Symantec™ Deployment Solution 8.5 powered by Altiris™ technology User Guide
Legal Notice

Copyright © 2018 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, the Checkmark Logo and are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party (“Third Party Programs”). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Please see the Third Party Legal Notice Appendix to this Documentation or TPIP ReadMe File accompanying this Symantec product for more information on the Third Party Programs.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

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

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

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

Symantec’s support offerings include the following:

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

For information about Symantec’s support offerings, you can visit our website at the following URL:

support.symantec.com

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

Contacting Technical Support

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

support.symantec.com

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

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

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

**Licensing and registration**

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


**Customer service**

Customer service information is available at the following URL:


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

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

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

<table>
<thead>
<tr>
<th>Region</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asia-Pacific and Japan</td>
<td><a href="mailto:customercare@symantec.com">customercare@symantec.com</a></td>
</tr>
<tr>
<td>Europe, Middle-East, and Africa</td>
<td><a href="mailto:semea@symantec.com">semea@symantec.com</a></td>
</tr>
<tr>
<td>North America and Latin America</td>
<td><a href="mailto:supportsolutions@symantec.com">supportsolutions@symantec.com</a></td>
</tr>
</tbody>
</table>
Symantec™ Deployment Solution 8.1 powered by Altiris™ technology User Guide

Legal Notice

Copyright © 2018 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, the Checkmark Logo and Altiris and Altiris or Symantec trademark used in the product are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party (“Third Party Programs”). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Please see the Third Party Legal Notice Appendix to this Documentation or TPIP ReadMe File accompanying this Symantec product for more information on the Third Party Programs.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

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

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

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

Symantec’s support offerings include the following:

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

For information about Symantec’s support offerings, you can visit our website at the following URL:

support.symantec.com

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

Contacting Technical Support

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

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, DVDs, or manuals
Support agreement resources

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

Asia-Pacific and Japan                      customercare_apac@symantec.com
Europe, Middle-East, and Africa             semea@symantec.com
North America and Latin America            supportsolutions@symantec.com
Technical Support ............................................................................................... 4

Technical Support ............................................................................................... 9

Chapter 1 Introducing Deployment Solution ................................................. 17
  About Deployment Solution ................................................................. 17
  Components of Deployment Solution ................................................... 18
  About SSL communication in Deployment Solution .......................... 22
  About types of boot environments in Deployment Solution .............. 24
  Where to get more information ......................................................... 26

Chapter 2 Installing and uninstalling components ...................................... 29
  Preinstallation requirements for Deployment Solution .......................... 29
  Preparing site servers for Deployment Solution ..................................... 30
  Installing and uninstalling Deployment Solution components ............ 32
  Installing Network Boot Service on site server .................................... 35
  Installing and uninstalling Deployment Plug-in on client computers .......... 36
  Installing and uninstalling Automation Folder on client computers .......... 39
  Upgrading Deployment Solution components ...................................... 45

Chapter 3 Setting up client computers .................................................... 47
  About types of client computers in Deployment Solution .................... 47
  About predefined computers in Deployment Solution ......................... 48
  About supporting Mac computers ....................................................... 50
  Prerequisites for Mac computer setup ............................................... 51
  Setting up unknown client computers ................................................. 52
    Preparing unknown computers to boot with WinPE image .................. 54
    Preparing unknown computers to boot with LinuxPE ....................... 56
    Booting an unknown Mac computer in NetBoot environment ............ 58
    Performing tasks in preboot environment for Windows computers .......... 60
  Setting up predefined computers ...................................................... 62
    Referencing a sample CSV file ...................................................... 63
How to image a Windows 10 (1607) Anniversary update computer?

Chapter 6 Installing an operating system

About supported OS installed using Deployment Solution
Installing Windows OS on client computers
  Installing a Windows OS using Deployment Solution
  Erasing a Disk
  Creating disk partitions
  Adding OS licenses
  Adding or importing OS files
  Adding drivers to the Preboot database
  Adding drivers to the DeployAnywhere database
Installing Linux/ESX OS on client computers
  Installing Linux/ESX OS using Deployment Solution
Installing Mac OS using Deployment Solution
  Launching Symantec's Mac pre-OS Creation Utility
  Booting Mac computers with NetBoot image
  Installing Mac OS on an unknown computer
  Installing Mac OS on a predefined Mac computer
  Installing Mac OS on a managed computer
Sample scripted OS job

Chapter 7 Managing tasks and jobs

About deployment tasks and jobs
Deployment Solution task support matrix
Creating a deployment task
Combining tasks into a job
Scheduling a deployment job or task
Verifying the task status
Creating a Boot To task
Changing system configuration of computers in Deployment Solution
  Copying files and folders
  Adding drivers to the Preboot driver database
  Configuring the initial deployment settings
  Adding or importing predefined computers
  Creating system configuration settings
  Creating or modifying tokens in Deployment Solution
    About predefined tokens in Deployment Solution
    Adding tokens for deployment tasks
  Configuring multicast options to deploy image
Chapter 8  Capturing and distributing computer personalities ................................................................. 224
  Capturing and distributing personality .............................................. 224
  About capturing and distributing personalities ............................... 226
  About personality templates ........................................................ 227
  About migration settings ............................................................ 228
  Capturing a computer's personality ......................................... 229
  Distributing a computer's personality ........................................ 230

