Altiris™ Deployment Solution 7.1 SP1a MR1 from Symantec™ User Guide

Symantec™

Altiris™ Deployment Solution 7.1 SP1a from Symantec™ User Guide

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

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

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

Symantec's support offerings include the following:

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

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

www.symantec.com/business/support/

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

Contacting Technical Support

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

www.symantec.com/business/support/

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

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

- Product release level

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

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

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

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

Support agreement resources

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

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

Contents

Chapter 1

Introducing Deployment Solution

This chapter includes the following topics:

About Deployment Solution

Deployment Solution lets you integrate standard deployment features with Symantec Management Platform. It helps reduce the cost of deploying and managing servers, desktops, and notebooks from a centralized location in your environment. The solution offers OS deployment, configuration, PC personality migration, and software deployment across hardware platforms and OS types.

The following are the key features of Deployment Solution:

- Lets you mass-deploy hardware-independent images to new systems and existing systems using Symantec Ghost and RapiDeploy imaging tools.
- Lets you migrate to the latest Windows version; migrates user data, personality settings, and OS and application settings to the new operating system.
- Lets you configure each system based on standardized criteria, such as job function, user type, or location.
- Lets you change the system and the network settings.

- Supports the deployment of heterogeneous client and server operating systems, including Windows and Linux.
- Supports the deployment of heterogeneous client and server operating systems such as Windows and Linux on client and server computers.
- Lets you easily create the jobs and tasks that automate deployment and migration functions such as imaging, scripted OS installations, configurations, and software deployments.
- Supports industry-standard hardware-management capabilities such as Intel vPro, Pre-boot eXecution Environment (PXE), and Wake on LAN technologies.
- Lets you use role- and scope-based security to secure management features from unauthorized personnel.
- Supports the WinPE and the Linux preboot environments.
- Integrates with many Symantec products built on Symantec Management Platform: for example, Altiris solutions and security, backup and recovery, virtualization, data loss prevention, vulnerability assessment, and and other products.

The following are the key benefits of Deployment Solution:

- Reduces the costs that are associated with deploying, migrating, and provisioning desktops, laptops, and servers throughout the organization.
- Saves time and reduces human error over traditional PC deployments.
- Reduces end-user downtime by automating the deployment process.
- Increases IT efficiency through automated, repeatable deployment tasks.
- Provides tools for zero-touch migrations to reduce the costs that are associated with moving to a new operating system.

See "What you can do with Deployment Solution" on page 18.

See "About Imaging client computers" on page 63.

What's new in Deployment Solution 7.1 SP1a MR1

The Deployment Solution 7.1 SP1a MR1 contains the following enhancements:

Table 1-1 List of supported features

Feature	Description
Deploy Image with Ghost Partition Deployment	Deployment Solution now supports Ghost partition deployment. See "Setting advanced Deploy Image options" on page 76.
Predefined computers import with MAC address only	Predefined computers can be imported with only MAC address. See "About predefining computers" on page 103.
Install Windows OS with **Domain Join** option	The **Install Windows OS** task supports the **domain join** option. Client computer can also join domain without an inventory but inventory data option must be selected. FQDN must be used as domain credential. For example, Symantec.com\User and not Symantec\user. See "*Performing an OS installation*" on page 83.
Install Windows OS for Windows 7 SP1	**The Install Windows OS** task is supported for Windows 7 SP1.
Apply System Configuration supports tokens for hostname	Tokens can also be used to change the hostname using **Apply System Confuguration.** for example %Customtoken%,%Serialnumber% . See "Creating an Apply System Configuration task" on page 79.

Components of Deployment Solution

When you install Deployment Solution on Symantec Management Platform, the Deployment Solution components get integrated with Symantec Management Platform. The Deployment Solution leverages the platform capabilities to execute and schedule tasks, jobs, and policies, and set up site servers, use filters, and generate reports. The components of Deployment Solution help you manage the client computers in your environment.

Table 1-2 Deployment Solution components

Component	Description
Deployment Plug-in	The Deployment Plug-in is installed on client computers to manage deployment tasks. This plug-in enables you to create and deploy disk images, perform remote OS installation, change your system settings, and migrate the personality settings. The Deployment Plug-in replaces the former Deployment Solution 6.X agents, such as AClient, DAgent, or ADLAgent. If you need them, AClient and DAgent can coexist with the Deployment Plug-in. You can enable the Symantec firewall on the client computer and enable the Windows firewall on Notification Server. However, to install the Deployment Plug-in by pushing it to computers, you need to disable one of these firewalls. See "Installing Deployment Plug-in" on page 27.

Table 1-2 Deployment Solution components *(continued)*

Component	Description
Deployment site server component	Deployment site server components let you offload some of the traffic and workload from your primary Symantec Management Platform. You can set up multiple task servers and Deployment site server components to handle your jobs and tasks. Symantec Management Agent then uses the assigned Deployment site server components for all deployment processes. These processes include imaging, scripted OS installation, Copy file, and the tasks that are associated with packages. See "Installing Deployment site server components" on page 29. Deployment site server components can be installed on the site servers that are configured with both Package Services and Task Services. For more information, search for task server topics in the *Symantec Management Platform Help*. The components also include all of the tools that Deployment Solution needs. These tools include RapiDeploy, Ghost, and Boot Disk Creator. A Deployment share is created when the Deployment site server component is installed on a site server. The Deployment share is the location where all the tools, such as Ghost and RapiDeploy, other utilities, and images that are created are stored. The site server components also include the PXE service. See "About Pre-boot eXecution Environment (PXE)" on page 58.

Table 1-2 Deployment Solution components *(continued)*

Component	Description
Automation folder	Automation folder stores the preboot environment. With the help of the preboot environment (WinPE and Linux PE) the client computers are rebooted to the automation environment. The PXE server and automation folder can be used to reboot the client computer to the automation environment to perform deployment tasks. See "Installing an automation folder" on page 28. The preboot environment (WinPE) contains the `Boot.wim` file. This file is used to execute Deployment tasks. To reboot the client computer to an automation environment, the DNS should be configured on the network. Also, all computers in the network should be able to perform a Name Server Lookup. WinPE 2.1 and Linux are the only automation operating systems that Deployment Solution supports. Both preboot operating systems are installed with Deployment Solution. See "Setting up Deployment Solution " on page 24.
PXE server	The PXE server can be configured on Symantec Management Platform and the site server. This configuration helps to reboot the client computers to WinPE and Linux PE environments using the network interface. See "About Pre-boot eXecution Environment (PXE)" on page 58.

Table 1-2 Deployment Solution components *(continued)*

Component	Description
Imaging tools	Ghost and RapiDeploy are two disk imaging tools that run on the Windows (x86,x64)and Linux(x86)operating systems. These tools can also be used for creating backup disk images and image of disk partitions. These tools support NTFS,FAT(16,32),EXT2/3,and RAW file system,and HTTP and multicast imaging options. These tools support Windows only hardware-independent disk imaging which can be deployed to diverse client computers by using drivers from a centrally managed driver database. Although backup images are not hardware-independent and intended to be deployed on the same client.
Boot Disk Creator	Boot Disk Creator creates a boot disk using Windows and Linux preboot environment. Boot Disk Creator is run on the client computer to boot it in WinPE or LinuxPE. It can also create a bootable CD or USB. See "Creating a preboot configuration" on page 33.
Resource Import Tool	The Resource Import tool is used for importing existing Windows and Linux images. It is also used for adding Windows-scripted OS installation files. See "Importing an existing image" on page 73.
Driver Manager	Driver Manager provides the interface to perform driver operations such as adding and deleting data from the DeployAnywhere driver database and the Boot Disk Creator driver database. See "Adding drivers to a driver database" on page 36.

Table 1-2 Deployment Solution components *(continued)*

Component	Description
DeployAnywhere	Deploy Anywhere enables you to deploy the Windows operating system image to dissimilar hardware. It also enables you to perform a Windows-scripted installation on bare metal hardware. See "Deploying an image" on page 73. See "Windows OS installation options" on page 88.

What you can do with Deployment Solution

You can use Deployment Solution to handle many of your deployment needs.

From the **Settings** menu, select **Deployment** to view the options to configure Deployment Solution settings for the first time.

You can enable and disable policies by using the **Settings > All Settings** menu. Then, from the left pane expand **Settings > Agents/Plug-ins > Deployment and Migration** and select the operating system for which you want to enable the policy.

You can manage your tasks and jobs by using the **Manage > Jobs and Tasks** menu.

Table 1-3 What you can do with Deployment Solution

Task	Description
Enable policies to install the Deployment plug-in, automation folder, and Deployment site server component.	You can enable the policies that install the Deployment plug-in, automation folder, and Deployment site server component to the computers that you select. You need to enable these policies to complete the Deployment Solution installation. See "Installing Deployment Plug-in" on page 27. See "Installing an automation folder" on page 28. See "Installing Deployment site server components" on page 29.

Table 1-3 What you can do with Deployment Solution *(continued)*

Task	Description
Configure the deployment settings	You can configure the following to set up Deployment Solution: ■ Configure the preboot environment. ■ Add OS licenses. ■ Add OS files. ■ Add drivers to diver database. ■ Configure multicast settings. ■ Configure initial deployment settings. ■ Configure system settings. ■ Configure Sysprep imaging. ■ Import predefined computers. See "Setting up Deployment Solution " on page 24.
Reboot the client computers	You can reboot the client computers to an automation, a production, and the Pre-boot eXecution Environment (PXE) to perform deployment-related tasks and manage the client computers. See "About rebooting client computers" on page 57.
Image client computers	You can create disk images to deploy to multiple client computers. You can also create backup images to copy the contents of a single computer. See "About Imaging client computers" on page 63.
Perform scripted OS installations	You can create a package that contains the source files you specify for a scripted OS installation. See "About OS installation" on page 83.
Capture and distribute computer personalities	You can migrate a computer's settings and user preferences to another computer using personalities. See "About capturing and distributing personalities" on page 93.
Install executable through **Copy file** option	You can copy the installation `.msi` or `.exe` file by using the **Copy file** option. See "About copying files and folders" on page 99.
Import predefined computers	You can predefine computers in a CSV file and then import the predefined computers to your environment. See "About predefining computers" on page 103.

Table 1-3 What you can do with Deployment Solution *(continued)*

Task	Description
Manage jobs and tasks	You can choose from several task types to create deployment tasks. For example, you can create a task that captures or deploys a disk image. See "About deployment tasks and jobs" on page 49. See "Creating a deployment task" on page 52. You can combine several tasks or jobs into one job to run sequentially. You can also specify condition statements for your job. Your tasks execute only if they meet the conditions that you specify. See "Combining tasks into a job" on page 53. You can schedule a task to run immediately or at a later time that you specify. You can also choose the computers that the task runs on. See "Scheduling a deployment task" on page 53. You can check the status of your deployment tasks by running a report. See "Verifying the task status" on page 54.
View Deployment reports	Deployment Solution provides the following reports that you can access from the **Reports > All Reports > Deployment and Migration** menu: ■ **Computers with Deployment Plug-in Installed** - A list of all of the managed computers that have the Deployment Plug-in installed on them. ■ **Computers with Deployment Tasks Execution Status** - A list of details about all of the Deployment tasks that executed so far.
Remove unwanted packages and resources	You can remove the packages and resources that are not required in your environment. See "About removing unwanted packages and resources" on page 107.

Where to get more information

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

Table 1-4 Documentation resources

Document	Description	Location
Release Notes	Information about new features and important issues.	The **Product Support** page, which is available at the following URL: http://www.symantec.com/business/support/all_products.jsp When you open your product's support page, look for the **Documentation** link on the right side of the page.
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 **Product Support** page, which is available at the following URL: http://www.symantec.com/business/support/all_products.jsp When you open your product's support page, look for the **Documentation** link on the right side of the page.
Help	Information about how to use this product, including detailed technical information and instructions for performing common tasks. Help is available at the solution level and at the suite level. This information is available in HTML help format.	The Documentation Library, which is available in the Symantec Management Console on the **Help** menu. Context-sensitive help is available for most screens in the Symantec Management Console. You can open context-sensitive help in the following ways: ■ The F1 key when the page is active. ■ The Context command, which is available in the Symantec Management Console on the **Help** menu.

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

Table 1-5 Symantec product information resources

Resource	Description	Location
SymWISE Support Knowledgebase	Articles, incidents, and issues about Symantec products.	http://www.symantec.com/business/theme.jsp?themeid=support-knowledgebase

Table 1-5 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.	http://www.symantec.com/connect/endpoint-management

Chapter 2

Setting up Deployment Solution

This chapter includes the following topics:

Setting up Deployment Solution

From the **Settings > Deployment** menu, an administrator can perform several tasks, such as managing package, configuring deployment-specific settings, and managing OS licenses.

As a prerequisite to setting up Deployment Solution, ensure that the package server is installed on Symantec Management Platform and on all remote site servers. This installation helps you to perform the replication of packages and Deployment Solution tasks successfully.

The tasks to set up Deployment Solution are listed in sequential order in the following table. Follow this sequence when you configure Deployment Solution for the first time. However, you can also complete these tasks in the order that you need them.

See "Configuring the initial deployment settings" on page 40.

Table 2-1 Process for setting up Deployment Solution

Step	Action	Description
Step 1	Enable predefined install policies.	Enable the predefined policies to install the Deployment Plug-in, the automation folder, and the Deployment site server. See "Installing Deployment Plug-in" on page 27. See "Installing an automation folder" on page 28. See "Installing Deployment site server components" on page 29.
Step 1	Configure your Sysprep options using the **Sysprep Imaging Configuration** option.	You can browse to and upload the Deploy.cab file. See "Configuring the Sysprep imaging" on page 44.
Step 2	Add a license using the **OS Licenses** option.	You can track all of your licenses for all of your operating systems. You can also add licenses on this page. See "Adding OS licenses" on page 43.

Table 2-1 Process for setting up Deployment Solution *(continued)*

Step	Action	Description
Step 3	Create your PXE configuration using the **Preboot Configurations** option.	You can create your PXE preboot configuration settings. From your configuration settings, a PXE image is also created through a task-based policy at a site server level. You can also set up a PXE image for an unmanaged computer. See "Creating a preboot configuration" on page 33. You can configure your PXE server in another step. See "Configuring the PXE Server" on page 32.
Step 4	(Optional) Install automation folders.	You can install an automation folder using a policy. See "Installing an automation folder" on page 28.
Step 5	Configure your PXE server using the **PXE Server Configuration** option.	You can configure your PXE server and select the PXE boot image to use. You can also limit the bandwidth that is used and how many computers receive the automation at one time. See "Configuring the PXE Server" on page 32.
Step 6	Add drivers to the driver database using the **Driver Management** option.	You can view the drivers that are in your deployment environment. You can manage the driver's database package that is stored in the DeployAnywhere and the preboot database. By default, the package replicates to all of the site servers in your environment. See "Adding drivers to the Preboot database" on page 38.

Table 2-1 Process for setting up Deployment Solution *(continued)*

Step	Action	Description
Step 7	Configure multicast settings for deploying images using the **Image Multicasting** option.	You can configure the multicast options to simultaneously deploy images to multiple computers. See "Image Multicasting options " on page 40.
Step 8	Determine what Deployment jobs or tasks run when an unknown computer performs a PXE Boot using the **Initial Deployment** option.	You can set the task list for a new computer that boots to the network. See "Configuring the initial deployment settings" on page 40.
Step 9	Import predefined computers using the **Predefined computers** option.	You can predefine computers in a CSV file. Then, you can import this file to add the predefined computers to your environment. See "Importing predefined computers" on page 43.
Step 10	Set up system settings using the **System Configurations** option.	You can configure the domain and the network adapters to be used for the client computers. See "Setting the system configuration" on page 45.

Preinstallation requirements for Deployment Solution

Before you start the Deployment Solution installation, you must verify the following:

- Symantec Installation Manager (SIM) is installed.
- Symantec Management Platform is installed.
- Symantec Management Agent for UNIX and Windows is preinstalled on the client computers.
- Symantec Management Agent for Unix, Linux, and MAC is installed if you plan to use UNIX and Mac client computers.
- JRE 1.5 or later enabled browser is required.
- Symantec Administrator Software Development Kit (SASDK) is installed if you plan to use the Web Services API.

