configure the WinPE image using the **Manage Preboot Configurations** option from the console. Enable the NBS policy on the site server before you configure the WinPE image. If you configure a WinPE image before installing the NBS on a site server, then you have to recreate the environment. Every time a WinPE image is configured and saved, Notification Server (NS) distributes the image to all the NBS site servers of a network.

Deployment Solution lets you create preboot configurations for the following versions of WinPE:

- WinPE 3.1
- WinPE 4.0
- WinPE 5.x
  It includes WinPE 5.0 or WinPE 5.1
- WinPE 10 (From 8.0 HF 2)

To create a preboot configuration, you must first download and install the Windows AIK or the Windows ADK kit based on the Windows preboot environment. After the WAIK folder is created, you must import the AIK or the ADK into Deployment Solution.

Note: In case of a hierarchy setup and multiple WinPE, Symantec recommends that same version of WinPE is installed on the parent notification server and the child notification server before the replication of the preboot configuration.

- For WinPE 3.1, you must also download and install the Windows AIK for Windows 7. After you install the Windows AIK for Windows 7, follow the Windows AIK Supplement for Windows 7 SP1 instructions to create the preboot environment for WinPE 3.1.
- For WinPE 4.0, you must download and install the Windows ADK for Windows 8.
- For WinPE 5.1, after you download and install the Windows ADK for Windows 8.1 Update, you must also execute the steps that are mentioned in the article WinPE 5.0 to WinPE 5.1. Follow the following URL:
  http://technet.microsoft.com/en-in/library/dn613859.aspx
  If you do not follow the steps then by default the WAIK folder is created for WinPE 5.0.
- For WinPE 10, download and install Windows ADK for Windows 10.
  Remove the older ADK's from the computer by running the older ADK setup file from other ADK's.

  Note: Microsoft does not allow multiple ADKs on the same computer.

Note: If Windows ADK (8.0/8.1) and the Windows AIK are installed together on the Notification Server computer before the installation of Deployment Solution, the WAIK folders for both the ADK and AIK are created, however the PEInstall for the higher version will be created.

How to change a preboot configuration?

Follow the following steps to change from one WinPE to another WinPE:

To change a preboot configuration

1. In the Symantec management console, navigate to **Settings > Deployment > Manage Preboot Configurations**.
2. In the Preboot Configuration dialog box, from the **Change WinPE** list, select the WinPE.
3. In the **Policy Rules/Actions** section, select the PEInstall and click on **Recreate Preboot Environment**.

An automation environment is created when you install an Automation Folder containing the WinPE package on a client computer. To install an Automation Folder, you must enable the **Deployment Automation folder for Windows (x64) -Install** or the **Deployment Automation folder for Windows (x86) -Install** policy through the console. By default, Deployment Solution creates a **PEInstall** folder for Windows computers. For Windows, you can create automation folders of either or both x86 and x64 architectures. These automation folders are created on the Notification Server computer and are installed on the client computers after you enable the predefined deployment **Automation Folder Plug-in** policy through the Symantec Management Console. Deployment Solution lets you create and use Windows x64-bit PXE image to boot UEFI computers in preboot environment.

You can add a new driver to an existing preboot configuration. After you add the driver, you must recreate that preboot configuration using the **Recreate Preboot Environment** option from the **Preboot Configuration** page.

To use the preboot configuration, disable the administrative rights and the User Account Control (UAC) settings.

You can access either of the following menus to create and configure a preboot environment:

- **Settings > Deployment > Create Preboot Configuration**
  Settings > Deployment > Manage Preboot Configuration
- **Settings > All Settings > Deployment & Migration > Preboot Configuration**
  Settings > All Settings > Deployment > Preboot Configuration

To create WinPE 4.0 preboot configuration, you must have the Windows Assessment and Deployment Kit (ADK) for Windows 8 installed on Notification Server. If the ADK for Windows 8 is not installed on the Notification Server, then a message is displayed on the **Create Preboot Configuration** page that displays the link to download the Windows Assessment and Deployment Kit (ADK) for Windows 8. You must first download and install the Windows ADK for Windows 8 and then update the BDC package to include the WAIK folder that is required to create the WinPE preboot environment.

To create a preboot configuration

1 In the Symantec Management Console, on the **Settings** menu, click **Deployment > Create Preboot Configurations**.

In the Symantec Management Console, on the **Settings** menu, click **Deployment > Manage Preboot Configurations**.

Select the WinPE version for which you want to create a preboot configuration.

Change WinPE

Select the WinPE version for which you want to create a Windows preboot configuration.

Deployment Solution lets you create preboot configurations for the following version of WinPE:

- WinPE 3.1
  - **Download and install the Windows AIK for Windows 7 and Supplement for Windows 7 SP1**

    This option is displayed if the Windows Automated Installation Kit (AIK) for Windows 7 is not installed on Notification Server.

    Note: To use WinPE 3.1 as a preboot environment, you must first download and install the Windows AIK for Windows 7 followed by installing the Windows AIK Supplement for Windows 7 SP1.

  - **Then import the Windows AIK install into DS**

    Lets you modify the BDC package to include the WAIK folder that is installed after you install the Windows Automated Installation Kit (AIK)for Windows 7.
- WinPE 4.0
  - **Download and install the Windows ADK for Windows 8**

    This option is displayed if the Windows Assessment and Deployment Kit (ADK) for Windows 8 is not installed on Notification Server.

    Ensure that you select the following options while installing the ADK for Windows 8:
    - Deployment Tools
    - Windows Preinstallation Environment (Windows PE)
  - **Then import the Windows ADK install into DS**

    Lets you modify the BDC package to include the WAIK folder that is installed after you install the Windows Assessment and Deployment Kit (ADK) for Windows 8.
- WinPE 5.x
  - **Download and install the Windows ADK for Windows 8.1 Update**

    This option is displayed if the Windows Assessment and Deployment Kit (ADK) for Windows 8.1 is not installed on Notification Server.

    Ensure that you select the following options while installing the ADK for Windows 8.1:
    - Deployment Tools
    - Windows Preinstallation Environment (Windows PE)

    Note: To create the WAIK folder for WinPE 5.1, you must follow the steps that are mentioned in the article, WinPE 5.0 to WinPE 5.1. If you do not follow the instructions that are mentioned in the article, then by default, the WAIK folder is created for WinPE 5.0.

  - **Then import the Windows ADK install into DS**

    Lets you modify the BDC package to include the WAIK folder that is installed after you install the Windows Assessment and Deployment Kit (ADK) for Windows 8.1.
- WinPE 10 (From 8.0 HF2 onwards)

  Download and install the Windows ADK for Windows 10 Update

  This option is displayed if the Windows Assessment and Deployment Kit (ADK) for Windows 10 is not installed on Notification Server.

  Note: Remove older ADK's from the computer by running the older ADK setup file from other

ADK's. Microsoft does not allow multiple ADK's on the same computer.

Ensure that you select the following options while installing the ADK for Windows 10:

- Deployment Tools
- Windows Preinstallation Environment (Windows PE)

For more information, refer to the following article:

Info3561

If ADK for Windows 8 is not installed on Notification server, then the following fields are displayed:

Download and install the Windows ADK for Windows 8	Links to the website from which you can download the Windows Assessment and Deployment Kit (ADK) for Windows 8. This option is displayed if the Windows Assessment and Deployment Kit (ADK) for Windows 8 is not installed on Notification Server. Ensure that you select the following options while installing the ADK for Windows 8: ■ Deployment Tools ■ Windows Preinstallation Environment (Windows PE)
Then import the Windows ADK install into DS	Lets you modify the BDC package to include the WAIK folder that is installed after you install the Windows Assessment and Deployment Kit (ADK) for Windows 8.

2 On the **Create Preboot Configurations** page, click **Add**.

On the **Manage Preboot Configurations** page, click **Add**.

3 On the **Add Preboot Configurations** page, enter the name and description of the preboot configuration.

Operating System	Select Windows operating system. Select the WinPE version.
Architecture	Select x86 or x64 for Windows.
OEMextension	Select DS Agent as the OEM agent .

Lock the keyboard and mouse	For Windows, you can select this option to lock the keyboard and mouse while the computer is booted to the preboot environment.
Inject imaging tools	
Select which preboot environments to build	Select the type of preboot environment you want to configure. You can select from the following: ■ **PXE** This preboot configuration can be accessed only from the Network Boot Service (NBS) server. Only the client computers that are configured to boot to and from their network card can access the configuration. ■ **Automation Folder** This preboot configuration can be installed on the client computers by using policies. You can access these policies from Settings > Agent/Plug-ins > Deployment and Migration. This preboot configuration can be installed on the client computers by using policies. You can access these policies from Settings > Agent/Plug-ins > Deployment. ■ **Both PXE and Automation Folder** This option creates both types of configuration.

4 On the **Add Preboot Configurations** page, click **OK**.

5 On the **Preboot Configurations** page, click **Save changes**.

If you are reading this procedure as a part of a process, return to the process by clicking on the following link:

See “Preparing unknown computers to boot with WinPE image ” on page 27.

Booting managed Windows computer with WinPE image

Deployment Solution lets you redeploy a managed computer that is installed with the Windows operating system (OS) to a preboot environment. The managed

computer redeploys to the preboot environment using the WinPE image that Deployment Solution supports, after you execute the **Boot To** deployment task.

The following process lets you reboot a Windows managed computer to the preboot environment using a configured WinPE image. After the computer reboots to the preboot environment, you can execute any deployment tasks on the computer.

You must perform the following steps to reboot a managed computer with a WinPE image:

Table 2-4 Booting a managed computer with WinPE image

Step	Action	Description
Step 1	Launch the console	Launch the Symantec Management Console. You can launch the console either from the Start menu of the Notification Server computer or from any computer of the network. To access the console from a different computer, you must type the following: http://<IP address of NS>/altiris/console
Step 2	Install the **Network Boot Service** on a site server	You must install the **Network Boot Service** (NBS) on a site server and also enable the policy before you configure the client computer to boot in the preboot environment. See "Installing Network Boot Service on site server" on page 29.
Step 3	Create a WinPE image	Create a WinPE image through the **Create Preboot Configurations** dialog box of the console. Create a WinPE image through the **Manage Preboot Configurations** dialog box of the console.
Step 4	Configure NBS settings for managed computer	Configure the NBS settings for the managed client computer from the console. For the managed computer, you configure the **NBS General Settings** that lets you select the WinPE image to boot the client computer with and also configure the boot menu. Besides, you can also configure the **NBS Global Setting** that lets you filter computers based on MAC address to which the NBS site server must or must not respond.
Step 5	(optional) Set up the **Re-Deployment (Managed Computer) menu** in the **Initial Deployment Settings** dialog box	In the **Initial Deployment Settings** dialog box, you can configure the **Re-Deployment (Managed Computer) menu** to execute jobs or tasks on the managed computer after the computer boots in the preboot environment. See "Configuring the initial deployment settings" on page 47.

Table 2-4 Booting a managed computer with WinPE image *(continued)*

Step	Action	Description
Step 6	Execute **Boot To** PXE task	Execute the **Boot To** task and select the **PXE/NetBoot image** option in the **Create New Task** dialog box.
Step 7	Execute tasks or jobs after the client computer boots to preboot environment	After the Windows client computer boots to preboot environment, the Re-Deployment menu for managed computers is displayed. You can select all or specific tasks or jobs that you want to execute.

See "Preparing unknown computers to boot with WinPE image " on page 27.

Configuring the Sysprep imaging

Sysprep is the Microsoft utility that prepares computers for Windows deployments. All Windows platforms after Windows XP and Windows 2003 include Sysprep files as part of the OS installation.

Note: Sysprep disables the built-in administrator account and clears the administrator password when it prepares a computer for imaging. You might need to change the password on the client computer before logging on for the first time after deploying an image.

To configure Sysprep imaging

1. In the Symantec Management Console, on the **Settings** menu, click **Deployment** > **Sysprep Imaging Configuration**.
2. Based on the operating system, under **x86 Deploy.cab** or **x64 Deploy.cab**, click **Upload** to browse and upload the relevant .cab file.
3. Click **Save changes**.

See "Preparing to capture an image" on page 39.

Preparing to capture an image

The **Prepare for Image capture** task prepares a client computer before you create an image. This task is applicable for Windows and Linux operating systems only.

For Windows, the **Prepare for Capture Image** task uses Sysprep utility to remove the computer name, Security Identifier (SID), the operating system license, GUID of the agent, and some hardware-dependent drivers. You must always run this task

before creating a disk image. Sysprep also disables the built-in administrator account and clears the admin password.

For Linux, this task runs a preimage script to remove the configuration-related settings and prepare the computer for imaging.

See "Configuring the Sysprep imaging" on page 39.

You can choose several options while creating this task. You must create a deployment task before you run it.

To prepare for image capture

1. In the Symantec Management Console , from the **Manage** menu select **Jobs and tasks**.
2. In the right pane, right-click **Jobs and tasks** and select **New** > **Task**.
3. In the **Create new task** dialog box, under the **Deployment and Migration** folder select the **Prepare for Image Capture** task.

   In the **Create new task** dialog box, under the **Deployment** folder select the **Prepare for Image Capture** task.
4. Specify a name for the task on the first field.
5. Under the **Pre-Imaging** section, select either **Windows (using sysprep)** or **Linux** operating system.

   The fields and their descriptions are as follows:

Task name icon	Displays the default task name as Prepare for Image capture. You can edit the default task name to specify a relevant task name. For example, Prepare for image capture_Linux.
Pre-imaging	Lets you select the operating system for which you want to create a **Prepare for image capture** task. You can select from the following operating systems: ■ **Linux** ■ **Windows (using sysprep)** For Windows, you can select from the following: ■ **OS type** Select the version of Windows operating system. ■ **Product key** Select an operating system license that you use to restore the computer back to its original state after the task runs. If the license is not added to Deployment Solution, you can add one by clicking **New**. In the **Add OS License Key** dialog box, add the product key for the operating system that you select.

Enter credentials to rejoin a domain after capture is complete	Lets you join back the client computer to the domain after the task executes. Specify the credentials to join the domain in the **User name** , **Password**, and the **Confirm password** fields. This option is applicable for the Windows operating system only.
Run Sysprep with Admin credentials	Specify the administrator credentials. This option is added to address the disabled Start and Search options issue for Windows 10 operating system when the Sysprep task is run. While creating a **Prepare for Image capture** task for Windows 10, you must enter the administrator credentials of the client computer. If you upgrade from Deployment Solution 7.6 HF4, Symantec recommends that you update the **Prepare for Image capture** task of Windows 10 with the administrator credentials of the client computer.
Reboot to	Lets you select the environment to which you want to boot the client computer before you start the image creation process. You can either select **Automation** or **PXE**. If you select **PXE**, then you must also select the PXE image and the architecture from the drop-down lists. This option is applicable for both Linux and Windows operating systems.

Creating a Windows image

Deployment Solution lets you create disk images and backup images of Windows client computers. A disk image is an image that contains the application and settings that are present on a computer disk. Backup images retain the data and software of a specific computer. A backup image contains a snapshot of the hard disk of a computer. The difference between a disk image and a backup image is that a disk image can be used to deploy on multiple client computers whereas the backup image can be restored only to the computer that it was captured from. The image has the same name as the computer from which it was captured. You execute the **Create Image** task of Deployment Solution to create disk images and backup images.

Note: To create an image, if the Package Server is in a domain different from the SMP domain, then ensure that you add the SMP users to the Administrator group of the Package Server. All the users that you add must have read and write permissions on the Package Server.

To create a Windows image

1. In the Symantec Management Console, from the **Manage** menu select **Jobs and tasks**.
2. In the left pane, do either of the following:
   - Right-click **System Jobs and Tasks** and select **New** > **Task**.
   - Expand the **System Jobs and Tasks** and right-click **Deployment and Migration** to select **New** > **Task**.
     Expand the **System Jobs and Tasks** and right-click **Deployment** to select **New** > **Task**.
3. In the **Create New Task** dialog box, select **Deployment and Migration > Create Image** option.

   In the **Create New Task** dialog box, select **Deployment > Create Image** option.
4. The fields and their descriptions are as follows:

Task name icon	Displays the default task name as **Create Image**. You can edit the default task name to specify a relevant task name. For example, Create Image_Windows XP.
Image name	Enter a name for the image to be created. Image name supports only ASCII characters. If you use a token for image name, ensure that it is a valid predefined token. Otherwise, an image package with a blank name is created, which is difficult to locate when you want to deploy the image.
Description	Lets you enter a description, if required.

Image type

Lets you select the type of image that you want to capture.

Select from the following types of computer images:

- **Disk Image**
  The **Disk Image** can be deployed on multiple computers. These images are saved in a package on the package server and can be distributed to other package servers.
  If you intend to deploy a disk image using the option **Include DeployAnywhere for hardware independent imaging**, ensure that the **Prepare for Image capture** task is executed before the image is created. Otherwise, the client computer on which this disk image is deployed might get corrupted.
  See "Configuring the Sysprep imaging" on page 39.
- **Back-Up image**
  A **Back-Up Image** contains a snapshot of the hard disk of a computer. The backup images retain the data and software of a specific computer. A backup image can be restored only to the computer from which the image was captured. You can restore the image name same as the computer name if you use %COMPNAME% token as the image name.
  The images cannot be deployed on multiple computers and cannot be saved in a package and distributed to other package servers through the replication process. Back-up images are created if you want to image only a data disk, which is a disk without an operating system or a partition of a data disk.

5 On the **Create Image** page, you can set the **Advanced** imaging options. Following are the options that you can set with the description:

6 Click **OK**.

If you are reading this procedure as a part of a process, return to the process by clicking on the following link:

See "Creating and Deploying a Windows disk image" on page 23.

See "Creating a Deploy Image task" on page 44.

Creating a Deploy Image task

Deployment Solution lets you deploy a standard disk image on client computers using the **Deploy Image** task. After you deploy a new image, all the existing data and applications of the client computer are lost and the computer is restored to the state of the standard image.

To create a deploy image task

1 From the **Manage** menu, select **Jobs and tasks**.

2 On the right pane, right-click **Jobs and tasks** and select **New** > **Task**.

3 On the **Create new task** page, select **Deploy Image**.

The **Create** or **Deploy image** task can only be executed in the Automation environment.

4 Specify a name for the task on the first field.

5 Enter the following of the **Imaging** section:

Image Name	Enter the name of the image file to deploy. **Note:** For Linux, only the **Name** and **Image Name** fields are necessary. All of the other fields are optional.
Product Key	Select an operating system license that can be used to boot the computer back to a working state after the task runs. If the license has not been added to Deployment Solution, you can add one by clicking **New**. The **Current Key** option is available only for Windows Vista and later versions of the Windows operating system.

6 Select **Include DeployAnywhere for hardware independent imaging** check box to use DeployAnywhere.

You must check this option, to deploy the drivers that you added to the DeployAnywhere database. Selecting this check box runs DeployAnywhere after the image is deployed. DeployAnywhere runs while the computer is still running the WinPE preboot operating system. This option discovers what type of hardware is on the destination computer and creates a new HAL, which is deployed to boot the computer successfully.

If you intend to deploy a disk image using the option **Include DeployAnywhere for hardware independent imaging**, ensure that the **Prepare for Image capture** task was executed for Windows and Linux computers before the image was created. Otherwise, the client computer on which this disk image is deployed might get corrupted.

DeployAnywhere works only from within a WinPE preboot operating system.

7 Select **Enable tagging of the drivers** option to add tags to the **Tags** field. Drivers that are tagged are deployed forcefully on the client computers.

1 Select one of the following options from the **Sysprep Configuration** section:

Generate Sysprep configuration file using inventory data	The required information is obtained from the CMDB.
Custom Sysprep configuration file	Click **Browse** to select the custom Sysprep file that you created.

2 Enter the credentials in the **Credentials** section that are needed to join the client computer to a domain.

If the client computer was not in the domain before the image was deployed, you cannot add the computer to the domain even after the image is deployed. To bring the client computer to the domain, you have to create the **System Configuration** settings. Ensure that the disk image that you deploy is prepared after executing the **Prepare for Image capture task** so that the client computer joins the domain that is specified.

3 Click the **Advanced** tab to set the following:

Partition	Lets you decide the partitions on which you deploy the image. You can change the destination partition size by clicking the partition number. **Note:** For Data Partition or System reserve partition deployment do not use **DeployAnywhere**. For Linux, only Data Partition deployment is supported. To deploy Windows 7 with system reserved partition, create a job to run deploy system reserved partition and system partition in the same preboot environment.
Command-line	Lets you add command-line options for the imaging tool. For Ghost partition deployment, following command lines must not be used: `MODE,Size,SRC and DST values should not be used for command line`. **Note:** Ensure that you do not specify the switch -SZEE and select the Resize partition option simultaneously for the deploy image task.

Multicasting	Lets you configure the number of computers on which you want to multicast the image. You can override the default multicast settings that were set in **Settings** > **Deployment** > **Image Multicasting** . There must be at least one computer over the threshold value that you specify for multicasting. For example, if the threshold count is 2, there must be at least two client computers and one master computer, which is 3 in total, before multicasting is used in the session Deployment Solution does not support Multicast and Unicast options simultaneously if you use the Ghost imaging tool.
File Preservation	Lets you specify the files and folders that you want to preserve when the image is restored. This option is not supported if the client computer is installed with Linux operating system.
HTTP	Lets you add the credentials that are required to deploy an image, which was obtained from an HTTP site.

4 Click **OK**.

If you are reading this procedure as a part of a process, return to the process by clicking on the following link:

See "Creating and Deploying a Windows disk image" on page 23.

http://www.youtube.com/watch?v=V2ePrxlMaAc

Configuring the initial deployment settings

Initial Deployment settings is a job that you use to set up the initial set of tasks or jobs for unknown computers or managed computers after they boot to the preboot environment or the automation environment. For the unknown client computers, this job executes after the computers boot in the preboot environment, while for the managed computers, the job executes after the computers boot to preboot

environment or the automation environment. This **Initial Deployment** settings menu can be configured only for the Windows client computers.

For example, you have an unknown computer in the network that you want to boot in preboot environment first and then want to execute a set of tasks after the computer boots. The tasks that you want to execute on the computer are, **Deploy Image**, **Boot To** production, and then **Apply System Configuration**. You can wrap up these tasks in a job and then configure and schedule the Initial Deployment job for the unknown computers. After the unknown computers boots in the preboot environment, the Initial Deployment menu that you configured is displayed. You can choose the tasks or jobs that you want to execute from the displayed list. At this stage, you can also choose to deselect any task that you do not want to execute.

If you have managed computers that you want to boot in automation environment, then you can set the redeployment tasks through this **Initial Deployment** job menu. In the automation environment, after you boot the managed computer manually, the list of initial tasks that you have set in this menu are displayed.

You can configure the **Initial Deployment** job menu from the following options of the console:

- **Settings > Deployment > Initial Deployment** menu
- **Settings > All Settings > Deployment and Migration > Initial Deployment** option
  Settings > All Settings > Deployment > Initial Deployment option

To configure the initial deployment settings

1. In the Symantec Management Console, on the **Settings** menu, click **Deployment** > **Initial Deployment**.
2. In the **Initial Deployment Settings** dialog box, specify the values for the fields.
3. In the **Initial Deployment Settings** dialog box, click **Add** to add the tasks that you want to display in the job menu of the computer.
4. Select the default task for the initial deployment menu.

   The selected default task execution starts after the lapse of time specified. During the specified time, you can choose to run any other tasks that are displayed in the menu.
5. Click **Save changes**.

Installing Windows OS on client computers

Deployment Solution lets you install a Windows operating system (OS) on an unknown, a predefined, or a managed computer in an enterprise network. Windows

OS installation lets you remotely install the Windows OS on any desktop, laptop, or on a server that is independent of the computer's hardware configuration. Besides, you can create a Windows OS package with the required source files, and decide what source files are included in that package.

This process addresses how you must boot a client computer in the preboot environment by using a WinPE image. After the client computer boots in the preboot environment, the communication with Notification Server is established. You must then create a Windows OS installation package and then install the Windows OS by using the installation package.

You must perform the following steps to install Windows OS on a client computer:

Table 2-5 Installing Windows OS on a client computer

Step	Action	Description
Step 1	Launch the Symantec Management Console	Launch the Symantec Management Console. You can launch the console either from the Start menu of the Notification Server computer or from any computer of the network. To access the console from a different computer, you must type the following: http://<IP address of NS>/altiris/console
Step 2	Install and enable the Network Boot Service on a site server	Install the Network Boot Service (NBS) on a site server before you perform any other configurations. NBS is a component of Deployment Solution that you install and run as a service on a site server. NBS, once installed on a site server, handles all the communication with the Symantec Management Platform for Deployment Solution. See "Installing Network Boot Service on site server" on page 29.
Step 3	Create Windows preboot environment	Create and configure a Windows preboot environment using a PXE image. The PXE image is used to boot the client computer in a network in the preboot environment or the pre-OS state. A PXE image is saved on the site server on which NBS is configured. Therefore, ensure that NBS is running on the site server before you create the PXE image. See "Preparing unknown computers to boot with WinPE image " on page 27. See "Booting managed Windows computer with WinPE image" on page 37.

Table 2-5 Installing Windows OS on a client computer *(continued)*

Step	Action	Description
Step 4	Configure NBS based on the type of client computer that is to boot in preboot environment	Configure Network Boot Service (NBS) for the type of client computer that you want to boot in the preboot environment. The NBS settings are configured through **Settings > Deployment > NBS General Settings** menu of the console.
Step 5	Add or import OS files for OS installation package	Add or import OS package to manage the Windows OS source files. You can configure the import parameters for your package. To add OS package for Windows OS installation, from the Symantec Management Console, click **Settings** > **Deployment** > **OS Files** > **Add files**. To import the OS files to a Windows OS installation package, you can also use the **Deployment Solution Resource Import Tool**. This tool is located in the `<install_directory>/Altiris/Deployment/Tools` folder of the Notification Server computer. **Note:** You can add or import OS files to a Windows OS installation package before executing the **Install Windows OS** task. Alternatively, you can specify the files to be added or imported to the installation package at run-time while executing the **Install Windows OS** task.
Step 6	Add a Windows OS license to install Windows OS on the client computer	Add the Windows OS license for the corresponding OS through the Symantec Management Console so that you can track the OS licenses later. **Note:** You can add Windows OS license before executing the **Install Windows OS** task. Alternatively, you can specify the Windows OS license for the corresponding OS at run-time while executing the **Install Windows OS** task. See “Adding OS licenses” on page 53.
Step 7	(optional) Erase disk of client computer	Perform the **Erase Disk** task to erase the disks on the client computer. This action ensures that any preexisting data and partitions are removed from the computer. When you reallocate hardware, you can use this task to ensure that none of the old data can be retrieved. You can execute this step only when you want to wipe the client computer's disk clean of any preexisting data or disk partitions. See “Erasing a Disk” on page 53.

Table 2-5 Installing Windows OS on a client computer *(continued)*

Step	Action	Description
Step 8	Create disk partition on client computer	Execute the **Partition Disk** task to create partitions on the client computer's hard drive before you install the Windows OS. To install Windows OS on UEFI/EFI computers, the computer must have partitions created with GPT partition table type. The GPT partition is required because the **Partition disk** task of Deployment Solution is not applicable for the UEFI computers. See "Creating disk partitions" on page 55.
Step 9	Install a Windows OS on the client computer	Execute the **Install Windows OS** task to install the Windows OS on the client computer after the computer boots in the preboot environment. By default, after the Windows OS is installed, the client computer boots to the production environment. After you execute the **Install Windows OS** task on the computer, verify that the Windows OS is installed and the computer is in production environment. To boot the client computer in the production environment, use the **Boot To** task in a job after the **Install Windows OS** task. You can install Windows OS on UEFI/EFI computers using the default answer file or a custom answer file. See "Performing a Windows OS installation" on page 52.
Step 10	Perform Quick Run or schedule the **Install Windows OS** task	After a task is created, you can choose to either perform Quick Run or schedule the **Install Windows OS** task to run immediately or at a time that you want to execute on the client computer. You can specify the computer that the task runs on. Alternatively, you can choose to add the tasks in steps 7, 8, and 9 to the **Initial Deployment Job**. You can also create a job that contains the tasks and add the job to the **Initial Deployment Job** menu .

Table 2-5 Installing Windows OS on a client computer *(continued)*

Step	Action	Description
Step 11	Verify that the computer boots in the production environment	After you execute the **Install Windows OS** task on the computer, verify that the Windows OS is installed and the computer is in production environment. By default, the computer boots to the production environment after the task executes. After you execute the **Install Windows OS** task on the computer, verify that the Windows OS is installed and the computer is in production environment. To boot the client computer in the production environment, use the **Boot To** task in a job after the **Install Windows OS** task. To verify, from the Symantec Management Console, click **Manage** menu > **Computers** > select the computer name from the list of available computers. The details of the selected computer appear in the **General** pane. Verify the operating system that is installed on the computer. You can also view the status of the **Install Windows OS** task in the **Jobs/Tasks** list.

See "Configuring the initial deployment settings" on page 47.

Performing a Windows OS installation

You execute the **Install Windows OS** task of Deployment Solution to install Windows operating system (OS) on client computers. This task lets you install the Windows OS on bare metal computers that are added to a network as well as on managed computers. For installing the OS on bare metal computers, ensure that you execute the **Partition Disk** task to create partitions on the client computer's hard drive before you install the Windows OS.

See "Creating disk partitions" on page 55.

Before you install Windows OS on managed computers, ensure that you execute the **Erase Disk** task first followed by the **Partition Disk** task. You must also, ensure that the architecture of the automation folder that you installed on the managed computer and that of the operating system to be installed is the same.

After installing Windows OS if the client computer is not able to connect to the Symantec Management Platform, then check if the Symantec Management Agent (SMA) is installed

To install Windows OS on client computers

1. In the Symantec Management Console , from the **Manage** menu select **Jobs and tasks**.
2. On the right pane, right-click **Jobs and tasks** and select **New** > **Task**.
3. On the **Create new task** page, select **Install Windows OS**.
4. Specify a name for the task on the first field.
5. Select and enter the required information.
6. Click **OK**.

See "Erasing a Disk" on page 53.

Adding OS licenses

Before you decide to create and deploy a Windows operating system (OS) image, you must add the OS and the OS license through the console. The OS license is required during execution of the **Prepare for Image Capture** task on Windows client computers. The **OS Licenses** list stores the Volume License Keys (VLKs) that deploy the sysprep-enabled images.

To add OS licenses

1. In the Symantec Management Console, on the **Settings** menu, click **Deployment** > **OS Licenses**.
2. Click **Add**.
3. Choose the operating system from the drop-down list.
4. Type the product key.
5. (Optional) Type a description for the license.
6. Click **OK**.

   The new license is displayed in the **OS Licenses** list.

To add the OS license key for the corresponding OS installation package while executing the **Install Windows OS** task, click the **Add** button beside the **System Files -Product Key** field and then enter the license key.

See "Configuring the Sysprep imaging" on page 39.

Erasing a Disk

You can use the **Erase Disk** task to wipe a disk clean. Hence, the partitions along with data are removed from the client computer. When you reallocate hardware, you can use this task to ensure that none of the old data can be retrieved. You can

either delete the partitions of the disk, erase the system disk, or configure the task to erase all the disks. You cannot perform an **Erase Disk** task for a disk that is connected through a USB or FireWire interface.

You access the Erase Disk task from **Manage > Jobs and Tasks** menu. In the **Jobs and Tasks** window, expand **System Jobs and Tasks** and right-click **Deployment and Migration > New > Task** option. In the **Create New Task** dialog box, access **Deployment and Migration > Erase Disk**.

You access the Erase Disk task from **Manage > Jobs and Tasks** menu. In the **Jobs and Tasks** window, expand **System Jobs and Tasks** and right-click **Deployment > New > Task** option. In the **Create New Task** dialog box, access **Deployment > Erase Disk**.

To erase a disk

1. In the Symantec Management Console , from the **Manage** menu select **Jobs and tasks**.
2. On the right pane, right-click **Jobs and tasks** and select **New** > **Task**.
3. On the **Create new task** page, select **Erase Disk**.
4. Specify a name for the task on the first field.
5. Select one of the following options:

Task name icon	Lets you specify the name of the erase disk task.
Remove partitions	Lets you remove the selected partitions of the disk. Select the disk partition from the drop-down list of the **Disk selection** option and check the **Erase data** check box.

Erase disk	Lets you select from the following options to erase disk: ■ **System disk** Select this option if you want to erase system disk of the client computer in the WinPE environment. ■ **All disks** Select this option if you want to erase all disks. ■ **Secure erase** Select this option to erase data more than once. The following group of operations is performed on the hard drive six times: ■ All addressable locations are overwritten with 0x35. ■ All addressable locations are overwritten with 0xCA. ■ All addressable locations are overwritten with a pseudo-random character. ■ All addressable locations are verified in hardware using the Verify Sectors command to the disk. **Note:** Using the **Secure erase** option, this task has a 36-hour timeout value on the task server. If this task runs on a client that has a hard disk larger than 375 GB, the task reports as failed on the task server. However, the task continues to run on the client until it completes.
Advanced Options	Displays advanced options such as **Reboot**. Lets you restart the computer after the erase task completes.

6 Click **Ok**.

See "Creating disk partitions" on page 55.

Creating disk partitions

You can use **Partition Disk** option to create partitions on your disk. Before you install an OS using Deployment Solution, the drive must have partitions.

You access the **Partition Disk** task from **Manage > Jobs and Tasks** menu. In the **Jobs and Tasks** window, expand **System Jobs and Tasks** and right-click **Deployment and Migration > New > Task** option. In the **Create New Task** dialog box, access **Deployment and Migration > Partition Disk**.