Chapter 9  Removing unwanted packages/resources ....................... 232
  About removing unwanted packages and resources ...................... 232
  Deleting an image package ...................................................... 233
  Deleting an image resource ..................................................... 233
  Deleting a scripted install package ............................................ 234
  Deleting a copy file contents package ........................................ 234

Appendix A  Command-line switches .................................................... 236
  About command-line switches ................................................ 236
  About command-line switches for DeployAnywhere.exe .................. 240

Appendix B  Location of tools and packages ........................................ 243
  About location of Deployment Solution tools ............................ 243
  About location of Deployment Solution packages ....................... 244

Appendix C  Troubleshooting ............................................................... 246
  Troubleshooting Tip: General installation and configuration .......... 246
  Troubleshooting Tip: Imaging and Install OS task ....................... 247
  Troubleshooting Tip: PXE and automation environment ................ 251
  Troubleshooting Tip: Driver database management ....................... 252
  Troubleshooting Tip: Client Communication and Package Download
  Issues ...................................................................................... 253
  Troubleshooting Tip: Upgrade issues ........................................ 254

Appendix D  Answer files ....................................................................... 256
  About Windows and Linux answer files .................................... 256
  About Mac configuration file .................................................... 258

Glossary .......................................................................................... 260
Index ................................................................................................................... 262
Introducing Deployment Solution

This chapter includes the following topics:

- About Deployment Solution
- Components of Deployment Solution
- About SSL communication in Deployment Solution
- About types of boot environments in Deployment Solution
- Where to get more information

About Deployment Solution

Deployment Solution lets you integrate standard deployment features with Symantec Management Platform. The solution 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 migrate to the latest Windows version; migrates user data, personality settings, 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 such as Windows, Linux, and Mac 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-based and scope-based security to secure management features from unauthorized personnel.

■ Supports the WinPE, LinuxPE, and Mac 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 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.

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 1-1 Deployment Solution components

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deployment Plug-in</td>
<td>The Deployment Plug-in is installed on the client computers on which you want to execute deployment tasks. This plug-in lets you create and deploy disk images, perform remote operating system (OS) installation, change system settings, and migrate the personality settings. You can enable the Symantec firewall on the client computer and enable the Windows firewall on the Notification Server. However, to install the Deployment Plug-in by pushing it to computers, you need to disable one of these firewalls. See “Installing and uninstalling Deployment Plug-in on client computers” on page 36.</td>
</tr>
<tr>
<td>Deployment site server component</td>
<td>The Deployment Site Server Component was packaged with previous versions of Deployment Solution and was installed on the site servers. From the Deployment Solution 7.5 release onwards, installation of this component is deprecated, whereas, you can use the Upgrade policy to upgrade the older versions of this component.</td>
</tr>
</tbody>
</table>
### Table 1-1  Deployment Solution components (continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
</table>
| Automation folder | The automation folder is installed on a client computer and stores the preboot environment of a specific operating system. The preboot environment that is setup by the automation folder is also known as the automation environment.  

The automation folder can be installed on the client computers of Windows, Linux, and Mac operating systems. The automation folder uses the WinPE files of Windows OS and LinuxPE files of Linux OS to create the automation environment for the specific OS. For Mac, the folder uses the DSAutomation partition to boot the Mac client computers into the automation environment. The main advantage of the automation folder is that client computers can boot to the automation environment independent of the connection that is established with the Network Boot Service (NBS) setup on a site server.  

See "About PXE configuration using Network Boot Service" on page 83.  

**Note:** Ensure that the Deployment plug-in of the specific operating system is installed on the client computer on which the automation folder is created.  

See "Installing and uninstalling Automation Folder on client computers" on page 39.  