- Client computers have Pre-boot eXecution Environment (PXE) enabled on them.
- DHCP is up and running with PXE support
- Silverlight 4 is installed.
- The storage and the network drivers in your environment are collected.
- The remote site server is configured on the supported platform if you plan to manage clients in different subnet. For a remote site server to be configured, a package server and a task server should be installed on the supported platform.
- The package server is installed on Symantec Management Platform and on all remote site servers.
- DNS is properly configured. Clients computers inside different subnets should be able to ping to Symantec Management Platform and the remote site server using FQDN.

Installing Deployment Plug-in

Deployment Solution is installed on Symantec Management Platform and Deployment Plug-in is a component of Deployment Solution. Deployment Plug-in is installed on client computers to manage deployment tasks. This plug-in enables you to create and deploy disk images, perform remote OS installation, change your system settings, and migrate the personality settings.

Predefined policies to install, upgrade, and uninstall the Deployment plug-in are provided with Deployment Solution. It provides installation policies for 32-bit and 64-bit client computers. Hence, it supports Windows x64, Windows x86, and Linux x86. You can install the policy on your target computer.

If you plan to install Deployment Plug-in on a Linux operating system that has a static IP environment, ensure that you have manually entered the site server's and Symantec Management Platform server's name, and their IP addresses in `/etc/hosts` file.

You cannot install the Deployment Solution plug-in in a maintenance window by using the **Run once ASAP in maintenance window only** option. You are required to schedule the installation using the **Add Schedule** option.

See "What you can do with Deployment Solution" on page 18.

To install Deployment Plug-in

1. In the Symantec Management Console, on the **Settings** menu, click **Agent/Plug-ins > All Agents/Plug-ins**.
2. In the left pane, expand the **Agents/Plug-ins > Deployment and Migration** folders.
3. Choose either a Linux or Windows installation and expand the corresponding folder.
4. Click the **Deployment Plug-in - Install** policy.
5. In the right pane, in the **Program name** box, ensure that the correct policy is selected.
6. Under **Applied to**, select the computers that you want to install the plug-in on.
7. (Optional) Under **Schedule**, select when you want to install the plug-in.
8. (Optional) Click **Advanced** to check if the computers you selected are available at the exact time that you scheduled.

   You can also select start and end dates on this page.
9. Under **Extra schedule options**, select the options that you want.
10. Ensure that the policy is enabled.

    A green **On** symbol shows in the top right corner.
11. Click **Save changes**.

Installing an automation folder

An automation folder stores the preboot operating system. With the help of the preboot operating system (WinPE and Linux PE) the client computers are rebooted to the automation environment. Both the PXE server and the automation folder can be used to reboot the client computer to the automation environment to perform deployment tasks.

Predefined policies to install, upgrade, and uninstall the automation folder are provided with Deployment Solution. The automation folder is supported on Windows x64, Windows x86, and Linux x86. You can create your own 64-bit automation packages and policies using the preboot configuration options.

See "Configuring the preboot environment" on page 31.

Ensure that proper filters are set while installing the Deployment Plug-in and Automation Folder. Ensure that a 64-bit policy gets installed on 64-bit clients and 32-bit policies gets installed on 32-bit clients.

To install an automation folder

1. In the Symantec Management Console, on the **Settings** menu, click **Agent/Plug-ins > All Agents/Plug-ins**.
2. In the left pane, expand the **Agents/Plug-ins > Deployment and Migration** folders.
3. Choose either a Linux or Windows installation and expand the corresponding folder.
4. Click the **Automation Folder - Install** policy.
5. In the right pane, in the **Program name** box, ensure that the correct policy is selected.
6. Under **Applied to**, select the computers that you want to install the plug-in on.
7. Under **Schedule**, select when you want to install the plug-in.
8. (Optional) Click **Advanced** to check if the computers you selected are available at the exact time that you scheduled.

   You can also select start and end dates on this page.
9. Under **Extra schedule options**, select the options that you want.
10. Ensure that the policy is enabled.

    A green **On** symbol shows in the top right corner.
11. Click **Save changes**.

Installing Deployment site server components

Deployment site server component lets you offload some of the traffic and workload from your primary Symantec Management Platform. You can set up multiple task servers and Deployment site server components to handle your jobs and tasks. Symantec Management Agent then uses the assigned Deployment site server components for all deployment tasks. These tasks include imaging, scripted OS installation, copy file, and the tasks that are associated with packages. The tasks can be scheduled to run immediately or at a later specified time. This process improves scalability.

Before installing the Deployment components on a site server, you should install the Package Service and Task Service on that site server.

The following are the supported operating systems for Deployment site server components:

- Windows Server 2003 SP2

- Windows Server 2003 R2 SP2
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2008 R2 SP1

For the Linux operating system, if there is no domain controller present in the environment, then ensure that the Agent Connectivity Credential (ACC) configuration is set up as expected. Also, ensure that ACC is enabled on every site server that is configured in the environment. Ensure that user credentials for site server and the Symantec Management Platform server are the same.

See "Setting up ACC" on page 31.

All Deployment computer images and Personality Packages are created on the task server that each managed computer works with. To deploy an image that was created on a different task server, you must replicate that image to your task server. You can replicate the image using the package replication that is contained in Symantec Management Platform. You can also configure specific replication rules for disk image packages.

You must install the site server components before you can replicate packages, including driver packages. After the components are installed, your packages become valid and can then be replicated.

You can uninstall and upgrade the components by choosing the appropriate policy.

For more information, search for site server and task server topics in the *Symantec Management Platform Help*.

To install Deployment site server components

1. In the Symantec Management Console, on the **Settings** menu, click **Agent/Plug-ins** > **All Agents/Plug-ins**.
2. In the left pane, expand the **Agents/Plug-ins** > **Deployment and Migration** > **Windows** folders.
3. Click the **Deployment Site Server Components - Install** policy.
4. In the right pane, in the **Program name** box, ensure that the correct policy is enabled.
5. (Optional) Under **Schedule**, select when you want to install the components.
6. (Optional) Click **Advanced** to check if the computers you selected are available at the exact time that you scheduled.
7. Under **Extra schedule options**, select the options that you want.

8 Ensure that the policy is enabled.

A green **On** symbol shows in the top right corner.

9 Click **Save changes**.

Setting up ACC

For Linux operating system if there is no domain controller present in the environment, then ensure that the Agent Connectivity Credential (ACC) configuration is set up as expected. Also, ensure that ACC is enabled on every site server that is configured in the environment.

To set up ACC

1 In the Symantec Management Console, select **Settings** > **Agent/Plug-in** > **Global settings**.

2 Click the **Authentication** tab.

3 Select **Use these credentials** and enter the Symantec Management Platform user name and password.

4 Click **Save changes**.

5 In the Symantec Management Console, select **Settings** > **Notification Server** > **Site Server Settings**.

6 On the right pane, expand **Site Management** > **Settings** > **Package Service** > **Package Service Settings**.

7 On the left pane, under **Security Settings** select **Create the Agent Connectivity Credential on Package Servers (provided the ACC is not a domain account)** check box.

8 Click **Save changes**.

After the site server retrieves the updated policies from Notification Server, an ACC account is created on the site server for package download and task server connectivity.

See "Installing Deployment site server components" on page 29.

Configuring the preboot environment

You can configure the preboot environment to use for the tasks to perform in Deployment Solution. The process for configuring the preboot environment includes the following tasks

Configure the PXE server	You can configure the PXE server that was automatically installed when you installed Deployment Solution. By configuring the PXE server, you can respond to unknown and to predefined computers. By configuring the PXE server, you can also set a threshold for the number of client computer connections and the bandwidth to be used. See "Configuring the PXE Server" on page 32.
Create a preboot configuration	You can create a preboot configuration for creating a PXE image and a preboot installation file. See "Creating a preboot configuration" on page 33.

Configuring the PXE Server

You can configure the PXE server that was automatically installed when you installed Deployment Solution.

See "About Pre-boot eXecution Environment (PXE)" on page 58.

You can choose to respond to the unknown and to the predefined computers when you configure the PXE server. You can also select the PXE boot image to use for the unknown and the predefined computers. You can set the threshold on the number of computers that receive the automation simultaneously. You can also set the amount of bandwidth to use during the PXE process.

You can install multiple PXE servers by installing and configuring the site server components on a computer that is running Site Services.

Ensure that you start the Symantec services to start the PXE server.

For more information, search for site server topics in the *Symantec Management Platform Help*.

After entering some inputs, ensure that you do not leave the page idle for more than 20 minutes. Otherwise, you receive an error. You have to restart the browser or refresh the page to save the changes.

See "Setting up Deployment Solution " on page 24.

To configure the PXE server

1. In the **Symantec Management Console**, on the **Settings** menu, click **Deployment > PXE Server Configurations**.
2. Choose any of the following options.

Predefined Computers	Select the **Respond to predefined computers** check box and select the relevant PXE boot image from the drop-down list.
Unknown Computers	Select the **Respond to unknown computers** check box and select the relevant PXE boot image from the drop-down list.
Connectivity	■ Select the **Limit client connections** check box and specify the number of client connections you want. ■ Select the **Limit bandwidth** check box and specify the bandwidth to use during the PXE process. ■ Specify the MTU packet size.
Logging	Select the **Enable logging** check box to enable log creation.

3 Click **Save changes**.

See "Creating a preboot configuration" on page 33.

Creating a preboot configuration

You can create a preboot configuration for creating a PXE image. Tasks can then access and use that specific preboot configuration-based image. The preboot configuration can also be used to create preboot installation files.

See "About Pre-boot eXecution Environment (PXE)" on page 58.

You can select the operating system and the preboot environment into which you want to reboot the selected operating system. You can use the resource that is created to reboot to any job that requires you to reboot to the PXE or the automation folder, or both. If the preboot configuration is added, the server starts building the PXE image after the server requests an updated configuration.

See "Setting up Deployment Solution " on page 24.

You can also choose to edit or delete a preboot configuration.

See "Editing and deleting Preboot configurations" on page 35.

If a preboot configuration that you already created needs a new driver, you must recreate that preboot configuration with the newly added driver. If you create a preboot image before a remote site server is configured, then it is not registered

with new remote site server. You can either recreate the preboot environment for the selected image or create a new image.

See "To recreate a preboot environment" on page 35.

Symantec recommends against executing the bootwiz.exe. If you do so, the PXE images are not known to PXE and the task to reboot the client computers to PXE fails.

To use the preboot configuration, you must have administrative rights and the UAC settings must be disabled.

To create Preboot configurations

1. In the Symantec Management Console, on the **Settings** menu, click **Deployment > Create Preboot Configurations**.
2. On the **Preboot Configurations** page, click **Add**.
3. On the **Add Preboot Configuration** page, enter a name and description for your preboot configuration.
4. Select either the **WinPE** or **Linux** operating system.
5. For Windows, select the **x86** or **x64** architecture.

   You can also select both **x86** and **x64** architectures.

   For Linux, only the **x86** architecture is supported.
6. Select the **OEM extension** to use.
7. Select the preboot environment to build.
   - **PXE** - This preboot configuration can be accessed only from the PXE 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 computer by using policies.
   - **Both PXE and Automation folder** - This option builds both types of configurations.
8. Click **OK**.

9 Click **Save changes**.

Once the PXE image is created, you can then use it to perform deployment tasks.

When a client computer is booted to the PXE image, which has both the architectures selected, the client computer boots to x64 architecture only.

10 (Optional) If you have selected PXE, verify that the PXE image is created in the following path:

```
C:\Program Files\Altiris\Altiris Agent\Agents\Deployment\Task Handler\SBS\Images
```

To recreate a preboot environment

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

2 On the **Preboot Configurations** page, select the preboot configuration to edit from the available list.

3 Click the **Recreate Preboot Environment** link. This will display a message of caution.

Clicking Recreate Preboot Environment automatically saves your changes.Clicking Save changes after clicking Recreate Preboot Environment, resets the Recreate settings you have made for the Preboot Environment.

Clicking **Save changes** is not required when recreating a preboot environment.

See "Configuring the PXE Server" on page 32.

Editing and deleting Preboot configurations

You can choose to edit or delete the preboot configurations, if required.

To edit preboot configurations

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

2 On the **Preboot Configurations** page, select the preboot configuration to edit from the listed configurations and click the edit icon.

3 On the **Edit Preboot Configuration** page, make the required changes.

Consider the following while editing the preboot configurations:

- If **Both PXE and Automation folder** option was selected earlier, then the options to select **PXE** and **Automation folder** is disabled.
- If both the **Architecture**, x86 and x64, were selected earlier, then the options to select a single architecture is disabled.

- The operating system once selected cannot be edited.

4 Click **OK** to save the changes.

To delete preboot configurations

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

2 On the **Preboot Configurations** page, select the preboot configuration to delete from the listed configurations and click the delete icon.

3 Click **OK** to confirm to delete the preboot configuration.

4 Click **Save changes**.

See "Creating a preboot configuration" on page 33.

Adding drivers to a driver database

Deployment Solution lets you add drivers to the driver database to ensure the successful completion of Windows OS installation and Windows image deployment tasks. By adding drivers to the driver database, you eliminate the need for manual driver installations. When you add drivers to the driver database, missing drivers and newly discovered drivers are automatically added to the image.

You can add drivers to the following driver databases:

DeployAnywhere Adding drivers to the DeployAnywhere driver database helps in making the task of imaging and scripted OS installation hardware independent. Hence, deploying of image to client computers and performing an OS installation do not fail due to hardware dependencies.

The DeployAnywhere driver database supports only the Windows operating system.

See "Adding drivers to the DeployAnywhere database" on page 37.

Preboot

Adding drivers to the Preboot database helps the preboot images to support mass storage devices (MSDs) and network interface cards (NICs). These drivers are added to the preboot images. These preboot images are deployed through the preboot environment. It ensures that you can reboot the client computers successfully to automation or to PXE.

The Preboot driver database supports the Windows and Linux operating systems.

You cannot add non-critical drivers to preboot database.

See "Adding drivers to the Preboot database" on page 38.

Driver databases lets you perform the following functionalities:

- List drivers for DeployAnywhere and Preboot databases.
- Add drivers to DeployAnywhere and Preboot databases by folder.
- Delete drivers from the DeployAnywhere database only.
- Search for drivers in DeployAnywhere and Preboot databases.
  The search does not display any results if you use \ in your search string. The search option lets you search based on the driver name, applicable OS, type of driver, and device ID.
- View device details of the selected driver by clicking **More Info**.

Adding drivers to the DeployAnywhere database

The DeployAnywhere driver database helps make image deployment and scripted operating system installation tasks hardware-independent. DeployAnywhere focuses on the device drivers that are critical because the retargeted system has to be managed remotely. During a Windows scripted operating system installation, if any required driver is missing, it takes the missing drivers from the DeployAnywhere driver database.

See "Adding drivers to a driver database" on page 36.

DeployAnywhere supports only the Windows operating system.

DeployAnywhere supports the following critical driver types:

- Mass storage device (MSD)
- Network interface card (NIC)

The MSDs are critical because they allow the resident operating system to boot while network drivers ensure that the retargeted node is managed remotely.

DeployAnywhere supports the following non-critical driver types:

- Graphics
- Audio
- Keyboard
- Mouse
- USB
- CD-ROM
- Printer
- Bluetooth
- Multimedia
- Modem

You can also add drivers to the Preboot database.

See "Adding drivers to the Preboot database" on page 38.

To add a new driver to the DeployAnywhere driver database

1. In the Symantec Management Console, on the **Settings** menu, click **Deployment > Driver Management**.
2. Click the **DeployAnywhere** tab.
3. (Optional) To view details of a driver, select the driver from the list and click **More Info**.
4. Click **Add**.
5. Browse to select the driver to add .
6. Click **OK**.

Adding drivers to the Preboot database

You can add drivers to the Preboot database. You can use these drivers for your preboot PXE configurations needs.

See "About Pre-boot eXecution Environment (PXE)" on page 58.

BootWiz.exe is stored in the `\Program Files\Altiris\Altiris Agent\Agents\Deployment\Task Handler\bootwiz` directory.

See "Setting up Deployment Solution " on page 24.

If a preboot configuration that you already created needs a new driver, you must regenerate that preboot configuration.

See "Creating a preboot configuration" on page 33.

You can also add drivers to the DeployAnywhere database.

See "Adding drivers to the DeployAnywhere database" on page 37.