You access the **Partition Disk** task from **Manage > Jobs and Tasks** menu. In the **Jobs and Tasks** window, expand **System Jobs and Tasks** and right-click **Deployment > New > Task** option. In the **Create New Task** dialog box, access **Deployment > Partition Disk**.

The drive that you want to partition must not contain any previous partitions on it. If the drive was previously used and contains partitions, you can use the **Erase Disk** task to delete those partitions.

BIOS	NTFS	Align must not be set	Mark as Active option must be selected
UEFI/EFI	EFI	Align must be set to 1MB	(optional) Mark as Active option must be selected
UEFI/EFI	MSR	Align must be set to 1MB	(optional) Mark as Active option must be selected
UEFI/EFI	NTFS	Align must not be set	Mark as Active option must not be selected

See "Erasing a Disk" on page 53.

To create disk partitions

1. In the Symantec Management Console, from the **Manage** menu select **Jobs and tasks**.
2. On the right pane, right-click **Jobs and tasks** and select **New** > **Task**.
3. On the **Create new task** page, select **Partition Disk**.
4. Specify a name for the task on the first field.
5. Click **Add**.
6. On the **Add Partition** dialog box, select and enter the required information.
7. Click **OK**
8. On the **Create New Task** page, click **OK**.

Chapter 3

Discovery and Inventory

This chapter includes the following topics:

Discovery methods for Windows computers

Before you can manage computers, you must do the following:

- 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 discover Windows computers by doing the following:

- Searching for all Windows computers on your network that are registered on a specific domain
- Searching for all Windows computers on your network that match the organizational units that you specify

If you want to discover the computers that are running on other operating systems, you can use Network Discovery.

Table 3-1 Discovery methods for Windows computers

Method	Description
Resource discovery	Searches the specified domain for all computers that are registered on that domain. You must choose at least one of the Domain Browse List or Domain Membership options. See "Discovering computers with domain resource discovery" on page 58.
Microsoft Active Directory Import	Lets you import the computer resources that match the organizational units that you specify. You can also filter the computers that have been active within a specific number of days or that are running a specific Windows operating system. This method returns detailed information on the operating systems for each of your discovered computers and is the preferred method. See "Importing resources using Microsoft Active Directory Import" on page 62.

You can use these discovery methods to discover all your computers in domains, or you can target computers in a single domain.

Discovering computers with domain resource discovery

You can discover Windows computers by searching domain resource information. Discovered computers have a resource created for them in the CMDB. You can run a discovery manually or use a schedule. After a discovery is run, you can view the reports that show your discovery results.

This database contains the following information on each discovered computer:

- Name (Domain Browse List and Domain Membership)
- OS name (Domain Browse List and Domain Membership)
- Main version (Domain Browse List)

- Minor version (Domain Browse List)
- Platform (Domain Browse List)

See "Discovery methods for Windows computers" on page 57.

Note: The status message on the **Resource Discovery** page shows the last time that discovery was run manually from the page. The time is not updated to show any subsequent scheduled discovery that has been run.

To discover computers with domain resource discovery

1. In the Symantec Management Console, on the **Actions** menu, click **Discover** > **Import Domain Membership/WINS**.
2. On the **Domain Membership/WINS Import** page, under **Domains to search**, type the name of a domain you want to search, and then click the add icon.
3. (Optional) To enter a different user name and password for the domain so that Notification Server has access, complete the following steps in order:
   - Select the domain.
   - Click the pencil icon.
   - Click **Use these credentials**.
   - Enter the user name and password, and then click **OK**.
4. Select at least one of the following options:

Domain Browse List

This method is designed for small, peer-to-peer environments.

The method uses the network browse list to discover all computers on the domain. The browse option discovers all computers that share files or printers or are running the Windows Messenger Service.These computers include Windows NT/2000/2003/2008/95/98/98 SE/ME/XP/7/8.

This method can also discover computers in a workgroup that meet the search criteria.

The Domain Browse List works by enumerating the records in the computer browse list. This computer browse list was designed for a small, peer-to-peer environment, so it does not scale to large environments well.

When Notification Server performs a Domain Browse List discovery, it requests a copy of the computer browse list. The browse list includes additional information such as the computer's operating system and version. It then does a reverse lookup of the computer's name to get its IP address.

You might have problems discovering computers using this method if the following conditions exist:

- The computer is not in the computer browse list.
- The computer is in the computer browse list but not registered as sharing files.
- It can take between 15 minutes and 51 minutes for changes to be reflected in the computer browse list.

The Domain Browse List discovery method gets as much of the computer browse list as it can and as fast as it can. This method can overload a PDC in a large domain or a multi-domain environment. Symantec recommends that you run this outside business hours, preferably over a weekend.

Domain Membership This option discovers all computers with trust accounts in the domain. It can discover computers in Windows NT 4.0 domains or Windows 2000 and later Active Directory domains. This method finds all Windows NT/2000/2003/2008/XP/7/8 computers in the domain. However, any Windows 95/98/98 SE/ME computers are not found.

Note: Limited information can be discovered on computers in NT 4.0 domains. For example, the specific operating system of the computer is not known.

Domain Membership discovery works by enumerating the computer accounts in the specified domains.

When you add a Windows Windows NT/2000/2003/2008/XP/7/8 computer to a domain, a computer account is created in that domain. The computer uses this account to authenticate with the domain so the computer can authenticate user logons using a secure connection. Windows 9x computers do not create a computer account, which is why you cannot find Windows 9x computers using this method.

When discovering computers using the Domain Membership method, Notification Server catalogs these accounts. Unlike the Domain Browse List method, these accounts have no additional information beyond the computer's name. Notification Server still does a reverse lookup on the name to get its IP address.

5 Choose one of the following options:

Discover now	Click **Discover Now**.
Set schedule	Under **Scheduling Options**, in the **Schedule** drop-down list, specify the schedule of the import.

6 Click **Save changes**.

7 To view the discovery results, do the following:

- Click **View Discovery Reports**.
- In the **Resource Discovery Reports** window, right-click a report and click **Open in New Window**.
- Enter the parameters for the report.
- Click **Refresh**.

Importing resources using Microsoft Active Directory Import

You can import all of the computers that are registered in your Active Directory. Alternatively, you can choose to import only the computers that match the criteria you specify.

See "About Microsoft Active Directory Import" on page 63.

When you install the Symantec Management Platform, you can use Microsoft Active Directory Import to import all your computers. You can then target the unmanaged computers for Symantec Management Agent installation. Microsoft Active Directory Import is the preferred method for identifying new and unmanaged computers. It returns detailed information on the operating systems for each of your discovered computers.

You can also use Microsoft Active Directory Import to create Symantec Management Platform accounts and roles from Windows users and groups. You import Windows users and groups so that you do not have to manually create Symantec Management Platform accounts and roles. Microsoft Active Directory Import has a resource import rule for importing role and account resources. When this rule runs, it duplicates the Windows user and group structure in Symantec Management Platform. It creates a Symantec Management Platform account for all of the Windows users in the selected security groups. It also creates Symantec Management Platform roles for each of the selected security groups. Finally, it puts the newly created Symantec Management accounts into the Symantec Management Platform roles where the corresponding Windows user is put into the corresponding Windows group.

After the initial import, you can configure resource import the rules that regularly check Active Directory for new or changed resources and then import the appropriate resources to the CMDB.

When you configure resource import rules, you can specify the Active Directory source structure from which to import. You can apply the constraints that filter the imported computers according to your requirements. For example, you can import only the computers that have changed their computer account password within a particular number of days or those that are running a particular Windows operating system.

Table 3-2 Process for importing resources using Microsoft Active Directory Import

Step	Action	Description
Step 1	Configure the appropriate resource import rules.	You can create any new resource import rules that you want and modify the existing rules to suit your requirements. You can also delete any rules that you no longer need. See "Creating and modifying resource import rules" on page 65.
Step 2	Schedule the resource import rules.	For each resource import rule, you can schedule full imports and update imports to run at appropriate intervals. See "Scheduling resource import rules" on page 68.
Step 3	Configure the Directory Synchronization schedule.	The Directory Synchronization schedule identifies previously imported the resources that no longer exist in Active Directory and removes them from the CMDB. See "Configuring the Directory Synchronization schedule" on page 69.
Step 4	(Optional) Run a resource import rule manually.	You can run a resource import rule manually at any time. You can run the rule as a full import or an update import. See "Running resource import rules manually" on page 70.

About Microsoft Active Directory Import

The Microsoft Active Directory Import feature of the Symantec Management Platform lets you import Active Directory objects, such as users, computers, sites, and subnets, into the CMDB. This feature lets you leverage the data that already exists in Active Directory without re-creating it. You can schedule regular imports to keep your CMDB populated with up-to-date resources, allowing better management of your environment.

Microsoft Active Directory Import uses Lightweight Directory Access Protocol (LDAP) to provide one-way synchronization from Active Directory to the Symantec Management Platform. LDAP is the same protocol used by standard Active Directory administration tools. Microsoft Active Directory Import supports Windows 2003 and 2008 domains.

To use Microsoft Active Directory Import, you need to define the appropriate resource import rules to import the resources that you want. You can schedule the resource import rules to run at regular intervals, and you can run them manually at any time. When you run a resource import rule, you can import all of the appropriate data (a full import). Alternatively, you can import the data that is new or changed in Active Directory since the previous import (an update import). As part of the import process,

you can automatically create filters or organizational groups based on the organizational units, security groups, and distribution groups that are set up in Active Directory. These filters can be used to specify resource targets to which you apply policies and tasks.

See "Importing resources using Microsoft Active Directory Import" on page 62.

During the import process, the computers from Active Directory are matched with managed computers in the CMDB, using the computer name and domain. However, Microsoft Active Directory Import imports all computers that the resource import rules identify, regardless of their Symantec Management Agent installation status. Importing all computers lets you import new and unmanaged computers and then target those computers for Symantec Management Agent installation.

Note: You can also discover new and unmanaged Windows computers using Resource Discovery.

See "Discovery methods for Windows computers" on page 57.

If there are any errors in the import process, you can check the Symantec Management Platform status log for information. The status log can be accessed from the Start menu on the Symantec Management Platform computer: **All Programs > Symantec > Diagnostics > Altiris Log Viewer**.

The Symantec Management Platform includes a number of reports that provide information on Microsoft Active Directory Import activities. These reports are stored in the **Reports > Notification Server Management > Microsoft Active Directory** folder.

About importing resource associations

Microsoft Active Directory not only stores objects, it also stores relationships between objects. Microsoft Active Directory Import can extract these relationships from Active Directory and create the appropriate resources and resource associations in the CMDB. Microsoft Active Directory Import supports four resource associations for users and one resource association between subnets and sites. For the User resource you can also define a new association.

Table 3-3 Resource associations supported by Microsoft Active Directory Import

Resource association	Description
User - Company	Creates a Company resource for the imported User based on its "company" attribute in Active Directory.

Table 3-3 Resource associations supported by Microsoft Active Directory Import *(continued)*

Resource association	Description
User - Department	Creates a Department resource for the imported User based on its "department" attribute in Active Directory.
User - User	Creates one or more User resources for the imported User based on its "directReports" attribute in Active Directory.
User - User	Creates a User resource for the imported User based on its "manager" attribute in Active Directory.
Site - Subnet	Creates one or more Subnet resources for the imported Site based on its "siteObjectBL" attribute in Active Directory.
Subnet - Site	Creates a Site resource for the imported Subnet based on its "siteObject" attribute in Active Directory.

The **Enable Resource Associations** window lets you use these relationships in a resource import rule to import other related resources that are not explicitly specified in the rule. By default, all of the available resource associations are enabled.

See "Creating and modifying resource import rules" on page 65.

Creating and modifying resource import rules

Resource import rules let you specify the resources that you want to import from Active Directory.

Six default resource import rules are supplied with the Symantec Management Platform, one for each of the supported resource types: User, Computer, Print Queue, Site, Subnet, and Role and Account. You can modify these rules to suit your requirements, or you can create new rules to import the resources that you want.

You can configure a rule to automatically create filters or organizational groups based on the Active Directory organizational units, security groups, and distribution groups from which the rule imports resources. These filters can then be used to specify resource targets to which you apply policies and tasks.

You can schedule your resource import rules to update the CMDB at regular intervals, or you can run a particular rule manually at any time. Running your resource import rules periodically ensures that any changes to Active Directory are reflected in the CMDB.

This task is a step in the process for importing resources using Microsoft Active Directory Import.

See "Importing resources using Microsoft Active Directory Import" on page 62.

To create or modify a resource import rule

1 In the Symantec Management Console, on the **Actions** menu, click **Discover > Import Microsoft Active Directory**.

2 On the **Microsoft Active Directory Import** page, perform one of the following tasks:

To create a new resource import rule	In the toolbar, click **Create a new import rule**. The new rule is added to the list of resource import rules.
To modify an existing resource import rule	In the list of resource import rules, select the appropriate rule.
To delete a resource import rule	In the list of resource import rules, select the appropriate rule, and then in the toolbar, click **Delete the selected import rule**.

3 In the resource import rule that you want to modify, for each of the highlighted links, click the link, and then specify the appropriate settings.

Specified resource type (default setting), Computer, User, Site, Subnet	Specify the domain type and resource type that you want to import and the appropriate Active Directory source structure.
Specified data source (default setting)	Specify the domain or server (domain controller) and the appropriate account credentials from which you want to import resources.

None (default setting)	When you click this link, one of the following dialog boxes appears: ■ **Select Organizational Unit (OU)** Select the Active Directory organizational units or Containers (whichever corresponds to the source structure that you specified in the **Resource Selection** window) from which to import resources. When you select an organizational unit or container, you can choose whether or not to include its descendants. ■ **Select Security Groups** or **Select Distribution Groups** Select the particular Active Directory groups from which to import users and groups. The **Select Security Groups** dialog box only appears for the rule that imports role and account resources.
Specified column mappings (default setting), Default column mappings	Specify the mapping between the Symantec Management Platform CMDB and Active Directory resource data fields. You can use these mappings to import additional attributes when the Active Directory schema has been extended.
All computers, **All users**	Specify the appropriate criteria to constrain the imported resources to only those that match the specified criteria. A resource is imported only if it meets all of the specified criteria.
These resource associations	Specify the resource associations that you want to use to import other related resources that are not explicitly specified in the resource import rule. By default, all of the available resource associations are enabled. Microsoft Active Directory Import can extract these relationships from Active Directory and create the appropriate resources and resource associations in the CMDB. See "About importing resource associations" on page 64.
Specified schedules	Specify the schedules that are used to import resources. You can specify schedules for full and update data imports. See "Scheduling resource import rules" on page 68.

4 Check the appropriate **Enabled** boxes to enable the importing of computer, user, subnet, and site resources.

5 Click **Apply**.

Scheduling resource import rules

For each resource import rule, you can specify the appropriate Full Import and Update Import schedules. A full import imports all resources from the targeted domain controller or domain. An update import imports only the resources that have changed since the last time the resource import rule ran.

A single resource import rule may include both schedules, or you may configure different full import and update import rules. If you configure a specific update import rule, we recommend that the rule targets a domain controller rather than a domain.

An update import runs as a full import if any of the following are true:

- The rule is run for the first time.
- The domain or server that is specified in the rule has changed.
- The domain controller that the rule previously imported from is not available.

If necessary, you can override the schedule and run a resource import rule manually at any time.

See "Creating and modifying resource import rules" on page 65.

See "Running resource import rules manually" on page 70.

This task is a step in the process for importing resources using Microsoft Active Directory Import.

See "Importing resources using Microsoft Active Directory Import" on page 62.

To schedule resource import rules

1. In the Symantec Management Console, on the **Actions** menu, click **Discover > Import Microsoft Active Directory**.
2. On the **Microsoft Active Directory Import** page, beside the resource import rule that you want to schedule, check **Enabled**.
3. In the resource import rule description, click **Specified schedules**.
4. In the **Rule Scheduling** window, set up either or both of the following schedules:

Full Import Schedule	Imports all of the resources that the resource import rule identifies.
Update Schedule	Imports only the new and modified resources that the resource import rule identifies.

   See "To set up a schedule" on page 69.
5. Click **OK** to close the **Rule Scheduling** page.
6. Click **Apply**.

To set up a schedule

1. Under the appropriate schedule, check **Enable**.
2. In the **Schedule** drop-down list, select one of the following schedules:

At date/time	Specify the appropriate date and time. If you want the schedule to repeat, check **Repeat every**, and then specify the repeat interval.
Shared schedule	Select the appropriate shared schedule.

Configuring the Directory Synchronization schedule

To keep the CMDB synchronized with Active Directory resources, you need to configure the appropriate Directory Synchronization schedule. The Directory Synchronization schedule identifies any previously imported resources that no longer exist in Active Directory and removes them from the CMDB. It also detects any resources that have been renamed or moved outside of the organizational units from which they were initially imported, and deletes the corresponding records from the CMDB.

Warning: If you move a computer from a domain to a workgroup, you must delete the computer's record from Active Directory to avoid duplication in the CMDB.

This task is a step in the process for importing resources using Microsoft Active Directory Import.

See "Importing resources using Microsoft Active Directory Import" on page 62.

To configure the Directory Synchronization schedule

1. In the Symantec Management Console, on the **Actions** menu, click **Discover > Import Microsoft Active Directory**.
2. In the **Microsoft Active Directory Import** page, under **Directory Synchronization Schedule**, check **Enabled**.

3 In the **Schedule** drop-down list, select one of the following schedules:

At date/time	Specify the appropriate date and time. If you want the schedule to repeat, check **Repeat every**, and then specify the repeat interval.
Shared schedule	Select the appropriate shared schedule.

4 Click **Apply**.

Running resource import rules manually

If you need to import particular resources immediately, you can run the appropriate resource import rule manually. You can run the resource import rule as a full import or an update import. Running a resource import rule manually has no effect on its schedule, if one is enabled.

See "Scheduling resource import rules" on page 68.

This task is a step in the process for importing resources using Microsoft Active Directory Import.

See "Importing resources using Microsoft Active Directory Import" on page 62.

To run resource import rules manually

1 In the Symantec Management Console, on the **Actions** menu, click **Discover > Import Microsoft Active Directory**.

2 In the **Microsoft Active Directory Import** page, select the resource import rule that you want to run.

3 Click one of the following options:

Run the selected import rule now (Full Import)	Runs a full import of the selected resource import rule.
Run the selected import rule now (Update Import)	Runs an update import of the selected resource import rule.

4 If you want to stop the import process for any reason, click **Stop**.

About Inventory Solution

Inventory Solution lets you gather inventory data about computers, users, operating systems, and installed software applications in your environment. The application metering feature also lets you monitor and deny the usage of software applications on your network.

Note: You can track usage of managed software products, meter, and deny Win64 and Win32 applications on Windows XP and above computers only. Software-based usage tracking and application metering are not supported on Windows server.

Inventory Solution lets you gather inventory on Windows, UNIX, Linux, and Mac computers.

For a complete list of supported platforms and versions, see release notes at the following URL:

http://www.symantec.com/docs/DOC9471

Policies and tasks let you gather inventory and perform application metering. You can use predefined inventory policies, configure them, or create new policies and tasks according to your needs.

The inventory data is stored in the Configuration Management Database (CMDB). The CMDB provides a central store of data that is used across the Symantec Management Platform.

For more information, see the topics about the CMDB in the *IT Management Suite Administration Guide*

You can gather the following types of inventory data:

Basic inventory data	Computer name, domain, installed operating system, etc.
Standard inventory data	Hardware and software components, file properties, etc.
Custom inventory data	Additional data beyond the predefined data classes in Inventory Solution.
Application metering inventory data	Start, stop, deny events and summary data of monitored software applications.
Baseline inventory data	Information about files and registry settings on computers.
Inventory for Network Devices	Inventory data from the discovered devices in your network.

Inventory Solution provides a web-based management console, policies to alert you about critical information, and predefined or custom reports that let you analyze gathered inventory data.

Inventory Solution also has the following features:

- Supports zero-footprint configuration.
- Operates in always connected, sometimes connected, and standalone computing environments.
- Can be installed to run on a recurring basis with the Symantec Management Agent.
- Posts data through SMB and/or HTTP.
- Lets you meter, track, or deny the usage of one or more software applications and harvest unused software licenses.

Symantec™ Inventory Pack for Servers powered by Altiris™ technology is a separate product that lets you gather server-based inventory data from servers.

See "About Inventory Pack for Servers " on page 72.

Additional Symantec products let you gather inventory data from managed computers, network devices, and Windows, UNIX, Linux, and Mac servers.

See "Where to get more information" on page 20.

About Inventory Pack for Servers

Inventory Pack for Servers is a separate product with a separate license. It runs on top of Inventory Solution and uses the Inventory Pack for Servers Plug-in. Inventory Pack for Servers lets you gather inventory on Windows, UNIX and Linux computers.

Inventory Pack for Servers is part of the Server Management Suite.

You can use different methods to gather inventory data about server-class software that is installed on servers.

Server Inventory is supported for the following server applications:

- Oracle Database 9i (Enterprise Edition, Standard Edition)
- Oracle Database 10g (Enterprise Edition, Standard Edition, Standard Edition One)
- Oracle Database 11g (Enterprise Edition, Standard Edition, Standard Edition One)

Note: For Oracle, only standalone server configurations are supported. Distributed configuration modes (such as Application Cluster, Oracle Streams, Oracle Dataguard, Oracle Standby Database, etc.) are not supported.

- Microsoft SQL Server 2008
- Microsoft SQL Server 2012
- Microsoft SQL Server 2014
- Microsoft SQL Server 2016
- Microsoft SQL Server clusters
- Microsoft Exchange Server
- Microsoft DHCP server
- Microsoft DNS server
- Microsoft RAS server
- Microsoft IIS
- MySQL 5.7.x (not supported for Windows)
- Apache HTTP Server 2.x
- Network load balancing
- System DSN

Note: Only the servers that are installed as a native package into the default directories are supported.

When creating an Inventory task, the Administrator needs to provide credentials to connect to the database, otherwise inventory only collects limited information.

For a complete list of supported platforms and versions, see release notes at the following URL:

http://www.symantec.com/docs/DOC9471

See "About Inventory Solution" on page 71.

Gathering inventory on Windows servers

You can gather inventory data by running automated policies and tasks on managed computers. To gather inventory, you need to install the Symantec Management Agent and Inventory Pack for Servers Plug-in on target computers. The inventory

policies and tasks use the Plug-in to perform the inventory scan on the target computer. The inventory data is sent to the Configuration Management Database (CMDB).

See "About Inventory Pack for Servers " on page 72.

Inventory policies let you gather inventory on a recurring schedule. Inventory Solution includes the predefined inventory policies that you can use to gather inventory. You can also create and configure your own inventory policies. You can use unique policies and schedules for different kinds of inventory. For example, you can have one policy collect hardware inventory daily, and another policy collect software inventory weekly.

Table 3-4 Process for gathering inventory on Windows servers

Step	Action	Description
Step 1	Prepare managed computers for inventory.	Target computers must have Symantec Management Agent and Inventory Pack for Servers Plug-in installed. See "Preparing managed computers for inventory" on page 75.
Step 2	Turn on an inventory policy or task, or create a new inventory policy or task.	You need to turn on and configure a policy or a task to collect inventory. You can use an existing policy or create and configure your own policies or tasks. See "Gathering inventory with predefined inventory policies" on page 76. See "Creating and configuring inventory policies and tasks" on page 78.
Step 3	(Optional) Configure custom inventory policy schedules.	An inventory policy with the custom schedule does not run automatically as soon as possible after the custom schedule is created and on any new computer that joins the target collection. You can configure the custom policy schedule to run the policy immediately once and on a recurring schedule later. See "Scheduling custom inventory policies to run immediately once and on a recurring schedule later" on page 79.
Step 4	View inventory results.	You can view the gathered inventory data in reports or in the Resource Manager.

Video: For more information about gathering inventory, see Gathering Inventory with Inventory Solution Video on Symantec Connect.

Preparing managed computers for inventory

Inventory policies and tasks require that the target computers have Symantec Management Agent installed on them.

Table 3-5 Process for preparing managed computers for inventory

Step	Action	Description
Step 1	Discover the computers that you want to manage.	You can discover the computers that are not yet managed by Symantec Management Agent. When computers are discovered, resource objects are created for them in the Configuration Management Database (CMDB). You may have discovered computers when you installed the Symantec Management Platform or when you added new computers to the network. For more information, see the topics about the resource discovery in the *IT Management Suite Administration Guide* at the following URL: http://www.symantec.com/docs/DOC9469
Step 2	Install Symantec Management Agent on the computers.	You may have performed this task when you installed the Symantec Management Platform or when you added new computers to the network. You can also install Symantec Management Agent manually. For more information, see the topic about methods for installing Symantec Management Agent for Windows, UNIX, Linux, and Mac computers in the *IT Management Suite Installation and Upgrade Guide*at the following URL: http://www.symantec.com/docs/DOC9500
Step 3	Install or upgrade the plug-in on the managed computers.	To gather inventory on managed computers, you must install or upgrade Inventory Plug-in and Inventory Pack for Servers Plug-in. See "Installing the Inventory Plug-in" on page 75.

Installing the Inventory Plug-in

To gather inventory data on managed computers, you must install Inventory Plug-in on them.

If you have Inventory Pack for Servers, you can use the Inventory Pack for Servers Plug-in.

To install a plug-in, you configure the policy that installs the plug-in on managed computers. You choose the group of computers on which the policy runs, and when it runs. If you choose a group that contains a computer that already has the plug-in

installed, the task is ignored on that computer. When you turn on the policy, the plug-in is automatically installed on any new computer that is a member of the target group.

By default, no plug-in installation policies are turned on. If you install Inventory Solution for the first time, you must manually turn on the policies to install the Inventory Plug-in.

Before you perform this task, you must install Symantec Management Agent on target computers.

This task is a step in the process for preparing managed computers for inventory.

To install the Inventory Plug-in

1. In the **Symantec Management Console**, on the **Actions** menu, click **Agents/Plug-ins > Rollout Agents/Plug-ins**.
2. In the left pane, under **Agents/Plug-ins**, expand **Discovery and Inventory > Windows/UNIX/Linux/Mac**, and then click the policy for the plug-in that you want to install.
3. In the right pane, on the toolbar, click **Apply to** to choose the computers on which you want to install the plug-in.

   For more information, see the topics about specifying the targets of a policy and specifying filtering rules in the *IT Management Suite 8.0 Administration Guide* at the following URL:

   http://www.symantec.com/docs/DOC8632
4. Under **Schedule**, on the toolbar, click **Schedule**, and then schedule the policy to run on managed computers.
5. On the plug-in install page, turn on the policy.

   At the upper right of the page, click the colored circle, and then click **On**.
6. Click **Save changes**.

The next step is to gather inventory on your client computers.

See "Gathering inventory with predefined inventory policies" on page 76.

Gathering inventory with predefined inventory policies

You can gather inventory data from managed computers with predefined inventory policies. You can also configure the predefined policies to meet your needs. If you want to configure a predefined policy, Symantec recommends that you clone it, and then configure the copy.

To use inventory policies or tasks, you must install Inventory Pack for Servers Plug-in on target computers.

Note: You can manually run an original or modified predefined inventory policy on the managed Windows computers. You can do it after the policy automatically runs on the computer at least once.

See "About running inventory policies and tasks on Windows computers using `InvSoln.exe`" on page 81.

This task is a step in the process for gathering inventory on Windows servers.

See "Gathering inventory on Windows servers" on page 73.

Before you perform these steps, ensure that you have prepared the managed computers for inventory.

To turn on predefined inventory policies

1. In the **Symantec Management Console**, on the **Manage** menu, click **Policies**.
2. In the left pane, expand **Discovery and Inventory > Inventory**, and then click the predefined inventory policy that you want to use.
3. On the inventory policy page, turn on the policy.

   At the upper right of the page, click the colored circle, and then click **On**.
4. Click **Save changes**.

To clone and configure predefined inventory policies

1. In the **Symantec Management Console**, browse to the predefined inventory policy that you want to clone.
2. Right-click the policy, and then click **Clone**.
3. Give the cloned policy a unique name, and then click **OK**.
4. On the inventory policy page, configure the policy options according to your needs.

   For more information about the options, click the page, and then press the **F1** key.
5. On the inventory policy page, turn on the policy.

   At the upper right of the page, click the colored circle, and then click **On**.
6. Click **Save changes**.

The next step is to wait for the client computers to receive the new policy and report the inventory results, and then view the data that is stored in the Configuration Management Database (CMDB).

Creating and configuring inventory policies and tasks

In the Task Management Portal, you can create new inventory policies or tasks. You can configure policies and tasks to meet your further needs.

Before you can use inventory policies or tasks, you must install Inventory Pack for Servers Plug-in on target computers.

Note: You can manually run an inventory policy or task on the target Windows computer. You can do it after the policy or task is automatically run on the computer at least once.

See "About running inventory policies and tasks on Windows computers using `InvSoln.exe`" on page 81.

This task is a step in the process for gathering inventory on managed computers.

See "Gathering inventory on Windows servers" on page 73.

To create and configure inventory policies

1. In the **Symantec Management Console**, on the **Home** menu, click **Discovery and Inventory > Inventory**.
2. In the **Inventory Policy status** Web Part, click **New**.
3. On the inventory policy page, configure the policy options according to your needs.

   For more information about the options, click the page, and then press the **F1** key.
4. (Optional) Click **Advanced** to configure the data classes, the policy run options, or the software inventory rules, and then click **OK**.

   The scope of collected inventory information depends on the account permissions. For example, if a particular user account does not have permission to access a file, the information about this file is not collected. Also, the information about some inventory and server inventory data classes (Task Scheduler Windows, File Share Windows, etc.) cannot be collected if the user does not have administrator rights.

   For more information about the options in the **Advanced Options** dialog box, click the dialog box, and then press the **F1** key.

5 On the inventory policy page, turn on the policy.

At the upper right of the page, click the colored circle, and then click **On**.

6 Click **Save changes**.

To create and configure inventory tasks

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

2 In the left pane, navigate to the folder where you want to create an inventory task, right-click the folder, and then click **New > Task**.

For example, to create an inventory task in the **Inventory** folder, expand **Jobs and Tasks > System Jobs and Tasks > Discovery and Inventory**, right-click **Inventory**, and then click **New > Task**.

3 In the **Create New Task** dialog box, in the left pane, under **Discovery and Inventory**, click **Gather Inventory**.

4 In the right pane, give the task a descriptive name and select the types of inventory to gather.

5 (Optional) Click **Advanced** to configure the data classes, the task run options, or the software inventory rules, and then click **OK**.

For more information about the options in the **Advanced Options** dialog box, click the dialog box, and then press the **F1** key.

6 Click **OK** to save the task.

7 On the task page, schedule the task to run on managed computers.

For more information, see the topic about adding a schedule to a policy, task, or job in the *IT Management Suite Administration Guide*.

8 Click **Save changes**.

The next step is to wait for the client computers to receive the new policy or task and report the results, and then view the data that is stored in the Configuration Management Database (CMDB).

Scheduling custom inventory policies to run immediately once and on a recurring schedule later

You can create a custom inventory policy with the custom schedule set according to your needs. The custom inventory policy does not run automatically as soon as possible (ASAP) after the custom schedule is created. The policy does not run automatically ASAP on any new computer that joins the target collection.

However, you can manually specify the two custom schedules that behave as follows:

- The first schedule runs the policy once at the nearest time after the schedule is created on the current set of managed computers and on any new computer that joins the target collection later
- The second schedule reruns the policy later at the predefined time.

Before you perform this step, ensure that you have prepared the managed computers for inventory.

To schedule custom inventory policies to run immediately once and on a recurring schedule later

1. In the **Symantec Management Console**, on the **Manage** menu, click **Policies**.
2. In the left pane, click **Discovery and Inventory > Inventory**, and then, in the right pane, select the inventory policy that you want to schedule.
3. Under **Ensure my inventory is current**, click **Custom schedule**.
4. In the **Edit Policy Schedule** dialog box, select **Use agent time** for the time zone.
5. To specify the schedule that runs the policy once immediately on the current set of managed computers and on any new computer that joins the target group later, perform the following steps in order
   - Click **Add schedule > Scheduled time**, and then specify the schedule that expires in the next few minutes.
     For example, if the current time is 7:50 A.M., set the schedule to 8:00 A.M.
   - Click **No repeat**, in the **Repeat schedule** dialog box, click **No repeat**, and then click **OK**.
6. To specify the schedule that reruns the policy later at the predefined time, perform the following steps in order:
   - Click **Add schedule > Scheduled time**, and then specify the schedule
   - Click **No repeat**, in the **Repeat schedule** dialog box, specify the appropriate frequency, and then click **OK**.
7. In the **Edit Policy Schedule** dialog box, click **OK**.
8. Under **Applies To/Compliance**, define the set of managed computers to which you want to apply the policy.
9. On the inventory policy page, turn on the policy.

   At the upper right of the page, click the colored circle, and then click **On**.
10. Click **Save changes**.

The next step is to wait for the client computers to receive the new policy and report the results, and then view the data that is stored in the Configuration Management Database (CMDB).

About running inventory policies and tasks on Windows computers using `InvSoln.exe`

Inventory Solution provides the utility `InvSoln.exe` that lets you run inventory policies and tasks on managed Windows computers. You may need to initiate inventory scans on managed Windows computers in the following cases:

- You want to re-run inventory policies and tasks according to your needs. You want to initiate inventory scans and view the progress window during the inventory scans.
- You need to troubleshoot the problems that may arise when you run inventory policies or tasks from the Notification Server computer.
  For example, Symantec support can quickly gather the inventory on Windows computers to diagnose any inventory data class issue.