To boot the client computers to an automation environment, DNS must be configured on the network. All computers in the network must also be able to perform a Name Server Lookup. The installation, uninstallation, and upgrade of the automation folder is triggered and rolled out as a policy for all the operating systems. You can configure the policy through the **Settings > Agent/Plug-ins > Deployment** menu of the console. |
<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Boot Service server</td>
<td>The Network Boot Service (NBS) is installed on a site server and comprises of the following two services:</td>
</tr>
<tr>
<td></td>
<td>■ PXE service and Boot Service Discovery Protocol (BSDP) service SymantecNetworkBootService(PXE and BSDP)</td>
</tr>
<tr>
<td></td>
<td>■ TFTP service SymantecNetworkBootServiceTftp</td>
</tr>
<tr>
<td></td>
<td>The PXE service of NBS boots the client computers in the preboot environment using the PXE image whereas the BSDP is required to create the Netboot image for the Mac computers. The PXE image is used for the Windows and Linux client computers. The BSDP must be enabled in the NBS configuration settings dialog box.</td>
</tr>
<tr>
<td></td>
<td>The NBS also provides configuration of the TFTP service, logging levels for PXE image deployment, and configuration of the network settings.</td>
</tr>
<tr>
<td></td>
<td>See “About Network Boot Service” on page 84.</td>
</tr>
<tr>
<td>Imaging tools</td>
<td>The Ghost disk imaging tool runs on the Windows (x86, x64), Linux (x86, x64) operating systems. The Ghost tool can also be used for creating backup disk images and images of disk partitions.</td>
</tr>
<tr>
<td></td>
<td>These tools support NTFS, FAT (16,32), EXT2/3, RAW, XFS (only for RHEL 7) file system, and HTTP and multicast imaging options. Ghost supports Windows only hardware-independent disk imaging which can be deployed to diverse client computers by using drivers from a centrally managed driver database. Backup images are not hardware-independent and are intended to be deployed on the same client computer.</td>
</tr>
<tr>
<td></td>
<td>For Mac operating system disk imaging, the symDeploMac imaging tool is used. Symantec recommends that you use the combo update to make the images hardware-independent. Backup imaging is not supported for Mac.</td>
</tr>
<tr>
<td>Boot Disk Creator</td>
<td>Boot Disk Creator (BDC) creates a boot disk using the Windows or Linux preboot operating systems. BDC can also create a bootable CD or USB.</td>
</tr>
<tr>
<td>Resource Import Tool</td>
<td>The Resource Import tool is used for importing the existing Windows and Linux images. The tool is also used for adding Windows-scripted OS installation files.</td>
</tr>
<tr>
<td></td>
<td>See “Importing images using Resource Import tool” on page 142.</td>
</tr>
<tr>
<td>Component</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Driver Manager</td>
<td>Driver Manager provides the interface to perform driver operations such as adding and deleting data from the DeployAnywhere driver database and the Preboot driver database.</td>
</tr>
<tr>
<td>DeployAnywhere</td>
<td>DeployAnywhere lets you deploy the Windows operating system image to dissimilar hardware. DeployAnywhere also lets you perform a Windows-scripted installation on bare metal computer. See &quot;Deploying a Windows image&quot; on page 116.</td>
</tr>
<tr>
<td>Deployment Task Server Component</td>
<td>The Deployment Task Server Component of Deployment Solution is deployed on a site server on which the Task Service executes. The Task Server Component is installed on the site server, which is assigned to perform tasks specific to Deployment Solution. This component can be installed on the Windows x86 or Windows x64 site servers only. The Deployment Task Server Component installation or uninstallation is triggered as a policy of Deployment Solution. By default, this policy is turned on. This policy can be set through the Settings &gt; Agent/Plug-ins &gt; Deployment &gt; Windows folder of the console.</td>
</tr>
<tr>
<td>Deployment Package Server Component</td>
<td>The Deployment Package Server Component of Deployment Solution is deployed on a site server on which the Package Service executes. This component is installed on the site server, which is assigned to Deployment Solution to store the product-specific packages or files. This component can be installed on the Windows x86 or Windows x64 site servers only on which Microsoft .NET Framework 4.5 is installed. The Deployment Package Server Component installation or uninstallation is triggered as a policy of Deployment Solution. By default, this policy is turned on. This policy can be set through the Settings &gt; Agent/Plug-ins &gt; Deployment folder of the console.</td>
</tr>
</tbody>
</table>

See “Preparing site servers for Deployment Solution ” on page 30.

About SSL communication in Deployment Solution

Deployment Solution facilitates communication between the client computers and Notification Server (NS), Task Server (TS), and Package Server (PS) using the SSL mode of communication. This secured mode of communication is achieved by installing the SSL...
certificate that is downloaded from the NS, TS, or PS on the client computer after the computer boots in the preboot environment and production environment. In Deployment Solution, the **Extract SSL Certificate** policy downloads and installs the SSL certificate from the IIS locations of NS, PS and TS to their respective predefined web location. The agent that is specific for the operating system and is installed on the client computers in the preboot environment then downloads and installs the SSL certificate from the NS, PS, and TS web locations to the predefined location of the client computer.

Following are the agents that are present in the preboot environment of the specific operating system:

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Agent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows operating system</td>
<td>PECTAgent</td>
</tr>
<tr>
<td>Linux operating system</td>
<td>ULM</td>
</tr>
<tr>
<td>Mac operating system</td>
<td>ULM</td>
</tr>
</tbody>
</table>

To configure NS, PS and TS for IIS and HTTPS refer to the *Symantec™ IT Management Suite powered by Altiris™ technology Installation and Upgrade Guide*.

For Windows client computer, the PECTAgent that is installed in the preboot environment locates the SSL certificate on the client computer and then uses the certificate to communicate with the NS, PS, and TS sequentially. The PECTAgent of the computer then tries to connect to the NS using the HTTPS protocol. If the SSL certificate expires, you must manually renew and install the certificate on the NS and then rollout the Extract SSL certificate policy.

For Mac client computers, install the utility aex-getsscert and then execute the following command to download the SSL certificate from NS, PS, and TS to the client computer:

```
/usr/bin/aex-getsscert <IP/HOSTNAME>
```

For Linux client computers, to facilitate communication with the PS, execute the following command to download the SSL certificate from the PS to the client computer:

```
aex-getsscert <IP> yes
```

**Note:** For Linux and Mac, if the package server is configured on the SSL, then you must manually install the package server’s SSL certificate on the client computers in the preboot environment and production environment to facilitate communication between the package server and the client computers.

The location of the SSL certificate that is downloaded from the IIS of the NS, PS, and the TS is stored on the servers and the client computer location as follows:

**HTTPS location of NS**

https://<server name/ or IP address >

/Altiris/NS/NSCap/Bin/Deployment/Certificates
Introducing Deployment Solution

About types of boot environments in Deployment Solution

In Deployment Solution, the environment in which the client computer can boot into is known as the boot environment. Deployment Solution lets you boot the computers in the pre-OS installation stage or in the post-OS installation stage. The pre-OS installation stage of a client computer is the Preboot environment and the post-OS installation stage is the Production environment.