To add drivers to the Preboot database

1. In the Symantec Management Console, on the **Settings** menu, click **Deployment > Driver Management**.
2. Click the **Preboot** tab.
3. (Optional) To view details of a driver, select the driver from the list and click **More Info**.
4. Click **Add**.
5. Browse to select the required the driver to add.
6. Select the relevant operating system: **WinPE**, or **Linux**.
7. Select the relevant architecture: **x86** or **x64**.
8. Click **OK**.

   The new driver is used when you create a new configuration.

Configuring multicast options to deploy image

Deployment Solution uses the multicasting abilities of the RapiDeploy and Ghost imaging tools to simultaneously deploy images to a group of computers. You use the options on the **Image Multicasting** page to specify the IP range, port range, and other settings to use with multicasting.

See "About images" on page 66.

See "About Imaging client computers" on page 63.

To configure multicast options

1. In the Symantec Management Console, on the **Settings** menu, click **Deployment** > **Image Multicasting**.
2. Select the required options or click **Restore defaults** to use the default settings.

   See "Image Multicasting options " on page 40.
3. Click **Save changes**.

Image Multicasting options

Deployment Solution uses the multicasting abilities of the RapiDeploy and Ghost imaging tools to simultaneously deploy images to a group of computers. The following table describes the Image multicasting options.

See "About images" on page 66.

See "About Imaging client computers" on page 63.

See "Configuring multicast options to deploy image" on page 39.

Table 2-2 **Image Multicasting** options

Option	Description
IP range	The range of IP addresses to use for image deployment.
Port range	The range of port numbers to use for image deployment.
Threshold	The minimum number of clients that need to be part of the group before multicasting is used.
Speed	The maximum speed to use when multicasting to avoid flooding the network with too much traffic. As this number increases, there is a greater chance for dropped packets and slower speeds to occur.
Timeout	The maximum number of seconds to wait for the specified number of clients to join the group. If this number is reached, your images are deployed separately.

Configuring the initial deployment settings

The initial deployment menu is loaded from the Symantec Management Platform and allows for the selection of a task or job to run on the computer.

The unmanaged computer boots from a network card and asks for a PXE server. The PXE server receives this request and compares the computer against its list of known computers. After the server determines that the computer is unknown it sends a preboot image to the computer. This preboot image is the image that you configured in the **PXE Server Configuration** page to respond to the unknown computers.

After the unknown computer receives the preboot PXE image, the pre-OS runs and requests a task server. Because the computer is unknown, it receives an initial deployment menu that contains a preconfigured job or task. According to the default job or the task set for the initial deployment, the task is scheduled on the

client computers. It also specifies how long those tasks display on the new computer.

See "Setting up Deployment Solution " on page 24.

See "What you can do with Deployment Solution" on page 18.

To configure the initial deployment settings

1. In the Symantec Management Console, on the **Settings** menu, click **Deployment** > **Initial Deployment** .
2. Select how long to display the task menu before the default task is performed.
3. Select whether to run a default task or job, or to turn off the computer after the initial deployment menu is displayed for the specified time.
4. Click **Add** to add any tasks that you want to display in the **Initial Deployment** menu.
5. 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.
6. Click **Save changes**.

Adding OS files

You can add files to your package in Deployment Solution. You can configure the import parameters for your package. Ensure that JRE 1.5 or later installed to add files to your package.

After you add the OS Files from the Symantec Management Console , the files are added to the following location:

`Program Files\Altiris\Altiris Agent\Agents\Deployment\Task Handler\SOI directory`.

See "About OS installation" on page 83.

To add OS files

1. From the **Settings** menu, select **Deployment** > **OS Files**.
2. Click **Add files**.
3. Enter a name that you want assigned to your file package in the **Name** field.
4. Enter a description that you want assigned to your file package in the **Description** field.

5 Under the **OS Type** section, select the platform for the operating system from the **Platform** drop-down list.

6 Under the **OS source** section, click **Add Files** to add files to be used during the scripted OS installation.

For 32-bit Windows XP and 2003, select `I386` folder. For 64-bit Windows XP and 2003, select both `AMD64` and `I386` folders. For Windows Vista and later versions of the operating systems, select the `Sources` folder.

Deployment Solution also provides the option to import the OS files. For more information, see

See "Importing OS files" on page 42.

Importing OS files

You can use the **Deployment Solution Resource Import Tool** to import OS files from the OS sources.

To import OS files

1 Browse to `\C:\Program Files\Altiris\Altiris Agent\Agents\Deployment\Task Handler\Tools"` or `[Altiris Agent Install Dir]\Agents\Deployment\Task Handler\Tools` and execute the `ResourceImportTool.exe`.

You can execute this tool from Symantec Management Platform or from Site Server.

Ensure that you run this tool only from Symantec Management Platform.

2 On the **Deployment Solution Resource Import Tool**, click the **OS file Import** tab.

3 Enter a name for the OS file in the **Name of OS file package** field.

4 Enter a description for the OS file package.

5 Select the OS platform from the **OS Platform** drop-down list.

6 Click **Add OS Folder** to browse and select the sources for the selected OS platform.

7 Click **Import**.

8 A message indicating the successful upload of OS file is displayed. Acknowledge the message and close the **Deployment Solution Resource Import Tool**.

See "Adding OS files" on page 41.

Adding OS licenses

Before you use Sysprep with a Deployment job or task, you need to select the OS and the corresponding OS license for the job. This information must be configured before the job is created.

See "Configuring the Sysprep imaging" on page 44.

The **OS Licenses** list stores the Volume License Keys (VLKs) that deploy the Sysprep-enabled images.

See "Setting up Deployment Solution " on page 24.

See "What you can do with Deployment Solution" on page 18.

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**.

   Your new license displays in the **OS Licenses** list.

Importing predefined computers

You can import a predefined computer to assign jobs to unmanaged computers. An unmanaged computer does not yet have the Symantec Management Agent or the Deployment plug-in installed on it.

See "About deployment tasks and jobs" on page 49.

When a computer performs a PXE Boot, the PectAgent sends the basic inventory from preboot environment of the imported computer in form of the new computer's name and MAC address. Hence name and MAc address are mandatory fields.

See "About predefining computers" on page 103.

Ensure that you have set the preboot image to respond to predefined computers. In case the preboot image is not set, an error is displayed when you import the predefined computers.

See "Configuring the PXE Server" on page 32.

To import predefined computer

1. In the Symantec Management Console, on the **Settings** menu, click **Deployment > Predefined Computers**.
2. Click **Import Computers**, and then navigate to the `.txt` or the `.csv` file containing the information about the computers to import.

   You can copy a sample `Pre-DefinedComputers.csv` file from the `\Program Files\Altiris\Notification Server\NSCap\bin\Win32\X86\Deployment\Sample\PreDefinedComputers` folder.
3. From the **Manage** menu, select **Computers** to view the details of imported predefined computers.

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.

When you use the **Prepare for Image capture** task, Deployment Solution automatically uses the Sysprep files. However, for that task to work on Windows XP, you must upload its `deploy.cab` file into Deployment Solution using the **Sysprep Imaging Configuration** option. Sysprep imaging is supported for Windows x86 and x64 only.

See "Preparing to capture an image" on page 68.

When you work with Microsoft domains, each computer must use a unique Windows SID. SIDs are security IDs that are used with Windows NT and later operating systems. Before you deploy Windows images, you should remove the existing SID from a computer to avoid causing network problems. The **Prepare for Image capture** task automatically strips the SIDs from each computer using Sysprep.

You can then create an image using the **Create image** task and deploy the resulting image to multiple computers.

Sysprep also 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.

See "Setting up Deployment Solution " on page 24.

To configure Sysprep imaging

1 In the Symantec Management Console, on the **Settings** menu, click **Deployment** > **Sysprep Imaging Configuration**.

2 Based on your platform, under **x86 Deploy.cab** or **x64 Deploy.cab**, click **Upload** to browse and upload the relevant .cab file.

3 Click **Save changes**.

Setting the system configuration

The system configuration settings contain the network, domain, and other settings that are applied to computers after they are imaged. You can create or update system configuration settings. These settings are applied to computers after you deploy a disk image or apply a system configuration using a task server.

See "Deploying an image" on page 73.

When you distribute a generic Sysprep-enabled image, the system configuration settings are applied to the computer for the initial setup. The same configuration settings can be applied to multiple computers using the name range feature.

You can create a backup image or distribute a Sysprep-enabled image to computers that have the Deployment plug-in installed on them. In this case, you can choose to retain and restore all existing configuration settings. You can also choose to reconfigure these settings.

After the image is deployed, you are required to create the **System Configurations** to bring the client computers to domain in the following scenarios.

- Client computers are bare metal computers
- Client computers were not on domain before the image was deployed.

The credentials are either a local administrator account or a domain account (if you join the computer to a domain).

See "Setting up Deployment Solution " on page 24.

See "What you can do with Deployment Solution" on page 18.

To create system configuration settings

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

2 Click **New system configuration**.

3 On the **Create System Configuration** page, type a name and description for the new configuration settings.

4 On the **Computer Information** tab and the **Network Adapters** tab, select and enter the required information.

See "System configuration editor options" on page ?.

5 Click **OK**.

System configuration editor options

You can create or update system configuration settings with the configuration editor. These settings are applied to computers after you deploy a disk image or apply a system configuration using a task server.

The credentials are either a local administrator account or a domain account (if you join the computer to a domain).

See "Setting the system configuration" on page 45.

Table 2-3 System Configuration editor options

Tab	Options	Description
Computer Information	**Computer name** or **Name range**	Select **Computer name** and enter a computer name or select **Name range** and click **Define range** to specify a new computer range. For computer names, you can use tokens. For example, %CustomerToken%, %SERIALNUMBER%. If you select **Computer name**, you can select **Leave existing** for a computer that is not stored in the database. In this instance, the default name that the Windows installation generates is used. If you select **Name range** you can use the same configuration for multiple computers. Computers are named using a fixed string and a value. Additionally, if you use a name range with a static IP address on the **Network Adapter** tab, the IP address you specify is incremented as well. The fixed text appears before the number range. If the append option is selected, the text appears after the number range. The range is the number that you want to start with. This string increment is by 1 for each computer that receives the configuration.

Table 2-3 System Configuration editor options *(continued)*

Tab	Options	Description
	Workgroup or **Domain**	Select **Workgroup** and enter a workgroup name for the new configuration or select **Domain** and enter the domain name. If you select Domain, you have to also specify the following: ■ Organizational unit ■ Administrative domain user name and password
Network Adapters	**Domain Suffix**	Enter a domain suffix or you can also select **Leave existing**.
	Network adapter	Select a network adapter from the drop-down list and click **Add** to add it to the configuration or **Remove** to remove it from the configuration. Then, select one of the following: ■ **Leave existing** to use the default DHCP or IP address. ■ **Use DHCP to obtain IP address** and click **Advanced** to create IP interfaces, gateway, and DNS. ■ **Assign a static IP address** if you use the **Name Range** feature and enter **IP Address**, **Subnet mask**, **Default gateway**, **DNS1**, and **DNS2**. If you change an IP address from DHCP to static, you need to supply the subnet mask and gateway. Even if they are the same as they were when you used DHCP, you need to supply these numbers. These values are not stored when you use DHCP. Click **Advanced** to create IP interfaces, gateway, and DNS. You can add multiple NIC, but it is not supported for SUSE client computers.

Adding tokens

Deployment Solution provides you with the option to create tokenized scripts. It also provides you with some predefined tokens that you can use.

To add tokens

1. In the Symantec Management Console, on the **Settings** menu, click **Deployment** > **Token**.
2. Click **New token**.
3. Enter a name for the token in the **Token name** filed.
4. Enter the SQL statement for the token.
5. Click **Validate SQL** to validate the SQL statement.
6. Click **Save changes**.

Chapter 3

Managing tasks and jobs

This chapter includes the following topics:

About deployment tasks and jobs

Deployment Solution manages computers using tasks and jobs. Tasks are individual processes, such as creating an image or capturing a computer's personality. Each task can be scheduled and run.

Jobs are a combination of tasks. Each job can be assigned to specific computer, and each job specifies the order in which each task runs.

You must create each task before it appears in your **Manage > Jobs and Tasks > System Jobs and Tasks > Deployment and Migration** list.

See "Creating a deployment task" on page 52.

See "Combining tasks into a job" on page 53.

See "Scheduling a deployment task" on page 53.

See "Verifying the task status" on page 54.

If a computer does not yet have the Symantec Management Agent or the Deployment plug-in installed, you can import a predefined computer. Predefined computers let you assign jobs to unmanaged computers.

See "Importing predefined computers" on page 43.

You can create Client Jobs and Server Jobs in Symantec Management Platform. These two job types are identical with one exception. Server Jobs guarantee that the exact same task sequence and execution path is followed for all nodes. For example, the logic for a job specifies that the job stops if one of the tasks fails. When that task fails or times out in one node, that job stops for all of the nodes.

Deployment Solution provides the following predefined tasks.

Table 3-1 Predefined deployment tasks

Task	Description
Apply System Configuration	Applies the new configurations to a computer. See "Setting the system configuration" on page 45.
Capture Personality	Uses PC Transplant to capture a computer's settings and files (personality). See "Capturing computer personality" on page 96.
Copy File	Copies the specified files and folders to a destination computer. See "Copying files and folders options" on page 100.
Create Image	Creates disk images and backup images. See "Creating an image" on page 69.
Deploy Image	Deploys the disk image files (not the backup image files). See "Deploying an image" on page 73.
Capture Personality	Capture's the personality of the computer. See "Capturing computer personality" on page 96.
Distribute Personality	Installs a previously captured computer personality. See "Distributing computer personality" on page 97.
Erase Disk	Cleans a disk. You can configure this task to meet DoD standards. See "Erasing a Disk" on page 85.
Install Linux OS	Performs a scripted OS install of Linux. See "Performing a LINUX OS installation" on page 89.

Table 3-1 Predefined deployment tasks *(continued)*

Task	Description
Install Windows OS	Performs a scripted OS install of Windows. See "Performing a Windows OS installation" on page 87.
Partition Disk	Creates the disk partitions on a hard drive. See "Creating disk partitions" on page 86.
Prepare for Image capture	Runs Microsoft Sysprep. See "Configuring the Sysprep imaging" on page 44. See "Preparing to capture an image" on page 68.
Reboot To	Instructs a computer to boot to the production OS, PXE, or automation folder. See "Creating a Reboot to task" on page 60.
Restore BackUp Image	Deploys the backup image files (not the disk image files). See "Restoring a backup image" on page 77.

You can also create many other types of tasks that work with Deployment Solution to add more functionality. For example, you can create the following types of tasks:

- A **Run Script** task that lets you use a scripting language such as Perl or Python. The **Run Script** task supports many scripting languages and predefined tokens. For more information, search for run script task topics in the *Symantec Management Platform Help*.
- An inventory task that gathers much more information than the Deployment Solution reports provide. The inventory tasks are listed in the Symantec Management Console on the **Create New Task** page under **Discovery and Inventory**.
- A **Power Control** task that provides many of the capabilities that were included in previous versions of the Deployment Solution product. For more information, search for power control task topics in the *Symantec Management Platform Help*.
- A **Power Management** task that integrates out-of-bounds (OOB) management capabilities with traditional Deployment Solution tasks. For more information, search for power management topics in the *Real-Time Console Infrastructure Help*.

Creating a deployment task

You can create many kinds of deployment tasks, such as changing the Windows system settings or applying a predefined system configuration setting. You can also capture or deploy a disk image or personality and create or restore a backup image.

See "About deployment tasks and jobs" on page 49.

After a deployment task is created, it is listed under the **Jobs and Tasks > Deployment and Migration** folder. Click any task to view the properties of that task. You can drag and drop tasks to other folders and manually create folders. Any folders that you create do not display until you create a task or job in that folder. Several tasks can also be combined into one job.

See "Combining tasks into a job" on page 53.

A task cannot be deleted if it is currently in use by a job or policy. You can use the **Jobs and Tasks** view to see what jobs and policies use each task.

Tasks can be renamed, deleted, cloned, moved, and scheduled by right-clicking the task and selecting the corresponding option.

See "Changing network settings" on page 55.

See "What you can do with Deployment Solution" on page 18.