Note that to gather inventory correctly the user running InvSoln.exe needs to have local administrator rights.

On Windows computers, after you install Inventory Solution, the Inventory Pack for Servers Plug-in must automatically run the modified predefined policy at least once. After the policy runs automatically, the configuration of the predefined policy is saved.

When you install Inventory Solution, the Inventory Plug-in saves the `InvSoln.exe` utility and the default task configuration files for the predefined inventory policies to the following locations on managed Windows computers:

- `InvSoln.exe` is located at `%ProgramFiles%\Altiris\Altiris Agent\Agents\Inventory Agent`
- The default task configuration files are located at `%ProgramFiles%\Altiris\Altiris Agent\Agents\Inventory Agent\InvTaskConfig`

After a predefined inventory policy runs on a Windows client computer, the corresponding task configuration file is replaced in its location by the reference for policy configuration with the same policy name. The actual policy configuration is associated with this reference.

You can use `InvSoln.exe` to collect inventory on client computers with predefined or custom inventory policies and tasks.

To run the predefined inventory policies on Windows client computers with the `InvSoln.exe` utility, run the following commands at the command prompt:

Table 3-6 Default commands to run the predefined inventory policies

Command	Description
`InvSoln.exe /dhi`	The command to run the predefined policy **Collect Delta Hardware Inventory**.
`InvSoln.exe /dswi`	The command to run the predefined policy **Collect Delta Software Inventory**.
`InvSoln.exe /fi`	The command to run the predefined policy **Collect Full Inventory**.
`InvSoln.exe /dsi`	The command to run the predefined policy **Collect Delta Server Inventory**. Note that the command runs inventory collection only when the Inventory Pack for Servers Plug-in is installed on client computers.
`InvSoln.exe /fsi`	The command to run the predefined policy **Collect Full Server Inventory**. Note that the command runs inventory collection only when the Inventory Pack for Servers Plug-in is installed on client computers.

You can modify the predefined policy on the Notification Server computer. After Inventory Pack for Servers Plug-in receives and runs the modified policy, the default task configuration of the predefined policy gets overwritten on managed Windows computers. You can then use the default commands to run the modified predefined policies.

See "Gathering inventory with predefined inventory policies" on page 76.

When the predefined policy runs on managed Windows computers, the progress window for gathering inventory does not appear by default. To view the progress window during the inventory scan, you can run the `/p true` command-line switch at the command prompt. To hide the progress window during the inventory scan, you can run the `/p false` command line switch at the command prompt. By specifying the `/p true` or `/p false` command line options, you update the configuration of the policy or task, and save it for future use.

For example, to run the **Collect Delta Hardware Inventory** policy and view the progress window, you run the following command:

```
InvSoln.exe /dhi /p true
```

To view the details of other available command-line options, you can run one of the following commands at the command-prompt:

```
InvSoln.exe /?
```

```
InvSoln.exe /Help
```

You can create a new inventory policy or task on the Notification Server computer. When you configure the policy or task, you specify the managed Windows computers to which the policy or task applies. After the Plug-in receives and runs the new policy or task, the reference for the configuration of the policy or task is saved to the following location on managed Windows computers:

```
%ProgramFiles%\Altiris\Altiris Agent\Agents\Inventory
Agent\InvTaskConfig
```

For example, if you create a policy **Select HW Data classes**, the Plug-in saves the reference for policy configuration `Select HW Data classes.xml`. If you create a **Gather Inventory** task, the Plug-in saves the reference for task configuration `Gather Inventory.xml`.

You can use the `InvSoln.exe` utility and the saved reference to run the newly created inventory policy or task on managed Windows computers, and then view the progress window. To do this, you run the following command at the command-prompt:

```
InvSoln.exe /i "%ProgramFiles%\Altiris\Altiris Agent\Agents\Inventory
Agent\InvTaskConfig\%reference-file-name%" /p true
```

For example, to run the **Select HW Data classes** policy and view the progress window, you run the following command:

```
InvSoln.exe /i "%ProgramFiles%\Altiris\Altiris Agent\Agents\Inventory
Agent\InvTaskConfig\Select HW Data classes.xml" /p true
```

To run the **Gather Inventory** task and hide the progress window, you run the following command:

```
InvSoln.exe /i "%ProgramFiles%\Altiris\Altiris Agent\Agents\Inventory
Agent\InvTaskConfig\Gather Inventory.xml" /p false
```

See “Creating and configuring inventory policies and tasks” on page 78.

Gathering inventory using stand-alone packages

Stand-alone packages let you gather inventory on the computers that are not managed through Symantec Management Agent.

Table 3-7 Process for gathering inventory using stand-alone packages

Step	Action	Description
Step 1	Create a stand-alone inventory package.	You create stand-alone inventory packages in the Symantec Management Console. See "Creating, editing, or cloning stand-alone inventory packages" on page 84.
Step 2	Run the stand-alone inventory package on the target computers.	You run the stand-alone packages that gather the inventory data on the target computers. To run a stand-alone package, you need to have administrator rights. See "Running stand-alone inventory packages on target Windows servers" on page 88. **Warning:** Stand-alone inventory fails on client computers that have Inventory Plug-in installed on them.
Step 3	If necessary, manually copy inventory data to the Notification Server computer.	If the target computers cannot communicate directly with the Notification Server computer, you must manually report the inventory data. See "Manually reporting standalone inventory data" on page 91.
Step 4	View inventory results.	You can view the gathered inventory data in reports or in the Resource Manager.

Creating, editing, or cloning stand-alone inventory packages

You can create, edit, or clone stand-alone inventory packages. When you configure a package, you specify how the data is reported to the Notification Server computer. The inventory data is stored in files with an NSE extension.

By default, your stand-alone inventory packages are located on your Notification Server computer in the following location:

```
%InstallDir%\Altiris\Notification
Server\NSCap\bin\Win32\X86\Inventory\StandalonePackages
```

This task is a step in the process for gathering inventory using stand-alone packages.

See "Gathering inventory using stand-alone packages" on page 83.

To create, edit, or clone a stand-alone inventory package

1. In the **Symantec Management Console**, on the **Settings** menu, click **All Settings**.
2. In the left pane, under **Settings**, expand **Discovery and Inventory > Inventory Solution**, and then click **Stand-alone Inventory Packages**.
3. In the right pane, do one of the following:
   - To create a new package, click **New package**.
   - To edit a package, select an existing package and click the **Edit** symbol.
   - To create an identical copy of a package, select a package, and then click **Clone package**.
     On the **Cloning the package** page, name the package, and then click **OK**.
4. Name and describe the package.
5. Configure the package options.

   See "Stand-alone inventory package options" on page 85.
6. Click **OK**.
7. You can view the properties of the package from the **Stand-alone Inventory Packages** page.

   The properties include the path of the package file as well as the configuration settings of the package.

The next step is to run the stand-alone package on the target computer.

See "Running stand-alone inventory packages on target Windows servers" on page 88.

Stand-alone inventory package options

When you create or edit a stand-alone inventory package, you can configure its settings. You define the type of inventory gathered, where to store the data, etc. You can view the properties of a package from the main **Stand-alone Inventory Packages** page.

You specify where to store the inventory data on the basis of the access that the target computers have to the Notification Server computer.

See "Gathering inventory using stand-alone packages" on page 83.

See "Creating, editing, or cloning stand-alone inventory packages" on page 84.

See "Running stand-alone inventory packages on target Windows servers" on page 88.

Note: When the package is run, you can override some of these settings with a command-line switch.

See "Stand-alone inventory package command-line switches" on page 89.

Table 3-8 Stand-alone inventory package options

Setting	Description
Select the types of inventory to gather	You can specify the type of inventory data to gather. To select a detailed set of data, click **Advanced**.
When running on the target computer	The option **Show progress** opens a dialog box on the computer that is running the package. The dialog box displays the data classes that are gathered, and where the data is posted after the inventory is completed.
After running on the target computer	The option **Keep the inventory cached for future comparisons** lets you keep the inventory data cached so that you can compare the inventory data in the future. Inventory data comparisons are performed using command-line switches. See "Running stand-alone inventory packages on target Windows servers" on page 88.

Table 3-8 Stand-alone inventory package options *(continued)*

Setting	Description
Send inventory data to	This option lets you specify where the inventory data is stored after it is gathered. You can choose from the following options: ■ **Notification Server** You can use this option if the target computers can communicate with the Notification Server computer using HTTP (port 80 open) or HTTPS (port 443 open). When the package is run, the inventory data is automatically sent to the Notification Server computer. The URL that is used is displayed on the page. ■ **Folder** You can store the data on the local computer, on a share, or on the Notification Server computer. When the package is run, the inventory data is automatically saved on that share. Inventory data files are stored with an NSE extension. If target computers can access a shared folder on the Notification Server computer, you can store it directly on a share on the server. The Notification Server computer share to use with this option is: *notification_server_name*\NSCap\EvtInbox If the target computer cannot access the Notification Server computer, you can store the inventory data on the local computer. You can also store it on another computer that is not the Notification Server computer. You must then manually copy the files to the Notification Server computer. You may have to use this option for the following types of computers: ■ Computers that are not regularly attached to the network. ■ Computers that are outside the intranet that the Notification Server computer is on. You can specify a share or a path on the local computer. If you specify a local path, a folder is created on each target computer. For example, C:\Inventory_Data Inventory data files are stored with an NSE extension. You can also use environment variables when specifying the path to the folder. For example, \\IntermediateShare\`%computername%` If standalone inventory fails to post the NSEs to the specified target (an HTTP or HTTPS location or a folder), it deletes the NSE, NSI, and BAK files from the following folders `%programfiles%\Altiris\NSI` and `%programfiles%\Altiris\Inventory\Outbox`. When the standalone inventory runs next time, it recreates the inventory. The **NSI** and **Outbox** folders are removed if they are empty. This procedure ensures that the standalone inventory reports correct inventory to the Notification Server computer even if the users are running stand-alone inventory packages with the `/SendChangedInventory` command-line switch.

Table 3-8 Stand-alone inventory package options *(continued)*

Setting	Description
Advanced	You can configure advanced settings for running a stand-alone inventory package.

Running stand-alone inventory packages on target Windows servers

After you create stand-alone inventory packages on Notification Server, you run the packages on target computers to gather inventory data. Stand-alone inventory packages are EXE files.

See "Creating, editing, or cloning stand-alone inventory packages" on page 84.

To run a stand-alone package and gather the inventory correctly, the logged on user must be a local administrator.

This task is a step in the process for gathering inventory using stand-alone packages.

See "Gathering inventory using stand-alone packages" on page 83.

To run stand-alone inventory packages on target Windows servers

1. Make the stand-alone inventory package available to the target computers.

   See "About methods for making stand-alone inventory packages available to target Windows servers" on page 89.

2. (Optional) Use command-line switches to modify the default behavior of the package.

   See "Stand-alone inventory package command-line switches" on page 89.

3. Run the stand-alone inventory package.

4. (Optional) If you distribute the stand-alone inventory packages manually, you must also manually copy the inventory data files to the Notification Server computer after you run the package.

   See "Manually reporting standalone inventory data" on page 91.

The next step is to view the inventory results.

If necessary, you can also manually copy the inventory data to Notification Server computer.

See "Manually reporting standalone inventory data" on page 91.

About methods for making stand-alone inventory packages available to target Windows servers

Before you can run stand-alone inventory package, you must make it available to the target computers.

See "Running stand-alone inventory packages on target Windows servers" on page 88.

You can use different methods to make the packages available to target computers. The method that you use affects how the inventory data is reported back to Notification Server.

Table 3-9 Methods for making the stand-alone inventory packages available to target Windows servers

Method	Description
Packages are made available on the Notification Server computer.	If target computers can communicate with the Notification Server computer, you can make the stand-alone inventory packages available on the Notification Server computer. Target computers can access the packages in following ways: ■ From a Notification Server URL (port 80 open for HTTP and port 443 open for HTTPS) ■ From a Notification Server share See "Stand-alone inventory package options" on page 85. When you create a package, you can view the paths for the package on the **Stand-alone Inventory Packages** page.
Packages are distributed manually.	If the target computer cannot access the Notification Server computer using a URL or share, you can manually distribute the package. For example, you can email the package or place it on a different server's share or URL. If you use this method, you must manually copy the inventory data files to the Notification Server computer after you run the package. See "Manually reporting standalone inventory data" on page 91.

Stand-alone inventory package command-line switches

When you run a stand-alone inventory package, the package uses the options that you specified when you created the package. When you run a package, you can use command-line switches to modify default behavior.

See "Stand-alone inventory package options" on page 85.

See "Running stand-alone inventory packages on target Windows servers" on page 88.

These switches are not case-sensitive.

Table 3-10 Stand-alone inventory package command-line switches

Command-line switch	Description
`/EnableVerboseLog`	By default, all the errors are logged. If you specify `/EnableVerboseLog` at the command line, it enables verbose logging. If verbose logging is enabled, the trace messages are also logged. The log is stored on the local computers at the following locations: ■ On managed computers, in *`InstallDir`*`\Altiris\Altiris Agent\Logs` folder, as `Agent*.log` ■ On unmanaged computers, in *`%ProgramFiles%`*`\Altiris\Altiris Agent\Logs` folder, as `a*.log`.
`/SendChangedInventory`	By default, a stand-alone inventory package reports all the gathered inventory data. If you use this switch, the package reports only the inventory data that has changed since the last scan. To gather only changed data, the package compares the gathered inventory data to the previously collected data, if the previous data was cached. To cache inventory data, check **Keep the inventory cached for future comparisons** in the package configuration page. See "Creating, editing, or cloning stand-alone inventory packages" on page 84. If no previous inventory data is present, all gathered inventory is reported. If you have multiple Notification Servers, do not use this option if you report data to a server that does not have any previously gathered data stored on it.
`/SendInventoryTo` *destination*	Use this switch to override the value for the **Send inventory data to** option that is specified in the stand-alone package. The destination can be either an http(s) link to the Notification Server computer or a folder path. For example, you can store the NSE on a USB drive. You can use environment variables when specifying the destination. For example, you can use the following command: *`package_name`*`.exe /SendInventoryTo \\`*`server_name`*`\Inventory\%COMPUTERNAME%.` This command creates a separate folder for each computer at `\`*`server_name`*`\Inventory` and stores the NSEs in that folder. The folder is the same as the target computer's name.

Manually reporting standalone inventory data

When the stand-alone inventory package runs, its settings or a command-line switch determine where the inventory data is stored. If the stand-alone inventory package saves the inventory data to a location other than the Notification Server computer, you must manually copy the inventory data.

See "Running stand-alone inventory packages on target Windows servers" on page 88.

The inventory data is stored in files with an NSE extension. The NSE files must be copied to a Notification Server computer by a user who has rights to the server. Generally, any user on a managed computer has sufficient rights.

This task is a step in the process for gathering inventory using stand-alone packages.

See "Gathering inventory using stand-alone packages" on page 83.

Manually reporting standalone inventory data

- Copy the inventory files to the following folder:

  `\\notification_server_name\NSCap\EvtInbox`

  When the files are copied, the inventory data is stored in the Configuration Management Database (CMDB).

Gathering software inventory

Software inventory gathers information about the standard and the custom software applications that are installed on your computers. Software inventory data helps you analyze different aspects of your resources.

Table 3-11 Process for gathering software inventory

Step	Action	Description
Step 1	(Optional for Windows computers) Prepare managed computers for inventory.	Target computers must be managed and have the Inventory Plug-in installed. The Symantec Management Agent and the Inventory Pack for Servers Plug-in are not required if you use the stand-alone inventory packages for the following purposes: ■ To gather basic software application file inventory ■ To gather inventory of Windows **Add or Remove Programs** list

Table 3-11 Process for gathering software inventory *(continued)*

Step	Action	Description
Step 2	Use the software inventory method that meets your needs.	You can use different methods to gather different types of software data: ■ Basic software application file inventory ■ Inventory of Windows **Add or Remove Programs** list. ■ Targeted software inventory on Windows computers. ■ Gathering and validation of software information with the Software Catalog Data Provider See "Methods for gathering software inventory on Windows Servers" on page 93.
Step 3	View software inventory results.	You can view the gathered software inventory data in the inventory reports, the Resource Manager, and the Symantec Management Console **Software** views.

About gathering software inventory on Windows servers

Software inventory collects information about the applications that are installed on your managed computers to help you analyze different aspects of your resources.

For example, you can identify the computers that do not meet minimum security requirements, do not have antivirus software or application updates installed. You can also find out the number of installed instances of an application to prepare for a software license audit, or check whether a specific software is installed on your managed computers

Software inventory tasks or policies scan the managed computers for the available software applications, and then report the collected information to Notification Server. You can collect information about both standard applications and custom software applications that are installed on your managed computers.

For more information, see the topics about managing software in the *IT Management Suite Administration Guide*.

See "About targeted software inventory" on page 94.

See "Configuring the schedule for Software Catalog Data Provider Inventory task" on page 98.

Methods for gathering software inventory on Windows Servers

You can gather inventory about the software applications that are installed in your environment. For example, you can gather information about the application version, build number, and manufacturer.

Note: If a manufacturer does not provide the version of the software, a version is not populated for the relevant software component.

When you perform a software inventory, you can use different methods to gather different types of data.

Table 3-12 Methods for gathering software inventory

Method	Description
Basic software application file inventory	This software inventory method scans the file system on managed computers and reports software inventory based on the software application `.EXE` files that are found. For example, it reports file name, size, path, and so on. In addition to the file properties, the information about the key executables for the installed applications is collected as follows: ■ For each user, the inventory agent scans the Start Menu folder for .lnk files and collects the information about where the links point to. ■ For each user, the inventory agent scans the registry for the installed MSIs, and then each MSI is scanned for the included binaries that have a corresponding .lnk item in the MSI database. To gather basic software application file inventory on managed computers, you create, configure, and turn on the inventory policy with the **File Properties - manufacturer, version, size, internal name, etc.** box checked. See "Creating and configuring inventory policies and tasks" on page 78. To gather basic standalone inventory on unmanaged Windows computers, you create, configure, and run the stand-alone inventory package with the **File Properties - manufacturer, version, size, internal name, etc.** box checked. See "Creating, editing, or cloning stand-alone inventory packages" on page 84. See "Running stand-alone inventory packages on target Windows servers" on page 88. Beside collecting file properties based on inventory rules, inventory agent collects information about key executables for installed applications: 1) For each user scan Start Menu folder for .lnk files and collect information about executables where link points to 2) For each user scan registry for installed MSIs and each found MSI scan for included binaries that have corresponding .lnk item in MSI database. Collect information about these executables.

Table 3-12 Methods for gathering software inventory *(continued)*

Method	Description
Inventory of Windows **Add or Remove Programs** list	This software inventory method uses the **Software Discovery** task to collect the information about the installed software applications. You can gather information about the applications that are in the **Add or Remove Programs** list on managed computers (MSI cache). Note that when Inventory Solution is installed, it turns off any schedules for the **Software Discovery** task. Instead, it uses the schedules of the Inventory policies that use it. To use this method on managed computers, you create, configure, and turn on the inventory policy with the **Software – Windows Add/Remove Programs and UNIX/Linux/Mac software packages** box checked. This box is checked by default. See "Creating and configuring inventory policies and tasks" on page 78. See "Creating, editing, or cloning stand-alone inventory packages" on page 84. See "Running stand-alone inventory packages on target Windows servers" on page 88.
Targeted software inventory on Windows computers	This software inventory method lets you use rules to identify specific software applications. To use this method, you run the **Targeted Software Inventory** policy. See "Running a targeted software inventory on Windows servers" on page 96.
Gathering software information and validating it using the Software Catalog Data Provider	The Software Catalog Data Provider is a component of Inventory Solution that can be used to import software inventory data into the Software Catalog. The Software Catalog Data Provider is installed with Inventory Solution. The Software Catalog Data Provider provides a list of known software applications and predefined software products that is imported in the Configuration Management Database (CMDB). When you perform software inventory, the gathered data about software applications can be compared to the list of known applications and predefined software products. If the application data matches, it helps ensure that your software inventory data is accurate and lets you manage installed software at the product level. See "About Software Catalog Data Provider" on page 97.

See "About gathering software inventory on Windows servers" on page 92.

About targeted software inventory

Targeted software inventory feature determines whether a specific software is installed on managed computers. To find the software, it uses the software resource and detection rule information that is defined in the Software Catalog. This feature works with Windows computers only.

See "Methods for gathering software inventory on Windows Servers" on page 93.

See “Running a targeted software inventory on Windows servers” on page 96.

To find the software, targeted software inventory feature uses the following information that is defined in the Software Catalog:

- Software resource.
  A software resource consists of the metadata that describes a specific instance of a software application. A software resource is associated with the physical package file that installs the software. On the **Targeted Software Inventory** policy page, you specify the software that you want to inventory. The policy then reports the computers that contain the software.
- The detection rule of a software resource.
  The detection rule that is associated with a software resource can be used to create a policy to determine if that software resource is installed on a given computer.
- The file associations of a software resource.
  The files that are associated with a software resource can be used to analyze the Inventory Solution file scan data to determine what software is installed on a given computer.

You can use the software information that is defined in the Software Catalog to determine whether a specific software is installed on one or more managed computers.

The **Targeted Software Inventory** policy populates the inventory cache on each managed computer with the currently installed software data. That data is communicated to the Notification Server computer.

The software that you inventory must be defined as a software resource in the Software Catalog. It must also have at least one detection rule.

You can see the results of the Targeted Software Inventory in the **Installed Software** report. This report lists the software that is marked as installed, its version, count, and company name. To view additional details such as the computers on which the software is installed, its user account, and domain, right-click the software, and then click **View Details**. You access the **Installed Software** report from the **Reports** menu, at **All Reports > Discovery and Inventory > Inventory > Cross-platform > Software/Applications > Software**. You can also access this report from the Resource Manager.

See “Configuring the schedule for Software Catalog Data Provider Inventory task” on page 98.

See “About gathering software inventory on Windows servers” on page 92.

Running a targeted software inventory on Windows servers

Targeted software inventory determines whether specific software is installed on managed computers. To find the software, it uses the software resource and detection rule information that is defined in the Software Catalog.

See "About targeted software inventory" on page 94.

Before you perform this step, ensure that you have prepared the managed computers for inventory.

To run a targeted software inventory

1. In the **Symantec Management Console**, on the **Manage** menu, click **Policies**.
2. In the left pane, expand **Discovery and Inventory**.
3. Right-click **Targeted Software Inventory**, and then click **New > Targeted Software Inventory**.
4. On the **New Targeted Software Inventory** page, do the following

Policy name	Type a name for this policy. Because the description does not always appear, make the name descriptive enough to easily identify this policy.
Add description	Type a description to further identify this policy.

5. Under **Software to inventory** section, on the toolbar, click **Select Software**.
6. In the **Select Software** dialog box, in the **Available software** list, click one or more software resources, add them to the **Selected software** list, and then click **OK**.
7. To edit the detection rule for a software resource, under the **Software to inventory**, click the software resource, and then click **Edit Rule**.

   For more information, see the topics about creating or editing inventory rules in the *IT Management Suite Administration Guide*.
8. On the policy page, expand the **Schedule** section, and then configure the policy schedule.
9. Expand the **Applied to** section, and then click the managed computers that you want to apply the policy to.
10. Turn on the policy.

    At the upper right of the page, click the colored circle, and then click **On**.
11. Click **Save changes**.

The next step is to wait for the client computers to receive the new policy and report the inventory results, and then view the data that is stored in the Configuration Management Database (CMDB).

About Software Catalog Data Provider

The Software Catalog Data Provider (SCDP) is a component of Inventory Solution that can be used to identify the software that has been detected on the client computers in your environment and that cannot be identified otherwise. For example, components that were not installed with an MSI-based installer and cannot be found in the **Add/Remove Programs** list.

The **Software Catalog Data Provider Inventory** task identifies installed software and compares the information gathered by the inventory of file properties to the lists of known applications (software components) that is provided by SCDP. If a match is found, the software component can be created and imported into the Software Catalog. You can then manage your installed software.

By default, the **Software Catalog Data Provider Inventory** task runs automatically once a week on Wednesday. However, you can configure the schedule according to your needs to control which data is imported into the Software Catalog.

Note: The software in your environment can be detected either by running a software scan or with the help of SCDP. If both methods are used at the same time, duplicate software components can be created. Symantec recommends that you choose only one of these methods and disable the other.

Table 3-13 Components of Software Catalog Data Provider

Component	Description
A list of known components (**Data Provider Summary**)	An .xml file that contains a list of software resources. To view this file, do one of the following: ■ In the **Symantec Management Console**, on the **Settings** menu, click **Console > Views**, and then, in the left pane, click **Software > Data Provider Summary**. ■ In the **Symantec Management Console**, on the **Settings** menu, click **All Settings > Software > Data Provider > Providers > Data Provider Management,** in the left pane right-click **Software Catalog Data Provider**, and then click **View Data Provider Summary**.

Table 3-13 Components of Software Catalog Data Provider *(continued)*

Component	Description
Software Catalog Data Provider task	When the SCDP is installed, this task automatically gathers information about known applications that are available in **Software Catalog Data Provider**. If **Software Catalog Data Provider** data file is updated, you need to start this task manually. On the task page, select the option **Gather** to update the list of known components into CMDB. **Warning:** If you run this task with the option Import selected, it results in a database with an excessive amount of software components which may be very difficult to manage.
Software Catalog Data Provider Inventory task	This task runs by default every Wednesday and compares gathered file properties inventory to the list of known components (shown in **Data Provider Summary**). If the data matches, the **Software Catalog Data Provider** task runs for the matched components with the **Import** option enabled and creates software components with the minimum metadata (company (vendor) name, software name, version, and language).

See "Configuring the schedule for Software Catalog Data Provider Inventory task" on page 98.

Configuring the schedule for Software Catalog Data Provider Inventory task

By default, the **Software Catalog Data Provider Inventory** task runs automatically once a week on Wednesday. You can configure the schedule according to your needs to control which data is imported into the Software Catalog.

To configure the schedule for Software Catalog Data Provider Inventory task

1. In the Symantec Management Console, on the **Settings** menu, click **All Settings**.
2. In the left pane, under **Settings**, click **Software > Data Provider > Software Catalog Data Provider Inventory**.
3. Under **Task Status**, click **New Schedule**.
4. In the **New Schedule** dialog box, under **Schedule**, configure the schedule for the task, and then click **Schedule**.

See "About Software Catalog Data Provider" on page 97.

Gathering custom inventory

Custom inventory lets you configure the set of inventory data that is gathered and reported to the Configuration Management Database (CMDB).

Table 3-14 Process for gathering custom inventory

Step	Action	Description
Step 1	Prepare managed computers for inventory.	Target computers must be managed by Symantec Management Agent.
Step 2	Create a custom data class.	After you create a custom data class, you can add, edit, and delete its attributes. See "Creating and configuring a data class" on page 100.
Step 3	Create a task with scripting logic and schedule it to run on the managed computers.	You can create a new task, or clone an existing sample task. You can use the script that is included in the sample task or you can create your own logic. Depending on the platform, you can write the logic in JavaScript, shell script, or other scripting languages. See "Creating a custom inventory script task" on page 102.
Step 4	View custom inventory results.	You can view the gathered custom inventory data for a data class in the Resource Manager.

About custom inventory data classes

A data class is a table in the Configuration Management Database (CMDB). For example, the **Processor_Ex** data class is the **Inv_Processor_Ex** table in the CMDB. Each data class has a set of attributes that define its properties.

Table 3-15 Example of attributes of the **Processor Extension** data class

Attribute	Description
Device ID	Specifies the unique index that is used to identify the device.
L2 Cache Size	Specifies the size of the Level 2 processor cache in kilobytes.
L2 Cache Speed	Specifies the clock speed of the Level 2 processor cache in megahertz.

You can create a data class, and then add, edit, or delete its attributes. A configured data class is referred to as a custom data class.

See "Creating and configuring a data class" on page 100.

After you configure a data class, you can create a task, configure the task script, and roll it out to the managed computers.

See "Creating a custom inventory script task" on page 102.

The custom inventory script task that runs on the managed computers generates a Notification Server Event (NSE) that contains inventory for a data class. A unique GUID identifies each data class. The inventory in the NSE is coupled with the GUID of a data class.

Note: The script that gathers inventory on Windows computers contains a reference to the GUID of a custom data class. Every time you create or edit an existing custom data class, a new GUID is assigned to this data class. You must manually update the script with the new GUID, if it refers to the older GUID for the same custom data class.

Creating and configuring a data class

In the Symantec Management Console, you can create a custom data class, add, edit, and delete data class attributes, and change the position of the attribute. You can also find the GUID and view the data in the data class.

Note that every time you modify an attribute and save the changes, a new GUID is assigned to this data class.

See "About custom inventory data classes" on page 99.

This task is a step in the process for gathering custom inventory.

See "Gathering custom inventory" on page 99.

For more information, see the topics about custom inventory data classes and about gathering custom inventory in the *Inventory Solution User Guide*.

Before you perform this step, ensure that you have prepared managed computers for inventory.

To create and configure a data class

1. In the Symantec Management Console, on the **Settings** menu, click **All Settings**.
2. In the left pane, under **Settings**, expand **Discovery and Inventory > Inventory Solution**, and then click **Manage Custom Data classes**.
3. To create a data class, do the following:
   - On the **Manage Custom Data Classes** page, click **New data class**.
   - On the **New Data Class** page, type a name and a description for the data class, and then click **OK**.
     The name of the new data class must be unique.
4. To configure a data class, on the **Manage Custom Data Classes** page, in the data classes list, click the data class.

   You can add data class attributes, edit, or delete them.
5. (Optional) To add an attribute to the data class, do the following:
   - On the toolbar, click **Add attribute**.
   - In the **Data Class Attributes** dialog box, specify the details of the attribute.
     To add an attribute that uniquely defines a row in the data class, in the **Key** drop-down list, click **Yes**. After you do this, the attribute always has a unique value that is other than NULL.
     To add an attribute that should never be empty or blank, in the **Data required** drop-down list, click **Yes**.
     If, in the **Key** drop-down list, you click **Yes**, the **Data required** option is automatically set to **Yes**. To change this option, in the **Key** drop-down list, click **No**.
   - Click **OK**.
6. (Optional) To edit or delete the data class attributes, the attribute, and then, on the toolbar, click the **Edit** or **Delete** symbol.
7. (Optional) To let the data class store inventory of multiple objects, on the **Manage Custom Data Classes** page, check **Allow multiple rows from a single computer resource**. The data class can store the inventory of services, user accounts, files, network cards, and other objects.

8 (Optional) To specify the sequence of the attributes, on the **Manage Custom Data Classes** page, click an attribute, and then click the up arrow or down arrow.

When you report inventory values for the columns in a Notification Server Event (NSE), the attributes are identified by the column ID instead of the column name, so the order of attributes in a data class must be correct

9 Click **Save changes**.

Warning: It is very important that you save the changes. When you create any data class or add any attributes, all the information is stored in memory. Nothing is created in the database and on details page, no GUID is yet assigned. As a result, a 00000000-0000-0000-0000-000000000000 GUID is displayed in the property of the data class. Only after you click **Save changes** on the **Manage Custom Data Classes** page, the data class is saved in the database, and the GUID is generated. Note that the GUID changes every time you make changes to the definition of the data class and save it.

---

10 (Optional) Copy and paste the GUID of the data class that you created for further use.

The next step is to create a custom inventory script task.

See "Creating a custom inventory script task" on page 102.

Creating a custom inventory script task

After you have created the custom inventory data class, you create and configure a custom inventory script task that gathers the custom inventory.

See "Creating and configuring a data class" on page 100.

To create a custom inventory script task, you can clone a sample script task and configure it with the custom data classes that you created. You can also create and configure a custom inventory script task on the **Jobs and Tasks** portal page.

When you configure your custom inventory script, you can insert tokens in the script and create or edit tokens.

For more information, see the topics about the **Run script task** page and the **Tokens** page in the *IT Management Suite Administration Guide*.

This task is a step in the process for gathering custom inventory.

See "Gathering custom inventory" on page 99.

To clone a sample custom inventory script task

1. In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**.
2. In the left pane, under **Jobs and Tasks**, expand **Samples > Discovery and Inventory > Inventory samples > Custom**.
3. Right-click the sample custom inventory script task, and then click **Clone**.
4. In the **Clone** dialog box, give the cloned script a descriptive name and click **OK**.
5. (Optional) Configure the sample script, and then click **Save changes**.

   See "Configuring the custom inventory sample script" on page 104.
6. Under **Task Status**, do one of the following:
   - To schedule the task to run on managed computers, click **New Schedule**.
   - To perform a quick run of the task on managed computers, click **Quick Run**.
7. Click **Save changes**.

To create a custom inventory script task

1. In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**.
2. In the left pane, navigate to the folder where you want to create a custom inventory script task, right-click the folder, and then click **New > Task**.

   For example, to create a task in the **Jobs and Tasks** folder, right-click **Jobs and Tasks**, and then click **New > Task**.

   To create a task in the **Inventory** folder, expand **Jobs and Tasks > System Jobs and Tasks > Discovery and Inventory**, right-click **Inventory**, and then click **New > Task**.
3. In the **Create New Task** dialog box, in the left pane, click **Run Script**.
4. In the right pane, type a descriptive name for the task.
5. In the **Script type** drop-down list, click the script type.
6. Enter your own script or copy a sample custom inventory script to the script editor.