The different types of boot environments that the client computers boot into are as follows:

■ Preboot environment
Deployment Solution lets you boot client computers in the preboot environment using a preboot configuration. The preboot configuration consists of the preboot operating system, Deployment Plug-in, and the agent that is specific for the operating system.

Windows  PECTAgent
Linux     ULM agent
Mac       ULM agent

You can boot the client computers in the preboot environment in one of the following ways:

- **PXE**
  A PXE configuration is distributed to the client computer over the network.

- **Automation folder**
  An automation folder configuration is installed on the client computers.
  See “Installing and uninstalling Automation Folder on client computers” on page 39.

- **Production environment**
  The production environment is the environment into which a client computer boots after an operating system is installed on the computer.

<table>
<thead>
<tr>
<th>Environment</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preboot environment using the PXE configuration</td>
<td>Deployment Solution lets you boot client computers in preboot environment using a PXE configuration. The PXE configuration is distributed to the client computer over the network using the Network Boot Service (NBS). In Deployment Solution, the PXE service, SymantecNetworkBootServicePxe and BSDP, is a part of the NBS. Following are the OS-specific PXE configurations:</td>
</tr>
<tr>
<td></td>
<td>- WinPE for Windows</td>
</tr>
<tr>
<td></td>
<td>- LinuxPE for Linux</td>
</tr>
<tr>
<td></td>
<td>- NetBoot for Mac</td>
</tr>
</tbody>
</table>
Table 1-2  Types of boot environments in Deployment Solution (continued)

<table>
<thead>
<tr>
<th>Environment</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preboot environment using the automation folder</td>
<td>Deployment Solution facilitates you to create a preboot environment that is installed locally on the client computer. The automation folder configuration that you create is stored on the Notification Server computer and is installed on the client computer when the Deployment automation folder - install policy of the specific OS is enabled. The client computers having a static IP address can boot to the preboot state by using the automation folder only, and not through the PXE environment.</td>
</tr>
<tr>
<td>Production</td>
<td>The production environment is the environment into which a client computer boots after an operating system is installed on the computer. To resume live operations after completing the deployment tasks or maintenance tasks, you must boot the client computers into the production environment.</td>
</tr>
</tbody>
</table>

Where to get more information

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

Table 1-3  Documentation resources

<table>
<thead>
<tr>
<th>Document</th>
<th>Description</th>
</tr>
</thead>
</table>
| Release Notes | Information about new features and important issues.                                                                                                                                                                                                                                                                                                                                                                                                             The Supported Products A-Z page, which is available at the following URL: https://www.symantec.com/products/products-az  
Open your product's support page, and then under Common Topics, click Release Notes. |
| User Guide | Information about how to use this product, including detailed technical information and instructions for performing common tasks.                                                                                                                                                                                                                                                                                                                                 | The Documentation Library, which is available in the Symantec Management Console on the Help menu.  
The Supported Products A-Z page, which is available at the following URL: https://www.symantec.com/products/products-az  
Open your product's support page, and then under Common Topics, click Documentation. |
In addition to the product documentation, you can use the following resources to learn about Symantec products.

### Table 1-4  Symantec product information resources

<table>
<thead>
<tr>
<th>Resource</th>
<th>Description</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>SymWISE Support Knowledgebase</td>
<td>Articles, incidents, and issues about Symantec products.</td>
<td>Knowledge Base</td>
</tr>
<tr>
<td>Cloud Unified Help System</td>
<td>All available IT Management Suite and solution guides are accessible from this Symantec Unified Help System that is launched on cloud.</td>
<td>Unified Help System</td>
</tr>
<tr>
<td>Resource</td>
<td>Description</td>
<td>Location</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Symantec Connect</td>
<td>An online resource that contains forums, articles, blogs, downloads, events, videos, groups, and ideas for users of Symantec products.</td>
<td></td>
</tr>
</tbody>
</table>

The links to various groups on Connect are as follows:

- Deployment and Imaging
- Discovery and Inventory
- ITMS Administrator
- Mac Management
- Monitor Solution and Server Health
- Patch Management
- Reporting
- ServiceDesk and Workflow
- Software Management
- Server Management
- Workspace Virtualization and Streaming
Installing and uninstalling components

This chapter includes the following topics:

- Preinstallation requirements for Deployment Solution
- Preparing site servers for Deployment Solution
- Installing and uninstalling Deployment Solution components
- Installing Network Boot Service on site server
- Installing and un-installing Deployment Plug-in on client computers
- Installing and un-installing Automation Folder on client computers
- Upgrading Deployment Solution components

Preinstallation requirements for Deployment Solution

You must ensure that the preinstallation requirements are met before you install Deployment Solution.

The preinstallation requirements for Deployment Solution are as follows:

- Symantec Installation Manager (SIM) is installed.
- Symantec Management Platform is installed.
- Symantec Management Agent for Windows, Linux, and Mac is pre-installed on the client computers if you want to execute any tasks.
- Symantec Administrator Software Development Kit (SASDK) is installed if you plan to use the Web Services API.
- Ensure that the client computers have Pre-boot eXecution Environment (PXE) enabled in BIOS or UEFI.
- NBS site service is configured and turned on for the Initial Deployment job that is scheduled for the unknown computers that are added into the network.
- Silverlight 5 is installed.
- The storage and the network drivers in your environment are collected.
- The remote site server is configured on the supported operating system if you plan to manage client computers in different subnet.
- DNS is properly configured
  Clients computers inside different subnets should be able to communicate with the Symantec Management Platform and the remote site server using FQDN.