To create a deployment task

1. In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**.
2. In the right pane, click **Create a new job or task**.
3. On the **Create New Task** page, in the left page, expand the **Deployment and Migration** folder.
4. Click one of the task types.
5. Add any necessary information, and choose the options you want.

   Make sure that you give your task a unique and meaningful name.
6. Click **OK**.
7. Schedule the task.

   See "Scheduling a deployment task" on page 53.

Combining tasks into a job

You can use jobs to group several tasks together, so that they all run consecutively. You can combine deployment-specific tasks with other tasks in a single job.

Jobs also have the condition statements that you can specify. Your tasks are then executed only if they meet the conditions that you specify.

Jobs can be renamed, deleted, cloned, moved, and scheduled by right-clicking the job and selecting the corresponding option.

You can drag and drop jobs to other folders and manually create folders. Any folders that you create do not display until you create a task or job in that folder.

For more information, search for topics on creating a job in the *Symantec Management Platform Help*.

See "What you can do with Deployment Solution" on page 18.

To combine tasks into a job

1. In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**.
2. In the left pane, right-click the folder where you want the job to be stored in, and then click **New Client Job** or **New Server Job**.
3. In the right pane, create or add the tasks you want.

   You can click **New** to add new jobs or tasks to your job. You can also click **Add Existing** to add existing jobs or tasks to your job.

   You can use the arrows to order the tasks.

   See "Creating a deployment task" on page 52.
4. Select whether the job should fail if any task fails.
5. Click **OK**.

You can edit, order, and add or delete the tasks in a job. Right-clicking selects the job that you want to change, and then you can use the options in the right pane.

Scheduling a deployment task

You can schedule a task to run immediately or at a time that you specify. You can also choose the computers that the task runs on.

See "What you can do with Deployment Solution" on page 18.

To schedule a task

1. In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**.
2. In the left pane, expand the **Jobs and Tasks** > **System Jobs and Tasks** > **Deployment and Migration** folders.
3. Click the job that you want to schedule.
4. (Optional) If you want the task to run immediately, in the right pane, click **Quick Run**. Select the name of the computer that you want the task to run on, and then click **Run**.

   You can schedule the task to run on only one computer using the **Quick Run** option.
5. If you want to schedule the task to run at a later time or you want to schedule multiple computers, click **New Schedule**.
6. Choose the date and time that you want the task to run.

   You can also select the task to run at specific intervals.
7. Select the **Run Options** that you want.
8. Select the computers that you want the task to run on.
9. Click **Schedule**.

Verifying the task status

You can check the state of any tasks that previously ran.

See "About deployment tasks and jobs" on page 49.

See "What you can do with Deployment Solution" on page 18.

You can choose different options for your report, and then click **Refresh** to see the updated results.

To verify the task status

1. In the Symantec Management Console, on the **Reports** menu, click **All Reports**.
2. In the right pane, expand the **Reports** > **Deployment and Migration** folders.
3. Click **Computers with Deployment Tasks Execution Status**.
4. Select the name of the tasks that you want to check the status of.
5. Select a status.

6 Select an image name.

7 Select a time frame.

The report runs, and the right pane is updated with the information that you requested.

Changing network settings

You can apply a system configuration to a computer. You can update a computer name, join a domain, or change network settings.

See "Creating a deployment task" on page 52.

To change network settings

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

2 In the right pane, click **Create a new job or task**.

3 On the **Create New Task** page, in the left pane, expand the **Deployment and Migration** folder.

4 Click **Apply System Configuration**.

5 (Optional) In the right pane, select a predefined configuration.

You can click **Edit configuration** to edit an existing configuration.

See "Creating an Apply System Configuration task" on page 79.

You can also choose to restore the system configuration by using the inventory data.

6 If the target computer is in a Domain, select the corresponding check box.

Enter the credentials for the Domain.

7 Click **OK**.

8 Schedule the task.

See "Scheduling a deployment task" on page 53.

Chapter 4

Rebooting client computers

This chapter includes the following topics:

About rebooting client computers

Before you perform any deployment tasks, you are required to reboot the client computer to an automation environment or the Pre-boot eXecution Environment. After the deployment task is completed, you reboot the client computer back to the production environment to resume live operations.

See "About automation environment" on page 57.

See "About Pre-boot eXecution Environment (PXE)" on page 58.

See "About Production environment" on page 60.

To reboot the client computers to an automation environment, the Pre-boot eXecution Environment , or the production environment, you have to create and execute a **Reboot to** task.

See "Creating a Reboot to task" on page 60.

About automation environment

Deployment Solution has the ability to set up client computers before the normal operating system loads. The managed client computers are prebooted into an

environment in which they can communicate with Deployment Solution. This environment is known as an automation environment and you can reboot the client computers to an automation environment only when you have enabled the **Deployment Automation Folder - Install** policy.

See "Installing an automation folder" on page 28.

To reboot the client computers to an automation environment, you have to create and execute a **Reboot to** task.

See "Creating a Reboot to task" on page 60.

A client computer with a 64-bit Linux operating system cannot be rebooted to an automation environment.

Reboot the client computers to an automation environment to perform the following deployment tasks:

- Create an image.
- Deploy an image.
- Restore a backup image.
- Copy a file.
- Erase a disk.
- Install Windows or Linux OS.
- Partition a disk.

About Pre-boot eXecution Environment (PXE)

The Pre-boot eXecution Environment (PXE) is an environment that you can use to reboot computers using a network interface. This process is independent of your hard disks or installed operating systems.

Deployment site server components include PXE. You cannot uninstall PXE from a computer without uninstalling all of the deployment components.

See "Components of Deployment Solution" on page 13.

You can configure PXE by using the PXE server configuration option. However, changing the PXE configuration automatically affects PXE on all Deployment site servers in your environment.

See "Configuring the PXE Server" on page 32.

The preboot configuration policy also affects all Deployment site servers. After each Deployment site server processes this policy, PXE offers the same bootstrap menu and images to the clients that boot to PXE. Each Deployment site server

receives this policy from Symantec Management Platform and implements the policy settings in a preboot image. The site server creates new preboot images each time it receives new preboot policy configurations. If you remove configurations from the preboot policy, the site server removes the corresponding preboot images.

See "Creating a preboot configuration" on page 33.

Warning: You should not try to clone the PXE policies. If you make changes to a cloned policy copy, unknown consequences might occur. You cannot determine what version of the policy Deployment Solution implemented.

You can add drivers for a preboot image. The addition of drivers ensures that the PXE image supports new hardware.

See "Adding drivers to the Preboot database" on page 38.

You can have more than one Deployment site server on a broadcast domain. However, you must ensure that all Deployment site servers on this kind of domain are assigned to the same Symantec Management Platform site.

For example, if a client on this domain sends a PXE request, you cannot tell which Deployment site server might respond. If the responding server does not know that a PXE reboot task exists, the server instructs the client to boot from the next available device. Usually that device is the hard drive. All client computers with a PXE reboot task must receive a PXE reboot image, no matter which site server responds. All Deployment site servers that are assigned to the same Symantec Management Platform site receive instructions to supply the corresponding preboot image.

See "Creating a Reboot to task" on page 60.

Warning: Before you reboot to PXE, ensure that you have started the Windows firewall service and opened the ports 4011 and 69. Otherwise, rebooting to PXE might fail.

Reboot the client computers to PXE to perform the following deployment tasks if you plan to use the PXE image:

- Create an image.
- Deploy an image.
- Restore a backup image.
- Copy a file.

- Erase a disk.
- Install Windows or Linux OS.
- Partition a disk.

About Production environment

To resume live operations after completing deployment tasks or maintenance tasks, you must reboot the client computers back to the production environment. During this process, you must use the operating system of the computer, also known as DiskOS. You are required to execute the **Reboot to** task to reboot the client computer to the production environment.

See "Creating a Reboot to task" on page 60.

Creating a Reboot to task

You can start computers in an automation environment to run tasks, such as scripts. You can choose to reboot to a PXE or a production environment.

Do not mix PXE with automation partitions or folders on a client. You can use PXE or automation partitions or folders but not both environments together.

Assign this task only if you want to perform a custom automation task.

See "About deployment tasks and jobs" on page 49.

To create a Reboot to task

1. In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**.
2. In the right pane, right-click **Jobs and Tasks > New > Task**.
3. On the **Create New Task** page, under **Deployment and Migration**, click **Reboot to**.
4. Enter a name for the **Reboot to** task.
5. Select one of the following:

Automation	Select this environment to reboot client computers to perform any deployment tasks. A client computer with 64-bit Linux operating system cannot be rebooted to an automation environment. If you reboot the Linux client computer that has a static IP environment, ensure that you manually enter the following information: ■ site server's name ■ Symantec Management Platform server's name ■ site server and Symantec Management Platform server's IP addresses in `/etc/hosts` file in automation folder package.
PXE	Select this environment if you plan to use PXE images. Select the image and the architecture from the drop-down lists. **Warning:** Before you reboot to PXE, ensure that you have started the Windows firewall service and opened the ports 4011 and 69. Otherwise, rebooting to PXE might fail.
Production	Select this environment if you have completed the deployment task and now want to resume live operations.

6 Click **OK**.

7 Schedule the task.

See "Scheduling a deployment task" on page 53.

Chapter 5

Imaging computers

This chapter includes the following topics:

About Imaging client computers

Imaging is the copying of the contents of a computer's hard disk into a single compressed file or a set of files. The single compressed file or set of files is referred to as an image. By creating an image the contents of the hard disk, including configuration information and applications can be copied to the hard disk of other computers. Imaging is useful where one system has to be replicated on a number of computers as the users need the same system and applications.

For Windows, the images that are deployed to multiple computers are prepared using Microsoft Sysprep to remove drivers, the security ID (SID), and other computer-specific settings. Sysprep also disables the built-in administrator account and clears the administrator password. You can also use the **Prepare for Image Capture** task on Linux to remove all configuration-specific settings, such as host name, IP address, and so on. You can perform this task before you reboot to automation environment using the preimage script.

Before performing the imaging tasks configure the following settings:

- Configure the Sysprep imaging.
  See "Configuring the Sysprep imaging" on page 44.
- Configure image multicasting. Configure this option if you want to simultaneously deploy an image to multiple computers.
  See "Image Multicasting options " on page 40.
- Manage driver database. Add drivers to **DeployAnywhere** database and to **Preboot** database to ensure that images are deployed successfully.
  See "Adding drivers to a driver database" on page 36.

You should also ensure that the package server is installed on the Symantec Management Platform, where the remote site server are installed. This lets you perform the task replication and package replication successfully.

Table 5-1 Process for creating and deploying an image

Step	Action	Description
Step 1	Prepare a reference computer for imaging.	The reference computer contains the core software and settings that you want to use on each computer.
Step 2	(XP and Windows 2003 only) Install Sysprep files on the reference computer.	You need to copy the `support\tools\deploy.cab` file from your Windows XP installation disk or service pack to the `c:\sysprep\deploy.cab` file on the source computer. See "Configuring the Sysprep imaging" on page 44.
Step 3	Add an operating system license.	The operating system license is used to re-license your reference computer after Sysprep runs. See "Adding OS licenses" on page 43. For Linux, this step is optional.

Table 5-1 Process for creating and deploying an image *(continued)*

Step	Action	Description
Step 4	Reboot to Automation folder or PXE	Reboot the client computer to Automation folder or if you to use a PXE image, reboot to PXE. See "About rebooting client computers" on page 57.
Step 5	(Optional) Prepare for image capture	Perform this task if you want to perform a sysprep imaging and use the **Include DeployAnywhere for hardware independent imaging** option. If you deploy a disk image using the **Include DeployAnywhere for hardware independent imaging** option and you have not preformed the **Prepare for Image capture** task, the client computer image gets corrupted. See "Configuring the Sysprep imaging" on page 44. See "Preparing to capture an image" on page 68.
Step 6	Create an image.	You can create disk images and backup images. See "Creating an image" on page 69.
Step 7	Deploy an image	You can deploy an image that you previously created. Perform this step if you created a disk image. See "Deploying an image" on page 73.
Step 8	(Optional) Restore the backup image that you previously created.	You can restore the exact state that a computer was in when it was imaged. Perform this step if you created a backup image. See "Restoring a backup image" on page 77.
Step 9	Deploy images to new computers.	You can use **Initial Deployment** to image the new computers in your environment. See "Deploying an image to new computers " on page 78.
Step 10	Reboot to Production	After completing the imaging task, reboot the client computer to Production to resume live operations. See "About rebooting client computers" on page 57.

See "About images" on page 66.

See "About deployment tasks and jobs" on page 49.

About images

Computer images contain the entire content of a computer's hard drive. These contents include the operating system, applications, and user data. For Windows and Linux, you can create images using either Ghost or RapiDeploy. Both are included in Deployment Solution.

See "Image Multicasting options " on page 40.

You can create disk images or backup images.

When you run a task to create an image, the following steps occur:

- An image file is created.
- A Notification Server package is created (for disk images only).
  See "About disk image packages" on page 67.
- A resource for the image is added to the CMDB.
  See "About image resources" on page 66.

A new folder and image file is created each time that you run a task to capture an image. If you run the same task on the same computer three times, you have three different folders and image files for that computer.

You can do one of the following things to avoid the duplication problem:

- Edit the disk creation task to use a unique image name.
- Create a new task that you configure to use a different image name.

Images are created on the task server that the source computer is configured to work with.

About image resources

When an image is created, a Symantec Management Platform resource for that image is also created. The image resource is used when you build tasks to deploy your images.

See "About images" on page 66.

The Symantec Management Console uses the resource list to display what images can be deployed. However, the console does not verify if the image file already exists. If your image file is deleted from the server, it is still possible to create a task to deploy the deleted image. In this case, the task fails.

You can view a list of your image resources from the **Manage > All Resources > Default > All Resources > Software Component > Image Resource** menu. You can also right-click a resource to access the Resource Manager.

If you delete the image resource name using the **Resource Manager**, it does not delete the physical image file from the server. After you delete the image resource name, you must remove the image file from the server.

See "Deleting an image package" on page 108.

About disk image packages

A Symantec Management Platform package is created for all disk images when you run the **Disk Image** task. You can then use this package to distribute the image to other package servers.

See "About images" on page 66.

Disk images are stored on the Deployment share of the Deployment site server. Each image is stored in a separate folder that is specified by a GUID. Information about the image is also stored in the CMDB as an image resource.

You can view your disk image packages from the **Manage** > **Computers** menu or from the **Manage > All Resources > Default > All Resources > Package** menu. You can also view them from the **Settings > All Settings > Deployment and Migration > Disk Images** menu.

You can configure how the image package is distributed to additional package servers using the **Settings > All Settings** menu. After you select the package you want, you can then select what servers get the image from the **Package Servers** tab.

You can choose from the following package distribution options:

- All package servers.
- Individual package servers.
- Package servers by site.
- Package servers automatically with manual prestaging.

You can also delete packages.

See "Deleting an image package" on page 108.

Preparing to capture an image

You can run the **Prepare for Image Capture** task to get ready to capture a disk image.

See "About deployment tasks and jobs" on page 49.

See "About Imaging client computers" on page 63.

For Windows, this task uses Sysprep to remove the computer name (SID), the operating system license, and some hardware-dependent drivers. You should always run this task before creating a disk image and if you want to use DeployAnywhere for hardware independent imaging. 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 44.

You can choose several options while creating this task.

See "Preparing to capture an image" on page 68.

You must create a deployment task before you can run it.

To prepare for image capture

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 **Prepare for Image Capture**.

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

5 Under the **Pre-Imaging** section, select **Windows (using sysprep)** or **Linux** operating system.

If you select **Windows (using sysprep)**, enter the following information:

OS type	Select the type of operating system the task is run on from the drop-down list.
Product key	Select an operating system license that can be used to restore the computer back to its original state after the task runs. If the license has not been added to Deployment Solution, you can add one by clicking **New**.
Enter credentials to rejoin a domain after capture is complete	Enter the user name and password that the computer needs to join the domain again. Enter the password again in the **Confirm password** field.
Reboot to	Select the preboot type to use to start the image creation process. You can either select **Automation** or **PXE**. If you select **PXE** you also need to select the PXE image and the architecture from the drop-down lists.

See "Creating an image" on page 69.

Creating an image

You can create disk images and backup images with the **Create Image** task.

You can deploy disk images to multiple computers. This process removes all of the Windows operating system settings from any captured images. Your computer restarts multiple times during this process.