   To insert a token to your custom inventory script, do the following:
   - In the **Insert token** drop-down list, click the token that you want to insert.
   - Click **Insert**.

To access a sample custom inventory script, do the following:

- In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**.
- In the left pane, under **Jobs and Tasks**, expand **Samples > Discovery and Inventory > Inventory samples > Custom**.

7 (Optional) In the **Create New Task** dialog box, in the script editor, configure the script.

See "Configuring the custom inventory sample script" on page 104.

8 (Optional) To configure the advanced options for running the custom inventory script task, do the following:

- Click **Advanced**, and then, on the **Script** tab, configure the options according to your needs.
- In the **Task options** tab, configure the settings for running the script task, and the maximum possible length of the script task.
- Click **OK**.

9 In the **Create New Task** dialog box, click **OK**.

10 On the **Run Script** page, under **Task Status**, do one of the following:

- To schedule the task to run on managed computers, click **New Schedule**.
- To perform a quick run of the task on managed computers, click **Quick Run**.

11 Click **Save changes**.

The next step is to wait for the client computers to receive the new task and report the results, and then view the data that is stored in the Configuration Management Database (CMDB).

Configuring the custom inventory sample script

Symantec recommends that you clone the existing custom inventory script task sample, and then configure it according to your needs. The sample script for Windows already contains the required code for a WMI query. You only need to add your own logic to gather the necessary data and to populate the attribute variables in the script.

Note: Every time you create or edit an existing custom data class, a new GUID is assigned to this data class. You must manually update the script with the new GUID, if it refers to the older GUID for the same custom data class.

See "Creating a custom inventory script task" on page 102.

See "Gathering custom inventory" on page 99.

To configure the custom inventory sample script for Windows

1 Clone or open an existing sample of the custom inventory script task.

2 Specify the values that you want to gather.

Example:

```
strComputer = "."

Set objWMIService = GetObject("winmgmts:" &

"{impersonationLevel=impersonate}!\\" & strComputer &
"\root\cimv2")

'Fire WMI Query

Set objCIMObj = objWMIService.ExecQuery("select * from
CIM_processor")
```

3 Replace the GUID in the script with the GUID of the data class that you created.

Example:

```
set objDCInstance = nse.AddDataClass ("{e8220123-4987-4b5e-bc39-
ec6eaea312ef}")
```

To access the GUID of the data class that you created, do the following:

- In the Symantec Management Console, on the **Settings** menu, click **All Settings**.
- In the left pane, under **Settings**, expand **Discovery and Inventory > Inventory Solution**, and then click **Manage Custom Data classes**.
- On the **Manage Custom Data Classes** page, click the data class, and then, under **Manage Custom Data Classes**, on the toolbar, click the **Details** symbol.

4 Update attributes of the data class.

Example:

```
For each objInfo in objCIMObj

'Add a new row

dim objDataRow

set objDataRow = objDataClass.AddRow

'Set columns

objDataRow.SetField 0, objInfo.DeviceID

objDataRow.SetField 1, objInfo.L2CacheSize

objDataRow.SetField 2, objInfo.L2CacheSpeed

Next
```

5 Click **Save changes**.

Gathering agentless inventory

You can gather agentless inventory data from discovered SNMP-enabled network devices and enter that data in the Configuration Management Database (CMDB).

See "About gathering agentless inventory" on page 107.

The process for gathering agentless inventory from network devices is as follows:

Table 3-16 Process for gathering inventory of network devices

Step	Action	Description
Step 1	Discover network devices.	You can only gather inventory of the devices that are already discovered. For more information, see topics about Network Discovery in the *IT Management Suite Administration Guide*.
Step 2	Use SNMP data mapping tables to define how to map SNMP devices to the data that you want to gather.	SNMP data mapping tables identify the data fields that you want to gather and apply the settings to the selected device types.

Table 3-16 Process for gathering inventory of network devices *(continued)*

Step	Action	Description
Step 3	Create agentless inventory tasks.	You create and schedule tasks to collect inventory. You can create the tasks either with inventory wizard or manually. See "Creating agentless inventory tasks using the wizard" on page 108. See "Manually creating, scheduling, modifying, and stopping agentless inventory tasks" on page 109.
Step 4	View agentless inventory data.	You can view the gathered inventory data in the Resource Manager or on the **Agentless Inventory** page. See "Viewing agentless inventory results" on page 111.

About gathering agentless inventory

Inventory for Network Devices lets you gather agentless inventory data from the discovered SNMP network devices such as computers, network printers, network-attached storage devices, and network backup devices. To gather inventory, agentless tasks run on discovered devices and report the data to Notification Server. The data is stored in the Configuration Management Database (CMDB). You can configure the automated tasks that are scheduled to run at regular intervals to keep your inventory data current.

See "Gathering agentless inventory" on page 106.

When you configure agentless inventory tasks, you specify the following:

- Which devices to inventory
- When to run the task

You can configure multiple tasks to meet your needs.

You can create and configure agentless inventory tasks in the following ways:

Creating a task with Agentless Inventory wizard.	The wizard guides you through the creation and configuration of agentless inventory tasks. You can later edit the advanced settings and schedules of a task on the task page. See "Creating agentless inventory tasks using the wizard" on page 108.

Creating a task manually	You can manually create tasks from the **Agentless Inventory Tasks** Web Part. This option lets you configure more advanced settings and schedules. See "Manually creating, scheduling, modifying, and stopping agentless inventory tasks" on page 109.

You can only gather inventory from the SNMP-enabled devices on your network that are already discovered. Run the **Network Discovery** task to discover your network devices and create resources for them in the CMDB. Make sure that the connection profile of the **Network Discovery** task has the SNMP turned on.

For more information, see topics about Network Discovery in the *IT Management Suite Administration Guide*.

Agentless inventory tasks use connection profiles to manage the protocols that are used to communicate with network devices. Connection profiles are components of the Symantec Management Platform. When a device is discovered, a resource for that device is created in the CMDB. The resource keeps a record of the protocols that were used to communicate with the device. When you use agentless inventory tasks, you do not specify a connection profile or protocols. Agentless inventory tasks automatically use the same protocols that were enabled when the device was discovered.

For more information, see the topics about resource discovery and using connection profiles in the *IT Management Suite Administration Guide*.

Creating agentless inventory tasks using the wizard

The wizard guides you through the process of creating agentless inventory tasks and configuring basic settings. You can later configure the advanced settings and schedule the tasks on the task page.

This task is a step in the process of gathering agentless inventory from network devices.

See "Gathering agentless inventory" on page 106.

Before you perform theis step, ensure that you have mapped the SNMP devices to the data that you want to gather.

To create agentless inventory tasks for network devices using the inventory wizard

1. In the Symantec Management Console, on the **Home** menu, click **Discovery and Inventory > Agentless Inventory**.
2. In the **Agentless Inventory Quick Start** Web Part, click **Run inventory wizard**.

3 In the **Agentless inventory task creation** wizard, on the **Choose devices to inventory** page, do the following, and then click **Next**:

- Select **Choose devices**, and then, in the drop-down list, click the group of target devices that you want to gather inventory from.
  For more information, see topics about using filters and organizational views in the *IT Management Suite Administration Guide*.
- Under **Include Device Types**, check the types of devices that you want to gather inventory from.
- (Optional) To gather inventory from an individual device, in the wizard, select **Individual device**, and then, in the drop-down list, click the device from which you want to gather inventory.
  This list includes all SNMP-enabled devices that have been previously discovered and have resources in the Configuration Management Database (CMDB).

4 On the **Inventory network task name** page, type a name for the task, and then click **Next**.

5 On the **Schedule task** page, configure the task schedule, and then click **Finish**.

See "To schedule agentless inventory tasks" on page 110.

6 (Optional) To view the created task, do one of the following:

- In the Symantec Management Console, on the **Home** menu, click **Discovery and Inventory > Agentless Inventory**, and then view the task in the **Agentless Inventory Tasks** Web Part.
  Note that to view the newly created task, you may need to click the **Refresh** symbol.
- In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**, and then, in the left pane, under **Jobs / Tasks**, expand **System Jobs and Tasks > Discovery and Inventory**.

The next step is to view the agentless inventory data.

See "Viewing agentless inventory results" on page 111.

Manually creating, scheduling, modifying, and stopping agentless inventory tasks

You can manually create, modify, and stop agentless inventory tasks on the **Agentless Inventory Home** page.

See "About gathering agentless inventory" on page 107.

This task is a step in the process for gathering agentless inventory.

See “Gathering agentless inventory” on page 106.

Before you perform these steps, ensure that you have mapped the SNMP devices to the data that you want to gather.

To manually create agentless inventory tasks

1. In the Symantec Management Console, on the **Home** menu, click **Discovery and Inventory > Agentless Inventory**.
2. In the **Agentless Inventory Tasks** Web Part, on the **Available Tasks** tab, on the toolbar, click **New**.
3. In the **New Agentless Inventory Task** dialog box, give the task a descriptive name, and then do the following:
   - Select **Group of Devices**, and then, in the drop-down list, click the group of devices that you want to gather inventory from.
     For more information, see the topics about using filters and organizational views in the *IT Management Suite Administration Guide*.
   - Under **Group of Devices**, check the types of devices that you want to gather inventory from.
   - (Optional) To gather inventory from an individual device, select **Individual device**, and then, in the drop-down list, click the device that you want to gather inventory from
     This list includes all SNMP-enabled devices that have been previously discovered and have resources in the Configuration Management Database (CMDB).
   - (Optional) Click **Advanced**, specify the maximum number of threads per inventory task, and then click **OK**.
     During the inventory process, a separate thread is used for each device. The maximum number of threads is based on the amount of traffic that you want this task to generate and on the capacity of your Notification Server computer.
4. Click **OK**.

To schedule agentless inventory tasks

1. In the Symantec Management Console, on the **Home** menu, click **Discovery and Inventory > Agentless Inventory**.
2. In the **Agentless Inventory Tasks** Web Part, on the **Available Tasks** tab, click the task that you want to schedule, and then click **Schedule**.
3. In the **New Schedule** dialog box, configure the task schedule according to your needs, and then click **Schedule**.

To configure or stop agentless inventory tasks

1. In the Symantec Management Console, on the **Home** menu, click **Discovery and Inventory > Agentless Inventory**.
2. In the **Agentless Inventory Tasks** Web Part, on the **Available Tasks** tab, click the task that you want to schedule, and then do one of the following:
   - To configure the task run schedule, on the toolbar, click **Schedule**.
     In the **New Schedule** dialog box, configure the task according to your needs, and then click **Schedule**.
   - To configure the task settings, on the toolbar, click the **Edit** symbol.
     In the **New Agentless Inventory Task** dialog box, configure the task according to your needs, and then click **OK**.
   - To stop the task, click the **Tasks Run** tab, click the task that you want to stop, and then, on the toolbar, click **Stop**.

The next step is to view the agentless inventory data.

See "Viewing agentless inventory results" on page 111.

Viewing agentless inventory results

The data collected by the inventory tasks is stored in the CMDB.

You can view the collected data and the additional details about the devices in the **Resource Manager** or on the **Agentless Inventory Home** page

For more information, see the topics about **Resource Manager** in the *IT Management Suite Administration Guide*.

The **Agentless Inventory Home** page presents a data summary of inventoried network devices. On this page you can also see the status of agentless inventory tasks.

This task is a step in the process for gathering agentless inventory.

See "Gathering agentless inventory" on page 106.

To view agentless inventory data in the Resource Manager

1. In the Symantec Management Console, on the **Manage** menu, click **Resource**.
2. In the **Select Resource** dialog box, click the resource that you want to view, and then click **OK**.
3. On the **Resource Manager** page, on the toolbar, click **View > Inventory**, and then, in the navigation pane, under **Data Classes**, navigate to **Network Device Data** to view the inventory data.

To view agentless inventory data on the Agentless Inventory Home page

1. In the Symantec Management Console, on the **Home** menu, click **Dicovery and Inventory > Agentless Inventory**.
2. On the **Agentless Inventory Home** page, view the **Devices Inventoried By Type (Last 30 Days)** and **Agentless Inventory Tasks** Web Parts.

Gathering baseline inventory on Windows servers

Baseline inventory lets you track and compare the changes in files and registry keys on managed computers. You generate a baseline that identifies the files or registry settings of a computer. You can later run the compliance scans on your managed computers to compare their current files or registry keys with those in the baseline. The differences between the baseline scan and compliance scan data are reported to the Configuration Management Database (CMDB).

Table 3-17 Process for gathering baseline inventory

Step	Action	Description
Step 1	Prepare computers for gathering baseline inventory.	Target computers must be managed with Symantec Management Agent.
Step 2	Create and run a file or registry baseline task.	A file baseline task lets you perform the file baseline scan and generate a baseline that identifies the files of a computer. See "Running a file baseline or file compliance task" on page 114. A registry baseline task lets you perform the registry baseline scan and generate a baseline that identifies the registry settings of a computer. See "Running a registry baseline or registry compliance task" on page 116.

Table 3-17 Process for gathering baseline inventory *(continued)*

Step	Action	Description
Step 3	Create and run a file or registry compliance task.	A file compliance task lets you perform the file compliance scan on your managed computers to compare their current files with those in the baseline. See "Running a file baseline or file compliance task" on page 114. A registry compliance task lets you perform the registry compliance scan on your managed computers to compare their current registry settings with those in the baseline. See "Running a registry baseline or registry compliance task" on page 116.
Step 4	View baseline inventory results.	You can view baseline inventory data in **Baseline Reports**.

About baseline files

The baseline inventory process uses and creates several baseline files. A baseline configuration file contains options for running the scans. For example, you configure the files or registry keys to be included or excluded, the directories to scan, and so on. You can use the default configuration file, edit it, or create one or more custom configuration files. Configuration files for registry baselines are in INI format. The default registry baseline configuration file is `AexRegScan.ini`. Configuration files for file baselines are in INI format but have a .bls extension. The default file baseline configuration file is `local_master.bls`.

The local baseline tasks use the default configuration files.

The location of the default baseline configuration files and additional sample configuration files is as follows:

InstallDir`\Altiris\Notification Server\NSCap\bin\Win32\X86\Inventory\Application Management`

A baseline snapshot (BLS) file maintains a record of the files or registry settings on a computer at a given time. This data is gathered during a baseline scan that is based on the options in a baseline configuration file. Registry baseline snapshots are saved to a new file on the scanned computer in `.RBL` format.

File baseline snapshots are appended to the baseline configuration file. The location of the default baseline snapshot files is as follows:

%ProgramFiles%\Altiris\eXpress\Baseline

The file compliance scan and the registry compliance scan create output in XML format. This output is stored in Notification Server Events (NSEs) and reported to the Configuration Management Database (CMDB).

The default locations of the file baseline tasks and the registry baseline tasks, respectively, are as follows:

InstallDir\Altiris\Notification Server\NSCap\bin\Win32\X86\Inventory\Application Management\FileBaselinePackage

InstallDir\Altiris\Notification Server\NSCap\bin\Win32\X86\Inventory\Application Management\RegBaselinePackage

---

Warning: If you want to run a baseline task with custom configuration or snapshot after an offbox upgrade, you need to update the path to the configuration and snapshot files. After an upgrade, the host name of Notification Server may change, the path to the task files becomes invalid for the new server, and the baseline task with custom configuration or snapshot fails. If you define the UNC path to the task files using\\localhost\NSCap\..., the path defined before the upgrade remains valid after the upgrade.

You need to make sure that you copy or keep the baseline configurations and baseline snapshots that you want to use for compiling a custom baseline or comparing with a custom baseline when running these tasks. Otherwise, the task fails.

Running a file baseline or file compliance task

A file baseline task lets you perform the file baseline scan and gather data about the files on a computer at a given time. The data that is gathered during this scan is saved in a baseline snapshot (.BLS) file on the scanned computer.

A file compliance task lets you perform the file compliance scan. The files that are found during this scan of your managed computers are compared to the baseline snapshot. Baseline inventory also contains predefined reports to track baseline and compliance information.

To perform a file baseline scan, you create and run a **File Baseline** task. Symantec recommends that you run the file baseline task once to establish the baseline, and then re-run the file baseline task only when the standard configuration changes.

You should not run the file baseline task on a regular basis if the file baseline task and the file compliance task run on the same computer. If you do, you continually overwrite the file baseline snapshot file.

This task is a step in the process for gathering baseline inventory.

See "Gathering baseline inventory on Windows servers" on page 112.

Before you perform this step, ensure that you have prepared the managed computers for gathering baseline inventory.

To run a file baseline or file compliance task

1. In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**.
2. In the left pane, navigate to the folder where you want to create and run a file baseline task or a file compliance task, right-click the folder, and then click **New > Task**.

   For example, to create the task in the **Inventory** folder, expand **Jobs and Tasks > System Jobs and Tasks > Discovery and Inventory**, right-click **Inventory**, and then click **New > Task**.
3. In the **Create New Task** dialog box, in the left pane, under **Discovery and Inventory**, click **File Baseline**.
4. In the right pane, do one of the following:
   - To configure the file baseline task, click **Compile a baseline snapshot**.
   - To configure the file compliance task, click **Compare with a baseline snapshot**.

   For more information about the options, click the page and then press **F1**.
5. Click **OK**.
6. On the **File Baseline** task page, under **Task Status**, configure the task schedule.

   For more information, see the topic about adding a schedule to a policy, task, or job in the *IT Management Suite Administration Guide*.
7. Click **Save changes**.

To run a custom file baseline or file compliance task

1. In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**.
2. In the left pane, navigate to the folder where you want to create and run a file baseline task or a file compliance task, right-click the folder, and then click **New > Task**.

   For example, to create a task in the **Inventory** folder, expand **Jobs and Tasks > System Jobs and Tasks > Discovery and Inventory**, right-click **Inventory**, and then click **New > Task**.
3. In the **Create New Task** dialog box, in the left pane, under **Discovery and Inventory**, click **File Baseline**.
4. In the right pane, do one of the following:
   - To customize the baseline configuration, select **Compile a baseline snapshot**, and then select **Use custom baseline configuration**.
     Click **Create a baseline configuration with File Baseline Configuration Editor**. In the **File Configuration Editor**, configure the parameters for the baseline, and then save the .bls file and close the editor dialog box.
     Click **Browse**. In the dialog box that opens, navigate to the .bls file that you created, select the file, and then click **Open**.
   - To customize the compliance task, select **Compare with a baseline snapshot**, and then select **Compare with custom baseline snapshot**.
     (Optional) Click **Open File Baseline Snapshot Editor**. In the **File Snapshot Editor**, configure the parameters for the snapshot, and then save the .bls file and close the editor dialog box.
     Click **Browse**. In the dialog box that opens, navigate to the snapshot that you want to use, select the file, and then click **Open**.
5. (Optional) Click **Advanced**, and then, in the dialog box that opens, configure the download, run, and task setting.

   Click **OK**.
6. Click **OK**.

The next step is to wait for the client computers to receive the new task and report the results, and then view the data that is stored in the Configuration Management Database (CMDB).

Running a registry baseline or registry compliance task

A registry baseline task lets you perform the registry baseline scan and gather data about the registry settings on a computer at a given time. The data that is gathered

during this scan is saved in a registry baseline snapshot file (`.RBL`) on the scanned computer.

A registry compliance task lets you perform the registry compliance scan. The registry settings that are found during this scan of your managed computers are compared to the baseline snapshot.

To perform a registry baseline scan, you create and run a **Registry Baseline** task. Symantec recommends that you run each registry baseline task once to establish the baseline, and then run the registry baseline task only when the computer configuration changes.

You should not run the registry baseline task on a regular basis if the registry baseline task and the compliance task run on the same computer. If you do, you continually overwrite the baseline snapshot file.

This task is a step in the process for gathering baseline inventory.

See "Gathering baseline inventory on Windows servers" on page 112.

Before you perform this step, ensure that you have prepared the managed computers for gathering baseline inventory.

To run a registry baseline or registry compliance task

1. In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**.
2. In the left pane, navigate to the folder where you want to create and run a registry baseline task or a registry compliance task, right-click the folder, and then click**New > Task**.

   For example, to create the task in the **Inventory** folder, expand **Jobs and Tasks > System Jobs and Tasks > Discovery and Inventory**, right-click **Inventory**, and then click **New > Task**.
3. In the **Create New Task** dialog box, in the left pane, under **Discovery and Inventory**, click **Registry Baseline**.
4. In the right pane, do one of the following:
   - To configure the registry baseline task, click **Compile a baseline snapshot**.
   - To configure the registry compliance task, click **Compare with a baseline snapshot**.

   For more information about the options, click the page and then press **F1**.
5. Click **OK**.

6 On the **Registry Baseline** task page, under **Task Status**, configure the task schedule.

For more information, see the topic about adding a schedule to a policy, task, or job in the *IT Management Suite Administration Guide*.

7 Click **Save changes**.

To run a custom registry baseline or registry compliance task

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

In the left pane, navigate to the folder where you want to create a registry baseline task or a registry compliance task, right-click the folder, and then click **New > Task**.

For example, to create a task in the **Inventory** folder, expand **Jobs and tasks > System Jobs and Tasks > Discovery and Inventory**, right-click **Inventory**, and then click **New > Task**.

2 In the **Create New Task** dialog box, in the left pane, under **Discovery and Inventory**, click **Registry Baseline**.

3 In the right pane, do one of the following:

- To customize the baseline configuration, select **Compile a baseline snapshot**, and then select **Use custom baseline configuration**.
  Click **Create a registry configuration with Registry Baseline Configuration Editor**. In the **Registry Configuration Editor**, configure the parameters for the registry, and then save the .ini file and close the editor dialog box.
  Click **Browse**. In the dialog box that opens, navigate to the .ini file that you created, select the file, and then click **Open**.
- To customize the compliance task, select **Compare with a baseline snapshot**, and then select **Compare with custom baseline snapshot**.
  (Optional) Click **Open Registry Baseline Snapshot Editor**. In the **Registry Snapshot Editor**, configure the parameters for the snapshot, and then click **OK**.
  Under **Baseline configuration**, click **Browse**. In the dialog box that opens, navigate to the baseline configuration file that you want to use, select the file, and then click **Open**.
  Under **Baseline snapshot**, click **Browse**. In the dialog box that opens, navigate to the snapshot that you want to use, select the file, and then click **Open**.

4 (Optional) Click **Advanced**, and then, in the dialog box that opens, configure the download, run, and task settings.

   Click **OK**.

5 Click **OK**.

The next step is to wait for the client computers to receive the new task and report the results, and then view the data that is stored in the Configuration Management Database (CMDB).

Chapter 4

Patch Management

This chapter includes the following topics:

Preparing your environment for Patch Management

Patch Management Solution for Windows requires some components to be configured or enabled before others can function correctly. When you complete each task for the first time, you can also configure it for future automation. Automation is a key feature of Patch Management Solution for Windows as it reduces system administration workload and enhances overall security.

Table 4-1 Process for implementing Patch Management Solution for Windows

Step	Action	Description
Step 1	Install or upgrade the solution.	Use Symantec Installation Manager to install the solution.
Step 2	Install or upgrade the Symantec Management Agent.	Install or upgrade the Symantec Management Agent on every computer to which you want to send patches. For more information, see the topics about installing or upgrading the Symantec Management Agent in the *IT Management Suite Administration Guide*. See "Where to get more information" on page 20.
Step 3	Install or upgrade the software update plug-in.	Install the plug-in that manages all of the Patch Management Solution for Windows functionality on a client computer. See "Installing the software update plug-in" on page 122.
Step 4	Configure Windows software updates distribution	(Optional) Configure software update package distribution and program settings.
Step 5	Enable the **Windows Update** service.	On client computers, enable and configure the **Windows Update** service to make available the installation of software updates. You can configure the **Windows Update** service to start manually or automatically. Symantec recommends that you configure the **Windows Update** service to start manually. When you enable the **Manual** startup type setting, the service starts and remains started until a computer restart. **Warning:** When you enable the **Automatic** startup type setting, client computers may be restarted after the software update cycle is completed. For more information, see the following knowledge base article: http://www.symantec.com/docs/TECH41678
Step 6	Configure the software update files location settings.	(Optional) Configure the software update files storage location settings. See "Configuring software updates download location" on page 123.
Step 7	Configure the software updates installation settings.	(Optional) Configure the time when you want to perform software update installation and computer restarts. See "Configuring software updates installation settings" on page 125.

Table 4-1 Process for implementing Patch Management Solution for Windows *(continued)*

Step	Action	Description
Step 8	Configure the system assessment scan interval.	(Optional) Configure when to run the system assessment scan, which inventories managed computers for the software updates that they require. See "Configuring Windows System Assessment Scan policy" on page 126.
Step 9	Download the Windows software updates metadata.	Download the Windows software updates metadata and configure the metadata update schedule. See "Downloading the Windows software updates catalog" on page 127.

Installing the software update plug-in

The software update plug-in manages all of the Patch Management Solution for Windows functionality on a client computer. When the system assessment scan tool reports to Notification Server that a certain software update is required for a managed computer, the update is then sent to the software update plug-in. The software update plug-in ensures that the update is applicable and not already installed, and then installs it.

After you install the software update plug-in on a managed computer, the **Software Updates** tab appears in the Symantec Management Agent user interface. This tab displays the status of software updates for that computer. If the tab is not visible, in the Symantec Management Agent, click **View > Software Updates**. To open the Symantec Management Agent user interface, click the Symantec Management Agent icon in the system tray of the managed computer.

See "Installing the software update plug-in" on page 122.

Note: If you have a large number of computers where you want to install the software update plug-in, consider deploying it during off-peak hours to minimize network traffic. Deploying the software update plug-in can take some time, depending on the number of managed computers and the Symantec Management Agent settings.

See "Preparing your environment for Patch Management" on page 120.

To install the software update plug-in

1. In the Symantec Management Console, on the **Actions** menu, click **Agents/Plug-ins > Rollout Agents/Plug-ins**.
2. In the left pane, expand **Software > Patch Management > Software Update Plug-in Install**.
3. (Optional) In the right pane, make any necessary changes.

   For help, press **F1** or, on the **Help** menu, click **Context**.
4. In the upper right corner of the page, click the colored circle, and then click **On**.
5. Click **Save changes**.

The next step is to configure software update package distribution and program settings.

Configuring software updates download location

You can configure to which location on Notification Server the software updates should be downloaded.

The settings that you configure apply to Windows and Linux components of Patch Management Solution.

See "Preparing your environment for Patch Management" on page 120.

To configure software updates download location

1. In the Symantec Management Console, on the **Settings** menu, click **All Settings**.
2. In the left pane, expand **Software > Patch Management > Core Services**.
3. In the right pane, on the **Locations** tab, specify the software updates download location.
4. Click **Save Changes**.

If you change the location and you want to relocate existing software update packages, use the **Check Software Update Package Integrity** task.

The next step is to configure the software updates installation settings.

Running compliance and vulnerability reports

You can view and manage your patch management data through reports. Reports give you the information that is specific to Patch Management Solution. For example,

you can use compliance reports to determine how many urgent software updates your managed computers require.

Reports let you view information in various ways. You can see your information in tables or graphically in charts. You can also drill down on specific items in a report to obtain additional information.

You can download or distribute software updates directly from reports by right-clicking the update name in the report.

Table 4-2 Patch Management Solution reports

Report type	Description
Compliance reports	Compliance reports let you quickly determine which software updates your managed computers require. Compliance reports are used to determine if the computers are up-to-date with the latest software updates. These reports are also used to check if a particular software bulletin or update is installed on your managed computers. This capability is useful if a specific security issue affects your network environment, and a certain update addresses the problem.
Diagnostics reports	The diagnostics reports display vulnerability summary and software update plug-in installation information.
Remediation status reports	The remediation status reports summarize and detail software update associations and activities.
Software bulletins reports	The software bulletins reports summarize and detail software bulletins activity and status.

To view Patch Management reports

1. In the Symantec Management Console, on the **Reports** menu, click **All Reports**.
2. In the left pane, expand **Software > Patch Management**.
3. Click the report that you want to view.

   For example, click **Compliance > Windows Compliance by Bulletin**.
4. If you want to view more information about an update, right-click any update, and then click **Resource Manager**.

   Each type of compliance report opens a different Resource Manager, depending on the type of results. For example, the **Windows Compliance by Computer** report opens a computer-type Resource Manager. When you open a Resource Manager for a software update, you can click **Summaries > Software Bulletin Details**, and, under **Additional Information**, you can find a hyperlink to the Microsoft TechNet article on the bulletin.

The next step is to review and distribute available software updates.

See “Downloading and distributing software updates” on page 129.

See “Staging software bulletins” on page 128.

Creating and assigning custom severity levels

A software update marked critical may not necessarily be critical in your environment. You can create your own custom severity levels and assign them to software bulletins.

You first create custom severity levels, and then assign them to bulletins. You can alter custom severity levels. You cannot alter the vendor-specified severity levels.

The settings that you configure apply to Windows and Linux components of Patch Management Solution.

To create a custom severity level

1. In the Symantec Management Console, on the **Settings** menu, click **All Settings**.
2. In the left pane, expand **Software > Patch Management > Core Services**.
3. In the right pane, click the **Custom Severity** tab.
4. On the **Custom Severity** tab, in the **Severity Level** box, type the name that you want to give the custom severity level. For example, "Install right away!"
5. Click **Add**.
6. Click **Move Up** or **Move Down** to position the custom severity levels in the list.
7. Click **Save Changes**.

To assign a custom severity level to a software bulletin

1. In the Symantec Management Console, on the **Actions** menu, click **Software > Patch Remediation Center**.
2. On the **Patch Remediation Center** page, in the software bulletin list, right-click a software bulletin, and then click **Custom Severity**.
3. Click a severity level.
4. Click **Refresh** to view the new data in the **Custom Severity** column.

Configuring software updates installation settings

The **Default Software Update Plug-in Policy** page lets you configure when the software update plug-in can install software updates and restart the target computer.

See "Preparing your environment for Patch Management" on page 120.

To configure the software updates installation settings

1. In the Symantec Management Console, on the **Settings** menu, click **All Settings**.
2. In the left pane, expand **Agents/Plug-ins > Software > Patch Management > Windows > Default Software Update Plug-in Policy**.
3. In the right pane, configure when and how you want to install the updates, or leave the default values.
4. Click **Save changes**.

Configuring Windows System Assessment Scan policy

Windows system assessment scan detects applicable and installed updates on client computers with the software update plug-in installed. System assessment information is then used to determine which software updates are required. Based on this information, filters targeting the software update policies are created automatically.

System assessment scan runs automatically in the following cases:

- When the client computer receives a new or changed Windows Assessment Scan Policy
- When the client computer receives a new or changed Software Update policies
- According to the custom schedule defined by the user
- During the maintenance window
- Before an update is deployed
- After an update is deployed
- When Symantec Management Agent starts after a reboot that was initiated by an update deployment

To change the default scan settings, configure the Windows System Assessment Scan policy.

See "Preparing your environment for Patch Management" on page 120.

To configure Windows System Assessment Scan policy

1. In the Symantec Management Console, on the **Settings** menu, click **All Settings**.
2. In the left pane, expand **Software > Patch Management**, and then click **Windows System Assessment Scan**.

3 In the right pane, under **Schedule**, configure how often you want the system assessment scan to run on client computers.

If you want the plug-in to report inventory only if it has changed, check **Send Inventory Results Only if Changed** .

4 This option is checked by default.

5 (Optional) Under **Applied To**, choose on which client computers you want the scan to run.

Symantec recommends that you do not change the default filter from **Windows Computers with Software Update Plug-in Installed Target** unless you have a specific reason to do so.

6 Turn the policy on.

7 Click **Save changes**.

Downloading the Windows software updates catalog

You must download the Windows software updates catalog (patch management metadata, or patch management import files) before you can download software updates or create software update policies.

See "Preparing your environment for Patch Management" on page 120.

You may want to create a schedule for this task as well. This procedure ensures that you have the latest, most accurate data, and your software update tasks are kept up-to-date. Symantec recommends that you configure this task to run daily.

Before you perform this step, ensure that you have installed or upgraded the software update plug-in.

See "Installing the software update plug-in" on page 122.

To download the Windows software updates catalog immediately

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

2 In the left pane, expand **Jobs and Tasks > System Jobs and Tasks > Software > Patch Management > Import Patch Data for Windows**.

3 In the right pane, under **Vendors and Software**, click **Update**.

4 When the available products list import is complete, under **Vendors and Software**, check the software for which you want to download the patch management metadata.

5 (Optional) Make any other necessary changes.

6 Click **Save changes**.

7 Under **Task Status**, click **New Schedule**.

8 In the **New Schedule** dialog box, click **Now**, and then click **Schedule**.

To configure a schedule for downloading the software updates catalog

1 On the **Import Patch Data for Windows** page, under **Task Status**, click **New Schedule**.

2 In the **New Schedule** dialog box, click **Schedule**, and then configure a schedule on which to run this task.

Symantec recommends that you configure this task to run daily.

3 Click **Schedule**.

Staging software bulletins

You can download a software bulletin and its associated updates to the Notification Server computer.

Symantec recommends that you download only the bulletins that the target computers require. On the **Patch Remediation Center** page, in the compliance reports, you can view how many computers require an update.

After the updates are downloaded, you can create a software update policy to distribute the updates to managed computers.

See "Downloading and distributing software updates" on page 129.

When you choose to download a software bulletin, a task is created that downloads the associated software updates. Note that only one instance of a download task may run at same time for software update packages. A queue of download tasks may appear on Notification Server or a package server, and the software update packages may be downloaded with a delay. You can view the status of this task to troubleshoot the download of software updates.

See "Preparing your environment for Patch Management" on page 120.