See “Components of Deployment Solution” on page 18.

Preparing site servers for Deployment Solution

Deployment Solution comprises of the site server components that when installed on the site servers facilitate execution of deployment tasks on the client computers. The components are, Deployment Task Server Component and Deployment Package Server Component.

When you set up the site servers as Package Server and Task Server in the network, Notification Server is notified and the details of the Package Server and the Task Server are updated in the inventory. The updated inventory then updates the results for the predefined filters of the Deployment Task Server Component and the Deployment Package Server Component. These predefined filters define the target site server computers on which the Deployment Task Server Component and Deployment Package Server Component can be installed. By default, the policy to install the component is enabled. You can install the components on the site servers only when the policies are enabled.

To check if the Deployment Solution site server components are successfully installed, navigate to the following path and verify if the PSComponent folder or the TSComponet folder are created at the following path

<Install dir>/Program Files/Altiris/Altiris Agent/Agents/Deployment/

The Deployment Solution site server component installation policies and the menus to access them from console are as follows:
You can access the Task Server Component in one of the following ways:

- **Settings > All Settings > Agents/Plug-ins**
  In the left pane, expand the Settings > Agents/Plug-ins > Deployment folder. From the Deployment folder, select the Windows(x64) or Windows(x86) folder.

- **Settings > Agents/Plug-ins > All Agents and Plug-ins**
  In the left pane, expand the Agents/Plug-ins folder > Deployment folder. From the Deployment folder, select the Windows(x64) or Windows(x86) folder.

You can access the Package Server Component in one of the following ways:

- **Settings > All Settings > Agents/Plug-ins**
  In the left pane, expand the Settings > Agents/Plug-ins > Deployment folder. From the Deployment folder.

- **Settings > Agents/Plug-ins > All Agents and Plug-ins**
  In the left pane, expand the Agents/Plug-ins > Deployment folder.

To set up the site server components perform the following steps:

**Table 2-2**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Install Deployment Task Server Component on Task Server</td>
<td>Install the <strong>Deployment Task Server Component</strong> on a Task Server to execute the deployment-related tasks. See &quot;Installing and uninstalling Deployment Solution components&quot; on page 32.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Install Deployment Package Server Component on Package Server</td>
<td>Install the <strong>Deployment Package Server Component</strong> on a Package Server such that deployment packages can be stored on the server. See &quot;Installing and uninstalling Deployment Solution components&quot; on page 32.</td>
</tr>
</tbody>
</table>
Table 2-2  Setting up site servers for Deployment Solution  (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 3</td>
<td>Install the <strong>Network Boot Service</strong> on a site server</td>
<td>Install the <strong>Network Boot Service</strong> on a site server that contains the Pre-Boot Execution Environment (PXE and BSDP) and TFTP services. See “Installing Network Boot Service on site server” on page 35.</td>
</tr>
</tbody>
</table>

See “Installing Network Boot Service on site server” on page 35. See “Components of Deployment Solution” on page 18.

### Installing and uninstalling Deployment Solution components

Deployment Solution rolls out the installation and uninstallation of the site server components as a policy. The Deployment site server components include Deployment Package Server component and Deployment Task server component. The Deployment Task Server component can be installed on Windows x86 or x64 site servers. By default, the Deployment Package Server component-Install policy and the Deployment Task server component-Install policy are enabled. The Deployment Task Server component is rolled out on the site server on which Task service runs. The Deployment Package Server component is rolled out on the site server on which the Package service runs. For both Task Server component-Install policy and the Package Server component-Install policy the predefined target computers filter, filters the target site servers and installs the policy on the site server. Symantec recommends that you do not modify these set filters. If you want to modify the target computers then you must clone the default policy first and then modify the cloned policy.

---

**Note:** Ensure that you install the Deployment Package Server component only on the site servers on which IIS 7.0 or later versions are installed. All the site servers that are installed with IIS 7.0 or later versions are discovered automatically and listed for the Applied To filter of the Deployment Package Server Component - Install page of the console. You must not manually install the Deployment Package Server component on any site server other than the ones that are discovered and listed for the filter.

The Deployment Solution site server component policies and the menus to access them from the console are as follows:
You can access the Task Server Component in one of the following ways:

- **Settings > All Settings > Agents/Plug-ins**
  In the left pane, navigate to Settings folder > Agents/Plug-ins folder > Deployment folder. From the Deployment folder, select the Windows(x64) or Windows(x86) folder.

- **Settings > Agents/Plug-ins > All Agents and Plug-ins**
  In the left pane, expand the Agents/Plug-ins folder > Deployment folder. From the Deployment folder, select the Windows(x64) or Windows(x86) folder.

You can access the Package Server Component in one of the following ways:

- **Settings > All Settings > Agents/Plug-ins**
  In the left pane, expand the Settings folder > Agents/Plug-ins folder > Deployment folder. From the Deployment folder, select the Windows(x64) or Windows(x86) folder.

- **Settings > Agents/Plug-ins > All Agents and Plug-ins**
  In the left pane, expand the Agents/Plug-ins folder > Deployment folder. From the Deployment folder, select the Windows(x64) or Windows(x86) folder.