See "About Imaging client computers" on page 63.

Backup images retain the data and software of a specific computer. A backup image contains a snapshot of the hard disk of a computer. A 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.

By default, the first disk in the system is imaged using Ghost in **optimize for speed** mode. Other imaging tools are also available.

You can also choose advanced imaging options for this task.

See "Setting advanced Create Image options" on page 71.

To create an image

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 **Create Image**.
4. Specify a name for the task on the first field.
5. Enter the following information:

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	Enter a description, if required.
Imaging tool	Select the tool you want to use the create the image. You can choose from the following: ■ **Ghost** ■ **RapiDeploy**

Image type

You can select from the following two types of computer images:

- **Disk Image**
- **Back-Up Image**

Disk Image can be deployed to multiple computers (provisioning). These images are saved in a Notification Server package 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 was executed before the image was created. Otherwise, the client computer on which this disk image is deployed might get corrupted.

See "Configuring the Sysprep imaging" on page 44.

Back-Up Image is used to back up a single computer. These images should be deployed only to the same computer where they were created from. They should not be deployed to multiple computers. These images are not saved in a package and cannot be distributed to other package servers through the replication process. In case you want to image only a data disk (disk without operating system) or partition of a data disk, select the **Backup image** option.

Note: Windows Vista onwards RapiDeploy backup image requires BCDEdit.

Advanced

Lets you select from advanced imaging options, such as media spanning, command-line operations, and HTTP imaging.

See "Setting advanced Create Image options" on page 71.

6 Click **OK**.

Setting advanced Create Image options

The **Advanced** option on the **Create Image** task lets you configure additional options.

You can choose several other options while creating this task.

See "Creating an image" on page 69.

Table 5-2 Advanced **Create Image** options

Option	Description
Media	Determines at what point an image file is split into multiple files. The maximum size depends on the imaging tool (Ghost or RapiDeploy). If you use the RapiDeply imaging tool and select **Unlimited** option for maximum file size, Deployment Solution takes the maximum file size as 2 GB. 2 GB refers to zero split value. Otherwise, the split value that you entered is considered as the maximum file size. If the split value is less than 2 GB, the spans of the requested size are created. For IIS Web servers, by default spans of 2 GB are created. For the servers that are not IIS Web servers, by default the split size is unlimited. If you specify the split size as **0** or **-**, then no spans are created. Only a single image is created on the Web server. In case you are aware of any upload file size limit, you must specify that as maximum file size.
Command-line	Lets you add command-line options for the imaging tool.
HTTP	Lets you upload and download images via HTTP Web server. You need to set up the Internet Information Services (IIS) Manager to get HTTP imaging to work. Otherwise, if you try to use HTTP with the **Create Image** task, the job fails and returns a message that the file could not be created. For more information on setting up the web server in IIS: www.symantec.com/business/support/ For Ghost imaging tool, add the following Mime type: ■ **File Name Extension**: `.gho` and **MIME Type**: **`application/octet-stream`** ■ **File Name Extension**: `.ghs` and **MIME Type**: **`application/octet-stream`** For RapiDeploy imaging tool, add **File Name Extension**: `.img` and **MIME Type**: **`application/octet-stream`**. Ghost tool supports the HTTP web server configured on Windows 2008 IIS 7.5 and on Windows 2003 server IIS 6.0. However, RapiDeploy tool supports the HTTP configured only on Windows 2003 server IIS 6.0.

Importing an existing image

You can use the **Deployment Solution Resource Import Tool** to import an existing image. You can import images and then use them to deploy on client computers. **Deployment Solution Resource Import Tool** needs all the splitted files for a RapiDeploy image to be selected for the effectual import of the RapiDeploy image. Partial selection of files would show up as successful import, but will not lead to a valid image. If you want to import a splitted Ghost image, selection of one split automatically selects the other splits also.

Deployment Solution Resource Import Tool lets you import images that are located on HTTP Web server. User credentials are not required to access the located on HTTP Web server.

You can also import OS packages using the **Deployment Solution Resource Import Tool**.

See "Importing OS files" on page 42.

To import an existing image

1. Browse to `\C:\Program Files\Altiris\Altiris Agent\Agents\Deployment\Task Handler\Tools"` or `[Altiris Agent Install Dir]\Agents\Deployment\Task Handler\Tools` and execute the `ResourceImportTool.exe`.

   You can execute this tool from Symantec Management Platform or from Site Server.

   Ensure that you run this tool only from Symantec Management Platform.
2. On the **Deployment Solution Resource Import Tool**, click browse to `C:\DS_Resources\Win7 Image`, and open required `.gho` or `.img` file.
3. From the **Select OS**, select **Windows 7 Professional**.
4. Click **Import**.
5. A message indicating the successful upload of image is displayed. Acknowledge the message and close the **Deployment Solution Resource Import Tool**.

See "About Imaging client computers" on page 63.

Deploying an image

You can restore a computer and deploy a standard, Sysprep-enabled disk image with the **Deploy Image** task. All of the existing data and applications on the client are lost, and the computer is restored to the state of the standard image.

On Windows Server 2008, you might need to change the password on the client computer before logging on for the first time after this task runs. Sysprep clears the administrator password when it prepares a computer for imaging. You can avoid having to manually change the password by creating a custom answer file. The answer file should include a plain text password. You can then use the answer file while you deploy your images on remote computers.

See "Configuring the Sysprep imaging" on page 44.

See "About deployment tasks and jobs" on page 49.

If the computer has the Deployment plug-in installed, the computer configuration is saved and restored after the image is applied. The computer configuration contains the computer name, network settings, and domain.

See "About Imaging client computers" on page 63.

If Initial Deployment is used, you select the configuration settings to apply to the computer after it is imaged. To deploy a new computer that does not have an operating system, use Initial Deployment.

See "Deploying an image to new computers " on page 78.

If the computer is a member of a domain, supply the appropriate credentials to rejoin the domain.

You can create an image that retains its data and software by creating a backup image. You must create a deployment task before you can run it.

See "Creating an image" on page 69.

For Linux operating systems, deploying disk images and backup images does not fully support the resizer file system. Image deployment supports only the SUSE Ext3 file system. If you have a resizer partition, you must use the -raw switch when you image the partition to preserve its structure.

Linux IDE images should be deployed on computers having the Linux IDE disk. SCSI disk images should also be deployed on computers having the SCSI disk image.

To deploy an image

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 from the **Imaging** section:

Image Name	Enter the name of the image file to deploy. 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.

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. The HAL and the required drivers that Sysprep removed are then deployed to help the computer boot 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 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 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.

Ensure that the built in administrator is enabled if you want to perform sysprep imaging on Windows 7. By default, on Windows 7 the built in administrator is disabled.

8 Enter the credentials that are needed to join the client computer to a domain.

If the client computer was not on domain before the image was deployed, it does not come to domain even after the image is deployed. To bring the client computer to domain, you have to create the **System Configuration** settings.

See "Setting the system configuration" on page 45.

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

- **Partition**
- **Command-line**
- **File Preservation**
- **Multicasting**
- **HTTP**

See "Setting advanced Deploy Image options" on page 76.

10 Click **OK**.

If you deploy an image on a Linux client computer, you must reinstall the Automation folder on that client computer.

Setting advanced Deploy Image options

The **Advanced** option on the **Deploy Image** task lets you configure additional options.

You can also set up other imaging options for this task.

See "Deploying an image" on page 73.

Table 5-3 Advanced **Deploy Image** options

Option	Description
Partition	This setting determines what partitions are deployed. 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 same Preboot environment.

Table 5-3 Advanced **Deploy Image** options *(continued)*

Option	Description
Command-line	Lets you add command-line options for the imaging tool. For Ghost partition deployment, following command lines should not be used: `MODE,Size,SRC and DST values should not be used for command line.`
Multicasting	You can 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** . If the threshold count is 2, there must be at least two client computers and one master computer before multicasting is used in this session. Deployment Solution does not support Multicast and Unicast options simultaneously if you use the Ghost imaging tool.
File Preservation	You can specify the files and folders that you want to preserve when the image is restored. This option is not supported if the client computer has Linux operating system.
HTTP	Adds the credentials that are needed to deploy an image that was obtained from an HTTP site.

Restoring a backup image

The computers that you image are restored to the exact state they were in when the image was created. A backup disk image can be restored only to the computer from which it was captured.

Deployment Solution uses *%computername%* as the default name of the backup image.

You can use the **Advanced** settings to preserve any files that are on the disk.

See "About Imaging client computers" on page 63.

See "About deployment tasks and jobs" on page 49.

To restore a backup image:

1. In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**.
2. On the right pane, right-click **Jobs and tasks** and select **New** > **Task**.
3. On the **Create New Task** page, click **Restore Backup Image**.
4. Select the image name to restore.
5. (Optional) Click **Advanced** to specify additional parameters.

   The additional parameters include the following options:

   - Partition resizing settings
   - Command-line switches for the imaging engine (Ghost or RapiDeploy)
   - Files and folders to preserve in the target computer during an image restore
   - HTTP server settings

   Click **OK** to save your options.
6. Click **OK**.
7. Schedule the task.

   See "Scheduling a deployment task" on page 53.

Deploying an image to new computers

You can set up new computers using a standard image. You can then start those computers with an automation disk that loads the software to execute a predefined task server task. The predefined task can deploy a disk image and install software.

Table 5-4 Process for deploying new computers

Step	Action	Description
Step 1	Capture a Sysprep-enabled image for distribution to multiple computers.	For Windows, you can use Microsoft Sysprep to prepare images. Sysprep removes drivers, the security ID (SID), and other computer-specific settings. See "About Imaging client computers" on page 63.

Table 5-4 Process for deploying new computers *(continued)*

Step	Action	Description
Step 2	Create a **Deploy Image** task.	You can specify the Sysprep-enabled image that you captured and the system configuration that you want to apply to new computers. See "Deploying an image" on page 73. See "Setting the system configuration" on page 45.
Step 3	Add the **Deploy Image** task to your initial deployment menu.	You can add tasks to the start menu of a new computer. See "Configuring the initial deployment settings" on page 40.
Step 4	Reboot the client using PXE.	You can boot computers with PXE using a network interface. This process is independent of your hard disks or installed operating systems. See "About Pre-boot eXecution Environment (PXE)" on page 58.
Step 5	Start the new computer using the automation disk, and select the task that you created from the Initial Deployment menu.	A new computer is defined as a computer that is not known to the database. An Initial Deployment task can be used only on new computers.

Creating an Apply System Configuration task

You can create or update system configuration settings with the configuration editor. These settings are applied to computers after you deploy a disk image or apply a system configuration using a task server.

For computer names, host name can also use tokens. For example:%CustomerToken, %SERIALNUMBER%.

The credentials are either a local administrator account or a domain account (if you join the computer to a domain).

See "Setting the system configuration" on page 45.

To create an Apply System Configuration task

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 **Apply System Configuration**.
4. Specify a name for the task on the first field.
5. Select one of the following options:

Use a predefined system configuration	Select the relevant configuration from the drop-down list or click **New** to create a new configuration. You can also click edit to edit the system configurations. For more information on System Configuration settings: See "System configuration editor options" on page 46.
Restore system configuration using inventory data	If you select this option you have to provide the following credentials if the client computer is a member of a domain. ■ **Domain Name** ■ **User name** ■ **Password** ■ **Confirm Password**

6. Click **OK**.
7. Schedule the task.

   See "Scheduling a deployment task" on page 53.

   If you execute this task on a Linux client computer, ensure that you run the send basic inventory command on the client computer. This command updates the inventory details on the Symantec Management Platform.

Setting Advanced Deploy Image Options for multicasting

You can override the default settings for a single task. You can use the options that are specified under Advanced tab to specify the customized settings. The advanced option on the Deploy image lets you add the settings.

You can use the **Manage** view to change the settings.

Setting Advanced Deploy Image Options

1. In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks.**
2. In the left pane, right-click **Jobs and Task**and click **New >Task**.
3. On the create new task page, in the right pane, expand the **Deployment and Migration folder**.
4. Click**Deploy Image** in the task pane.
5. Click the **Advanced** tab
6. In the **Multicasting** tab, check**To override the default multicast settings, change the values below** to change the settings for multicast
7. Set the values for the options and click **OK**.

Chapter 6

Performing an OS installation

This chapter includes the following topics:

About OS installation

Deployment Solution provides the option to perform the automated OS installation for Windows and Linux executed over the network. This installation allows operating system to be installed in a remote and an unattended fashion, reducing the costs, and complexity of deployments. Users can remotely provision any desktop, laptop, or server with a single scripted installation regardless of computer hardware configuration. Scripted installations provide a reliable and a customizable method for deployment in heterogeneous hardware environments and an efficient way to build and maintain gold master configurations. Applications and files can also be integrated with scripted installations, enabling complete systems provisioning.

Client computer can also join domain without having inventory but inventory data option must be selected.FQDN must be used as domain credential. For example Symantec.com\user and not Symantec\user.

You can create an operating system package and decide what source files are included in that package. The source files include all of the files that are needed for a scripted install. You can use the **Install Windows OS** or **Install Linux OS** tasks to perform a scripted install for Windows or Linux.

See "Windows OS installation options" on page 88.

See "Performing a LINUX OS installation" on page 89.

You can add files to your package using the **OS Files** option in the **Settings** menu. You can provide a name, provide a description, and choose the platform for your package.

See "Adding OS files" on page 41.

You can also delete files from your package. Only the package that is in the database is deleted. If your physical files exist in other places, the files are not deleted from those locations.

See "About removing unwanted packages and resources" on page 107.

If after performing an OS installation duplicate resources are created, this is due to MAC address and name of the computer being changed simultaneously. This generally occurs for virtual computers as by default they use randomly generated MAC addresses, which can change. To avoid this, ensure that all virtual computers have statically defined MAC addresses before changing the Computer name or domain name.

Sample scripted OS job

You can create an OS installation job, which contains the following tasks.

See "About OS installation" on page 83.

The following sample task list assumes that the disk contained data previously and that it is known in the CMDB:

- **Reboot to PXE**
  Loads a preboot operating system so that other tasks can run.
  See "Creating a Reboot to task" on page 60.
- **Erase Disk**
  Wipes the disk clean, ensuring that all data and all partitions are erased.
  See "Erasing a Disk" on page 85.
- **Partition Disk**
  Configures the clean drive with a partition.
  See "Partition Disk options" on page 87.
- **Install Windows OS/Install Linux OS**

Runs the scripted install for the Windows or Linux operating system.
See "Windows OS installation options" on page 88.
See "LINUX OS installation options" on page 90.

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 cannot perform an Erase Disk task if you on a disk that is connected through a USB or FireWire interface.

See "About deployment tasks and jobs" on page 49.

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:

Remove partitions	Select the partition you want to delete from the disk selection drop-down list. This selection deletes the partition table. Select **Erase data** check box to delete the partition table with data.
Erase Disk	Select **System disk** for WinPE environment. Otherwise, select **All disk** to erase all the disks present. You must select the **Secure erase** check box.

See "Erase Disk options" on page 85.

6. Click **Ok**.

Erase Disk options

You can choose to erase a disk to reallocate it hardware. You can choose to delete the partitions of the disk or clean the entire system.

You can choose to erase only the system disk. Or, you can configure the task to erase all of the disks. The Erase disk task does not operate on any disk that is connected via the USB or FireWire interface

You must select the **Secure erase** check box to wipe the 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.

Creating disk partitions

You can use **Partition Disk** option to create partitions on your disk.

Before you perform a scripted OS installation, your drive must have partitions.

See "About OS installation" on page 83.

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.

See "Erasing a Disk" on page 85.

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 and click **OK**.

   See "Partition Disk options" on page 87.
7. On the **Create New Task** page, click **OK**.

Partition Disk options

You can run the **Partition Disk** task to create partitions on a disk drive.

See "About deployment tasks and jobs" on page 49.

You must create a deployment task before you can run it.

See "Creating disk partitions" on page 86.

You can configure the following options while creating this task.

Table 6-1 **Partition Disk** options

Option	Description
Is Secondary disk	The disk that you want to partition is a secondary disk.
Disk Number	The drive that the partition is created on.
Format	The format of the partition: **Fat32**, **NTFS**, and **EXT**.
Partition	The type of partition to create: **Extended**, **Logical**, and **Primary**. By default, **Extended** is selected.
Mark Partition as Active	The partition is active. This option is selected automatically for **Primary** partitions. For **Extended** and **Logical**, this option is disabled. If there are more than one primary partitions, then only one partition can be active at a time.
Size - Percent	The size of the partition as a percentage of the total drive.
Size - Fixed Size	The size of the partition as a specific size.