Before you perform this step, esure that you have run the compliance and vulnerability reports.

See "Running compliance and vulnerability reports" on page 123.

To download software updates

1. In the Symantec Management Console, on the **Actions** menu, click **Software > Patch Remediation Center**.
2. In the right pane, in the **Show** drop-down box, click **Windows Compliance by Bulletin**, and then click the **Refresh** symbol.

   These reports let you see which updates the client computers require.
3. Select the bulletins that you want to download.

   For example, select the bulletins that have a high number in the **Not Installed** column. You can select multiple items while holding down the Shift or Control key.
4. Right-click the selected bulletins, and then click **Download Packages**.

   You can close the status dialog box or leave it open in a new window; the download continues in the background.

To view the status of a software updates download

1. In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**.
2. In the left pane, expand **System Jobs and Tasks > Software > Patch Management > Download Software Update Package**.
3. In the right pane, view the status of download tasks.

The next step is to view the results.

See "Viewing software update delivery results" on page 131.

Downloading and distributing software updates

You can stage software bulletins and download software update packages on the **Patch Remediation Center** page, where all available software updates are listed. You can also do this from any Patch Management Solution report.

When you stage a software bulletin, all associated updates are downloaded to the Notification Server computer.

When the number in the **Updates** column equals the number in the **Downloaded** column, all updates for the software bulletin have been downloaded. Also, the value in the **Staged** column changes to **True**.

You can choose to download the software update packages and distribute them to the client computers at a later time. You can also distribute the software updates once the download is complete.

See “Staging software bulletins” on page 128.

Sometimes, not all software updates can be downloaded for a software bulletin. For example, Microsoft may stop hosting the bulletin or relocate it. You cannot create a software update policy unless all updates for a particular software bulletin or update have been downloaded.

When distributing updates, you should consider the effects it can possibly have on your network environment. Symantec recommends that you distribute new updates to a test environment first.

To deliver and install the software updates to the appropriate computers, you must create software update policies.

The **Distribute Software Updates** wizard lets you create software update policies. If the associated software updates are not yet downloaded, Patch Management Solution creates a download task. When download is completed, the software update policy is distributed to the target computers.

If you want to install a Service Pack, Symantec recommends that you create a software update policy for this service pack only, without any other bulletins included in it. Also, in the wizard, check the **Allow immediate restart if required** box.

The policies that you create are stored in the **Manage > Policies > Software > Patch Management > Software Update Policies** folder. You can view the details of the policy and change settings if necessary.

You can view the software update policies distribution results in reports.

See “Viewing software update delivery results” on page 131.

See “Preparing your environment for Patch Management” on page 120.

Before you perform this step, ansure that you have run the compliance and vulnerability reports.

See “Running compliance and vulnerability reports” on page 123.

To distribute software updates

1. In the Symantec Management Console, on the **Actions** menu, click **Software > Patch Remediation Center**.
2. In the right pane, in the **Show** drop-down box, click **Windows Compliance by Bulletin**, and then click the **Refresh** symbol.

   These reports let you see which updates the target computers require.
3. Click the bulletins that you want to distribute.

   For example, click the bulletins that have a high number in the **Not Installed** column. You can select multiple items while holding down the Shift or Control key.

4 Right-click the selected bulletins, and then click **Distribute Packages**.

5 (Optional) Configure the settings as needed.

6 Click **Next**.

7 (Optional) On the second page of the wizard, check the updates that you want to distribute.

8 At the upper right of the page, click the colored circle, and then click **On**.

You can also turn on the policy later.

9 Click **Distribute software updates**.

The next step is to view the results.

Viewing software update delivery results

The **Windows Software Update Delivery - Details** report summarizes the results of all scheduled Microsoft software update policies. It shows you which computers the software update tasks target, and if the updates have been successfully installed. The report also shows you if any software update tasks failed, or if they have not yet been completed.

Patch Management Solution for Windows also provides other reports that you can view.

See "Preparing your environment for Patch Management" on page 120.

To view the software update delivery summary report

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

2 In the left pane, expand **Software > Patch Management > Remediation Status**, and then click **Windows Software Update Delivery - Details**.

Chapter 5

Software Management

This chapter includes the following topics:

- Installing and managing a virtual software layer with a Quick Delivery or Package Delivery task
- Installing and managing a virtual software layer with a Managed Software Delivery policy

What you can do with Software Management Solution

Software Management Solution lets you distribute and manage the software that is used in your organization.

Table 5-1 What you can do with Software Management Solution

Task	Description
Configure the default settings for Managed Software Delivery policies.	Configuration settings control the behavior of Managed Software Delivery policies. Rather than configuring these settings individually for each policy, you can configure the default settings that apply to all new Managed Software Delivery policies. Then you can change the settings for a specific policy only when needed. See "Configuring the default settings for Managed Software Delivery" on page 136.
Perform an advanced software delivery.	Managed Software Delivery simplifies your advanced software deliveries by letting you deliver software as a unit, which can include multiple software resources and their dependencies. For example, you can create a single Managed Software Delivery policy that installs an application and its associated patches and service packs. Managed Software Delivery can also run any task at any stage of the delivery. See "About advanced software deliveries" on page 138. See "Performing an advanced software delivery" on page 138.
Perform a quick delivery of a single software resource.	You can perform a quick delivery of a single software resource that runs with minimum configuration. You can use the task-based Quick Delivery method to specify the software to deliver, the action to perform, and the computers to deliver to. Because the software resources and the delivery settings are predefined, Quick Delivery makes it easy for administrators and non-administrators to deliver software. See "Performing a quick delivery of a single software resource" on page 140.
Deliver a package without defining a software resource.	Package Delivery lets you quickly push out any package regardless of whether it is associated with a software resource. See "Delivering a package without defining a software resource" on page 142.
Deliver software to fulfill user requests.	By using the Software Portal, users can request and install software through a Web-based interface with little or no administrator involvement.

Table 5-1 What you can do with Software Management Solution *(continued)*

Task	Description
Manage Windows Installer installations on client computers.	You can create policies and tasks to manage Windows Installer applications on managed computers as follows: ■ Repair Windows Installer applications. You can proactively identify and repair broken applications on selected computers. If an application needs repair, a repair command is sent to the Windows Installer service to initiate self-repair. See "Repairing Windows Installer applications" on page 147. ■ Update the source paths for Windows Installer applications. You can update the source paths of Windows Installer applications with resilient source paths. The updated source paths point to the package servers that you designate. If an application needs modification or repair, Windows Installer can access the needed installation file from one of these servers. See "Updating the source paths of Windows Installer applications" on page 144.
Manage virtual applications.	You can use software virtualization to facilitate the management of most Windows-based software on managed computers. Software virtualization lets you avoid conflicts between applications and quickly restore a broken application to its original installed state. Software Management Solution lets you perform the following virtualization actions: ■ Virtualize applications during a Managed Software Delivery installation. ■ Deliver and install virtual layers with any Software Management Solution delivery policy or task. ■ Manage the existing virtual layers on the client computers. See "Managing virtual applications" on page 153.

Implementing Software Management Framework

Because Software Management Framework is part of the Symantec Management Platform, you do not need to perform a separate installation or configuration. However, before you use Software Management Framework, you must set it up and prepare it for use.

Before you implement Software Management Framework, you should become familiar with its components, benefits, and other useful information.

Table 5-2 Process for implementing Software Management Framework

Step	Action	Description
Step 1	Install the Symantec Management Agent to manage client computers and install the Software Management Framework Agent.	A managed computer is the one on which the Symantec Management Agent is installed. The Symantec Management Agent is the software that establishes communication between the Notification Server computer and the computers in your network. The Software Management Framework agent is installed on the client computers along with the Symantec Management Agent. Therefore, separate installation and configuration are unnecessary. The Symantec Management Console does not contain a user interface for viewing, installing, or configuring the agent. The Software Management Framework agent runs on the client computers to perform the following functions: ■ Manage the agent and plug-in rollout technology for the Symantec Management Platform. ■ Perform the Software Discovery scan in Software Management Framework. Software Discovery scans managed computers and collects information about the Windows software that they contain. ■ Create and update a client-side software cache that keeps track of the software that is installed and discovered on the client computer. ■ Manage all the software delivery functions in Software Management Solution. Software deliveries are closely integrated with the software resources in the Software Catalog. The Software Management Framework agent manages the package downloads and other aspects of software delivery. You may have performed this step when you installed Notification Server or when you added new computers to the network.
Step 2	Configure security roles for Software Management Framework.	Administrators need the appropriate privileges to manage the packages in the Software Library and the software resources in the Software Catalog.
Step 3	Set up the Software Library.	The Software Library is the physical source for your managed packages. Set up a library directory for each server installation.

Table 5-2 Process for implementing Software Management Framework *(continued)*

Step	Action	Description
Step 4	(Optional) Configure settings for managing the Software Catalog and its contents.	You can configure the following settings for Software Management Framework: ■ **Clean up File Resources** Periodically delete any files that might be left in the database after file resources are deleted. ■ **Known-As** Use known-as associations to associate the unique identifiers of two software resources so that they are identified as being the same software ■ **Installation Error Code Descriptions** Associate informative descriptions with the installation error codes that appear on reports.
Step 5	Populate the Software Catalog with software resources.	The software resources that you plan to manage must be defined in the Software Catalog. A software resource provides a common way to describe the software so that all software-related actions can identify it accurately. The software resource data is stored in the Software Catalog.

Configuring the default settings for Managed Software Delivery

Configuration settings control the behavior of new Managed Software Delivery policies. Rather than configuring these settings individually for each policy, you can configure the default settings that apply to all new Managed Software Delivery policies. Then you can change the settings for a specific policy only when needed.

The default settings speed up the creation of Managed Software Delivery policies and promote consistency among them.

You can override the default settings for Managed Software Delivery as follows:

- When you create a Managed Software Delivery policy manually
- When you edit an existing Managed Software Delivery policy

Changing the default settings does not change the settings in the Managed Software Delivery policies that were created earlier.

Software Management Solution settings control the behavior of the software-related policies and tasks. The default settings let administrators create policies and tasks without having to enter the details that they are not familiar with. Instead, a more experienced administrator can configure the default settings that apply to all the new policies and tasks that are created. When necessary, the administrator who runs the specific policies and tasks can change the settings.

Table 5-3 Sources of default settings for Software Management policies and tasks

Policy or task	Source of default settings
Managed Software Delivery	All new managed software delivery policies inherit the default settings that are defined on the **Managed Delivery Settings** page. You can override the default settings for specific Managed Software Delivery policies. Changing the default managed software delivery settings does not affect the execution of the managed software delivery policies that were created earlier.
Package Delivery Quick Delivery Source Path Update Software Virtualization Windows Installer Repair	Some of the task settings are predefined. Other settings for these tasks are obtained from the Task Management settings or the Symantec Management Agent settings. You can override the settings for specific tasks.

To configure default settings for Managed Software Delivery

1. In the Symantec Management Console, on the **Settings** menu, click **All Settings**.
2. In the left pane, expand **Software**, and then click **Managed Delivery Settings**.
3. On the **Managed Delivery Settings** page, configure the settings on the following tabs:

Schedule	Lets you define the schedule on which a Managed Software Delivery policy runs.
Download	Lets you define how a Managed Software Delivery policy's downloads are handled.
Run	Lets you define how a Managed Software Delivery policy runs on the client computer.

4 Click **Save changes**.

About advanced software deliveries

Managed Software Delivery simplifies advanced software deliveries by letting you deliver software as a unit, which can include multiple software resources as well as dependencies. For example, you can create a single Managed Software Delivery policy that installs an application and its associated patches and service packs. Managed Software Delivery can also run any task at any stage of the delivery. For example, it can run a task that performs a restart or runs a script.

Managed Software Delivery is a policy-based delivery method that lets you configure advanced delivery settings.

See "Performing an advanced software delivery" on page 138.

Managed Software Delivery allows you to do the following:

- Intelligently perform the compliance checks and the remediation actions that let you deliver software and manage it.
- Leverage the software resource information and the logic that is in the Software Catalog such as dependencies, packages, and detection rules.
- Save bandwidth by downloading packages only when they are needed. If a client computer does not have the appropriate configuration for the software or if the software is already installed, the package is not downloaded.
- To perform multiple delivery actions with a single policy.

The software that you deliver in this way must be defined as a software resource in the Software Catalog.

If you need to perform a Quick Delivery of a single software resource, use Quick Delivery instead of Managed Software Delivery.

See "Performing a quick delivery of a single software resource" on page 140.

Performing an advanced software delivery

You can perform advanced software deliveries and manage the software that is installed on the managed computers.

See "About advanced software deliveries" on page 138.

The software that you want to deliver must be definded as a software resource in the Software Catalog.

Table 5-4 Process for performing advanced software deliveries

Step	Action	Description
Step 1	Create a Managed Software Delivery policy.	The options for creating a Managed Software Delivery policy are as follows: ■ Use the **Managed Software Delivery** wizard. The **Managed Software Delivery** wizard provides a quick way to create and schedule a policy for a single software resource and its dependency software. Symantec recommends that you use the wizard because it can include any dependency software and warn you of software associations automatically. ■ Create the policy manually. Use this method to create a Managed Software Delivery policy when you need to add multiple software resources and tasks or override the default settings. You also can publish the policy to the Software Portal. However, you must add any dependency software or determine software associations yourself. You can also edit the policy that you created with the wizard.
Step 2	(Optional) Edit the Managed Software Delivery policy.	You can edit the Managed Software Delivery policy to change or add functionality as follows: ■ Add software resources or tasks and arrange the order in which they run. ■ Change the settings of the entire policy. ■ Change the settings of specific software resources and tasks. ■ Edit the schedule or the destinations.
Step 3	Choose the delivery destinations.	Choose the computers that you want to deliver the software to. When you use the **Managed Software Delivery** wizard to create the policy, you select the destinations in the wizard.
Step 4	Schedule the policy.	Define the schedule on which a Managed Software Delivery policy runs. You schedule the compliance check and the remediation check separately. When you use the **Managed Software Delivery** wizard to create the policy, you can define the schedule during the wizard.
Step 5	After the policy runs, view reports.	The Software Management reports let you monitor the software deliveries. The delivery reports provide information about the status of the software downloads and executions. For example, the software downloads for each computer, including the status and the download date. The compliance reports provide information about the compliance actions and the remediation actions.

Performing a quick delivery of a single software resource

You can perform a quick delivery of a single software resource that runs with minimum configuration. You can use the task-based Quick Delivery method to specify the software to deliver, the action to perform, and the computers to deliver to.

Because the software resources and the delivery settings are predefined, Quick Delivery makes it easy for administrators and non-administrators to deliver software. For example, help desk personnel can easily deliver hotfixes because all they have to do is select the correct hotfix from the Software Catalog. They do not need to know which package to select or how to create the command line.

Most organizations can use Quick Delivery for the majority of their software delivery needs. Quick Delivery helps you reduce the amount of time that you spend on routine deliveries so that you can devote more time to advanced activities.

The software that you deliver in this way must be defined as a deliverable software resource in the Software Catalog. It must also have at least one command line.

After the initial instance of a Quick Delivery task runs, you can edit and rerun it. For example, you can deliver the software to different computers or run a different command line on the same computers. You can also edit the delivery settings for the task. For example, you can change the user credentials under which the task runs.

If you need to perform compliance checks or other advanced delivery activities, use Managed Software Delivery instead of Quick Delivery.

See "About advanced software deliveries" on page 138.

Table 5-5 Process for performing a quick delivery of a single software resource

Step	Action	Description
Step 1	Create a Quick Delivery task.	The options for creating a Quick Delivery task are as follows: ■ Use the **Quick Delivery** wizard. The **Quick Delivery** wizard let you create and run a Quick Delivery task with minimum configuration. ■ Create and configure the task manually. Use this method when you need to to configure the default settings of the task or run the task on a specific schedule. You can also configure the task that you created with a wizard.

Table 5-5 Process for performing a quick delivery of a single software resource *(continued)*

Step	Action	Description
Step 2	(Optional) Configure the task settings.	Every task inherits the default run settings. You can override the default settings for a particular task. For example, if you want to deliver a large package over slow network, you may want to increase the **End task after** value.
Step 3	Schedule the task and choose the delivery destinations.	When you use the **Quick Delivery** wizard to create the task, you choose the destinations in the wizard. Those destinations apply to that instance of the task only. You do not have to schedule the task because it runs as soon as possible. When you edit the task or create it without the wizard, you define the schedule and the delivery destinations every time you run the task. The options for scheduling the task are as follows: ■ Run the task now. This option runs the task as soon as possible, unless it must wait for a maintenance window. **Note:** On computers with Cloud-enabled Management this option only works like a schedule. Computers with Cloud-enabled Management receive the task from the task server that depends on the task agent schedule. Symantec recommends that you increase the default timeout period in the advanced options for the tasks that are scheduled on computers with Cloud-enabled Management. An increased timeout period can significantly improve software delivery for Quick Delivery to computers with Cloud-enabled Management. By default, the **End task after** is set to 300 minutes (five hours). A recommended value to change the timeout period to is 1440 minutes (24 hours). The maximum timeout is 2160 minutes (36 hours). ■ Schedule the task to run at a specific time.
Step 4	After the task runs, view the reports.	The Software Management reports let you monitor the software deliveries. The delivery reports provide information about the status of the software downloads and executions. For example, the software downloads for each computer, including the status and the download date.

Delivering a package without defining a software resource

Package Delivery method lets you deliver any package regardless of whether it is associated with a software resource.

You may need to use Package Delivery for the following purposes:

- To deliver a package that you choose not to manage in the Software Catalog.
- To quickly deliver a new package that is not yet in the Software Catalog.
- To deliver a package that is in the Software Catalog, but with a command line that is not defined for the package.
  For example, a package is in the Software Catalog and is associated with predefined command lines. You need to deliver that package with a specialized command line, but you do not have the privileges to edit the package or its software resource. You can create a Package Delivery task for that package and type the command line that you need.
- To run a task that you migrated from the Task Server Plug-in in Software Delivery Solution 6.x to Software Management Solution 7.x.
  The migrated tasks let you perform deliveries with the same configurations as the 6.x tasks.

Table 5-6 Process for delivering a package without defining a software resource

Step	Action	Description
Step 1	Create a Package Delivery task.	A Package Delivery task lets you perform a routine package delivery.
Step 2	(Optional) Change the task settings.	Every task inherits the default settings that control how the task runs. You can override the default settings for a particular task. For example, if you want to deliver a large package over slow network, you may want to increase the **End task after** value.

Table 5-6 Process for delivering a package without defining a software resource *(continued)*

Step	Action	Description
Step 3	Schedule the task and choose the delivery destinations.	Define the schedule and the delivery destinations every time you run the task. Your options for scheduling the task are as follows: ■ Run the task now. This option runs the task as soon as possible, unless it must wait for a maintenance window. ■ Schedule the task to run at a specific time.
Step 4	After the task runs, view the reports.	The Software Management reports let you monitor the software deliveries. The delivery reports provide information about the status of the software downloads and executions. For example, the software downloads for each computer, including the status and the download date.

Introducing Windows Installer applications

You can create policies and tasks to manage Windows Installer applications on managed computers. The policies and the tasks work with Windows Installer to enhance its functionality.

You can manage Windows Installer applications in the following ways:

Initiate the repair of Windows Installer applications.	You can proactively identify and repair broken applications on selected computers. If an application needs repair, a repair command is sent to the Windows Installer service to initiate self-repair. You can use a policy or a task to identify the applications that need repair.

Update the source paths for Windows Installer applications.	You can update the source paths of Windows Installer applications with resilient source paths. The updated source paths point to the package servers that you designate. If an application needs modification or repair, Windows Installer can access the needed installation file from one of these servers. You can use a policy or a task to update the source paths.
View reports to monitor the state of Windows Installer applications.	When you create policies or tasks to manage Windows Installer applications, data is gathered on broken applications and inaccessible source paths. The Application Management reports that are listed under the Software reports display this data. You can use this data to monitor the state of Windows Installer applications. For example, the **Software Resources - Broken Elements** report displays the computers that had broken applications during a specified date range. For each computer, the report lists each occurrence of a broken application and identifies its broken element.

Updating the source paths of Windows Installer applications

You can update the source paths of Windows Installer applications with resilient source paths. The updated source paths point to the package servers that you designate. If an application needs modification or repair, Windows Installer can access the needed installation file from one of these servers.

You can use a policy or a task to perform resilient source path updates of Windows Installer applications on managed computers.

When a Windows Installer application is broken, Windows Installer can repair or modify it, but only if the original installation file is accessible. When Windows Installer tries to modify or repair an application, it uses the application's source path to access the installation file. This source path is based on the application's package code. Without resilient source paths, if the installation file is no longer available, the modification or repair fails. With resilient source paths, Windows Installer can look for the installation file on a set of package servers that you designate.

For example, the software delivery policies and tasks in Software Management Solution typically install packages from a package server. If that package server becomes unavailable, a Windows Installer application that was installed from that server cannot be repaired. To avoid this problem, update the application's source paths to point to additional servers from which the installation file can be accessed.

You can perform resilient source path updates of Windows Installer applications with a policy or a task as follows:

Policy
: Use a policy as your primary means to update the source paths of Windows Installer applications. A policy can update the source paths of existing applications, but also the source paths of the applications that are installed in the future. To include the applications that are not yet installed, schedule the policy to run repeatedly.

  A Source Path Update policy updates all the Windows Installer applications that are installed on the client computer.

Task
: Use a task when you need to update the source path of a specific application and the update needs to be done immediately. For example, a Windows Installer repair might fail because the server that distributed the application is out of service. You can create a task to update the source path for that application.

  A Source Path Update task can update a specific application or all the Windows Installer applications that are installed on the client computer.

The Software Management Solution plug-in must be installed on the client computers for you to update source paths.

Table 5-7 Process for updating source paths for Windows Installer applications

Step	Action	Description
Step 1	Configure a policy or create a task to update the source paths of Windows Installer applications.	A Source Path Update policy or task adds resilient source paths to Windows Installer applications on managed computers. See "Configuring a Source Path Update policy" on page 146. You can also create a Source Path Update task from a software resource in the Software Catalog. If you create the task from a software resource, you select the computers that the task applies to and the task runs immediately.
Step 2	(Optional, task only) Configure the task settings.	Every task inherits the default settings that control how it runs. You can override the default settings for a particular task. You cannot change the settings for a Source Path Update policy.

Table 5-7 Process for updating source paths for Windows Installer applications *(continued)*

Step	Action	Description
Step 3	(Task only) Schedule the task and select the delivery destinations.	The options for scheduling the task are as follows: ■ Run the task now. This option runs the task as soon as possible, unless it must wait for a maintenance window. ■ Schedule the task to run at a specific time. This additional step is not necessary for the policy because you schedule it as part of its configuration.
Step 4	View the **Software Resources - Inaccessible Source Paths** report.	This report lists the computers that had Windows Installer applications with inaccessible source paths during the most recent scan. Use this report to identify the changes that you need to make to resolve inaccessible source path problems. This report is one of the Application Management reports listed under the Software reports.

Configuring a Source Path Update policy

To update the source paths of Windows Installer applications with resilient source paths, you need to configure a Source Path Update policy. Configuring the policy is a step in the process of updating the source paths of Windows Installer applications.

See "Updating the source paths of Windows Installer applications" on page 144.

After you configure the policy, it runs as scheduled on the specified computers or for the specified users. If you schedule the policy to repeat, it can continue to check and update the source paths.

To configure a Source Path Update policy

1. In the Symantec Management Console, on the **Settings** menu, click **All Settings**.
2. In the left pane, expand **Software > Application Management > Windows**, and then click **Source Path Update**.

3 In the right pane, on the **Source Path Update** page, under **Settings**, specify the package servers to use as follows:

First Server to Use	Lets you select the first server to use as a source path. You can click **Any Server** or you can select a specific server from the list. The package server that you select must be accessible to the computers that are specified in the policy. To optimize bandwidth, select specific package servers to serve as the source paths for Windows Installer applications. Servers between the first and last are used in order of response speed. If you do not select specific package servers, the update begins with the fastest-responding server and works toward the slowest. It then ends with the Notification Server computer.
Last Server to Use	Lets you select the last server to use as a source path. You can click **Any Server** or you can select a specific server from the list. The package server that you select must be accessible to the computers that are specified in the policy.

4 In **Maximum Number of Servers**, type the maximum number of servers to use for the source path update.

5 Under **Schedule**, configure the schedule for the policy.

To run this policy on a recurring basis, under **Schedule**, click **No repeat**, and then, in the **Repeat Schedule** dialog box, choose the repeat interval.

For more information, see the topics about specifying a policy schedule in *Altiris™ IT Management Suite Administration Guide from Symantec™*.

6 Under **Applied to**, choose the computers or users to which the policy applies.

For more information, see the topics about specifying the targets of a policy or task in *Altiris™ IT Management Suite Administration Guide from Symantec™*.

7 Turn on the policy.

At the upper right of the page, click the colored circle, and then click **On**.

8 Click **Save changes**.

Repairing Windows Installer applications

You can proactively identify and repair broken Windows Installer applications on managed computers even before the user encounters a problem. If an application

needs repair, a repair command is sent to the Windows Installer service to initiate self-repair.

You can repair Windows Installer applications on managed computers with a policy or task as follows:

Policy	Use a policy as your primary means to repair Windows Installer applications. A policy not only repairs the applications that are currently broken, but it can also repair any applications that break in the future. To repair current and future applications, schedule the policy to run on a recurring basis. A policy can perform a quick repair or a full repair.
Task	Symantec recommends that you use a task to repair a specific application. For example, if a user reports a broken application, you can create a task to repair that specific application on that user's computer. A task can perform a full repair only.

Note: Windows Installer repair task or policy fail on computers with Cloud-enabled management if the software installation package for a broken Windows Installer application is not available.

See "Repairing Windows Installer applications" on page 147.

The Software Management Solution plug-in must be installed on the client computers for you to perform Windows Installer repairs.

Instead of using a Windows Installer Repair policy or task to repair Windows Installer applications, you can use the remediation feature of Managed Software Delivery. Managed Software Delivery provides more control over the criteria that are used to determine when a repair is needed. Instead of a predefined key path, it uses the metadata that is associated with the software resource, that is defined in the Software Catalog. Managed Software Delivery can also repair multiple software resources with a single policy. A Windows Installer Repair policy or task can repair one application or all applications.

Table 5-8 Process for repairing Windows Installer applications

Step	Action	Description
Step 1	Configure a policy or create a task.	Configure a Windows Installer Repair policy to check and repair Windows Installer applications on a recurring basis. See "Configuring a Windows Installer Repair policy" on page 149. Create a Windows Installer Repair task to repair a specific application.

Table 5-8 Process for repairing Windows Installer applications *(continued)*

Step	Action	Description
Step 2	(Optional, task only) Configure the task settings.	Every task inherits the default settings that control how it runs. You can override the default settings for a particular task. You cannot change the settings for a Windows Installer Repair policy.
Step 3	(Task only) Schedule the task and choose the delivery destinations.	Your options for scheduling the task are as follows: ■ Run the task now. This option runs the task as soon as possible, unless it must wait for a maintenance window. ■ Schedule the task to run at a specific time. This additional step is not necessary for the policy because you schedule it as part of its configuration.
Step 4	View the Application Management reports that identify broken elements.	These reports display the Windows Installer applications that had broken elements during a specified time range. The reports also identify the element that is broken. If an application could not be repaired, the **Software Resources - Current Broken Elements** report displays details about why the repair failed. Use these reports to help you resolve broken Windows Installer applications. These reports are listed under the **Software** reports.

Configuring a Windows Installer Repair policy

To repair Windows Installer applications on managed computers, configure a Windows Installer Repair policy. Symantec recommends that you use a policy to check and repair Windows Installer applications on a recurring basis. This is a step in the process for repairing Windows Installer applications.

See "Repairing Windows Installer applications" on page 147.

After you configure the policy, it runs as scheduled on the specified computers or for the specified users. Whenever the policy discovers a broken application, it initiates a repair. If you schedule the policy to repeat, it can continue to check and repair the applications.

You can clone a Windows Installer Repair policy to create policies with different schedules for different computers. To do that, right-click a policy, and the click **Clone**.

To configure a Windows Installer Repair policy

1. In the Symantec Management Console, on the **Settings** menu, click **All Settings**.
2. In the left pane, expand **Software > Application Management > Windows**, and then click one of the following options:

   - **Windows Installer Full Repair**

Type of scan	Runs a Quick Scan, like the quick repair, and then runs a deep scan. The deep scan identifies Windows Installer applications and verifies that all of the component's resources are installed correctly. If any element of a component is not installed correctly, the policy or the task repairs that component and reports the results.
Scan time and resources	A Windows Installer Full Repair takes more time and resources than a Windows Installer Quick Repair.
What it discovers	A full repair discovers every Windows Installer application that needs repair while a quick repair might not.
Method for performing the repair	Use a policy or a task.

   - **Windows Installer Quick Repair**

Type of scan	Runs a Quick Scan that identifies Windows Installer applications and verifies that each component's key path is installed correctly. If the component's key path is not installed correctly, the policy tries to repair the component and reports the results. For example, if the Microsoft Word key path file, winword.exe, is not installed in the correct path, the policy tries to repair Word.
Scan time and resources	A Windows Installer Quick Repair takes less time and fewer resources than a Windows Installer Full Repair.
What it discovers	A quick repair discovers only broken or missing key paths. If a component has other missing or broken files, a quick repair might not repair them.
Method for performing the repair	Use a policy.

3 In the right pane, under **Schedule**, on the toolbar, click **Add schedule**, and then specify the schedule for the policy.

To run this policy on a recurring basis, under **Schedule**, click **No repeat** and then, in the **Repeat Schedule** dialog box, select the repeat interval.

For more information, see the topics about specifying a policy schedule in *Altiris™ IT Management Suite Administration Guide from Symantec™*.

4 Under **Applied to**, specify the computers or users to which the policy applies.

For more information, see the topics about applying a policy to targets, computers, resources, and users in *Altiris™ IT Management Suite Administration Guide from Symantec™*.

5 Turn on the policy.

At the upper right of the page, click the colored circle, and then click **On**.

6 Click **Save changes**.

About software virtualization

Software virtualization lets you create virtual software layers. These layers consist of one or more Windows-based applications or sets of data. A virtual software layer contains all the files and registry settings of the application or the set of data.

Software virtualization requires a licensed version of the Symantec Workspace Virtualization Agent to be installed on the client computers.

See “Installing the Symantec Workspace Virtualization Agent ” on page 152.

When you install a virtual software layer on a computer, the contents of the layer are placed in a protected folder on the hard drive. This protected folder is referred to as the redirection area. The files and registry settings of a layer are placed in subfolders in the redirection area. When you activate a layer on a computer, its contents are layered over the base file system and registry. The contents of the layer appear where they would be if they were installed with a normal installation.

For example, if you install a virtual software layer for Firefox, its files are placed in a subdirectory of C:\fslrdr. After you activate the layer for Firefox, the filter driver displays the files for Firefox in C:\Program Files.

To accomplish this virtualization process, software virtualization uses a file system filter driver. This filter driver intercepts requests to the file system and the registry, and then redirects the requests to the active layer. The filter driver aggregates the real file system and the virtual file system into one view for the user. This filter driver is the main component of the Symantec Workspace Virtualization Agent.

Because software virtualization uses redirection, it can maintain discrete settings and file versions for different applications on a single computer. When you use software virtualization, a required version of a file is never overwritten, and the problem of conflicting DLL files is eliminated.

See "Managing virtual applications" on page 153.

Installing the Symantec Workspace Virtualization Agent

(Windows only)

If you plan to use software virtualization to manage Windows-based software on client computers, install the Symantec Workspace Virtualization Agent on those computers.

See "Managing virtual applications" on page 153.

The Symantec Workspace Virtualization Agent requires that the Software Management Solution plug-in is installed on the client computers.

To install the Symantec Workspace Virtualization Agent

1. In the Symantec Management Console, on the **Settings** menu, click **Agents/Plug-ins > All Agents/Plug-ins**.
2. In the left pane, expand **Software > Software Management > Workspace Virtualization**, and then click **Install SWV agents**.
3. On the **Install SWV agents** page, on the **Software** tab, click **Advanced options**.
4. In the **Advanced options** dialog box, on the **Results-based actions** tab, and in the **Action** drop-down list select **Restart computer**.

   Without this step, the installation process performs silently, and you have to manually restart the computer to finish the installation. Note that a computer restart is required before the Symantec Workspace Virtualization Agent operates properly.
5. In the **Applied to** section, on the toolbar, click **Apply to**, and then choose where to install the Symantec Workspace Virtualization agent.
6. In the **Schedule** section, configure the policy schedule.
7. At the upper right of the page, click the colored circle, and then click **On**.
8. Click **Save changes**.

Managing virtual applications

You can use software virtualization to facilitate the management of most Windows-based software on client computers.

See "About software virtualization" on page 151.

Software virtualization requires a licensed version of the Symantec Workspace Virtualization Agent to be installed on the client computers.

See "Installing the Symantec Workspace Virtualization Agent " on page 152.