---

**Note:** Ensure that both the Deployment site server component -Install policy and the Deployment site server component - Uninstall policy are not running at the same time as this causes conflict.

---

To install or uninstall a Deployment Solution component

1. In the Symantec Management Console, select **Settings > Agents/Plug-ins > All Agents/Plug-ins**.

2. In the **Agents/Plug-ins** page, on the left pane tree, expand the **Deployment** folder.

3. In the **Deployment** folder, select the policy from one of the following:

   - **Deployment Task Server Component (x64) - Install**
   - **Deployment Task Server Component (x86) - Install**
   - **Deployment Package Server Components - Install**
   - **Deployment Task Server Component (x64) – Uninstall**
   - **Deployment Task Server Component (x86) – Uninstall**
Deployment Package Server Component - Uninstall

4 On the right-side pane, you can view the details of the selected policy. Symantec recommends that you do not modify the default settings of the policy. If you want to modify the settings, first clone the policy and then modify the cloned policy.

The details of the fields are as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Program Name</strong></td>
<td>Displays the name of the program that is applicable.</td>
</tr>
<tr>
<td><strong>Enable Verbose Reporting of Status Events</strong></td>
<td>This option sends the package status events to Notification Server. The Notification Server Event Capture settings in the Global Symantec Management Agent Settings policy take precedence to the Enable Verbose Reporting setting here. Events are sent only if they are enabled in the Global Symantec Management Agent Settings policy.</td>
</tr>
<tr>
<td><strong>Applied to</strong></td>
<td>Displays the computers to which the policy applies. By default, Deployment Solution lists the targets in the textbox, as per the predefined filter that is set for the SMP. A target is a group of computers that are created as per the set filter.</td>
</tr>
<tr>
<td><strong>Package Multicast</strong></td>
<td>This option disables the package download through multicast. Multicast slows down the rollout of a package, so you can turn it off for an urgent patch. Additionally, in some environments multicast does not work. For example, multicast has to be disabled for routers and switches. The Package Multicast settings in the Global Symantec Management Agent Settings policy take precedence to the settings here.</td>
</tr>
<tr>
<td><strong>Schedule</strong></td>
<td>The policy schedule is displayed. By default, the options that are configured in the Extra Schedule Options field are applicable. Symantec recommends maintaining these settings. By default, the Run once ASAP and the User can run options are selected.</td>
</tr>
</tbody>
</table>
The Extra Schedule Options that are selected by default are as follows:

- Run once ASAP
- User can run

5. Click **Save changes** to save the configuration settings of the policy.

See “Preparing site servers for Deployment Solution” on page 30.

## Installing Network Boot Service on site server

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

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

See “About Network Boot Service” on page 84.

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

---

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

---

**To install NBS service on site server**

1. In the Symantec Management Console, navigate to **Settings > Notification Server > Site Server settings** menu.

2. In the **Site Management** window, expand **Site Server** node in the tree.

3. On the **Site Servers** page, click **New** under the **Detailed Information** pane.

4. In the **Select Computers** dialog box, select the Windows computers that you want to configure as site server and click **OK**.

5. In the **Add/Remove services** dialog box, check the **Network Boot Service** option for the site servers that you select.
Installing and uninstalling Deployment Plug-in on client computers

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

The Deployment Plug-in is specific to an operating system and Deployment Solution contains plug-ins for Windows, Linux, and Mac operating systems.

The Deployment Plug-ins of the different OS are as follows:

- Windows
  - Deployment Plug-in for Windows (x86)
  - Deployment Plug-in for Windows (x64)

- Linux
  - Deployment Plug-in for Linux (x86)
  - Deployment Plug-in for Linux (x64)

- Mac
  - Deployment Plug-in for Mac

Deployment Solution plug-ins are rolled out as predefined policies on the client computers. The predefined policies that are associated with the plug-ins are related to the installation, uninstallation, and upgrade of the plug-ins. The policies are rolled out on the client computers after you enable them through the console. For Linux and Mac client computers, if the package server is configured on HTTPS, and the SSL certificate is not installed on the client computer then you must manually download and install the SSL certificate on the client computer so that the Deployment Plug-in is installed on the client 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.
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 folders.

3. Expand the Windows, Linux, or Mac folder and select from the following Deployment Plug-in Install policies:
   - Deployment Plug-in for Linux (x86) - Install
   - Deployment Plug-in for Linux (x64) - Install
   - Deployment Plug-in for Mac-Install
   - Deployment Plug-in for Windows (x64)-Install
   - Deployment Plug-in for Windows (x86)-Install

4. On the right-side pane, you can view the details of the selected policy. Symantec recommends that you do not modify the default settings of the policy. If you want to modify the settings, first clone the policy and then modify the cloned policy.

The details of the fields are as follows:

**Program Name**  Displays the name of the program that is applicable.

**Enable Verbose Reporting of Status Events**  This option sends the package status events to Notification Server. The Notification Server Event Capture settings in the Global Symantec Management Agent Settings policy take precedence to the Enable Verbose Reporting setting here. Events are sent only if they are enabled in the Global Symantec Management Agent Settings policy.