Performing a Windows OS installation

Before you perform the **Windows OS installation** task on bare metal computer, your hard drive must have the proper partitions. You might need to run the **Partition Disk** task first to create partitions on your hard drive.

Before you perform the **Windows OS installation** task on the managed computer, perform the **Erase Disk** task and follow it with the **Partition Disk** task. Also, ensure that the architecture of the **Automation Folder** on the managed client computer and the operating system to be installed is the same.

For more information:

See "Erasing a Disk" on page 85.

See "Creating disk partitions" on page 86.

To perform Windows OS installation

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.

   See "Windows OS installation options" on page 88.
6. Click **OK**

Windows OS installation options

You can run the **Install Windows OS** task to install the Windows operating system.

See "Performing a Windows OS installation" on page 87.

You can choose from several options while creating this task.

Table 6-2 **Install Windows OS** options

Option	Description
OS source	The source of your operating system. You can use the drop-down list to select a the sources of previously installed operating system. You can also add new OS packages by clicking **Add**. See "Adding OS files" on page 41.
Product Key	The license for the operating system. You can use the drop-down list to select a previously added license. You can also add licenses by clicking **Add**. See "Adding OS files" on page 41.
Install drivers from Driver Database during OS installation	Installs the missing drivers required for a successful installation.

Table 6-2 **Install Windows OS** options *(continued)*

Option	Description
Configuration	The configuration options are as follows: ■ **Use Inventory data to reconfigure computer** Uses the information that is stored in the CMDB to configure the computer for name and to join domain. Client computer can also join domain without an inventory but inventory data option must be selected. FQDN must be used as domain credential. For example, Symantec.com\User and not Symantec\user. ■ **Use default configuration settings** Uses the default settings. ■ **Configuration file** Uses a custom answer file.
Advanced	The advanced options. These options include a specific drive to install on the operating system. You can also set the region for the language and keyboard and the type of video settings to use.

Performing a LINUX OS installation

Before you run a Linux OS installation task, your hard drive must have the proper partitions. You might need to run the **Partition Disk** task first to create partitions on your hard drive.

See "Partition Disk options" on page 87.

You must create a deployment task before you can run it.

See "Creating disk partitions" on page 86.

Ensure that the package server is installed on the Symantec Management Platform, where the remote site server are installed. This lets you perform the task replication and package replication successfully.

Linux OS installation supports SCSI and SATA devices as Linux preboot recognizes SCSI and SATA devices only.

To perform a Linux OS installation

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 Linux OS**.
4. Specify a name for the task on the first field.
5. Select and enter the required information.

   See "LINUX OS installation options" on page 90.
6. Click **OK**.
7. Schedule the task.

   See "Scheduling a deployment task" on page 53.

After performing the OS installation if due to network issues or any other reason the client computer is not able to connect to Symantec Management Platform, the Symantec Management Agent is not installed. In this case, you have to manually install the Symantec Management Agent.

By default, the password of the client computer on which you have installed the Linux OS is set to altiris.

LINUX OS installation options

You can run the **Install Linux OS** task to install the Linux operating system. Linux OS installation only supports SCSI devices.

See "Performing a LINUX OS installation" on page 89.

You can choose from several options while creating this task.

Table 6-3 **Install Linux OS** options

Option	Description
OS Flavor	The list of OS versions for Linux.
OS File location	The location where the OS file is stored. You can choose from FTP or HTTP location and enter its path. If you are providing an HTTP location, ensure that Anonymous access is enabled. Otherwise, the **Linux OS installation** task fails.
Configuration File	The configuration that you want to use for the installation.

Table 6-3 **Install Linux OS** options *(continued)*

Option	Description
Installation code	The code required for installation.
Disk number	A drop-down list with the disk number to be used for installation.

Chapter 7

Capturing and distributing computer personalities

This chapter includes the following topics:

About capturing and distributing personalities

You capture and distribute a computer's personality. Personalities are the files that contain the user data and application settings. Personalities contain the documents, the registry settings, and the configuration files that are associated with applications. They also contain many other windows settings. Personalities are usually captured as part of an operating system migration or as a backup. Capture and distributing of personalities is not supported on Linux operating system.

You can choose what settings to transplant.

See "About migration settings" on page 95.

Capturing and distributing of personalities is only supported for Windows XP, Windows Vista, and Windows 7. Both 64-bit operating systems and 32-bit operating systems are supported.

See "Capturing computer personality" on page 96.

See "Distributing computer personality" on page 97.

You can distribute a personality through a self-extracting executable file that is called a Personality Package. You create the Personality Packages that can be used for multiple purposes.

Packages can include the desktop, printer, network, application settings (such as favorites and contacts), and entire directory structures for your computers. You can create the packages that contain the most used directories, documents, and settings for a group of computers. You can also create packages for individual users on a shared computer. A user can then install the Personality Package on a computer. After you complete the work, each user can then uninstall the package so the computer is ready for another user.

You can also perform a real-time migration from one computer to another. In real-time migrations, you can map users and their properties, create user accounts, and install applications.

Personality Packages are based on the templates that you can run from command-line instructions to automate operating system migrations. You can build and edit your own templates to define the settings, file, and options that you want for your Personality Packages.

See "About personality templates" on page 94.

Note: In a hierarchy, the Deployment Solution license must be installed on each Notification Server to manage personalities. Licenses for PC Transplant are not replicated to child Notification Servers.

About personality templates

Before you create a Personality Package, you must specify what type of information to migrate. You can provide this type of information in a personality template file.

See "About capturing and distributing personalities" on page 93.

A template file is a blue print to what needs to be captured. It contains information about the settings and files that you want to migrate. Using a template reduces errors and allows deployment jobs to automatically create packages.

See "About migration settings" on page 95.

When you create a job to capture personalities, you must use a template. If you haven't created a template yet, you can use one of the default templates that are included with Deployment Solution.

You can use one of the following files to create a template:

- `Template.exe`, located in the PCT subfolder of the Deployment share.
- `PCTEdit.exe`, located in the PCT subfolder of the Deployment share. Selecting the **Tools > Template Builder** option from the editor's menu lets you edit an existing template or create a new one.

The first template option is to select the type of users to migrate.

You can specify either local users or domain users.

- **Capture Local Users**
  Migrates the settings for local users. By adding the domain to the **Redirect to domain** field, you can also migrate users to pre-existing domain accounts.
- **Capture Domain Users**
  You can migrate all of the users in a domain by selecting the **Capture domain users** option. You can also choose to migrate specific users by adding the user in the source fields and the destination fields.

You can use your templates as a separate utility or as part of a Deployment Solution job.

See "About deployment tasks and jobs" on page 49.

A deployment job might automatically modify the following template settings:

- -qm switch
  The quiet minimized switch is used unless a token is specified for the name of the package.
- **Advanced** users
  The users that are specified in the job's **Advanced** option and the template's users are both used.
- Package path
  The path in the deployment job is used for the package instead of the path in the template.

About migration settings

You can choose what settings to migrate.

You can choose to migrate settings from the following categories:

- Computer desktop settings
  These settings include Control Panel settings, desktop colors, and background information.
- Individual files and folders
- Specific file types

- Network settings
  These settings include the computer and domain name, folder and drive share assignments, and drive mappings for Windows.
- Application settings
  These settings include the unique menu bar options for a particular application. However, you cannot migrate applications. A2i text files determine the application settings that can be migrated and include the `Word.a2i`, `MS Outlook.a2i`, and `WinZip.a2i` files. Over 65 A2i files are included with Deployment Solution. You can also create custom A2i files using the A2i Builder utility.

Personality templates determine the individual files and folders to migrate. The computer that you use to build the Personality Package registers the file types that you can choose to migrate.

See "About personality templates" on page 94.

You determine what desktop and network settings to migrate based on the text files that are called Settings Files. These files are included with Deployment Solution and include the `Dsktop*.ini` and `Ntwrk*.ini` files.

See "About capturing and distributing personalities" on page 93.

Capturing computer personality

You can capture a computer's personality with the **Capture Personality** task. You can also choose how much data to capture, whether the files are compressed in your package, and where to store your package.

See "About capturing and distributing personalities" on page 93.

See "Distributing computer personality" on page 97.

Personality Packages are stored in the `Program Files\Altiris\Altiris Agent\Agents\Deployment\Task Handler\PCTPackages` directory. This directory contains several folders that are named with GUIDs. After you create a personality, the package is located in one of these folders.

Deployment Solution includes templates for many common applications. It also provides tools to help you create templates for new and custom applications.

See "About deployment tasks and jobs" on page 49.

To capture user settings

1. In the Symantec Management Console, on the **Actions** menu, click **Deployment** > **Capture Personality**.
2. On the **Capture Personality** page, enter a name for the task.

3 Type a unique personality name and a description.

If you capture multiple personalities, you can use the %COMPNAME% token as the personality name. This token creates a unique name for each personality based on managed client computer name .

4 Browse to select a template for your personality.

See "About personality templates" on page 94.

5 Select **Create Vista compatible file (pkg)** check box if you want to distribute personality to a computer with Windows Vista operating and above mentioned operating system.

6 Enter the credentials to secure the personality.

7 Click **OK**.

8 Schedule the task.

See "Scheduling a deployment task" on page 53.

Distributing computer personality

You can restore or distribute a personality that you previously captured by using the **Distribute Personality** task. .

See "About capturing and distributing personalities" on page 93.

See "Capturing computer personality" on page 96.

Personality Packages are stored in the `Program Files\Altiris\Altiris Agent\Agents\Deployment\Task Handler\PCTPackages` directory. This directory contains several folders that are named with GUIDs. After you create a personality, the package is located in one of these folders.

See "About deployment tasks and jobs" on page 49.

To restore user settings

1 In the Symantec Management Console, on the **Actions** menu, click **Deployment** > **Distribute Personality**.

2 On the **Distribute Personality** page, type the name for the task.

3 Type the name of the personality that you want to use.

If you distribute multiple personalities, you can use the %COMPNAME% token as the personality name. This token creates a unique name for each personality.

You can also browse to the personality file that you want to use.

4 Type the command-line to distribute the personality to.

5 Type the password if the personality is password protected.

6 Click **OK**.

7 Schedule the task.

See "Scheduling a deployment task" on page 53.

Chapter 8

Copying files and folders

This chapter includes the following topics:

About copying files and folders

Deployment Solution provides you with the option to copy files and folders from local and UNC locations to one or more computers. You can also use this option to install copied files, such as .msi, .exe, .vbs, and so on. The copy file feature is supported in automation and in production environments.

See "Copying files and folders" on page 99.

See "Copying files and folders options" on page 100.

Copying files and folders

Copy file and folder options let you copy files and folders from one UNC and local computer location to client computers. When you copy a file that already exists on a client computer, the earlier version of the file is overwritten. It also provides you the option to install executables using the command line switch.

To copy files and folders

1. In the Symantec Management Console, on the **Manage** menu click **Jobs and Tasks**.
2. In the left pane, right-click **Jobs and Tasks** and select **New > Task**.

3 On the **Create New Task** page, in the right pane, expand **Deployment and Migration folder** and select **Copy File**.

4 Type a name for the task in the first field.

5 Select the required options.

See "Copying files and folders options" on page 100.

6 Click **OK**.

7 Schedule the task.

See "Scheduling a deployment task" on page 53.

Copying files and folders options

You can use the **Copy File** task to copy files and folders and install files and applications. You can copy the installation `.msi` or `.exe` file by running this task. Then, you can install the application by using command-line switches.

See "About deployment tasks and jobs" on page 49.

You must create a deployment task before you can run it.

See "Copying files and folders" on page 99.

You can configure the following options while creating this task.

Table 8-1

Table 8-1 Options on the **Copy File** page

Option	Description
Copy file or **Copy folder**	The item that is copied. You can include subfolders.

Table 8-1 Options on the **Copy File** page *(continued)*

Option	Description
Source	The source of the file to copy. You can provide a local path or select an existing file from the Deployment share. If you want to copy a file that is not on Notification Server, make sure that you provide the credentials for the file. For the UNC option to work, you must provide the domain (or computer name) with the user name in the `domain\username` format. Any changes you make to a local file are not automatically updated in the **Copy File** task. For example, you copy a local file using this task and then make changes to that file. If you rerun the task, the same file that you previously copied is used. You must modify your task first and select the same file to ensure that your changes are correctly copied.
Location	The location to the files to upload or the location of files that are already uploaded.
User name, **Password**, and **Confirm password**	The credentials that you need to obtain the source files.
Destination	The location where the files are copied to.
Command Line	The command-line instructions to execute the copied file on the client computer. You can execute the *.msi, *.vbs, *.cmd, *.bat, *.vbe, *.wsf, and *.exe files using the command-line switch.
User name, **Password**, and **Confirm password**	The credentials that are needed to execute the command-line instructions.

Chapter 9

Predefining computers

This chapter includes the following topics:

About predefining computers

By predefining computers, you can configure the computers that are not connected to the system or that are not managed, and then save their details. You can add or update the computer resources into Symantec Management Platform through a CSV (comma-separated values) file. If you remove or change the order of the columns in the sample CSV file, the execution of the predefined computer task fails.

The computer resource can be any of the following computers:

- Bare metal computer.
- Computer not on network.
- Computer that Symantec Management Platform does not discover.

After the computers are predefined, you can then import them and boot for deployment and maintenance tasks.

See "Importing predefined computers" on page 43.

See "Booting predefined computers" on page 104.

When the predefined computers are booted to the automation environment, you can perform the tasks of imaging and system configuration. Then, you can reboot the predefined computers to the production environment to resume live operations.

See "Referencing a sample CSV file" on page 104.

Referencing a sample CSV file

When you create a CSV file, use the `predefinedComputerTemplate.csv` file in the `C:\Program Files\Altiris\Notification Server\NSCap\bin\Win32\X86\Deployment\Sample\PreDefinedComputers` folder. The `predefinedComputerTemplate.csv` file provides a sample import template you can access to test the predefined feature.

Predefined computer supports MAC address only import for client computers.

To reference a sample CSV file

1. Open the `predefinedComputerTemplate.csv` file using a Microsoft Excel spreadsheet that lets you add values to each identified column.
2. Save the file as a CSV file to import to the Symantec Management Platform Configuration Management Database (CMDB).
3. Open and edit the CSV file in English locale only.

See "Importing predefined computers" on page 43.

See "Booting predefined computers" on page 104.

Booting predefined computers

After you have imported the predefined computers you can boot them to perform various deployment tasks. Once the predefined computers are booted, the basic inventory of the computers is sent to Symantec Management Platform. The booted predefined computer's entry is removed from the **Settings > Deployment > Predefined computers** grid.

You can perform the following deployment tasks after booting the predefined computers:

- Copy file.
- Create image.
- Deploy image.
- Restore backup image.
- Erase disk.
- Partition disk.
- Install Windows OS and Linux OS.
- Reboot to PXE.
- Reboot to automation.

- Reboot to production.

After booting the predefined computer, you are required to update its inventory details on the Symantec Management Platform server. To update the inventory details, you have to manually send the inventory from the booted predefined computer.

To boot predefined computers

1. Set a PXE image to respond to predefined computers.

   See "Configuring the PXE Server" on page 32.

2. Import the predefined computers.

   See "Importing predefined computers" on page 43.

3. Restart the imported predefined computers.

   The imported predefined computer is booted to the PXE Boot image that is specified in the **PXE Server Configurations** page.

Chapter 10

Removing unwanted packages/resources

This chapter includes the following topics:

About removing unwanted packages and resources

Removing unwanted packages and resources helps you to maintain and manage the storage location. It also eliminates the occurrence of an error when you select and execute a task on a client computer.

Deployment Solution lets you delete the disk images that you have created. When a disk image is created, an image package and an image resource for that disk image are also created. Hence, when you delete a disk image you also have to delete the image package and the image resource associated with it. You can remove the unwanted packages and resources by using the options available in the menu.

See "Deleting an image package" on page 108.

See "Deleting an image resource" on page 108.

Deployment Solution also lets you delete the scripted install packages and the copy file contents package.