Table 5-9 Process for managing virtual applications

Step	Action	Description
Step 1	Virtualize the software.	You can perform the virtualization during installation. You can also use the following options for virtualizing software: ■ Repackage an application into a portable virtual software layer. ■ Import an existing VSA or XPF file into the Software Catalog to create a software resource.
Step 2	Install the software into a virtual software layer.	You can install the software into a virtual layer on the client computer at the same time that you virtualize the software. See "Virtualizing software during installation" on page 153. You also can use any delivery method to install a VSA or XPF file as a new layer and activate it on the client computer. See "Methods for installing and managing virtual software" on page 155.
Step 3	Manage the software that is installed in virtual software layers.	You can create a policy or task that executes a command line for a specific virtual software layer. When the layer command line runs on a managed computer, it performs an action on the layer. For example, if a virtual application is broken, you can create a task that executes a command line to reset the application's layer. The application is quickly restored to its original installed state. See "Methods for installing and managing virtual software" on page 155.
Step 4	View the Virtualized Software Resources reports.	You can use the reports to monitor the state of virtual applications. These reports are listed under the **Software** reports.

Virtualizing software during installation

(Windows only)

When you deliver Windows-based software with a Managed Software Delivery policy, you can choose to virtualize the software when it is installed. You should virtualize software if it conflicts with other software that could be installed on the same computer. When you virtualize software, you avoid conflicts between that application and other applications.

When you choose to virtualize software during installation, the Managed Software Delivery policy installs the software as follows:

If the Symantec Workspace Virtualization Agent is installed on the client computer	The policy performs the following actions: ■ Deactivates any active layers that are on the client computer. ■ Installs the software into a new layer. You can specify the layer name in the Managed Software Delivery policy. If you do not provide a layer name, the layer name defaults to the installation file name plus the command-line name. ■ Reactivates any layers that it deactivated.
If the Symantec Workspace Virtualization Agent is not installed on the client computer	The policy installs the software normally.

See “Managing virtual applications” on page 153.

If a virtual application is reset, it is possible to lose the data that the application creates or modifies. Before you use virtual applications, make sure that you understand how to prevent the loss of application data.

The application data is not saved in the application’s layer in the following situations:

- When the data is excluded with an exclude entry.
  An exclude entry excludes files from a layer and saves them in the base file system instead.
- When the data is saved in a data layer.
  You can create and deploy data layers to capture application data. When a data layer captures data from a virtual application, it is excluded from the application’s layer.
- When the data is not saved locally.
  For example, if a virtual application creates data and the data is saved on a network share, the data is excluded from the application’s layer.

See “About software virtualization” on page 151.

To virtualize software during installation

1. In the Symantec Management Console, create a Managed Software Delivery policy for the software to be virtualized.

   You can either use a Managed Software Delivery wizard, or create the policy manually.

2. On the policy page, on the **Policy settings** tab, under **Software distribution options**, or on the **Select software resource** page in the wizard, check **Install this policy's software into a virtual software layer**.

   Depending on how you create the policy, this check box appears in one of the following places:

   - In the Managed Software Delivery wizard, this check box appears on the **Select software resource** page.
     In the wizard, if the software resource has any defined conflicts with other software resources, those conflicts are listed with this option. Conflict associations between software resources are defined in the Software Catalog.
   - On the policy's edit page, this check box appears in the **Policy/Rules Actions** section, under **Software distribution options** on the **Policy settings** tab.

3. Configure the policy schedule and application settings according to your needs.

   See "Performing an advanced software delivery" on page 138.

4. At the upper right of the page, click the colored circle, and then click **On**.
5. Click **Save changes**.

Methods for installing and managing virtual software

(Windows only)

You can use any delivery task or policy to install software into a virtual layer on a client computer. You can use the same methods to manage the layer after it is installed.

The task or policy installs and manages the layer by running a command line that performs actions on the layer.

The methods for installing and managing virtual software, are as follows:

Table 5-10 Methods for installing and managing virtual software

Method	Description
Software Virtualization task	Lets you install a virtual software archive (VSA) or extensible package format (XPF) file to a managed computer and create a new virtual software layer. It also lets you manage any virtual software layer regardless of how the layer was created. Each action, including the installation, requires a separate task. You can also add a Software Virtualization task to a job or a Managed Software Delivery policy to perform more complex management tasks. See "Installing and managing a virtual software layer with a Software Virtualization task" on page 156.
Quick Delivery task Package Delivery task	Lets you install a virtual software archive (VSA) or extensible package format (XPF) file to a managed computer and create a new virtual software layer. It also lets you manage a virtual software layer that was created by installing a virtual software archive file. Each action, including the installation, requires a separate task. You can also create a Quick Delivery task or a Package Delivery task and add it to a Managed Software Delivery policy. See "Installing and managing a virtual software layer with a Quick Delivery or Package Delivery task" on page 158.
Managed Software Delivery policy	Lets you perform more complex management tasks. A Managed Software Delivery policy can create and manage new virtual software layers, and it can also manage existing layers. See "Installing and managing a virtual software layer with a Managed Software Delivery policy" on page 159. You can manage multiple virtual software layers at the same time. For example, you can create a policy that installs a new version of an application into a layer, and then deactivates the earlier version. To do this, you can add multiple Software Virtualization tasks, Quick Delivery tasks, or Package Delivery tasks to a Managed Software Delivery policy. If you need to manage a single virtual software layer, we recommend that you use one of the other methods.

Installing and managing a virtual software layer with a Software Virtualization task

(Windows only)

You can create a Software Virtualization task to deliver and install a virtual software archive (VSA) or extensible package format (XPF) file on managed computers. You

can also use a Software Virtualization task to manage any virtual software layer regardless of how the layer was created.

Note: If you want to create a Software Virtualization Command task that imports a VSA file or an XPF file, you must specify a layer name. When you specify a different layer name, the Software Virtualization import task fails. A workaround is to find out the layer name that the VSA file or XPF file contains. Once you find the name, you can type it in the **Create new task** dialog box, in the **Layer name** box.

A Software Virtualization task contains a command line for the specified virtual software layer. When the task runs on a client computer, it executes the command line that performs an action on the layer. Each action, including the installation, requires a separate task.

Table 5-11 Process for managing a virtual software layer with a Software Virtualization task

Step	Action	Description
Step 1	Create a Software Virtualization task.	When you create a task, you can choose the command to perform, and the layer on which to perform the command. If you install (import) a layer, you must select a VSA or an XPF file. If you perform any other command, you can specify any existing layer.
Step 2	(Optional) Configure the task settings.	Every task inherits the default settings that control how the task runs. You can override the default settings for a particular task.
Step 3	Schedule the task and choose the delivery destinations.	Define the schedule and the delivery destinations every time you run the task. Your options for scheduling the task are as follows: ■ Run the task now. This option runs the task as soon as possible, unless it must wait for a maintenance window. ■ Schedule the task to run at a specific time.
Step 4	View the **Virtualized Software Resources** reports.	You can use the reports to monitor the state of virtual applications. These reports are listed under the **Software** reports.

See "Managing virtual applications" on page 153.

Installing and managing a virtual software layer with a Quick Delivery or Package Delivery task

(Windows only)

You can create a Quick Delivery or Package Delivery task to deliver and install a virtual software archive (VSA) or an extensible package file (XPF) on managed computers. You can also use these tasks to manage a virtual software layer that was created by installing a virtual software archive file. If the software was virtualized during a Managed Software Delivery installation, you must use a Software Virtualization task to manage the layer.

See "Installing and managing a virtual software layer with a Software Virtualization task" on page 156.

A Quick Delivery or Package Delivery task contains a command line for the specified VSA or XPF file. When the task runs on a client computer, it executes the command line that performs an action on the layer. Each action, including the installation, requires a separate task.

Table 5-12 Process for installing and managing a virtual software layer with a Quick Delivery or Package Delivery task

Step	Action	Description
Step 1	Create a Quick Delivery task or a Package Delivery task.	The options for creating the task are as follows: ■ Use the **Quick Delivery** wizard. ■ Create a Quick Delivery task manually. ■ Create a Package Delivery task.
Step 2	On the task page, specify the software to install or manage.	Select the software resource that represents the VSA or XPF file to install or manage. If you plan to manage an existing layer, select the software resource that contains the VSAor XPF file that was installed to create the layer. In a Package Delivery task, you can also specify a virtual package that is not assigned to a software resource.
Step 3	On the task, page specify the action to perform.	Select a command line that specifies the action to perform. For example, you can install (import) the layer or you can deactivate an existing layer. In a Package Delivery task, if you selected a VSA or XPF file that does not have predefined command lines, you can type a valid command line.
Step 4	(Optional) Configure the task settings.	Every task inherits the default settings that control how the task runs. You can override the default settings for a particular task.

Table 5-12 Process for installing and managing a virtual software layer with a Quick Delivery or Package Delivery task *(continued)*

Step	Action	Description
Step 5	Schedule the task, and choose the delivery destinations.	Define the schedule and the delivery destinations every time you run the task. Your options for scheduling the task are as follows: ■ Run the task now. This option runs the task as soon as possible, unless it must wait for a maintenance window. ■ Schedule the task to run at a specific time.
Step 6	View the **Virtualized Software Resources** reports.	You can use the reports to monitor the state of virtual applications. These reports are listed under the **Software** reports.

See "Managing virtual applications" on page 153.

Installing and managing a virtual software layer with a Managed Software Delivery policy

(Windows only)

You can create Managed Software Delivery policies to create and manage new virtual software layers or manage existing layers on client computers.

A Managed Software Delivery policy lets you perform complex layer management tasks.

For example, you can create a Managed Software Delivery policy that manages virtual software layers as follows:

- Installs a new version of an application into a virtual software layer, and then deactivates or deletes the earlier version.
- Deactivates one version of an application and activates another version.

If you need to manage a single virtual software layer, use a Software Virtualization task, a Quick Delivery task, or a Package Delivery task.

See "Methods for installing and managing virtual software" on page 155.

The process for managing virtual software layers with a Managed Software Delivery policy is as follows:

Table 5-13 Process for managing virtual software layers with a Managed Software Delivery policy

Step	Action
Step 1	Create one or more Software Virtualization tasks, Quick Delivery tasks, or Package Delivery tasks that manage virtual software layers. See "Installing and managing a virtual software layer with a Software Virtualization task" on page 156. See "Installing and managing a virtual software layer with a Quick Delivery or Package Delivery task" on page 158.
Step 2	Create a Managed Software Delivery policy that manages a virtual software layer in one of the following ways: ■ Installs a software resource into a virtual software layer. ■ Manages a virtual software layer that was created by installing a virtual software archive (VSA) or extensible package format (XPF) file.
Step 3	Add the Software Virtualization tasks, Quick Delivery tasks, or Package Delivery tasks to the Managed Software Delivery policy.

Chapter 6

Virtualization of machines

This chapter includes the following topics:

About Virtual Machine Management

Virtual Machine Management is included in Altiris Server Management Suite from Symantec and should already be installed and deployed on your network. Virtual Machine Management lets you perform the virtualization process on your network. Virtualization is a technology that lets you make optimum use of the hardware resources of your organization. You can create various virtual server environments on a single physical server. Each virtual environment is isolated and functions independently from the physical server and from the other virtual environments.

Virtualization enhances the efficiency and productivity of the hardware resources and helps to reduce administrative costs.

The features of the Virtual Machine Management component let you get information from your virtualization infrastructure and bring it to your Server Management Suite environment. From there, this information can be consumed in the context of the broader systems management landscape. The pervasiveness of virtualization has made this a necessity as it becomes increasingly impractical to properly manage a server environment without intimate knowledge of the virtualization stack that is present and the ability to access key virtualization operations. The following three scenarios illustrate this critical need:

Scenario	Description
Host/VM ratio	Performing a traditional management operation, such as patch and virus scans on highly dense VM environments, produces unacceptable performance degradation. Using the knowledge of host/guest relationship in systems management policies enables intelligent, no-impact maintenance to be performed on those environments.
VM cloning	The bare-metal portion of server builds has been replaced by VM provisioning. Administrators need access to VM creation and cloning capabilities from within their systems management console to preserve their fine-tuned and highly customized automated build processes. A complete set of VM management options enables them to find the right balance between VM template proliferation and server build customization needs.
Host/VM resource consumption	Overall system performance is exponentially more sensitive to resource utilization in virtual environments. To aggravate matters, the hosting of increasing numbers of VMs on a single physical server means that glitches to a single operating environment can disrupt thousands of users. Having access in the systems management console for information on key virtualization performance indicators enables systems administrators to take a holistic approach to preventing and remediating critical system conditions.

Virtual Machine Management supports several guest operating systems. The Hyper-V Integration Services and VMware Tools are available for many of these guest operating systems. The **Shut Down** and **Restart** tasks are supported in the guest operating systems that support Hyper-V Integration Services and VMware Tools

About server virtualization

Server virtualization lets you divide a single physical server into multiple virtual environments. The virtual machines share the hardware resources of the physical server. The physical server is called the host and the virtual machine is called the guest.

The virtual machines behave like physical computers. Virtual machine shares the hardware resources of the host server. Each virtual machine also is independent and unaware of the other virtual machines that run on the same physical server.

In Virtual Machine Management, Hypervisor serves as a platform for the operating system of the virtual server. Currently, Virtual Machine Management supports the following Hypervisors:

- Hyper-V

- VMware

These platforms support the virtualization features, which are provided in the Virtual Machine Management component.

Virtual Machine Management component currently supports the following Hyper-V Hypervisors:

- Hyper-V (Win 2K8 R2 enterprise)
- Hyper-V (Win 2K8 R2 SP1)
- Hyper-V (Windows Server 2012)
- Hyper-V (Windows Server 2012 R2)

Virtual Machine Management component also supports VMware vCenter to centrally administer multiple ESX or ESXi hosts and virtual machines in a complex virtual environment. vCenter lets you manage virtual machines on ESX servers, which are discovered using vCenter credentials or managed by vCenter. vCenter lets you streamline all the virtual machine management tasks to have a better control over the virtual environment.

If ESX servers are managed and discovered through a vCenter then you can perform all the virtual machine management tasks except the **Create Virtual Disk** and **Delete Virtual Disk**. In case of the **Create Virtual Disk** and **Delete Virtual Disk** tasks, the credentials (user name and password) for vCenter and ESX server must be same for the successful execution of the task.

Virtual Machine Management component currently supports the following vCenter versions:

- vCenter 5.0
- vCenter 5.1
- vCenter 5.5
- vCenter 6.0

These vCenters can be used to manage ESXi 5.0, ESXi 5.1, ESXi 5.5, and ESXi 6.0.

See “Adding and managing vCenters or host servers” on page 163.

Adding and managing vCenters or host servers

In a large enterprise, Virtual Machine Management lets you gain better efficiency and productivity of the hardware resources by managing a virtual environment that is built on multiple hypervisors. It consumes the features available in VMware and

HyperV hypervisors and provides a common interface to the user to use the features in the context of the broader systems management landscape.

See "About server virtualization" on page 162.

To add and manage vCenters or host servers to Virtual Machine Management, you must perform the following tasks:

Table 6-1 Process for adding and managing vCenters or host servers

Step	Action	Description
Step 1	Discover and add a single or multiple vCenter or host servers.	Do one of the following depending on the way you want to add the vCenter or host server: ■ You can specify IP address of a single vCenter or host and quickly discover and add it to the network. See "Discovering and adding a single vCenter or host" on page 167. ■ You can discover multiple hosts and their virtual machines that are available in the network. The discovery data is added into the Configuration Management Database (CMDB). See "Discovering and adding multiple vCenter or hosts " on page 168.

Table 6-1 Process for adding and managing vCenters or host servers *(continued)*

Step	Action	Description
Step 2	Install the Virtual Machine Management Task Server Plug-in on the task server.	The Virtual Machine Management Task Server Plug-in lets you run the management tasks on your hosts and their virtual machines. The Virtual Machine Management Task Server Plug-in install policy is enabled by default. It installs the Virtual Machine Management Task Server Plug-in on the task server. You must install the Credential Manager (CM) and Pluggable Protocols Agents (PPA) Package on the remote task server to work with Virtual Machine Management. See "Installing the Virtual Machine Management Task Server Plug-in" on page 170.
Step 3	Collect the inventory on each hosts.	After you discover the Hyper-V and VMware host servers on your network, you can gather inventory of these servers and their virtual environments. See "Gathering inventory on the host" on page 171.

Table 6-1 Process for adding and managing vCenters or host servers *(continued)*

Step	Action	Description
Step 4	Execute the host level tasks on host servers.	After you gather the inventory on the Hyper-V and VMware host servers on your network, you can perform all the host level tasks. Virtual Machine Management facilitates you to perform following host level tasks: ■ Create Virtual Machine See "Creating a virtual machine on a host" on page 173. ■ Create Virtual Disk See "Creating a virtual disk on a host" on page 180. ■ Create Virtual Network See "Creating a virtual network on a host" on page 182. ■ Run Inventory See "Gathering inventory on the host" on page 171.
Step 5 (optional)	Execute the template level task on the existing template files, which are created on a host.	If you want to create a new virtual machine using the existing template files, which are created on a host then perform the template level task. The new virtual machine is created based on the virtual hardware, installed software, and other properties that are configured for the template.

Table 6-1 Process for adding and managing vCenters or host servers *(continued)*

Step	Action	Description
Step 6	Execute the guest level tasks on the guest machines that are created on the host servers	Once your guest machines are up and running, you can perform all the guest level tasks. Virtual Machine Management facilitates you to perform following guest level tasks: ■ Start or Stop a Virtual Machine ■ Suspend or Resume a Virtual Machine ■ Shutdown or Restart a Virtual Machine ■ Create a Snapshot See "Creating a snapshot " on page 184. ■ Revert a Snapshot See "Reverting a snapshot" on page 186. ■ Delete a Snapshot See "Deleting a snapshot" on page 187.

See "Permissions that Virtual Machine Management requires" on page 188.

Discovering and adding a single vCenter or host

The **Add Host** feature lets you find and add a specific host or vCenter to your network by only specifying its IP address. In this case, the network discovery task is run internally.

For better network discovery results, it is recommended to assign unique name and IP address to the virtual machines and templates, which are associated with the same Host.

The discovery task uses the default connection profile to discover the host or vCenter. So, before you discover and add a host or vCenter, ensure that the vCenter or Host credential is present and enabled for the respective protocol (WMI protocol for Hyper-V servers, and VMware protocol for ESX servers) in the default connection profile. When the host or vCenter is found, its data is added to the Configuration

Management Database (CMDB). Discovery ensures the right protocol and credential associations are made for future inventory operations.

See "Adding and managing vCenters or host servers" on page 163.

After a host or vCenter is added, you can view its data on the **Virtual Machine Management** home page. You can also run the Virtual Machine Management tasks on the host.

To discover and add a single host

1. In the Symantec Management Console, on the **Home** menu, click **Virtual Machine Management**.
2. In the left pane, click **Actions** > **Add Host**.
3. In the dialog box, type the IP address of the host or vCenter and click **OK**.

See "Permissions that Virtual Machine Management requires" on page 188.

Discovering and adding multiple vCenter or hosts

Before you can perform the Virtual Machine Management operations, you must discover the hosts or vCenters and associated virtual machines, and then gather inventory on each of the hosts.

For better network discovery results, it is recommended to assign unique names and IP addresses to the virtual machines and templates, which are associated with the same Host.

You can discover the virtual machines separately with the Network Discovery wizard on **Home > Discovery and Inventory > Network Discovery** or from **Manage > Jobs and Tasks > Discovery and Inventory**, but for VMM to work properly you must discover VMs using a host or vCenter credentials. Discovery ensures the right protocol and credential associations are made for future inventory operations.

After the hosts and their virtual machines are discovered, accordingly corresponding resources are created in the Configuration Management Database (CMDB). The **Virtual Machine Management** home page displays the hosts and their virtual machines that are available on your network.

Each time you add a host, vCenter or a virtual machine, you must launch the network discovery wizard to update the discovery data. You can also set up a recurring Network Discovery task by using a custom connection profile. You can choose **Discover Virtual managers VMware and HyperV** to target the new hosts, vCenters, and virtual machines in your environment.

For more information, see the topics about network discovery, connection profiles, and scheduling tasks in the *Symantec Management Platform User Guide*.

To discover the hosts

1. In the Symantec Management Console, on the **Home** menu, click **Virtual Machine Management**.
2. In the left pane, click **Actions** > **Getting Started**.
3. In the **Getting Started** dialog box, click **Launch Network Discovery Wizard**.
4. In the network discovery wizard, on the **Choose method of device discovery** page, specify a discovery method and then click **Next**.

   For more information, see the topic about methods for discovering network devices in the *Symantec Management Platform User Guide*.
5. On the **Enter network IP Ranges** page, specify the portions of the network to discover and then click **Next**.

   For more information, see the topic about selecting network ranges to discover in the *Symantec Management Platform User Guide*.
6. On the **Select device communication profile** page, select a connection profile.
7. To specify the VMware or WMI credentials, click the **Edit** symbol.

   The credentials that you specify, are automatically used for all other tasks that require credentials.

   Make sure that the VMware protocol is always turned on for vCenter and ESX servers, and WMI protocol is turned on for Hyper-V servers.
8. In the **Define Group Settings** dialog box, click **OK**.
9. Click **Next**.
10. On the **Enter task name** page, name the task and then click **Next**.
11. On the **Choose when to run the discovery** page, schedule the task and then click **Finish**.

See "Adding and managing vCenters or host servers" on page 163.

See "Permissions that Virtual Machine Management requires" on page 188.

About Virtual Machine Management Task Server Plug-in

For the Virtual Machine Management actions that you want to perform, you first need to create tasks on the host. The Virtual Machine Management Task Server Plug-in lets you manage your hosts and associated virtual machines. The plug-in runs the Virtual Machine Management tasks that you create.

The Virtual Machine Management Task Server Plug-in install policy installs the Virtual Machine Management Task Server Plug-in on the task server. You can

configure the task server on the Notification Server computer or on a separate remote task server. Virtual Machine Management can function out of the box with a single NS server and the Task Server that co-resides there. No additional configuration is needed for most of the small and medium environments.

See "Installing the Virtual Machine Management Task Server Plug-in" on page 170.

In a large enterprise, you can scale Virtual Machine Management by distributing VMM capabilities on additional remote task servers. You must install the Credential Manager (CM) and Pluggable Protocols Agents (PPA) Package on the remote task server to work with Virtual Machine Management. You can execute multiple tasks simultaneously on a task server. Tasks executed on the same resource are executed synchronously.

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

By default, the Virtual Machine Management Task Server Plug-in install policy is roll-out only on the Notification Server computer on which the task service is installed; the plug-in policy does not automatically roll-out on all the task servers. If you want to roll-out the VMM Plug-in install policy on a remote task server then you need to select the respective targets in the install policy and run that. The policy installs the Virtual Machine Management Task Server Plug-in on your task server.

The Virtual Machine Management Task Server Plug-in uses different components to communicate with the hosts. The VMware platform uses the web service and Hyper-V uses the Windows Management Instrumentation (WMI). The Virtual Machine Management Task Server Plug-in remotely connects to the host and runs the tasks that are applied to it.

The Virtual Machine Management Task Server Plug-in acts as a communication channel between the Notification Server computer, task server, and the host. The tasks are created in the Virtual Machine Management and sent to the task server for the Virtual Machine Management Task Server Plug-in. The Virtual Machine Management Task Server Plug-in selects the host where the task is specified to run. After the task runs, the host sends the result to the Virtual Machine Management Task Server Plug-in. The Virtual Machine Management Task Server Plug-in then creates a Notification Server Event (NSE) and sends it to the Notification Server computer. The Notification Server computer stores the event in the Configuration Management Database (CMDB).

Installing the Virtual Machine Management Task Server Plug-in

To perform any Virtual Machine Management tasks, you must install the Virtual Machine Management Task Server Plug-in on your task server.

The Virtual Machine Management Task Server Plug-in install policy is enabled by default. The Virtual Machine Management Task Server Plug-in install policy is roll out automatically only on the Notification Server computer on which the task service installed; the plug-in policy does not automatically roll-out on all the task servers. If you want to roll out the VMM plug-in install policy on a remote task server then you need to select respective targets in install policy and run that. The policy installs the Virtual Machine Management Task Server Plug-in on your task server.

See "About Virtual Machine Management Task Server Plug-in" on page 169.

To install the Virtual Machine Management Task Server Plug-in

1. In the Symantec Management Console, on the **Settings** menu, click **All Settings**.
2. In the left pane, under **Settings**, click **Agents/Plug-ins** > **Virtual Machine Management** > **Virtual Machine Management Task Server Plug-in - Install**.
3. On the **Virtual Machine Management Task Server Plug-in - Install** page, under **Applied to**, specify the target for the policy.

   For more information, see the topics about applying a policy to targets, computers, resources, and users in the *Symantec Management Platform User Guide*.
4. Under **Schedule**, specify a schedule for the policy.

   For more information, see the topics about specifying a policy schedule in the *Symantec Management Platform User Guide*.
5. Turn on the policy.

   At the upper right of the page, click the colored circle, and then click **On**.
6. Click **Save changes**.

See "Adding and managing vCenters or host servers" on page 163.

Gathering inventory on the host

After you discover the VMware vCenter, ESX server and Hyper-V servers on your network, you can gather inventory on these servers. Even though the discovery has been done on a vCenter, the inventory must be explicitly gathered on an ESX server.

See "Adding and managing vCenters or host servers" on page 163.

To gather inventory on the hosts, you must run a Virtual Machine Management Inventory task. The inventory task lets you collect the data about a host and its virtual environment.

For example you can collect information about the host name, IP address, system type, and hardware utilization. You can also collect information about the virtual machines, virtual disks, and the virtual networks that are created on the host.

The **Run Inventory** task is a host level task and can only be executed against a host. On executing an inventory task on a host, all the information about the virtual machines that are associated with the host, is automatically collected. You do not require to run the inventory tasks on the virtual machines as there is no separate inventory task for the virtual machines. If you have performed the **Network Discovery** task using vCenter credentials then you must execute separate inventory task on the host.

For example, if applying the **Network Discovery** task to a specific vCenter returns 10 associated ESX servers, then you must execute separate inventory task on each host to get the full information on the environments.

If the inventory is not gathered on a host then except the **Run Inventory** task, you are not allowed to perform any other host level or guest level tasks such as **Create Virtual Machine**, **Create Virtual Disk**, **Start**, **Stop**, etc. as these tasks are unaccessible from the Virtual Machine Management portal page and through all other access paths like **Actions > Virtual Machine Management > Create VM** (List of Hosts), **Manage > Jobs and Tasks**, or **Manage > All Resources > Asset > Network Resource > Computer**. In these scenarios, you must first execute the **Run Inventory** task on the host and then perform other host level and guest level tasks using the options available on different pages.

You can run the inventory task once or you can set it to run repeatedly and automatically update the inventory data. In Virtual Machine Management, there is a preconfigured inventory task called **VMM inventory**. It is scheduled by default to run at 6:30 P.M. daily on all hypervisors. You can edit or delete the preconfigured inventory task instance. If you want, you can create multiple new instances of the default inventory task through the **New Schedule** option that is provided on the inventory task page, and have different scheduled inventory run on single or multiple hypervisors

For more information, see the topics about how to gather inventory in the *Inventory Solution User Guide*.

To gather inventory on the host

1. In the Symantec Management Console, on the **Home** menu, click **Virtual Machine Management**.
2. In the left pane, do one of the following:
   - Click **Actions** > **Getting Started** and in the **Getting Started** window, click **Run Inventory Task**.

- Click the host, go to the host page on the right pane, under **Actions**, click **Run Inventory**.
- Right-click the host and click **Run Inventory**. All the discovered hosts are displayed in the left pane.

The above option can also be accessed on right-click of the host from **Manage > All Resources > Asset > Network Resource > Computer**.

3 On the inventory task page, under **Task Status**, specify a schedule for the task.

For more information, see the topics about specifying a schedule in the *Symantec Management Platform User Guide*.

To manually create a Virtual Machine Management Inventory task

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

2 In the left pane, under **Jobs and Tasks**, expand **System Jobs and Tasks**, and click **Virtual Machine Management**.

3 Right-click the **Inventory** folder and click **New** > **Task**.

4 In the tasks list, click **Inventory**.

5 On the inventory task page, give the task a name.

6 On the inventory task page, under **Task Status**, specify a schedule for the task.

For more information, see the topics about specifying a schedule in the *Symantec Management Platform User Guide*.

7 If you make changes in the task after you have created it, click **Save changes**.

Creating a virtual machine on a host

Virtual machines are created on a host. You can create the virtual machine with the **Create Virtual Machine** wizard. You can also manually create a task that creates a virtual machine. When you create a virtual machine using a task that is created manually from **Jobs and Tasks**, the virtual network that is associated with the virtual machine can only be of type internal.

You must configure the Deployment Solution job and enable the PXE service to send an automation image to all unknown computers before you provision a virtual machine. This step is optional and required only if you want to deploy an operating system on the virtual machine.

For more information about configuring a Deployment Solution job, setting up the PXE service and creating images, see the *Deployment Solution User Guide*.

Things you should consider before you create a virtual machine and use the OS deployment functionality with the **Create Virtual Machine** wizard:

- Select only the Deployment Solution job that contains the Partition task and Scripted OS installation task.
- Initial Deployment task of the Deployment Solution should not be enabled.
- When you select a network, make sure that it is external only.

To create a virtual machine and use the OS deployment functionality with the Create Virtual Machine wizard

1. In the Symantec Management Console, do one of the following:
   - From the **Actions** menu, select **Virtual Machine Management > Create VM**, and execute steps 3 to 9.
   - From the **Home** menu, click **Virtual Machine Management**, and execute steps 2 to 9.
2. In the left pane, do one of the following:
   - Click the host, go to the host page on the right pane, under **Actions**, click **Create Virtual Machine**.
   - Right-click the host and click **Create VM**.
     The above option can also be accessed on right-click of the host from **All Resources > Asset > Network Resource > Computer**.
3. In the **Create Virtual Machine** wizard, on the **Select Host** page, select the host from the list and then click **Next**. The **Select Host** page is displayed only if you are accessing **Create Virtual Machine** wizard from the **Actions** menu.

4 On the **Virtual Machine Details** page, specify the following virtual machine details and then click **Next**:

Name	Lets you specify a name for the virtual machine.
Description	Lets you specify a description about the virtual machine.
Guest OS	Lets you select a guest operating system.
OS version	Lets you select the appropriate version of the guest operating system. Ensure that you have chosen a correct guest operating system from the available **OS version** list and your host supports the guest operating system that you have selected. You can refer to VMware and Microsoft Hyper-V guest OS list for more information about the supported guest OS.
CPUs	Lets you select or specify the number of CPUs for the virtual machine. The number of CPUs you select depends on the number of logical processors on the host server. The maximum number of logical processors for the ESX server is 8, for the Hyper-V 2008 is 4, and for the Hyper-V 2012 is 8.
ISO path	Lets you select or specify the ISO path. This path is used for installing the guest operating system on the virtual machine. While creating a VM with the Deployment Solution job, it is recommended to leave this field blank.
Memory	Lets you specify the memory for the virtual machine in GB or MB.

5 On the **Select Disk** page, create a new disk or select an existing virtual disk, and then click **Next**.

6 On the **Select Network** page, do one of the following:

- Select **New** to create a new virtual network for the virtual machine. Now, you can enter a **Name** for the new virtual network and select an **Adapter** to which the network is connected.

- Select **Existing network** to use an existing network for creating the virtual machine. In case of VMware hypervisor, the existing network list includes 'Standard' or 'Virtual' switches. It also includes the 'Distributed switch port groups' networks, which are created through vSphere client; not from VMM solution. Currently, only the existing 'Distributed switch port groups' is supported.

In case of ESX hypervisors, while creating an internal or external network, the network name must be unique, whereas if you are using Hyper-V hypervisors, the network name can be duplicate.

7 Click **Next**.

8 On the **Select Datastore and Deployment Job** page, select a datastore and a deployment solution job.

9 Click **Finish**.

After you finish the wizard, a job is created. This job contains a task that creates a virtual machine and one task that schedules an operating system deployment job on it.

To create a virtual machine with the Create Virtual Machine wizard

1 In the Symantec Management Console, do one of the following:

- From the **Actions** menu, select **Virtual Machine Management > Create VM**, and execute steps 3 to 8.
- From the **Home** menu, click **Virtual Machine Management**, and execute steps 2 to 8.

2 In the left pane, do one of the following:

- Click the host, go to the host page on the right pane, under **Actions**, click **Create Virtual Machine**.
- Right-click the host and click **Create VM**.
  The above option can also be accessed on right click of the host from **All Resources > Asset > Network Resource > Computer**.

3 In the **Create Virtual Machine** wizard, on the **Select Host** page, select the host from the list and then click **Next**. The **Select Host** page is displayed only if you are accessing **Create Virtual Machine** wizard from the **Actions** menu.

4 On the **Virtual Machine Details** page, specify the following virtual machine details and then click **Next**:

Name	Lets you specify a name for the virtual machine.
Description	Lets you specify a description about the virtual machine.

Guest OS	Lets you select a guest operating system.
OS version	Lets you select the appropriate version of the guest operating system. Ensure that you have chosen a correct guest operating system from the available **OS version** list and your host supports the guest operating system that you have selected. You can refer to VMware and Microsoft Hyper-V guest OS list for more information about the supported guest OS.
CPUs	Lets you select or specify the number of CPUs for the virtual machine. The number of CPUs you select depends on the number of logical processors on the host server. The maximum number of logical processors for the ESX server is 8, for the Hyper-V 2008 is 4, and for the Hyper-V 2012 is 8.
ISO path	Lets you select or specify the ISO path. This path is used for installing the guest operating system on the virtual machine. For a specific host, the ISO paths are available for selection only if they are under the parent folder or a root folder of the host. In case of Hyper-V ISO files, the ISO paths are available for selection only in following scenarios: ■ ISO files are located under default Hyper-V disk path where .vhd files get saved. ■ ISO files, which are referred or used by existing VMs irrespective of file path location. If ISO files are not available for selection then you can specify the path manually.
Memory	Lets you specify the memory for the virtual machine in GB or MB.