**Applied to**  Displays the list of computers to which the policy applies. By default, Deployment Solution lists the targets in the textbox, as per the predefined filter that is set for the SMP. A target is a group of computers that are created as per the set filter.
Package Multicast

This option disables the package download through multicast. Multicast slows down the rollout of a package, so you can turn it off for an urgent patch. Additionally, in some environments multicast does not work. For example, multicast has to be disabled for routers and switches. The Package Multicast settings in the Global Symantec Management Agent Settings policy take precedence to the settings here.

Schedule

The policy schedule is displayed. By default, the options that are configured in the Extra Schedule Options field are applicable. Symantec recommends maintaining these settings. By default, the Run once ASAP and the User can run options are selected.

Extra Schedule Options

The Extra Schedule Options that are selected by default are as follows:

- Run once ASAP
- User can run

5 Click Save changes to save the configuration settings of the policy.

To uninstall 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 folders.

3 Expand the Windows, Linux, or Mac folder and select from the following Deployment Automation folder-Uninstall policies:

- Deployment Plug-in for Linux (x86) - Uninstall
- Deployment Plug-in for Linux (x64) - Uninstall
- Deployment Plug-in for Mac-Uninstall
- Deployment Plug-in for Windows (x64)-Uninstall
- Deployment Plug-in for Windows (x86)-Uninstall

4 On the right-side pane, you can specify the following fields:

Program Name Displays the name of the program that is applicable.
Enable Verbose Reporting of Status Events

This option sends the package status events to Notification Server. The Notification Server Event Capture settings in the Global Symantec Management Agent Settings policy take precedence to the Enable Verbose Reporting setting here. Events are sent only if they are enabled in the Global Symantec Management Agent Settings policy.

Applied to

Displays the list of computers to which the policy applies. By default, Deployment Solution lists the targets in the textbox, as per the predefined filter that is set for the SMP. A target is a group of computers that are created as per the set filter.

Package Multicast

This option disables the package download through multicast. Multicast slows down the rollout of a package, so you can turn it off for an urgent patch. Additionally, in some environments multicast does not work. For example, multicast has to be disabled for routers and switches. The Package Multicast settings in the Global Symantec Management Agent Settings policy take precedence to the settings here.

Schedule

The policy schedule is displayed. By default, the options that are configured in the Extra Schedule Options field are applicable. Symantec recommends maintaining these settings. By default, the Run once ASAP and the User can run options are selected.

Extra Schedule Options

The Extra Schedule Options that are selected by default are as follows:

- Run once ASAP
- User can run

5 Click Save changes to save the configuration settings of the policy.

Installing and uninstalling Automation Folder on client computers

An automation folder stores the preboot operating system on the client computers. The client computers use this functionality to boot in the preboot environment whenever required using
the preboot OS that is installed locally on the client computer. The preboot operating systems for Windows and Linux operating systems are, WinPE, and LinuxPE respectively. For the Mac computers, a NetBoot environment is contained in the automation folder that is installed on the client computer. In Deployment Solution the Deployment Automation folder -Install policy installs the Automation folder on the client computer and the Deployment Automation folder-Uninstall policy uninstalls the automation folder from the client computers. When you enable the policy, a green On symbol shows on the top right corner of the policy page.

For Windows, to use the ImageX tool in the automation environment, download the ImageX tool at the following location:

<Install_dir>:\Altiris\Deployment\Imaging\ImageX\<architectural Folder ex. X86 or x64>

After you add the ImageX tool in the specified location, recreate the automation folder preboot configuration to include the ImageX tool in the automation folder. If an automation folder already exists on the client computer, you must upgrade the automation folder. To upgrade the automation folder on the client computers, turn on the automation folder upgrade policies.

Note: For Linux and Mac client computers, to install the automation folder, if the package server is configured on HTTPS, and the SSL certificate is not installed on the client computers then you must manually download and install the SSL certificate on the client computers.

The advantages of using Automation Folder over PXE services of NBS are as follows:

- Lets you boot client computers faster than booting using PXE service of the NBS setup.
- The automation folder function is not affected or restricted by firewalls.
- The automation folder can boot the client computers that have static IP address.

The default location and size of the automation folder that is created on the client computer are as follows:

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Architecture</th>
<th>Default folder location</th>
<th>Approximate folder size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>x86</td>
<td>C:\Boot</td>
<td>214 MB</td>
</tr>
<tr>
<td>Windows</td>
<td>x64</td>
<td>C:\Boot</td>
<td>214 MB</td>
</tr>
<tr>
<td>Linux</td>
<td></td>
<td>/boot/altiris</td>
<td>32 MB</td>
</tr>
</tbody>
</table>
For Mac, the Deployment Automation folder for Mac - Install policy creates a DSAutomation volume on the disk volume where Symantec Management Agent (SMA) is installed. The automation volume uses only the available space on the volume that is installed with SMA and does not use any free space available on other volumes. Ensure that there is sufficient space on the volume on which you have installed the SMA. If a volume is already present with the name, DSAutomation then a new volume of name DSAutomationA is created.

You can also uninstall the automation volume with the uninstall policy for Mac automation folder. After you enable the Deployment Automation folder for Mac - Uninstall policy you must manually delete the DSAutomation partition that is present in the unmounted and unallocated state. If you do not want to run the uninstall policy to uninstall the automation folder from the client computer, then you must manually erase the disk and the volume from the client computer. If, you manually erase the disk and the volume of the client computer, then ensure that you clean the Non-volatile random-access memory (NVRAM) of the client computer.

To clean the NVRAM of a client computer, refer to http://support.apple.com/kb/HT1533 article. See “Configuring the preboot environment” on page 87.