See " Deleting a scripted install package " on page 109.

See "Deleting a copy file contents package" on page 110.

Deleting an image package

Image packages are created when you create a disk image. Both an image package and an image resource are created in addition to the actual image file.

See "About disk image packages" on page 67.

To delete all image references from the database, you also need to delete the image resource or personality resource.

See "Deleting an image resource" on page 108.

See "About removing unwanted packages and resources" on page 107.

To delete an image package

1. In the Symantec Management Console, on the **Settings** menu, click **All Settings**.
2. In the left pane, expand the **Settings** and the **Deployment and Migration** folders.
3. Click **Disk Images**.
4. Right-click the image package that you want to delete and click **Delete**.
5. On the **Delete Item** dialog box, click **OK**.

   The package is deleted.

Deleting an image resource

You must remove the image resource or personality resource to completely delete an image reference. These steps also apply to backup images and captured computer personalities.

To delete all image references from the database, you need to delete the image package first.

See "Deleting an image package" on page 108.

See "About removing unwanted packages and resources" on page 107.

To delete an image resource or personality resource

1. In the Symantec Management Console, on the **Manage** menu, click **Resource**.
2. From the **Group** drop-down menu, select **Image Resource** under **Software Component.**.
3. On the **Select Resource** page, click the image that you want to delete.
4. Click **OK**.

   The **Resource Manager** displays some of the details of the image that you selected. The path to the image file is not listed.
5. On the left pane, click **Delete**.

   The resource link is deleted from the database, but the actual image file is not deleted from disk. You need to delete the image file manually.

Deleting a scripted install package

You can delete the scripted install packages that are no longer required. These packages can be the ones with an incorrect operating system assigned to them. They can also be the ones for which all the scripted files were not saved due to system load.

Before you delete a scripted install package, ensure that there are no tasks associated with that package. Also, ensure that the jobs or tasks that are currently running are not associated with that scripted install package.

To completely remove a scripted install package, first delete it from the Symantec Management Platform, and then manually delete it from the Deployment Share. After deleting the scripted install package, update all the site servers to reflect the updated list of packages.

To delete a scripted install file

1. In the Symantec Management Console, on the **Manage** menu, click **Settings > All Settings**.
2. In the left pane, expand **Deployment and Migration > Scripted Install Files**.
3. Right-click the file you want to delete and select **Delete**.
4. Click **OK** on the confirmation message box.
5. On the Deployment Share, go to the following folder:

   ```
   \\localhost\Deployment\Task Handler\SOI
   ```
6. Delete the relevant scripted install package.

See "Deleting a copy file contents package" on page 110.

See “About removing unwanted packages and resources” on page 107.

Deleting a copy file contents package

You can delete the copy file contents packages that are no longer valid or required.

Before you delete a copy file contents package, ensure that there are no tasks associated with that package. If there are any associated tasks, delete them.

To completely remove a copy file contents package, first delete it from the Symantec Management Platform, and then manually delete it from the Deployment Share. After deleting the copy file contents package, update all the site servers to reflect the updated list of packages.

To delete a copy file contents package

1. In the Symantec Management Console, on the **Manage** menu, click **Settings > All Settings**.
2. In the left pane, expand **Deployment and Migration > Copy File Contents**.
3. Right-click the file you want to delete and select **Delete**.
4. Click **OK** on the confirmation message box.
5. On the Deployment Share, go to the following folder:

   ```
   \\localhost\Deployment\Task Handler\CopyFile
   ```

6. Delete the relevant copy file contents package.

See “ Deleting a scripted install package ” on page 109.

See “About removing unwanted packages and resources” on page 107.

Appendix A

Command-line switches

This appendix includes the following topics:

About command-line switches

The command-line switches are used during deployment of an image with Ghost and RapiDeploy imaging tools. In most cases, these switches apply to all versions of the Ghost executable. Any exceptions are noted in the switch description.

Table A-1 Ghost command line switches

Command-line switch	Description
-align = chs -align = 1mb	Lets you override the way in which the partitions are aligned when an individual partition or disk full of partitions is restored. This switch aligns the partition to the boundary as follows: **1** CHS: Aligns to a track or cylinder boundary **2** 1MB: Aligns with a boundary of 1 MB By default, a partition is aligned on the destination computer as it was on the source computer. **Note:** The 1MB alignment option supports Windows Vista.
-bfc	Handles bad FAT clusters when writing to disk. If this switch is set and the target partition is FAT, Symantec Ghost checks for and works around bad sectors, and all free sectors are verified. This option may slow Symantec Ghost operation substantially.

Table A-1 Ghost command line switches *(continued)*

Command-line switch	Description
-cns	Reverts the naming of spanned files to the system used by versions of Symantec Ghost prior to Symantec Ghost 6.5. If this switch is not used, then the naming of spanned files conforms to Microsoft application guidelines. You do not need to use this switch when reading an existing file. Use this switch when the first five characters in a file name must be unique. **Note:** Symantec Ghost supports long file names.
-fdsp	Preserves the signature bytes on the destination disk when performing a disk-to-disk or image-to-disk cloning operation
-fdsz	Clears the signature bytes on the destination disk. This is the default for disk-to-disk and image-to-disk operations.
-fis	Uses all available disk space when creating partitions. By default, Symantec Ghost often leaves a small amount of free space at the end of the disk. Because partitions must be aligned to cylinder boundaries, Symantec Ghost may leave up to 8 MB free even when -fis is specified.
-fmbr	Forces the disk to restore to a MBR-based disk.
-fro	Forces Symantec Ghost to continue cloning even if the source contains bad clusters
-ia	The image all switch forces Symantec Ghost to perform a sector-by-sector copy of all partitions. By default, when copying a partition from a disk to an image file or to another disk, Symantec Ghost examines the source partition and decides whether to copy just the files and directory structure or to do a sector-by-sector copy. If it understands the internal format of the partition, it defaults to copying the files and directory structure. Generally, this is the best option. However, if a disk has been set up with special hidden security files that are in specific positions on the partition, the only way to reproduce them accurately on the target partition is through a sector-by-sector copy. If you use this switch to create an image of a dynamic disk, then the image must be restored to a disk with identical geometry.
-ial	Forces a sector-by-sector copy of Linux partitions. Other partitions are copied normally

Table A-1 Ghost command line switches *(continued)*

Command-line switch	Description
-ib	The image boot switch copies the entire boot track, including the boot sector, when creating a disk image file or copying disk-to-disk. Use this switch when installed applications, such as boot-time utilities, use the boot track to store information. By default, Symantec Ghost copies only the boot sector and does not copy the remainder of the boot track. You cannot perform partition-to-partition or partition-to-image functions with the -ib switch
-id	The image disk switch is similar to -ia (image all), but also copies the boot track, as in -ib (image boot), extended partition tables, and unpartitioned space on the disk. When looking at an image with -id, you see the unpartitioned space and extended partitions in the list of partitions. The -id switch is primarily used by law enforcement agencies that require forensic images.
-ir	The image raw switch copies the entire disk, ignoring the partition table. This is useful when a disk does not contain a partition table in the standard PC format, or you do not want partitions to be realigned to track boundaries on the destination disk. Some operating systems may not be able to access unaligned partitions. Partitions cannot be resized during restore and you need an identical or larger disk
-limitswap	Limits the Linux swap space to 2GB.
-locktype= Type	Lets you lock an image file for use with a specific set of computers defined by the type chosen and the source computer. For example, ghost -locktype=P creates an image that can be used only on systems that have the same product name type as the source computer. On computers with multiple processors, the processorID bios lock option does not work as intended when running Ghost32.exe. In this situation, do not create or restore images with the -locktype parameter set to I. Other -locktype values work as intended.
-noindex	Prevents Symantec Ghost from creating an index when creating an image file. This slightly reduces the size of the image file and saves memory, but Ghost Explorer is much slower in reading the image file. This switch is useful if you are saving an image file from a large disk with very little memory.

Table A-1 Ghost command line switches *(continued)*

Command-line switch	Description
-noOSlayout	Prevents Ghost from updating the OS after a restore. By default, Ghost passes information about the restore to Windows, which then makes updates. This switch disables that function and preserves the disk exactly as restored
-ntc-	Disables NTFS contiguous run allocation.
-ntchkdsk	Sets the CHKDSK bit set on a copied NTFS volume. This causes Windows NT to check the integrity of the volume when it is started.
-ntexact	Attempts to arrange the restored NTFS volume in the same way as the source volume.
-pmbr	Specifies that the master boot record of the destination disk is to be preserved when performing a disk-to-disk or image-to-disk operation.
-preserveifexists	Preserves the specified files if they exist. The task does not fail if the specified files do not exist. To preserve files or directories other than the image file, the syntax is as follows: -preserveifexists=filepath[=newpath] [,filepath[=newpath]...] Each filepath can refer to an individual file or a directory. All files and subdirectories of a specified directory are preserved. If a file does not exist, then the restore fails. After a Clone step in a task, all preserved files are added back to the destination specified by the -preservedest=n switch, renaming them to newpath where specified. You must use the -preserveifexists switch with -preservedest.
-pwd and -pwd=x	Specifies that password protection be used when creating an image file. Use of a password does not securely encrypt the contents of the image. x indicates the password for the image file. If no password is given in the switch, Symantec Ghost prompts for one. You can enter a maximum of 10 alphanumeric characters.

Table A-1 Ghost command line switches *(continued)*

Command-line switch	Description
-split=x	Splits image file into x MB spans. Use this switch to create a forced-size volume set. For example, if you want to force smaller image files from a 1024-MB drive, you could specify 200-MB segments. For example: ghost.exe -split=200 This divides the image into 200-MB segments. If this switch is not used then an image is split at 2 GB in the following operations: • GhostCast • Peer-to-peer • Creating an image on a mapped-network drive If the operation runs locally on a FAT partition, then the image splits at 4 GB.
-sze	Sets the size for the destination partitions for either a disk restore or disk copy operation. When numbering partitions in the -sze switch, do not include the hidden Ghost partition. This switch is intended to be used in the Additional command line in the Console. All functionality of -sze switches is supported.
-szee	Forces Symantec Ghost to keep the sizes of all destination partitions the same size as in the source partition (no resizing). This switch can be used with or without the -clone switch.
-szef	Forces Symantec Ghost to keep the sizes of all destination partitions, except for the first one, the same size as in the source partition. The first partition uses the remaining disk space. This switch can be used with or without the -clone switch.
-szel	Forces Symantec Ghost to keep the sizes of all destination partitions, except for the last one, the same size as in the source partition. The last partition uses the remaining disk space. This switch can be used with or without the -clone switch.
-z	Runs compression when saving a disk or partition to an image file. The greater the compression, the slower the transmission, as follows: • -z or -z1: Low compression (fast transmission) • -z2: High compression (medium transmission) • -z3 through -z9: Higher compression (slower transmission)

Table A-2 Command line switches with or without -cns

With-CNS	Without -CNS
Filename .gho	Filename .gho.
Filename .001	Filen001.ghs
Filename .002	Filen002.ghs

Table A-3 RapiDeploy Command-line Switches

Command Line Switch	Description
-?	Shows command-line help.
-bsl:[maximum bandwidth]	Determines the maximum bandwidth to be used by the multicasting session. Example To limit the bandwidth to 5 Megabits per second, type rdeploy -bsl:5
-c[compression mode]	Sets the compression mode for image creation. Default balanced Modes • off (turn compression off) • size (make smallest image size with slight speed penalty) • speed (make a less compressed image in less time) • balanced (make a reasonable compressed image with a reduced speed penalty). Example To optimize image creation for speed, type rdeploy -mu -f[filename] -cspeed
-cfgfile:[filename]	Sets the configuration filename (default is lastrun.cfg). The configuration file provides information for post configuration. The default configuration file is lastrun.cfg that can be edited in a text editor with the specific information needed for the computer. This command is useful if you want to run imaging in a batch file using configuration information saved previously by the RapiDeploy program. (If you select the option to save settings in the RapiDeploy program, a configuration file will be created with the name lastrun.cfg.) You can rename lastrun.cfg and specify it in your batch file to apply configuration settings. Example If you have run RapiDeploy and have chosen the option to save configuration settings, you could rename lastrun.cfg to laptop1.cfg and use it in a batch file by typing the following: rdeploy -md -f[filename] -cfgfile:laptop1.cfg You can also put configuration files in a shared directory and load them from the network. See also -m[mode], -f[path & file name]
-checkdisk	Marks the partitions dirty so that checkdisk will run after the image is restored (works on all file systems). Note Post configuration will fail when this switch is used. Example rdeploy -mu -f[filename] -checkdisk See also -m[mode], -f[path & file name]

Table A-3 RapiDeploy Command-line Switches *(continued)*

Command Line Switch	Description
-d[hard disk number]	Specifies which hard disk to read from or write to, depending on whether you are uploading or downloading. This switch is used for computers that have more than one hard disk. Default Disk 1 Examples To download an image to disk 2, combine with the -md switch and type rdeploy -d2 -md -f[filename] To create an image from disk 2, combine with the -mu switch and type rdeploy -d2 -mu -f[filename] See also -m[mode], -f[path & file name]
-f[path & file name]	Used with the -m switch. In upload mode, it specifies the filename and location for storing an image file. In download mode it specifies which image file to restore. To create (upload) a regular image file, use an .img extension. To create a self-extracting executable image file, use an .exe extension Examples To upload an image file to disk g:, type rdeploy -mu -fg:\images\win98.img To upload a self-extracting executable image file, type rdeploy -mu -fg:\images\win98.exe See also -m[mode], -f[path & file name]
-forcebw	Forces the BootWorks partition to be restored. Use this switch when using PXE or to overwrite an existing BootWorks partition on the hard disk with the BootWorks partition in the image. Example To restore an image and have the BootWorks partition in the image replace an existing BootWorks partition on the hard disk, type rdeploy -md -f[filename] -forcebw See also -m[mode], -f[path & file name]
-forcegui	Forces the wizard to appear even if it doesn't have to. Use this switch to force the wizard to appear so that you can view or edit settings for each computer. Example To restore an image but first view or make changes in the settings, type rdeploy -md -f[filename] -forcegui See also -m[mode], -f[path & file name]
-forceoem	Forces the OEM partition to be restored. Use this switch to overwrite an OEM partition on the hard disk with an OEM partition in the image. Example To restore an image and have the OEM partition in the image replace an existing OEM partition on the hard disk, type rdeploy -md -f[filename] -forceoem See also -m[mode], -f[path & file name]

Table A-3 RapiDeploy Command-line Switches *(continued)*

Command Line Switch	Description
-frm:[name]	Specifies a FIRM file that contains a list of FIRM commands to be executed after a restore. A FIRM file is a text file containing FIRM commands to execute. Example After a computer has received an image, you can copy a file that is not in the image to the computer. For example, you may want to copy a .cfg file that a computer needs but is not in an image. rdeploy -md -f[filename] -frm:firm.txt In this example, you would have two files: • The FIRM file that includes the FIRM command to perform the copy, firm.txt • The file that you want copied to a computer, sample.cfg Both of these files must be in the RapiDeploy/FIRM application folder. The FIRM file, firm.txt, could have the following FIRM command: copy sample.cfg c:\sample.cfg In this example, after the image has been received, sample.cfg is copied from the RapiDeploy application folder on the server to the computer in the specified folder.
-h	Shows command-line help.
-i:[20..25]	Sets screen resolution. For information on setting VESA modes, see -ve:[31.34] Example To set screen resolution to VGA mode 23 (640x480x16), type rdeploy -i:23
-i[IDnumber]	Sets session ID when sending an image file to more than one computer. Use this switch with multicast sessions so the Master PC can identify Client PCs in the same session. Example To send an image to 10 Client PCs, type rdeploy -mdb -f[filename] -s9 -i5000001 Note -i500001 is given as an example. This value is an example of what the Deployment Server console would send for a session ID. See also -m[mode], -s[number of Client PCs], -f[path & file name]
-ip:[n.n.n.n:p]	Sets the multicast IP address and port. This can be used for two purposes: 1) To allow multicasting through a router that is set up to use a different multicast IP address, and 2) to separate multiple multicasting sessions more efficiently. If you are manually running multiple multicast sessions, you can specify a different multicast IP address for each session to allow the NIC itself to filter out unwanted packets from other sessions. This speeds up all sessions involved. Important Remember to put the port number at the end of the IP address after a colon. Example rdeploy -mdb -f[filename] -s9 -ip:224.2.0.3:401 See also -m[mode], -s[number of Client PCs], -f[path & file name]