5 On the **Select Disk** page, create a new disk or select a virtual disk and then click **Next**.

6 On the **Select Network** page, create or select a virtual network, and then click **Next**.

7 On the **Select Datastore and Deployment Job** page, select a datastore.

8 Click **Finish**.

After you finish the wizard, a task is created. This task creates a virtual machine with the specified configuration.

To manually create a task that creates a virtual machine

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

2 In the left pane, under **Jobs and Tasks**, expand **System Jobs and Tasks**, and click **Virtual Machine Management**.

3 Right-click the **Create Virtual Machine** folder and click **New** > **Task**.

4 In the tasks list, click **Create Virtual Machine**.

5 Give the task a name.

6 On the **VM Details** tab, specify the following virtual machine details:

Name	Lets you specify a name for the virtual machine.
Description	Lets you specify a description about the virtual machine.
Guest OS	Lets you select a guest operating system.
OS version	Lets you select the appropriate version of the guest operating system. Ensure that you have chosen a correct guest operating system from the available **OS version** list and your host supports the guest operating system that you have selected. You can refer to VMware and Microsoft Hyper-V guest OS list for more information about the supported guest OS.
Memory	Lets you specify the memory for the virtual machine in MB.
CPUs	Lets you specify the number of CPUs for the virtual machine. The number of CPUs depend on the number of logical processors on the host server. The maximum number of logical processors for the ESX server is 8, for the Hyper-V 2008 is 4, and for the Hyper-V 2012 is 8.

7 On the **Disk Details** tab, specify the disk details.

8 On the **Network Details** tab, specify the network details.

Here, the virtual network is created of type internal.

9 Click **OK**.

10 On the create virtual machine task page, under **Task Status**, specify a schedule for the task.

For more information, see the topics about adding a schedule in the *Symantec Management Platform User Guide*.

11 If you make changes in the task after you have created it, click **Save changes**.

Deleting a virtual machine from a host

You can delete a virtual machine from the host.

To delete a virtual machine

1 In the Symantec Management Console, on the **Home** menu, click **Virtual Machine Management**.

2 In the left pane, click the host.

3 On the host page, under **Virtual Machines and Templates**, do one of the following:

- Click the virtual machine and click **Actions** > **Delete VM**.
- Right-click the virtual machine and click **Delete VM**.

4 In the **Delete VM** dialog box, click **OK**.

After you finish the dialog box, a task is created in the **Manage > Jobs and Tasks** menu. This task deletes a virtual machine based on the specified details.

To manually create a task that deletes a virtual machine

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

2 In the left pane, under **Jobs and Tasks**, expand **System Jobs and Tasks**, and click **Virtual Machine Management**.

3 Right-click the **Delete Virtual Machine** folder and click **New > Task**.

4 In the tasks list, click **Delete Virtual Machine**.

5 Give the task a name.

6 On the delete virtual machine task page, under **Task Status**, specify a schedule for the task.

For more information, see the topics about adding a schedule in the *Symantec Management Platform User Guide*.

7 If you make changes in the task after you have created it, click **Save changes**.

See "Creating a virtual machine on a host" on page 173.

Creating a virtual disk on a host

While creating a virtual machine, you need to create or specify a virtual disk for it. The virtual disk is created on a host.

Note: VMware vCenter lets you manage and discover multiple hosts. In this case, for the successful creation of a virtual disk, the credentials for the host and the respective vCenter must be the same.

To create a virtual disk

1 In the Symantec Management Console, on the **Home** menu, click **Virtual Machine Management**.

2 In the left pane, do one of the following:

- Click the host, go to the host page on the right pane, under **Actions**, click **Create Virtual Disk**.
- Right-click the host, and click **Create Disk**.
  The above option can also be accessed on right-click of the host from **All Resources > Asset > Network Resource > Computer**.

3 In the **Create Disk** dialog box, specify the following disk settings:

Name	Lets you specify a name for the virtual disk.
Description	Lets you specify a description about the Virtual disk.
Capacity	Lets you specify the size of the virtual disk in GB or MB.
Datastore	Lets you select a datastore on which you want to create the virtual disk. This field displays data store name, its total storage capacity and total free space in GB. While selecting the datastore, do check the values in the **Capacity (GB)** and **Free Space(GB)** columns. This helps you to choose a correct datastore.

4 Click **OK**.

To manually create a task that creates a virtual disk

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

2 In the left pane, under **Jobs and Tasks**, click **Virtual Machine Management**.

3 Right-click the **Create Disk** folder and click **New** > **Task**.

4 In the tasks list, click **Create Disk**.

5 Give the task a name.

6 In the right pane, under **Software Setting**, specify the disk settings, and click **OK**.

7 On the create disk task page, under **Task Status**, specify a schedule for the task.

For more information, see the topics about adding a schedule in the *Symantec Management Platform User Guide*.

8 If you make changes in the task after you have created it, click **Save changes**.

Deleting a virtual disk from a host

Delete disk task lets you delete a disk on the host. When you delete a disk, it is also removed from the virtual disks list of the host.

Note: Virtual Machine Management component supports VMware vCenter to centrally manage and discover multiple hosts. In this case, for the successful deletion of a virtual disk, the credentials for the host and the respective vCenter must be the same.

To delete a virtual disk

1. In the Symantec Management Console, on the **Home** menu, click **Virtual Machine Management**.
2. In the left pane, click the host.
3. On the host page, under **Virtual Disk**, do one of the following:
   - Click the virtual disk and click **Actions** > **Delete**.
   - Right-click the virtual disk, and click **Delete**.
4. In the **Delete Disk** dialog box, click **OK**.

   After you finish the dialog box, a task is created in the **Manage > Jobs and Tasks** menu. This task deletes the virtual disk based on the specified details.

To manually create a task that deletes a virtual disk

1. In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**.
2. In the left pane, under **Jobs and Tasks**, expand **System Jobs and Tasks**, and click **Virtual Machine Management**.
3. Right-click the **Delete Virtual Disk** folder and click **New > Task**.
4. In the tasks list, click **Delete Virtual Disk**.
5. Give the task a name and specify the virtual disk name.
6. On the delete disk task page, under **Task Status**, specify a schedule for the task.

   For more information, see the topics about adding a schedule in the *Symantec Management Platform User Guide*.

Creating a virtual network on a host

While creating a virtual machine, you need to create or specify a virtual network that lets you connect the virtual machine to the host and to the network for accessing Internet or other computers. The **Create Virtual Network** task lets you create both internal as well as external virtual network from the VMM portal page. Currently, you can create only Standard or Virtual Switches networks.

If you are manually creating a task from **Jobs and Tasks** that creates a virtual network then you can create only internal network.

To create a virtual network

1. In the Symantec Management Console, on the **Home** menu, click **Virtual Machine Management**.
2. In the left pane, do one of the following:
   - Click the host, go to the host page on the right pane, and under **Actions**, click **Create Virtual Network**.
   - Right-click the host and click **Create Network**.
     The above option can also be accessed on right-click of the host from **All Resources > Asset > Network Resource > Computer**.
3. On the **Create Network** page, enter the name of the new virtual network, select the adapter to use for the network, and then click **OK**.

   In the **Adapters** drop-down list, you can see only those adapters (physical NICs), which are connected to the Standard or Virtual switches.

To manually create a task that creates a virtual network

1. In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**.
2. In the left pane, under **Jobs and Tasks**, expand **System Jobs and Tasks**, and click **Virtual Machine Management**.
3. Right-click the **Create Network** folder and click **New** > **Task**.
4. In the tasks list, click **Create Network**.
5. In the right pane, under **Software settings**, specify the network name, and click **OK**.
6. On the create network task page, under **Task Status**, specify a schedule for the task.

   For more information, see the topics about adding a schedule in the *Symantec Management Platform User Guide*.
7. If you make changes in the task after you have created it, click **Save changes**.

Deleting a virtual network from a host

You can delete a virtual network from a host. In case of VMware hypervisor, you can delete only the networks, which are Standard or Virtual switches.

To delete a virtual network

1. In the Symantec Management Console, on the **Home** menu, click **Virtual Machine Management**.
2. In the left pane, click a host.
3. On the host page, under **Virtual Network**, do one of the following:
   - Click the virtual network and click **Actions** > **Delete**.
   - Right-click the virtual network and click **Delete**.
4. In the **Delete virtual network** dialog box, click **OK**.

   After you finish the dialog box, a task is created in the **Manage > Jobs and Tasks** menu. This task deletes the virtual network based on the specified details.

To manually create a task that deletes a virtual network

1. In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**.
2. In the left pane, under **Jobs and Tasks**, expand **System Jobs and Tasks**, and click **Virtual Machine Management**.
3. Right-click the **Delete Virtual Network** folder and click **New > Task**.
4. In the tasks list, click **Delete Virtual Network**.
5. Give the task a name and specify the virtual network name.
6. On the delete network task page, under **Task Status**, specify a schedule for the task.

   For more information, see the topics about adding a schedule in the *Symantec Management Platform User Guide*.

Creating a snapshot

You can take the snapshot of a virtual machine any time. If you change the configurations of the virtual machines frequently, you can take the snapshots of individual configurations and return to them at any time.

To create a snapshot

1. In the Symantec Management Console, on the **Home** menu, click **Virtual Machine Management**.
2. In the left pane, do one of the following:

- Click the virtual machine, go to the virtual machine page on the right pane, and click **Actions > Create Snapshot**.
- Click the virtual machine, go to the **Snapshot details** section of the virtual machine page on the right pane, and click **Actions > Create Snapshot**.
- Right-click the virtual machine, and click **Create Snapshot**.

The above option can also be accessed on right click of the **All Resources > Asset > Network Resource > Computer > Virtual Machine**.

3 In the **Create Snapshot** dialog box, do one of the following:

- Select **Use the default snapshot name** option for creating a snapshot with default settings. By default, this option is selected.
  The name of the default snapshot is assigned in the following format:
  Virtual Machine Name Creation Date Creation Time.
  For example, TestVM 20-Aug-2011 20:30:20 PM.
- Select **Name** to manually enter the **Name** and **Description** of the snapshot.

4 Click **OK**.

A task is created in the **Manage > Jobs and Tasks** menu. This task creates a snapshot with the specified configuration.

5 To make changes to the task, update the configuration and click **Save changes**.

To manually create a task that creates a snapshot

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

2 In the left pane, under **Jobs and Tasks**, expand **System Jobs and Tasks**, and click **Virtual Machine Management**.

3 Right-click the **Create Snapshot** folder and click **New > Task**.

4 In the tasks list, click **Create Snapshot**.

5 Give the task a name and do one of the following:

- Select **Use the default snapshot name** option for creating a snapshot with default settings. By default, this option is selected.
  The name of the default snapshot is assigned in the following format:
  Virtual Machine Name Creation Date Creation Time.
  For example, TestVM 20-Aug-2011 20:30:20 PM.
- Select **Name** to manually enter the **Name** and **Description** of the snapshot.

6 Click **OK**.

7 On the create snapshot task page, under **Task Status**, specify a schedule for the task.

For more information, see the topics about adding a schedule in the *Symantec Management Platform User Guide*.

8 To make changes to the task, update the configuration and click **Save changes**.

Reverting a snapshot

When you take a snapshot of a virtual machine, it saves its current state. Later, if you face problems with the configured virtual machine, you can revert to its previous state. When you revert a snapshot, you lose all the changes that you made after you took the snapshot.

Note: If a virtual machine has multiple snapshots with the same name then on reverting a snapshot, the snapshot with the latest creation date gets reverted.

To revert a snapshot

1 In the Symantec Management Console, on the **Home** menu, click **Virtual Machine Management**.

2 In the left pane, click the virtual machine.

3 On the virtual machine page, under **Snapshot Details**, click **Actions > Revert Snapshot**.

You are prompted to revert the selected snapshot.

4 Click **OK**.

A task is created in the **Manage > Jobs and Tasks** menu. This task reverts a snapshot based on the specified details.

To manually create a task that reverts a snapshot

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

2 In the left pane, under **Jobs and Tasks**, expand **System Jobs and Tasks**, and click **Virtual Machine Management**.

3 Right-click the **Revert Snapshot** folder and click **New > Task**.

4 In the tasks list, click **Revert Snapshot**.

5 Give the task a name and do one of the following:

- Select **Revert the last snapshot** to revert the last snapshot. By default, this option is selected.

- Select **Revert this snapshot** to manually specify the name of the snapshot being reverted.

6 On the revert snapshot task page, under **Task Status**, specify a schedule for the task.

For more information, see the topics about adding a schedule in the *Symantec Management Platform User Guide*.

7 To make changes to the task, update the configuration and click **Savechanges**.

Deleting a snapshot

You can delete a snapshot when the virtual machine is in any mode. When you delete a snapshot, the contents of that snapshot are saved on the virtual disk and the data is not deleted. If you delete a snapshot, you cannot revert to its earlier state. Deleting a snapshot does not affect the current virtual machine state or other snapshots of the virtual machine. The time required for deleting a snapshot depends on the amount of snapshot data stored on the virtual disk.

Note: If a virtual machine has multiple snapshots with the same name then on deleting a snapshot, the snapshot with the latest creation date gets deleted.

To delete a snapshot

1 In the Symantec Management Console, on the **Home** menu, click **Virtual Machine Management**.

2 In the left pane, click the virtual machine.

3 On the virtual machine page, under **Snapshots Details**, click **Actions > Delete Snapshot** .

You are prompted for confirming the deletion of the selected snapshot.

4 Click **OK**.

A task is created in the **Manage > Jobs and Tasks** menu. This task deletes a snapshot based on the specified details.

To manually create a task that deletes a snapshot

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

2 In the left pane, under **Jobs and Tasks**, expand **System Jobs and Tasks**, and click **Virtual Machine Management**.

3 Right-click the **Delete Snapshot** folder and click **New > Task**.

4 In the tasks list, click **Delete Snapshot**.

5 Give the task a name and do one of the following:

- Select **Delete the last snapshot** to delete the last snapshot. By default, this option is selected.
- Select **Delete this snapshot** to manually specify the name of the snapshot being deleted.

6 On the delete snapshot task page, under **Task Status**, specify a schedule for the task.

For more information, see the topics about adding a schedule in the *Symantec Management Platform User Guide*.

7 To make changes to the task, update the configuration and click **Save changes**.

Permissions that Virtual Machine Management requires

For executing different VMM tasks an account or group needs to be given required permissions. You need to perform discovery tasks on a host or vCenter, and run inventory on hosts before you execute different VMM management tasks. Credentials used in the discovery tasks are used to execute various VMM tasks.

Executing VMM tasks on VMware Hypervisor (ESX/ESXi Host)

vCenter server or ESX/ESXi host gives access to the user based on the permissions given to him. When user discovers an ESX/ESXi host directly then permissions given on a host are used for VMM tasks execution, but if user discovers a host using vCenter then permissions given to him on vCenter are used for VMM task execution. Various permissions can be given to a user or group using the vSphere client. User permissions defined on an object take precedence over group permissions. If no user permissions are given then the user is given union of privileges given to the groups, to which user belongs for that object.

For detailed information about this please refer to Managing Users, Groups, Roles, and Permissions topic of the *vShpere Basic System Administration manual*.

You can directly discover a host using host credentials and execute different VMM tasks on it. Authorized users/groups on ESX/ESXi host are directly added to the list and given permissions when ESX/ESXi is installed. An administrator can add different users using User & Groups tab on vSphere client and give him required permission using the Permissions tab. By default, root user has administrative privileges. The vpxuser user is created with administrative privileges when a host is attached to a vCenter.

Table 6-2 Permissions required for executing VMM tasks on an ESX/ESXi host discovered directly

VMM task	Read-only	Administrator
Discovery	x	x
Run Inventory	x	x
Create/Delete VM		x
Create/Delete Disk		x
Create/Delete Network		x
Deploy VM (from template)*		x
Create/Revert/ Delete Snapshot		x
Power Mgmt. (Start, Stop, Suspend, Resume, Shutdown, Restart)		x

Note: The Deploy VM task is supported only on those ESX hosts, which are discovered using vCenter credentials.

You can discover a vCenter and execute VMM tasks on the hosts managed by the vCenter. After discovery, only the hosts for which you have access rights are listed. vCenter uses Windows mechanism for authentication and authorization. An Administrator can give permissions to a domain user or local windows user/group on vCenter to access vCenter infrastructure. Permissions Tab in vSphere client can be used to give necessary permission to a user/group.

Table 6-3 Permissions required for Executing VMM tasks on an ESX/ESXi host discovered using vCenter credentials/managed by vCenter:

VMM task	Read-only	Administrator	Power user	VM user
Discovery	x	x	x	x
Run Inventory	x	x	x	x
Create/Delete VM		x		
Create/Delete Disk		x		

Table 6-3 Permissions required for Executing VMM tasks on an ESX/ESXi host discovered using vCenter credentials/managed by vCenter: *(continued)*

VMM task	Read-only	Administrator	Power user	VM user
Create/Delete Network		x		
Deploy VM (from template)		x		
Create/Revert/ Delete Snapshot		x	x	
Power Mgmt. (Start, Stop, Suspend, Resume, Shutdown, Restart)		x	x	x

These are some default roles available to user. But user does have option to assign other default roles like Resource pool administrator, VMware consolidated backup user, Datastore consumer etc. Also user can create custom roles depending upon need.

Note: Because of current VMware API limitations, the Delete Disk and Create Disks tasks can only be executed using ESX server admin credentials. If your vCenter admin credentials are different than your ESX admin credentials, then you must discover your ESX server directly using its admin credentials to perform the Delete Disk and Create Disk tasks.

Executing VMM tasks on Hyper-V

Hyper-V uses Windows authentication mechanism. A domain user or a local user on windows with administrative privileges to the HyperV server is required to execute VMM tasks.

Table 6-4 Permissions required for Executing VMM tasks on Hyper-V permissions

VMM task	Administrator
Discovery	x
Run Inventory	x

Table 6-4 Permissions required for Executing VMM tasks on Hyper-V permissions *(continued)*

VMM task	Administrator
Create/Delete VM	x
Create/Delete Disk	x
Create/Delete Network	x
Deploy VM (from template)*	N/A
Create/Revert/ Delete Snapshot	x
Power Mgmt. (Start, Stop, Suspend, Resume, Shutdown, Restart)	x

Note: Hyper-V hypervisor does not support the Deploy VM task.

See "Adding and managing vCenters or host servers" on page 163.

Chapter 7

Server Health

This chapter includes the following topics:

About Monitor Solution

Monitor Solution lets you monitor various aspects of computer operating systems, applications, and device, such as events, processes, and performance. It helps you ensure that your servers and your devices function properly, and reduces the costs of server and network monitoring.

Monitor Solution continuously collects and analyzes data that is captured from computers and other devices on your network. When data is captured that meets the specified criteria, alerts can be raised to notify you and actions can be taken.

Monitor Solution lets you do the following:

- Collect detailed data from servers, applications, and network devices to diagnose the health of your environment.

- Collect comprehensive real-time and historical performance data to analyze trends and isolate recurring issues.
- Pinpoint problems, define their cause, and take automated actions to resolve them.

Monitor Solution supports both agent-based and agentless monitoring methods. It runs on the Symantec Management Platform and is a key component of Server Management Suite.

Monitor Plug-in or the Remote Monitoring Server gather the data that you want to monitor. The data is remotely managed from the Symantec Management Console. The Monitor Plug-in and the Remote Monitoring Server receive policies from the Notification Server computer. Monitor policies instruct the plug-in and Remote Monitoring Server of what actions to perform.

About Monitor Pack for Servers

Monitor Pack for Servers provides a number of monitor packs that monitor the health of your servers. Monitor packs contain monitor policies that monitor services and events of the server health, operating system, and applications.

Monitor Pack for Servers contains both agent-based and agentless monitoring policies. Agentless monitor policies let you monitor resources without the Monitor Plug-in.

See "Preparing managed computers for agent-based monitoring" on page 201.

See "About monitor server configuration" on page 195.

You can enable or disable the policies that are included in the monitor packs, or create new policies. Each monitor policy contains rules, metrics, and tasks that let you monitor your resources. Rules and metrics let you define the metric evaluation and metric data that you want to monitor. Tasks let you specify the automated actions that occur when the metric data reaches certain evaluation.

The Monitor Pack for Servers also includes numerous reports that help you analyze the data and tune the performance of your servers.

See "About viewing the monitor data" on page 214.

Table 7-1 Default monitor packs included in the Monitor Pack for Servers

Monitor pack	Description
AIX - Basic	This monitor pack lets you monitor the disk, memory, network, processor, and other aspects of AIX servers.

Table 7-1 Default monitor packs included in the Monitor Pack for Servers *(continued)*

Monitor pack	Description
Linux - Basic	This monitor pack lets you monitor the disk, memory, network, processor, and other aspects of Linux servers.
Linux Server Health	This monitor pack lets you monitor the health and performance of your Linux Servers. This pack is a single policy that you can apply to all your Linux Servers to quickly evaluate the operation system health and performance.
Solaris - Basic	This monitor pack lets you monitor disk, memory, network, processor, and other aspects of Solaris servers.
Windows 2003	This monitor pack lets you monitor the health and performance on the Windows 2003 servers including disk, memory, network, and processor.
Windows 2008	This monitor pack lets you monitor the health and performance on the Windows 2008 servers including disk, memory, network, and processor.
Windows 2012	This monitor pack lets you monitor the health and performance on the Windows 2012 servers including disk, memory, network, and processor.
Windows 2016	This monitor pack lets you monitor the health and performance on the Windows 2016 servers including disk, memory, network, and processor.
Windows Agentless Policy	This agentless monitor pack lets you monitor the availability and performance on the Windows 2003/2008 servers including disk, memory, network, and processor. The agentless monitor policy lets you monitor computers without installing Symantec Management Agent and Monitor Plug-in. Because the Monitor plug-in is not available, fewer aspects of the computers are available to be monitored.
Windows Server Health	This monitor pack lets you monitor the health and performance of your Windows Servers. This pack is a single policy that you can apply to all your Windows Servers to quickly evaluate the operation system health and performance.

Table 7-1 Default monitor packs included in the Monitor Pack for Servers *(continued)*

Monitor pack	Description
MS SQL	This Monitor pack lets you monitor the health and performance of your MS SQL Servers. This pack is a single policy that you can apply to all your MS SQL Servers to quickly evaluate the MS SQL Servers health and performance.

About monitor server configuration

You can configure the monitor server settings to meet your specific needs.

Table 7-2 Process for configuring the monitor server

Step	Action	Description
Step 1	Import a monitor pack.	Monitor packs include monitor policies, metrics, rules, and tasks for monitoring an operating system or application. Monitor packs also contain preconfigured monitor policies with preset thresholds and severities. You can import a monitor pack to monitor computers and devices. See "Importing monitor packs" on page 196.
Step 2	Set up database maintenance.	Monitor Solution collects data from monitor computers and stores it in the database. You can configure the database maintenance settings to define when data is summarized and purged. See "Configuring data purging" on page 196.
Step 3	Configure heartbeat monitoring settings.	Monitor Solution collects heartbeat signals from Monitor Plug-ins. You can configure the server-side heartbeat settings to define how often Monitor Solution checks for heartbeats. Specify the number of failures that are allowed to occur before Monitor Solution sends an alert to the Event Console. See "Configuring the monitor server heartbeat settings" on page 197.

Importing monitor packs

You use monitor packs to monitor different aspects of your computer resources and network to ensure their availability. Monitor packs include monitor policies, metrics, rules, and tasks for monitoring an operating system or application. Monitor packs also contain preconfigured monitor policies with preset thresholds and severities.

You can import monitor packs after the installation of Monitor Solution. Importing monitor packs lets you choose what functionality you want to install on your monitoring server, and when you want to install it.

See "About monitor server configuration" on page 195.

For more information page, see the topic about performing the First Time Setup configuration in the *IT Management Suite Administration Guide*.

To import monitor packs

1. In the Symantec Management Console, on the **Home** menu, click **Monitoring and Alerting**.
2. In the left pane, under **Monitoring and Alerting**, expand **Monitor > Policies**, and then click **Import Monitor Pack**.
3. On the **Import Monitor Pack** page, click the monitor pack that you want to import.
4. On the toolbar, click **Schedule**.
5. In the **Schedule Monitor Pack** dialog box, configure the schedule settings, and then click **OK**.

Configuring data purging

You can set the time when data summarization and purging occurs.

See "About monitor server configuration" on page 195.

To configure data purging

1. In the Symantec Management Console, on the **Home** menu, click **Monitoring and Alerting**.
2. In the left pane, under **Monitoring and Alerting**, expand **Monitor > Settings**, and then click **Monitor Server Settings**.
3. On the **Monitor Server Settings** page, click the **Purge Maintenance** tab.

4 On the **Purge Maintenance** tab, configure the following settings:

Detailed data	How long you want to store detailed numeric performance data before it is purged and summarized into hourly values.
Hourly summaries	How long you want to store hourly summarizations of numeric performance data before it is purged and summarized into daily values. The value that is used is the **Detailed data** value plus the value.
Daily summaries	How long you want to store daily summarizations of numeric performance data before it is purged from the database. The value that is used is the **Detailed data** value plus the **Hourly summaries** value plus the **Daily summaries** value.
String metric data	How long you want to store string data before it is purged from the database.
Process data	How long you want to store process data before it is purged from the database.
NT event data	How long you want to store NT event data before it is purged it from the database.
Command timeout	How much time should be allowed to pass before a purging timeout is declared.
Perform daily purge at	What time of the day the database purging should occur.

5 Click **Save changes**.

Configuring the monitor server heartbeat settings

You can configure the heartbeat settings for the monitor server. These settings control how often the monitor server checks for received heartbeats.

See “About monitor server configuration” on page 195.

To configure the monitor server heartbeat settings

1. In the Symantec Management Console , on the **Home** menu, click **Monitoring and Alerting**.
2. In the left pane, under **Monitoring and Alerting**, expand **Monitor > Settings**, and then click **Monitor Server Settings**.
3. On the **Monitor Server Settings** page, click the **Heartbeat** tab.
4. On the **Heartbeat** tab, configure the settings according to your needs, and then click **Save Changes**.

Downloading custom Monitor packs from the Symantec Connect Community

Symantec Connect is a source for both Symantec monitor packs and custom monitor packs provided by users and third parties. Customers can submit any type of Monitor pack that other customers may find useful. Monitor packs can vary from a single custom rule and metric to complex rules and metrics. You can also submit requests for Monitor packs on Symantec Connect. The product manager usually responds with information on whether this particular pack is in development or planned.

To download custom monitor packs

1. Find the IT Management Suite forum on Symantec Connect at

   http://www.symantec.com/connect/endpoint-management/forums/it-management-suite.
2. Do a search on "Monitor pack".

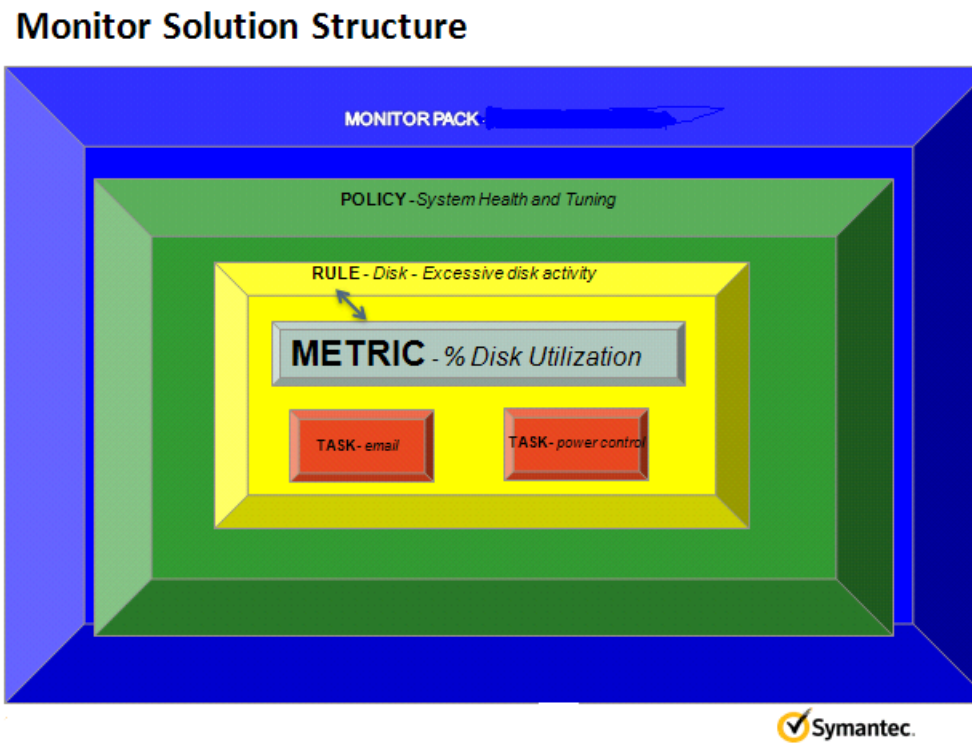
About Monitor Packs, policies, rules, metrics, and tasks

Each monitor pack contains policies, which contain rules and metrics used for collecting data, and which can trigger tasks. The data collected can be used either for trending (historical) or for alerting purposes.

- A policy is a category that describes the area you are monitoring. For example, one of your policies might be a system health and tuning policy.
- A policy is made up of a number of rules. A rule is a threshold definition that determines what conditions must occur in order for the rule to trigger. For example, a policy might contain a rule that measures excessive disk activity.

- Metrics within the rule constantly make values available to the rule evaluator mechanism. They answer the question: Does this value exceed the threshold mechanism defined in the rule?
- If yes, an alert is generated and subsequent tasks are triggered. Tasks let you define what should be done if a particular condition is met. There are two types of tasks: task server-based tasks (server side tasks), and Monitor agent tasks.

Figure 7-1 Monitor Solution structure



About agent-based versus agentless monitoring

Monitor Solution supports the following methods for monitoring servers:

- Agent-based monitoring, using a plug-in that extends the Symantec Management Agent
- Agentless monitoring, using standard protocols like WMI, SNMP and WSMan, and so forth. Monitor Solution Agentless is integrated into site servers and is

referred to as the Remote Monitoring Server (RMS). Agentless monitoring is dependent on the credentials that are used during the Network Discovery phase.

See "Setting up a remote monitoring site server" on page 203.

The general best practice is to use the plug-in where possible as it provides more monitoring capabilities and auto remediation and is less intrusive on the network bandwidth. The following table highlights some of the advantages and disadvantages of each approach.

Table 7-3 Comparison of agent-based and agentless monitoring

Agent-based monitoring	Agentless monitoring
Gathers much more information	Provides more limited monitoring capabilities (those available through the standard protocols).
Provides auto remediation	Is limited to the remediation capabilities through those protocols.
Is less intrusive on the network bandwidth. For example, the agent will send events to the central event console only when the threshold has been triggered. The auto remediation occurs even before the event has reached the central event console and is not dependent on the network.	Is dependent on the network; the metric values must be sent to the site server to be evaluated to determine if a threshold has been triggered.

About agentless monitoring

Agentless monitoring lets you monitor the computers that do not have Monitor Plug-in installed. You monitor these computers with agentless monitoring policies. Because Monitor Plug-in is not available on the computer, fewer aspects of the computer are available to be monitored. You use monitor service on a site server to perform agentless monitoring.

All agentless monitoring policies have a list of resource targets that are monitored. Each monitor service monitors the resources assigned to its server if an agentless monitoring policy targets those resources. Multiple site servers can monitor the same resource that is targeted by an agentless monitor policy. Also, different site servers can monitor different resources that are targeted by the same agentless monitor policy.

You can use agentless monitoring in the following situations:

- You cannot install Symantec Management Agent on the device that you want to monitor.
  For example, devices that have an embedded system.
- You want to monitor the availability of a server.
  In most cases, you need to use agentless monitoring to perform an availability (ping) monitor.

Preparing managed computers for agent-based monitoring

Some monitor tasks can only be performed on managed computers that have Symantec Management Agent installed on them. Remote Monitoring Server provides limited monitoring functionality without Monitor Plug-in. Detailed monitoring requires the installation of both Symantec Management Agent and Monitor Plug-in.

For more information, see the topics about the Symantec Management Agent in the *IT Management Suite Administration Guide*.

To prepare managed computers for monitoring, you must complete the following steps:

Table 7-4 Process for preparing managed computers for agent-based monitoring

Step	Action	Description
Step 1	Discover the computers that you want to manage.	Resource objects are created for the discovered computers in the Configuration Management Database (CMDB). You may have discovered computers when you installed Notification Server or when you added new computers to the network. For more information, see the *IT Management Suite Administration Guide*.
Step 2	Roll out Symantec Management Agent.	You may have performed this step when you installed Notification Server or when you added new computers to the network. For more information, see the *IT Management Suite Administration Guide*. Symantec Management Agent has two versions: one for Windows and one for UNIX, Linux, and Mac.

Table 7-4 Process for preparing managed computers for agent-based monitoring *(continued)*

Step	Action	Description
Step 3	Install Monitor Plug-in.	To monitor computers using agent-based monitoring, you must install Monitor Plug-in on target computers. See "Installing Monitor Plug-in" on page 202.

Installing Monitor Plug-in

To install Monitor Plug-in, you configure a policy that installs it on target computers. You specify a computer or a group of computers on which to install the plug-in, and schedule the policy run. The task is ignored on the computers that already have Monitor Plug-in installed. When the policy is on, it automatically installs Monitor Plug-in on any computers that are added to the network, and are members of the specified group.