Table A-3 RapiDeploy Command-line Switches *(continued)*

Command Line Switch	Description
-kap	Prevents rdeploy.exe from overwriting any existing partitions on the hard disk.
-kp[1-31]	(Download only) Prevents rdeploy.exe from overwriting a specified partition. n=partition 1 - 31 Example To keep partition 2 from being overwritten during imaging, type rdeploy -md -f[filename] -kp2 See also -m[mode], -f[path & file name]
-m[mode]	Sets the operating mode. Modes • u (Upload image) • d (Download image) • b (Multicast only) • ub (Upload and multicast image) • db (Download and multicast image) • client (Client mode) Examples To upload an image, type rdeploy -mu -f[filename] To designate a computer as a Client PC, type rdeploy -mclient See also -f[path & file name], -i[IDnumber]
-makeimx	Minimizes the number of disk swaps that occur when restoring a hard disk image that has been split across multiple CDs or other storage media. This switch causes RapiDeploy to create an .imx (IMage IndeX) file which contains data that may reside on other CDs. If RapiDeploy has access to the .imx file, it will not prompt you to insert any CD more than once. Use the -makeimx switch when you create an image. However, no switches are needed when restoring the image. Once the split image file has been created and you are ready to burn the image to CDs, put the .imx file on the CD with the first .img split image file. Subsequent split image files do not require the .imx file to be placed on the CD.
-mconv	Used with the -f switch to convert an existing image file (.img) to a self-extracting .exe file. (Does not upload or download; just converts the file.) Example To convert a file named WIN98.IMG, type rdeploy -mconv -fwin98.img See also -f[path & file name]
-mig:[filename]	Used to specify a migration file. Prompts before overwriting the drive. This is used mainly by PC Transplant Pro.
-nobw	Makes sure that a BootWorks partition does not exist in the destination, is not on the disk when restoring, and is not in the image when creating. Example To remove an existing BootWorks partition from a hard disk and exclude the BootWorks partition from being downloaded with an image, type rdeploy -md -f[filename] -nobw See also -m[mode], -f[path & file name]

Table A-3 RapiDeploy Command-line Switches *(continued)*

Command Line Switch	Description
-nocancel	Doesn't allow the user to cancel the imaging task.
-nooem	Makes sure that an OEM partition does not exist in the destination, is not on the disk when restoring, and is not in the image when creating. Example To remove an existing OEM partition from a hard disk and exclude the OEM partition in an images from being restored, type rdeploy -md -f[filename] -nooem See also -m[mode], -f[path & file name]
-noprompt	Prevents any need for user interaction, for example, clicking OK after an error occurs. This is very useful in scripting situations where there won't be a user present to hit a key.
-nt64k (Download only)	(NT computers only) Enables a 64K cluster size with a FAT16 partition. This allows you to resize a FAT16 partition up to 4 GB rather than the normal 2 GB limit. Example To change the size, type rdeploy -md -f[filename] -nt64k See also -m[mode], -f[path & file name]
-p[partition]	Specifies which partition to process. Parameters • n Number (1-31) uploads the partition (each partition must be designated separately) • b images the BootWorks partition (works for both hidden and embedded types) • oem images the oem partition Examples To upload an image of partition 2, type rdeploy -mu -p2 -f[filename] To upload multiple partitions, type rdeploy -mu -p2 -p3 -p4 -f[filename] To upload the BootWorks partition, type rdeploy -mu -pb -f[filename] To upload the oem partition, type rdeploy -mu -poem -f[filename] See also -m[mode], -f[path & file name]
-password:[pwd]	Specifies the image password. Passwords are case sensitive. Example To create a password-protected image file, type rdeploy -mu -f[filename] -password:Altiris To restore that file, type rdeploy -md -f[filename] -password:Altiris See also -m[mode], -f[path & file name]
-raw	Treats all partitions as raw. The Master PC reads and images a partition by sectors rather than by files. This switch makes the image drive geometry dependent (must have the same heads, cylinders, and tracks as the image source). Used mostly by Altiris Technical Support for troubleshooting, or it could be used to make sure that any extra data residing outside of the file system is included in the image.

Table A-3 RapiDeploy Command-line Switches *(continued)*

Command Line Switch	Description
-restoresig	Causes RapiDeploy to restore the unique disk signature in the MBR of the hard disk from which the image was created. Normally, RapiDeploy does not transfer the disk signature to the target computer when deploying an image. This switch can be used when restoring an image to the same or similar systems. The -szf switch may be needed in combination with the -restoresig switch. Example One This -restoresig switch has been added to the Distribute Disk Image job in the XP Embedded folder in the Samples folder to protect the Write Filter Partition. It is required for all Restore Image jobs for XPe Thin Clients. Example Two The -restoresig switch is needed when restoring an image to a Citrix Metaframe Server to preserve the alternate drive mappings. In this situation the -szf switch is also required. Note This switch will function only if no production partitions are being preserved on the hard drive when deploying the disk image.
-s[number of Client PCs]	Specifies the number of Client PCs included in a multicast session. When the Master PC detects the specified number of Client PCs, it automatically starts the multicast session. The number specified does not count the Master PC. Example To set the number of Client PCs that will be connecting to the Master PC in a multicast session to 9 computers, type rdeploy -mdb -f[filename] -s9 See also -m[mode], -f[path & file name]
-span	Prompts between each piece of an image file (if set when using the -split command), allowing you to insert new media. Example To prompt between each file in the image set, type rdeploy -mu -f[filename] -split:500 -span See also -m[mode], -f[path & file name]
-split:[n]	Breaks an image into multiple files of a specified size during an upload (in megabytes). Example To set the file size to 500 MB, type rdeploy -mu -f[filename] -split:500 See also -m[mode], -f[path & file name]
-szf	Use this switch to set fixed sizing for all partitions. By using this switch, RapiDeploy will use the original sizes that existed on the computer from which the image was created. Example If the original size of the partition to be downloaded was 250 MB and you want the destination partition to remain 250 MB, use the -szf switch. If the target disk has 500 MB of free space, you'll have a 250 MB fixed partition and 250 MB of free space.

Table A-3 RapiDeploy Command-line Switches *(continued)*

Command Line Switch	Description
-sz[parameter]	Resizes partitions during imaging. Syntax rdeploy -sz[#]:[x{m|p}] where # is the partition number and x is the size based on the number of megabytes or a percentage. Parameters • [x]m (Resize partitions in megabytes) • [x]p (Resize partitions as a percentage of hard disk size for primary partitions or the percentage of the extended partition for logical drives) Examples If the size of partition 2 being downloaded is 300 MB and you want it to fit in half of the 500 MB of disk space on the client disk, type rdeploy -sz2:50p -md -f[filename] This resizes the 300 MB partition to 250 MB, leaving the other 250 MB unused. You can set the target size for multiple partitions on the same command-line by including multiple instances of the switch: rdeploy -sz1:200m -sz2:50p -md -f[filename] See also -m[mode], -f[path & file name]
-text	Run in text mode instead of GUI mode. To use this switch, all settings must be specified at the command-line. Examples rdeploy -md -f[filename] -text or rdeploy -mu -f[filename] -text If you want to save a list of command-line parameters to a text file, you can use the -text parameter rdeploy -? -text > rdparams.txt See also -m[mode], -f[path & file name]

Table A-3 RapiDeploy Command-line Switches *(continued)*

Command Line Switch	Description
-threshold:[n]	This option applies only to the “Restore and Send” (-mdb) mode. We have found that when using a small number of clients, it is faster to perform individual downloads on each client than it is to multicast to all of them. There is a point where it becomes more efficient to multicast than it is to perform individual downloads. This “threshold” is where it becomes faster to multicast than to do individual downloads and can be specified by the -threshold:[n] command line parameter. Depending upon the network environment, this number may vary. You should perform a few tests to pick a good threshold value for your network. It may be a small number, like four, or it could be much larger, like 15. Once you have found this threshold value, you can specify this number on the command line and then RapiDeploy will, depending on the number of clients that connect, have them do individual downloads or have them multicast. The number [n] specifies the minimum number of clients that will need to connect to the master in order for it to multicast. For example, if you specify -threshold=5, and four or fewer clients connect to the master PC, it will have them all do individual downloads of the image. If five or more clients connect to that master, it will multicast to them. This becomes more important when multicasting across subnets with a router that does not support multicasting. If you start one master and nine clients (10 PCs total), three of which are on one side of the router and seven of which are on the other side, RapiDeploy will detect that there are only three on one side of the router and do individual downloads to them. It will also detect that seven are on the other side and multicast to them. RapiDeploy does all of this automatically. All you must supply is the threshold value to let RapiDeploy determine when it should multicast or not. Example Suppose you have determined that the threshold value for your network is five. In other words, you have found that multicasting from one master to five or more clients is faster than doing individual downloads to those clients and the master. You could then specify the following threshold value on the command line: rdeploy -mdb -f[filename] -s9 -threshold:5 See also -m[mode], -f[path & file name], -s[number of Client PCs]
-ve:[31.34]	Set VESA screen resolution. Example To set screen resolution to VESA mode 31 (640x480x256), type rdeploy -ve:31

Table A-3 RapiDeploy Command-line Switches *(continued)*

Command Line Switch	Description
-w[n]	When multicasting, specifies the maximum number of minutes to wait for Client PCs to connect. If all Client PCs connect, it will start right away. Default: 5 minutes (or until the specified number of Client PCs is connected). Example To set the timeout to wait for PC Clients to 10 minutes, type rdeploy -w10 -mdb -f[filename] -s9 See also -m[mode], -s[number of Client PCs]
-x	Causes the image to be saved as a self-extracting file. This setting will automatically be set if the image file name specified by the -f parameter ends with .EXE.

Appendix B

Troubleshooting

This appendix includes the following topics:

Troubleshooting

Table B-1

Table B-1 Troubleshooting

Issue	Description	Workaround
The following error message occurs when you create an image over HTTP with the -ID switch: `Not enough space on destination drive. Spanning is not supported on this drive.`	When you create a sector-by- sector image over HTTP, where HTTP is configured on Windows 2003 32-bit, IIS 6.0 displays the error message: Not enough space on destination drive. Spanning supported on this drive.	■ Use -split switch when you create image, where -split size is less than 2GB. ■ Configure HTTP on 64-Bit Windows.

Table B-1 Troubleshooting *(continued)*

Issue	Description	Workaround
Device in the Device Manager shows an exclamation mark after DA-SOI	When DA-SOI for Non critical drivers is executed,all the DeployAnywhere and scripted OS installations are performed. However when the operating system is up, the devices in the device manager appear with an exclamation mark and cannot be used. When the same drivers are applied to the device manually , the following warning/error message occurs: driver failed in windows logo test	If the unsigned drivers show an exclamation mark for the devices, use the following tag entry in the unattended answer file: DriverSigningPolicy
An error occurs when you join a Vista computer to a domain	You clone a Vista computer using an image that you prepared with Sysprep. Apply configuration changes. When you try to join the computer to a domain, the following error occurs: Windows can't complete the installation	Join the computer to a domain using a different task after the Clone task.
Preserved files on Vista computers have incorrect names	Windows Explorer (Vista) may not show the correct name for a folder that is preserved and renamed after a Clone task. This problem occurs if the renamed folder contains a copy of desktop.ini.	Find and delete the hidden file named desktop.ini inside the affected folders. Windows Explorer should then correctly display the folder name.

Table B-1 Troubleshooting *(continued)*

Issue	Description	Workaround
CRC files created by Symantec Ghost return a false result	By default, Symantec Ghost informs the operating system about the disk layout after a clone. However, that might cause the CRC files created by Symantec Ghost to return a false result. The false result could be that disks are not identical when they are identical. For example, after an image -to-disk restore, a CRC32 verify that operation might return an inaccurate CRC result because under WinPE, the source disk remains mounted by windows. Therefore, a CRC create on the source disk and then a verification on the destination disk may return an inaccurate CRC result because WinPE can change the source drive. The -noOs switch prevents ghost from updating the operating system with the destination disk changes. The source is mounted by Windows and therefore the CRC value may change due to system file changes by Windows and therefore the CRC value may change due to system file changes by Windows.	If the source image and destination disk have similar partition layouts, then be sure the system from mounting a file system driver once the clone is complete. This can happen on similarly partitioned disks even when you use the -nooslayout switch.

Table B-1 Troubleshooting *(continued)*

Issue	Description	Workaround
In IE8 native mode, the credentials on the Deploy Image task disappear when you type the credentials on the Deploy Image task and click Advanced.	In IE8 native mode, if a user types the credentials on Deploy image task, and clicks on **Advanced** tab, the credentials on Deploy image task does not appear.	Use the IE7 compatibility view in an IE8 Web browser. The credentials appear even after you click Advanced.

Table B-1 Troubleshooting *(continued)*

Issue	Description	Workaround
The **WHOAMI** does not get overwritten and PXE listens on the IP addresses that it picks up at startup.	PXE is not binding to the given IP address when the Symantec Boot Services server has two NIC cards installed on it.	

Table B-1 Troubleshooting *(continued)*

Issue	Description	Workaround
		This workaround is based on the following conditions: ■ Symantec boot services server is running on win2k8R2. ■ Symantec boot services server has two active NICs. ■ DHCP server and Symantec boot services server are bound on the same NIC. Assuming that the two NICs are A and B, perform the following to make the Symantec boot services server operational: ■ If you want to use the NIC B for SBS, you need to check the binding preference of this card. Perform the following steps on 2k8 R2 computer: Go to **Network > Properties> Change Adapter Settings**Both A and B NICs are present here. ■ On this window (network connections), press Alt (keyboard option).Then the file menu options are visible. Select the **Advanced** menu and click **Advanced Settings** . Change the connections order so that NIC B is set to the first row in the list. Click **Ok** to save the changes. You have changed the binding order of the NIC on your computer. ■ Now check the binding of the DHCP server and clicking the DHCP server by **Start > Run > dhcpmgmt.msc**. Click on the + option in the

Table B-1 Troubleshooting *(continued)*

Issue	Description	Workaround
		left pane so that the ipv4 and ipv6 options are visible. Then, right-click on the host name and click on the **Add/Remove** bindings menu. You can see the server Bindings properties window. Click on NIC B so that the binding can be set to IP of NIC B only. Then, click **Ok** to save the changes.
During Installation for Plug-in, a package is rolled out before the maintenance window starts on the client computer when Run once ASAP in maintenance window only is checked in	You cannot install the Deployment Solution plug-in in a maintenance window by using the **Run once ASAP** in maintenance window only option.	You are required to create a schedule using the **Add Schedule** option.

Table B-1 Troubleshooting *(continued)*

Issue	Description	Workaround
PXE-E77 error is received when the client computer is booted to a PXE image	If PXE images were created when SBS services were not running, you receive an error when you boot the client computer to that PXE image. The error that is received is PXE-E77.	Verify that all SBS services are running. If any of the following four services is not running, then start it manually: ■ Symantec netBoot interface ■ Symantec netBoot mtftp ■ Symantec netBoot NSiSignal ■ Symantec netBoot Server When the services are started, on the Deployment Solution console, click **Settings > Deployment > Create Preboot Configurations**. Select all the PXE images that were created when the SBS services were not running and click **Recreate Preboot environment** to recreate them. To prevent this issue from occurring, ensure that the PXE services are started and set to automatic before you create any preboot configurations.
The Deploy Image task gets error during the XP GHO image import when the Windows XP operating system boots with DeployAnywhere	When you execute the DeployImage task with the **DeployAnywhere** option enabled on a Windows XP computer, you encounter a non-functioning of the keyboard and mouse when booting the operating system. This problem does not recur frequently	You are required to connect to a different USB keyboard to continue with the installation.
The computer does not connect to the domain when Join Domain option is used from the OS install page	The computer does not connect to the DeployAnywhere domain when **Join Domain** option is used from the operating system install page.	**Join Domain** task can be performed using **Apply system configuration** task.

Table B-1 Troubleshooting *(continued)*

Issue	Description	Workaround
The Create Image task fails on Linux preos computer if the image name contains space	The **Create Image** on HTTP server fails if the image name contains space.	The image name must not contain any space.

Index

D

P

R

S

T

U

V

W