See "Preparing managed computers for agent-based monitoring" on page 201.

Before you install Monitor Plug-in, you must install Symantec Management Agent on target computers.

See "Preparing managed computers for agent-based monitoring" on page 201.

Note that Monitor Solution has separate plug-in rollout policies for 32-bit computers and 64-bit computers.

For more information, see the topic about performing the First Time Setup configuration in the *IT Management Suite Administration Guide*.

To install Monitor Plug-in

1. In the Symantec Management Console, on the **Home** menu, click **Monitoring and Alerting**.
2. In the left pane, under **Monitoring and Alerting**, expand **Monitor > Agents/Plug-ins**, expand the folder for the operating system or the application that you want to run the Plug-in on, and then expand the **Rollout** folder, and click the policy name.

   For example, expand **Windows > Rollout**, and then click **Monitor Plug-in for Windows x86 - Install**.
3. On the policy page, turn on the policy.

   At the upper right of the page, click the colored circle, and then click **On**.

4 On the policy page, under **Applied to**, on the toolbar, click **Apply to**, and choose the computers to install the plug-in on.

In most cases, you can use the default group to install the plug-in on all computers that do not have it installed.

5 On the policy page, under **Schedule**, on the toolbar, click **Schedule**, and then configure the schedule of the policy.

6 On the policy page, click **Save changes**.

Setting up a remote monitoring site server

You use monitor service on a site server to perform agentless monitoring. By default, monitor service is installed on the Notification Server computer. You can distribute the monitoring load to other site servers to reduce the load on Notification Server. You can also remove monitor service from the Notification Server computer to further reduce the load on this server.

You can set up as many monitoring site servers as you need.

Monitor service is integrated with the site server infrastructure. This integration lets you specify the resources that each site server monitors.

See "About agentless monitoring" on page 200.

To install monitor service on a remote site server, the server must be running one of the following operating systems:

- Microsoft Windows Server 2008 R2 x64
- Microsoft Windows Server 2012 R2 x64
- Microsoft Windows Server 2016

The **Potential Monitor Servers** filter automatically determines possible site servers. This filter is available on the **Manage** menu, under **Filters**. Agentless monitor policies do not require any special configuration to work with a monitor service on one or more site servers.

Warning: Symantec recommends that you only install monitor service on a computer that is secure and trusted. The security settings of the Notification Server computer must also apply to the site server computer.

Monitor service requires that you install the following on the site server:

- Symantec Management Agent.
- The Pluggable Protocols Architecture (PPA) client computer component.

- The credential manager client computer component.

Table 7-5 Process for setting up a remote monitoring site server

Step	Action	Description
Step 1	Install Symantec Management Agent on the site server.	A remote monitoring server requires Symantec Management Agent to be installed on the site server. For more information, see topics about the Symantec Management Agent in the *IT Management Suite Administration Guide*.
Step 2	Configure connection profiles on Notification Server.	Connection profiles must be configured on Notification Server computer for remote monitoring to work. Configure your connection profiles before you install the Pluggable Protocols Architecture (PPA) client computer component on the site server. For more information, see topics about connection profiles in the *IT Management Suite Administration Guide*.
Step 3	Install the Pluggable Protocols Architecture (PPA) client computer component on the site server.	A remote monitoring server depends on the Pluggable Protocols Architecture (PPA) client computer component to communicate with network devices and computers. When the Pluggable Protocols Architecture (PPA) client computer component is installed, the credential manager client computer component is also installed. See "Installing the Pluggable Protocols Architecture (PPA) client computer component on a site server" on page 205.
Step 4	Add monitor service to one or more site servers.	You can add monitor service to a site server on the site management page. See "Adding monitor service to a site server" on page 206.

Table 7-5 Process for setting up a remote monitoring site server *(continued)*

Step	Action	Description
Step 5	(Optional) Remove monitor service from Notification Server.	You can remove monitor service from Notification Server to reduce the load on this server. See "Removing monitor service from a site server" on page 208.
Step 6	Configure the remote monitoring server settings.	You can configure the remote monitoring server settings. These settings apply to all monitor site servers. See "Configuring remote monitoring server settings" on page 207.
Step 7	(Optional) View the monitor site server reports.	The monitor site server reports let you determine which site servers monitor the resources that your agentless monitor policies target. See "Viewing monitor site server reports" on page 209.

Installing the Pluggable Protocols Architecture (PPA) client computer component on a site server

Pluggable Protocols Architecture (PPA) includes a policy that can remotely install the Pluggable Protocols Architecture (PPA) client computer component on a site server. You must install this component on a site server before you can add monitor service to the site server. When the Pluggable Protocols Architecture (PPA) client computer component is installed, the credential manager client computer component is also installed. The policy that installs the credential manager client computer component configures the agent to automatically import credentials from Notification Server.

See "Setting up a remote monitoring site server" on page 203.

Warning: Symantec recommends that you only install monitor service on a computer that is secure and trusted. The security settings of the Notification Server computer must also apply to the site server computer.

To install the Pluggable Protocols Architecture (PPA) client computer component on a site server

1. In the Symantec Management Console, on the **Settings** menu, click **All Settings**.
2. In the left pane, under **Settings**, expand **Monitoring and Alerting > Protocol Management**, and then click **Install x86 Pluggable Protocols Agent Package** or **Install x64 Pluggable Protocols Agent Package** .
3. In the right pane, do the following:
   - Under **Applied to**, on the toolbar, click **Apply to**, and then configure the policy application.
     For more information, see topics about specifying the targets of a policy in the *IT Management Suite Administration Guide*.
   - Under **Schedule**, on the toolbar, click **Add schedule**, and then configure the policy run settings.
     For more information, see topics about specifying a policy schedule in the *IT Management Suite Administration Guide*.
   - Turn on the policy.
     At the upper right of the page, click the colored circle, and then click **On**.
4. Click **Save changes**.

   After Pluggable Protocols Architecture (PPA) and credential manager are installed, wait until Symantec Management Agent sends inventory information before adding a monitor service. You can confirm that the inventory information was sent on the site server, on the **Symantec Management Agent Settings** tab of the Symantec Management Agent user interface.

Adding monitor service to a site server

You use monitor service on a site server to perform agentless monitoring. Monitor service is installed on the Notification Server computer by default. You can also add monitor service to one or more site servers.

See "About agentless monitoring" on page 200.

Before you can add monitor service to a site server, you need to install the following components on that server:

- Symantec Management Agent.
- Pluggable Protocols Architecture (PPA) client computer component.
- Credential manager client computer component.

Credential manager client computer component is installed when you install Pluggable Protocols Architecture (PPA) client computer component. After Pluggable Protocols Architecture (PPA) and credential manager are installed, wait until the Symantec Management Agent sends inventory information before adding a monitor service.

See "Setting up a remote monitoring site server" on page 203.

Warning: Symantec recommends that you only install monitor service on a computer that is secure and trusted. The security settings of the Notification Server computer must also apply to the site server computer.

When you add monitor service to a site server, it is installed according to the schedule of the installation policy. Monitor service has installation policies for 64-bit and 32-bit computers. To access these installation policies, in the Symantec Management Console, on the **Settings** menu, click **Notification Server > Site Server Settings**, and then, in the right pane, expand the **Monitor Service** section.

To add monitor service to a site server

1. In the Symantec Management Console, on the **Settings** menu, click **Notification Server > Site Server Settings**.
2. In the right pane, under **Detailed Information**, on the toolbar, in the **View** drop-down list, click **Site Servers**.
3. Under **Detailed Information**, in the server list, click the site server, and then, on the toolbar, click the **Edit** symbol.
4. In the **Add/Remove Services** dialog box, check **Monitor Service**, and then click **Next**.

   You cannot check **Monitor Service**, if Pluggable Protocols Architecture (PPA) and credential manager are not installed on the site server.
5. In the **Add/Remove Services** dialog box, click **OK**.
6. To check the status of the installation, on the **Site Management** page, expand **Site Services > Monitor Service**.

   A pie chart displays the site servers that are installed, pending installation, or not installed.

Configuring remote monitoring server settings

You can configure the settings for the remote monitoring servers. You use a remote monitoring server and a monitor service to perform agentless monitoring.

See "About agentless monitoring" on page 200.

The remote monitoring server settings are the global settings that apply to all monitor site servers.

See "Setting up a remote monitoring site server" on page 203.

See "Adding monitor service to a site server" on page 206.

To configure remote monitoring server settings

1. In the Symantec Management Console, on the **Home** menu, click **Monitoring and Alerting**.
2. In the left pane, under **Monitoring and Alerting**, expand **Monitor > Settings**, and then click **Remote Monitoring Server Settings**.
3. In the right pane, under **Plug-in Config Settings**, click the following tabs to configure policy settings:
   - **General**
   - **Performance Tuning**
   - **Data Collection**
4. Turn on the policy.

   At the upper right of the page, click the colored circle, and then click **On**.
5. In the right pane, click **Save changes**.

Removing monitor service from a site server

You use monitor service on a site server to perform agentless monitoring. Monitor service is installed on the Notification Server computer by default. To reduce the load on Notification Server, you can remove monitor service from this server. You can also remove monitor service from any other site server.

See "Setting up a remote monitoring site server" on page 203.

To remove monitor service from a site server

1. In the Symantec Management Console, on the **Settings** menu, click **Notification Server > Site Server Settings**.
2. In the right pane, under **Detailed Information**, on the toolbar, in the **View** drop-down list, click **Site Servers**.
3. Under **Detailed Information**, in the server list, click the site server, and then, on the toolbar, click the **Edit** symbol.
4. In the **Add/Remove Services** dialog box, uncheck **Monitor Service**, and then click **Next**.
5. In the **Add/Remove Services** dialog box, click **OK**.

Viewing monitor site server reports

Monitor service on a site server lets you run agentless monitoring policies to monitor the resources that do not have Symantec Management Agent installed. The monitor site server reports let you determine which site servers monitor the resources that your agentless monitor policies target.

See “About agentless monitoring” on page 200.

The monitor site sever reports are as follows:

Monitored resources by RMS	This report lists the resources that the specified site server monitors.
Resources not monitored by RMS	This report lists the resources that no site server monitors.
RMS by Monitored resources	This report lists the site servers that monitor the specified resource.

To view monitor site server reports

1. In the Symantec Management Console, on the **Reports** menu, click **All Reports**.
2. In the left pane, under **Reports**, expand **Monitoring and Alerting > Monitor > Configuration > Monitor site server**.

Chapter 8

Event Console

This chapter includes the following topics:

About alerts

Alerts are the status messages that contain information about device or network health. Status messages are generated using standard monitoring protocols, such as SNMP.

Each status message that is received is converted into a common format that is called an alert. During conversion, alerts are associated with the affected resource in the CMDB and are assigned a severity and a status. Severity ranges from normal to critical, and alert status can be new, acknowledged, or resolved.

Alerts from multiple protocols are displayed using common severity and status. All received alerts are displayed in the Event Console.

See "About Event Console alert filters" on page 211.

About alert management

Alert management shows a consolidated view of device health across your network. You can view health by network layout, organizational group, or by directly monitoring the list of received alerts in the Event Console.

The Event Console reduces the need to maintain separate tools to monitor different devices. The Event Console collects SNMP traps and other status messages and displays them in a single location. All status messages are converted to a common

format that links each received message to the affected resource in the Configuration Management Database (CMDB). These formatted messages are called alerts.

See "About alerts" on page 210.

Advanced search features let you quickly find specific alerts or groups of alerts.

The Event Console also provides a rule-based triggering system that lets you create alert matching rules to process alerts in the following ways:

- Discard specific alerts from the database.
- Forward alerts to another management system.
- Execute task server tasks in response to specific alerts.
- Initiate a workflow in response to specific alerts.

Note: If the Notification Server computers and the SQL Server computers are not set to the same time and the same time zone, then any alerts that have occurred in the past few hours are not displayed in the Event Console.

About Event Console alert filters

The Event Console in Symantec Management Platform displays alerts in a grid layout. Alert filters let you sort the alerts so that you can analyze and manage them.

To view the alerts, in the Symantec Management Console, on the **Manage** menu, click **Events and Alerts**.

The Event Console contains several rule types that represent automated, event-based actions. The rule types include discarding, forwarding, task, and workflow rules. Discarding rules filter and discard matching alerts. Forwarding rules forward a Simple Network Management Protocol (SNMP) trap to a downstream listener. Task rules initiate Symantec Management Platform task server tasks. An event can automatically start a workflow process. This workflow process can pass along valuable event data.

See "About alerts" on page 210.

The advanced filter function lets you use advanced filters to manage alerts.

To filter the alerts, on the **Event Console** page, in the **Select a filter** drop-down list, click an alert type.

The color-coded status bar lets you see the number of alerts by severity level, as follows:

Violet	Undetermined

Blue	Informational
Yellow	Warning
Orange	Major
Red	Critical
Green	Normal

To view the information about a specific alert type, on the **Event Console** page, click the colour section of the status bar, and the grid view below changes. It shows only those alerts that match the severity level of the color that you clicked. For example, if you click yellow on the status bar, then the grid shows alerts with severity **Warning**. After you filter by severity level, in the **Select a filter** drop-down list, you can you can clear the selection to see the complete list of alerts again.

The toolbar on the **Event Console** page displays the following symbols:

Details	Opens the **Alert Details** dialog box for the chosen alert.
Acknowledge	Lets you acknowledge a chosen alert. In the **State** column, a blue flag indicates an acknowledged alert.
Resolve	Flags the chosen alert with a check mark in the **State** column. When you right-click a resolved alert, you can view alert details. You can also view the available rules for discarding the alert or open the **Resource Manager** in a new window. If you click **Discarding Rules** with a resolved alert selected, you can create a global discard filter rule or create a resource discard filter rule.
Actions	When you click an alert, and then on the toolbar, click the **Actions** symbol, you see the options that you see when you right-click a resolved alert.

When you click an alert, you can manage it by changing its severity to any of the following:

- **Undetermined**

- **Informational**
- **Warning**
- **Major**
- **Critical**
- **Normal**

On the **Alert Filter Settings** page, you can create and configure filters. To access this page, on the toolbar, click the symbol.

You can type the custom search criteria in the **Search** box, on the toolbar.

When you click a different filter in the drop-down list, the grid view displays the alerts that pertain to the selected filter. You can click any other control on the page, except **Refresh**, and the filter that you chose remains active.

Chapter 9

Historical and Real-Time Monitoring

This chapter includes the following topics:

About viewing the monitor data

Monitor Solution lets you view data about your monitored computers in different reports to ensure that all monitored computers and applications function properly.

You can view the data on the **Monitoring and Alerting** page or on the **Reports** page.

To view monitor data on the **Monitoring and Alerting** page, in the Symantec Management Console, on the **Home** menu, click **Monitoring and Alerting**.

The **Monitoring and Alerting** page includes the following Web parts:

Table 9-1 **Monitoring and Alerting** page Web parts

Web part	Description
Launch Performance Viewer	You use this Web part to enter the name of a computer and run the performance viewer. See "Viewing real-time performance data" on page 217.
Monitored Resources by Status	This Web part shows the monitored resources. The resources are organized according to severity status. The state of a computer is the most severe state of any triggered rule on the computer. For example, if one rule state is warning and another is critical, the overall state of the computer is critical. If all rule states are normal, and then one rule state changes to warning, the computer state is set to warning. This Web part also shows computers with Monitor Plug-in installed. You can click a computer, and then, on the toolbar, launch the Performance Viewer, the Resource Manager, or the Event console.
Monitor Site Servers Status	This Web part shows a list of Monitor Site Servers and their status.
Group View - Aggregate health by resource	This Web part shows the aggregate health of the devices and computers in your organizational groups.
Event Console	This Web part shows a consolidated view of all alerts that are raised.

To view the data on the Monitoring and Alerting page

1. In the Symantec Management Console, on the **Home** menu, click **Monitoring and Alerting**.
2. In the left pane, under **Monitoring and Alerting**, expand **Monitor > Reports**, and then navigate to the report that you want to view.

To view monitor data on the Reports page

1. In the Symantec Management Console, on the **Reports** menu, click **All Reports**.
2. In the left pane, under **Reports**, click **Monitoring and Alerting**, and then navigate to the report that you want to view.

Viewing historical performance data

The historical performance viewer is a component of Monitor Solution that lets you view historical performance data. Historical data is available from both Monitor Plug-in and Remote Monitor Server.

To view historical performance data

1. In the Symantec Management Console, on the **Actions** menu, click **Monitor > Historical**.
2. On the **Historical Performance Viewer** page, on the toolbar, in the **Device** box, type the name of the device, or click the **Select resource with historical data** symbol, and then choose a device from the resource list.
3. Specify the time period for which you want to view the data.

   The time period that you specified in **From** and **To** boxes, may contain no data in the beginning or at the end of the period. In this case, **Summarized View** shows only the actual time when the data is available. The empty timeline with no data in the beginning or at the end of the chart is not displayed.
4. On the toolbar, click **Metrics**.
5. In the **Available Metrics** dialog box, specify the metric data that you want to view, and then click **OK**.
6. In the **Summarized View** diagram, drag the mouse across the graph to specify the range that you want to view.
7. In the **Detailed View** box, choose a point on the graph.

   If available, the data that was last gathered for the selected point is displayed in **Processes**, **Events**, **Ports**, and **Text Data** Web parts.

   The **Metrics** Web part displays the average, minimum, and maximum values for the whole range of data that is displayed in the **Detailed View**. However, the **Last Value** and **Last Time** columns in the **Metrics** Web part display the value for the selected point. If the selected point has no value, these columns display the value that precedes this point. If no value is available for the metric in the **Detailed View**, the **Last Value** and **Last Time** columns are left blank in the **Metrics** Web part.

See “Viewing real-time performance data” on page 217.

Viewing real-time performance data

The Performance Viewer is a component of Monitor Solution that lets you view real-time performance data. Performance data is available from both Monitor Plug-in and Remote Monitor Server.

To view real-time performance data

1. In the Symantec Management Console, on the **Actions** menu, click **Monitor > Real-time**.
2. On the **Real-time Performance Viewer** page, on the toolbar, in the **Device** box, type the name of the device, or click the **Select resource with historical data** symbol, and then choose a device from the resource list.
3. In the **Registered Metrics** dialog box, check the metric data that you want to monitor, and then click **OK**.

   The performance viewer begins monitoring the computer and displays the following information:

Graph	This section displays graphical performance data. The data is scaled to fit within the limits of the graph. If you place the mouse pointer over a point on a graph line, the monitored metric data is displayed next to the mouse pointer. If you monitor multiple instance metrics, each instance has a separate graph line. You can use the **Select Metrics** option to monitor different metrics.
Metrics	This section displays all numeric metric data that is monitored.
Processes	This section displays the processes that are currently running on a monitored computer.
Events	This section displays all Windows NT event data.
Ports	This section displays the status of the monitored ports on the computer.
Text Data	This section displays the retrieved text data for command, custom DLL, custom COM object, WS-MAN, SNMP, SQL, and string-type Windows Management Instrumentation (WMI) metrics. The predefined WMI metrics are the only metrics that collect this type of data. If you create or use a custom DLL, COM object, SNMP, or command metric that retrieves this data, it is also displayed in this section.

See "Viewing historical performance data" on page 216.

Viewing the Monitor Alerts dashboard

After IT Analytics Solution is installed and configured, you can view any dashboards in Symantec Management Platform. For more information, see the *IT Analytics User Guide* at the following URL:

See "Generate a report on Monitor Solution metrics, trends, alerts, and actions" on page 219.

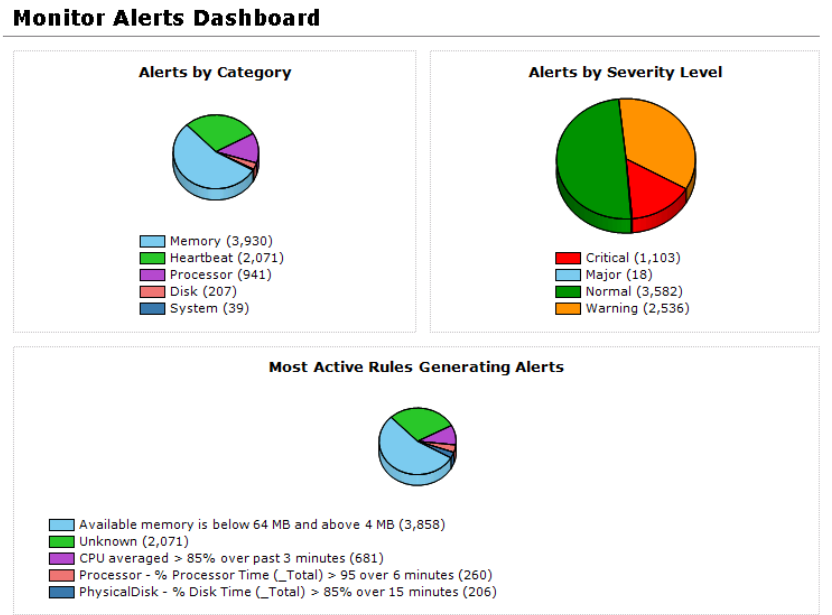
See "Generating ad-hoc reports with the IT Analytics Monitor Metrics cube" on page 221.

The dashboard displays the following information:

- Alerts by category (such as memory, heartbeat, network, processor)
- Alerts by severity level (critical, major, normal, warning)
- The most active rules that generate alerts (lists the rules that cause the most problems)

To view the Monitor Alerts dashboard

1. In the Symantec Management Console, navigate to **Home > Monitoring and Alerting > Monitor**.
2. Click **IT Analytics Monitor Alerts Dashboard**.
3. View the output, similar to the following screenshot:



Generate a report on Monitor Solution metrics, trends, alerts, and actions

After IT Analytics Solution is installed and configured, you can create IT Analytics reports in Symantec Management Platform. For more information, see the *IT Analytics User Guide*.

See "Generating ad-hoc reports with the IT Analytics Monitor Metrics cube" on page 221.

See "Viewing the Monitor Alerts dashboard" on page 218.

IT Analytics reports combine metrics, trends, alerts, and actions. They let you see what occurs with a particular metric over a period of time.

The report shows the following information:

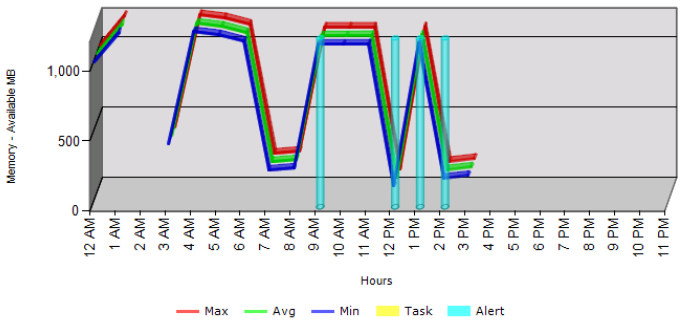
- How the metric trends over time
- Any alerts that were triggered
- Any remediation tasks that resolved the alert
- Notifications that were generated

- Details on individual timestamps

To generate the Monitor Metrics Trend report

1. In the Symantec Management Console, navigate to **Home > Monitoring and Alerting > Monitor**.
2. Select **IT Analytics reports,** then select the **Monitor Metrics Trend** report.
3. Select a date.
4. Select a computer resource.
5. Select a metric value, such as **Available memory in MB**.
6. Run the report.
7. View the output, similar to the following screenshot:

Monitor Metrics Trend



Hourly Details for Memory - Available MB

Hour	Min	Avg	Max	Alerts	Tasks
12 AM	989.00	989.00	989.00	0	0
1 AM	1,203.00	1,203.00	1,203.00	0	0
3 AM	404.00	404.00	404.00	0	0
4 AM	1,208.00	1,208.00	1,208.00	0	0
5 AM	1,186.00	1,186.00	1,186.00	0	0
6 AM	1,139.00	1,139.00	1,139.00	0	0
7 AM	219.00	219.00	219.00	0	0
8 AM	234.00	234.00	234.00	0	0
9 AM	1,118.00	1,118.00	1,118.00	2	0
10 AM	1,118.00	1,118.00	1,118.00	0	0
11 AM	1,119.00	1,119.00	1,119.00	0	0
12 PM	104.00	104.00	104.00	2	0
1 PM	1,123.00	1,123.00	1,123.00	4	0
2 PM	161.00	161.00	161.00	2	0
3 PM	181.00	181.00	181.00	0	0

Generating ad-hoc reports with the IT Analytics Monitor Metrics cube

After IT Analytics solution is installed and configured, you can create IT Analytics reports in Symantec Management Platform. For more information, see the *IT Analytics User Guide* at the following URL:

See "Generate a report on Monitor Solution metrics, trends, alerts, and actions" on page 219.

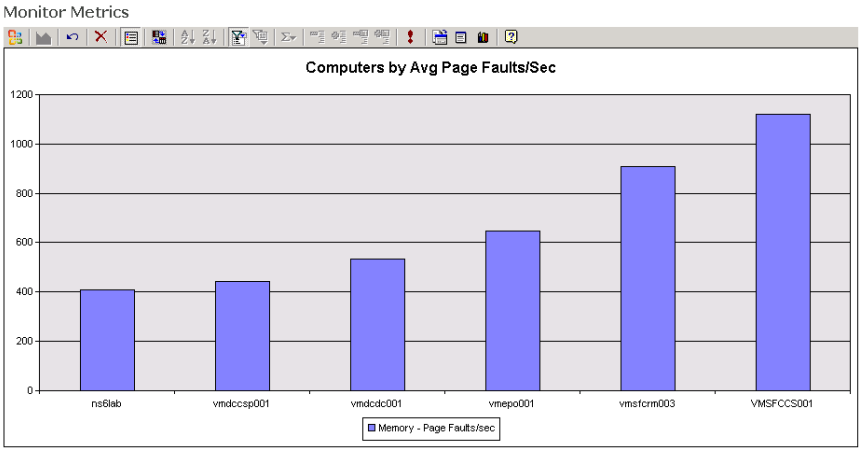
See "Viewing the Monitor Alerts dashboard" on page 218.

IT Analytics Monitor cubes allow for quick ad-hoc reporting and data mining from the data that is collected by Monitor Solution. IT Analytics currently ships with one Monitor Solution-related cube that supports UNIX/Linux environments, the Monitor Metrics cube.

The cube lets you do the following:

- Build a report by selecting tables and attributes, such as computer count, alert count, and action count, computer name, OS, event category, severity level, event message.
- Drill down into the computer, the OS, and see all the categories of alerts.
- Drill down on the alert categories, such as memory alerts and their severity.
- Turn this report into a chart for a graphical presentation.
- Drag and drop different report elements and refine the report ad hoc.

The following screenshot is an example of what this report might look like.



Chapter 10

Using Server Management Suite Portal page

This chapter includes the following topics:

Viewing the Server Management Suite Portal page

Server Management Suite Portal page consolidates the key information about your network resources into a single view. It contains different predefined Web parts. The Web parts on the Server Management Suite Portal page let you monitor the state of your computers and view the inventory data. For example, you can check the status of the recent software deliveries and find out the number of the Microsoft patches that need to be addressed. The network topology diagram provides you with an overview of the physical structure of your network.

Table 10-1 Default Web parts on the Server Management Suite Portal page

Web part	Description
Event Console	Event Console provides a consolidated view of all alerts that are raised. Event Console is part of the Server Management Suite, Client Management Suite, and IT Management Suite.
Monitored Resources by Status	The chart on this Monitor Solution Web part shows the severity status of all monitored resources. In the devices list you can select a computer and launch the Performance Viewer, the Resource Manager, or the Event console.

Table 10-1 Default Web parts on the Server Management Suite Portal page *(continued)*

Web part	Description
Topology View	This Web part provides a network topology diagram of the SNMP-enabled devices that are found in your network. Topology View Web part displays the data that you collect using Network Discovery tasks. See "Viewing network topology" on page 224.
Group View - Aggregate health by resource	This Web part shows the aggregate health of the devices and computers in your organizational groups. The Group View is installed as a part of the Monitor Solutions.
How current is my computer inventory?	This Web part of the Inventory Solution displays a graph that shows how many computers have reported inventory in a specified period of time. You can edit the period of the time that you want reported.
Recent Software Delivery Status	This Web part of the Software Management Solution lists all software deliveries and their status. Following delivery types are displayed: Managed Software Delivery, Quick Delivery, Package Delivery, and Legacy Software Delivery.
Microsoft Vulnerabilities	This graph reports the number and the severity of the Microsoft patches that need to be addressed. The Microsoft Vulnerabilities graph is a Web part of the Patch Management Solution.

To view the Server Management Suite Portal page

1. In the Symantec Management Console, on the **Home** menu, click **Server Management Suite Portal**.
2. View the Web parts.
3. (Optional) To customize the Server Management Suite Portal page, click **Edit**.

   You can edit or remove the predefined Web parts, or you can create new Web parts.

   For more information, see the topics about editing portal pages in the *IT Management Suite Administration Guide* at the following URL:

   http://www.symantec.com/docs/DOC8632

See "About Server Management Suite" on page 13.

Viewing network topology

The **Topology View** Web part provides a view of the SNMP-enabled network devices and the physical organization of your network. You see the status of all the network devices that are connected to your network and you can access the reports of each device.

Icons on the topology diagram let you identify the different SNMP-enabled network devices that are found. Labels on the icon indicate the status of each device. You can double-click the icon of the device to open the Event Console. When you right-click the icon, you can access other reports of the device and run different tasks.

In the **Topology View** Web part you can create groups and maps to document the network, troubleshoot the subnets, or plan infrastructure expansions.

Before you can view the topology diagram, you must collect the data about the SNMP-enabled devices on your network. Use the Network Discovery task to discover your network resources. Network Discovery lets you find routers, switches, hubs, network printers, Novell NetWare servers, and the computers that are running Windows, UNIX, Linux, and Mac OS X. The collected data is saved in the Configuration Management Database (CMDB). Make sure that the connection profile of the Network Discovery task has the SNMP turned on.

For more information, see the topics about discovering network devices in the *IT Management Suite Administration Guide* at the following URL:

http://www.symantec.com/docs/DOC8632

Note: The **Topology View** Web part does not display the SNMP-enabled devices that are discovered with the single device discovery task. When you create a Network Discovery task to collect the data for the **Topology View** Web part, you must set the range of the IP addresses that you want to discover.

The **Topology View** Web part is installed as a part of the Server Management Suite.

To view network topology

1. In the Symantec Management Console, on the **Home** menu, click **Server Management Suite Portal**.
2. On the **Topology View** Web part, click **Select device** and select the root device for the network topology.
3. (Optional) Edit the settings of the network topology view.

   The options on the **Topology View** Web part are as follows:

Root device	Lets you set any device of infrastructure type that is found in your network, as a root device for the topology view. When you click **Select root device**, the list of network devices available for selection as a root device is displayed. You can filter and search devices and set any of them as a root device. The layout of the network is rearranged according to the selection.
Open	Lets you select and display previously saved views.
Save	Lets you save the settings and topology layout of the current view. Type a descriptive name that helps you easily identify the view in the future.
Levels	Lets you select the depth of levels to display. The drop-down list gets filled dynamically, according to the number of levels of the actual network.
Display	Lets you hide or show different types of network devices.
Screen	Lets you display the **Topology View** Web part in the full screen mode.
Search device	Lets you search devices by name or IP address. After you type the item to search for in the **Search device** box, the view is refreshed automatically.

   After you make the changes, you can save the network topology view for further use.

See "Viewing the Server Management Suite Portal page" on page 222.

Chapter 11

Using Server Resource Manager Home page

This chapter includes the following topics:

Accessing the Server Resource Manager Home page

The **Server Resource Manager Home** page consolidates the most relevant inventory and monitoring data of a server resource into a single view.

Different reports let you easily check and ensure that any of your Windows, UNIX, or Linux servers functions properly. On the **Server Resource Manager Home** page you see the attributes of the server, and current disk utilization for all attached disks. You can view the different health and performance reports of your server. For example you can view the reports of processor, physical memory, disk I/O, network bandwidth, and disk space utilization.

The Web parts display the data in real time or for the last 24 hours. The real-time data is received directly from the managed computer. The historical data is taken from the Configuration Management Database (CMDB). When you want to see the report for longer than 24-hour period, click the historical diagram.

To gather the data for the Web parts that are displayed on the **Server Resource Manager Home** page, you must install the following agent and plug-ins on the target computers:

- Symantec Management Agent
- Inventory Plug-in
- Monitor Plug-in

You need to enable an Inventory policy and the **Windows Server Performance Health Monitor Policy** and assign them to a resource before the Server Resource Manager Home page is populated.

For more information, see the topics about preparing managed computers for inventory in the *Inventory Solution User Guide*, and about preparing managed computers for monitoring in the *Monitor Solution for Servers User Guide* at the following URLs:

http://www.symantec.com/docs/DOC8636

http://www.symantec.com/docs/DOC8707

See "Preparing managed computers for agent-based monitoring" on page 201.

The **Server Resource Manager Home** page lets you also access all the functions that are available in the Resource Manager.

For more information, see the topics about the Resource Manager functions in the *IT Management Suite Administration Guide*.

http://www.symantec.com/docs/DOC8632

When you have selected the **Server Resource Manager View** for a resource, this view is the default view for all resources.

The **Server Resource Manager Home** page is installed as a part of the Server Management Suite.

To access the Server Resource Manager Home page

1. In the Symantec Management Console, on the **Manage** menu, click **Resource**.
2. In the **Select Resource** dialog box, select the server resource that you want to manage, and then click **OK**
3. In **Resource Manager**, in the **Custom View** drop-down list, click **Server Resource Manager View**.