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 folders.

3  Expand the Windows, Linux, or Mac folder and select from the following Deployment Automation folder- Install policies:

   - Deployment Automation Folder for Linux - Install
   - Deployment Automation Folder for Mac-Install
   - Deployment Automation Folder for Windows (x64)-Install

### Table 2-3 Default location and size of automation folder (continued)

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Architecture</th>
<th>Default folder location</th>
<th>Approximate folder size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mac</td>
<td>-</td>
<td>/Volumes/DSAutomation</td>
<td>15 GB</td>
</tr>
</tbody>
</table>

In case a partition is already present with the name DSAutomation then a new folder is created with DSAutomationA name.
Note: You can enable the Deployment Automation Folder for Windows (x64)-Install policy when you install and import the Windows Assessment and Deployment Kit (ADK) for Windows 8 and the PEInstall package is created on Notification Server. After the PEInstall package is created on Notification Server, the PEInstall is available and enabled on the Preboot Configuration dialog box.

- Deployment Automation Folder for Windows (x86)-Install

Note: You can enable the Deployment Automation Folder for Windows (x86)-Install policy when you install and import the Windows Assessment and Deployment Kit (ADK) for Windows 8 and the PEInstall package is created on Notification Server. After the PEInstall package is created on Notification Server, the PEInstall is available and enabled on the Preboot Configuration dialog box.

4 On the right-side pane, you can view the details of the selected policy. Symantec recommends that you do not modify the default settings of the policy. If you want to modify the settings, first clone the policy and then modify the cloned policy.

The details of the fields are as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Program Name</td>
<td>Displays the name of the program that is applicable.</td>
</tr>
<tr>
<td>Enable Verbose Reporting of Status Events</td>
<td>This option sends the package status events to Notification Server. The Notification Server Event Capture settings in the Global Symantec Management Agent Settings policy take precedence to the Enable Verbose Reporting setting here. Events are sent only if they are enabled in the Global Symantec Management Agent Settings policy.</td>
</tr>
<tr>
<td>Applied to</td>
<td>Displays the list of computers to which the policy applies. By default, Deployment Solution lists the targets in the textbox, as per the predefined filter that is set for the SMP. A target is a group of computers that are created as per the set filter.</td>
</tr>
</tbody>
</table>
Package Multicast

This option disables the package download through multicast. Multicast slows down the rollout of a package, so you can turn it off for an urgent patch. Additionally, in some environments multicast does not work. For example, multicast has to be disabled for routers and switches. The Package Multicast settings in the Global Symantec Management Agent Settings policy take precedence to the settings here.

Schedule

The policy schedule is displayed. By default, the options that are configured in the Extra Schedule Options field are applicable. Symantec recommends maintaining these settings. By default, the Run once ASAP and the User can run options are selected.

Extra Schedule Options

The Extra Schedule Options that are selected by default are as follows:

- Run once ASAP
- User can run

5 Click Save changes to save the configuration settings of the policy.

To uninstall 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 folders.

3 Expand the Windows, Linux, or Mac folder and select from the following Deployment Automation folder- Uninstall policies:

- Deployment Automation Folder for Linux - Install
- Deployment Automation Folder for Mac-Uninstall
- Deployment Automation Folder for Windows (x64)-Uninstall
- Deployment Automation Folder for Windows (x86)-Uninstall

4 On the right-side pane, you can view the details of the selected policy. Symantec recommends that you do not modify the default settings of the policy. If you want to modify the settings, first clone the policy and then modify the cloned policy.

The details of the fields are as follows:
Program Name

Displays the name of the program that is applicable.

Enable Verbose Reporting of Status Events

This option sends the package status events to Notification Server. The **Notification Server Event Capture** settings in the **Global Symantec Management Agent Settings** policy take precedence to the **Enable Verbose Reporting** setting here. Events are sent only if they are enabled in the **Global Symantec Management Agent Settings** policy.

Applied to

Displays the list of computers to which the policy applies. By default, Deployment Solution lists the targets in the textbox, as per the predefined filter that is set for the SMP. A target is a group of computers that are created as per the set filter.

Package Multicast

This option disables the package download through multicast. Multicast slows down the rollout of a package, so you can turn it off for an urgent patch. Additionally, in some environments multicast does not work. For example, multicast has to be disabled for routers and switches. The **Package Multicast** settings in the **Global Symantec Management Agent Settings** policy take precedence to the settings here.

Schedule

The policy schedule is displayed. By default, the options that are configured in the **Extra Schedule Options** field are applicable. Symantec recommends maintaining these settings. By default, the **Run once ASAP** and the **User can run** options are selected.

Extra Schedule Options

The **Extra Schedule Options** that are selected by default are as follows:

- Run once ASAP
- User can run

5 Click **Save changes** to save the configuration settings of the policy.

See “Installing and uninstalling Deployment Plug-in on client computers” on page 36.
Upgrading Deployment Solution components

Deployment Solution lets you upgrade the Deployment Plug-in and Automation Folder of Windows, Linux, and Mac operating systems. You can upgrade the Deployment Site Server Components that are installed on the Windows site servers to the latest version using the upgrade policy. After the upgrade policy is rolled out from Symantec Management Platform, all the site servers on which the Deployment Site Server Component is installed, are automatically upgraded.

The upgrade policy uses filters to determine if an upgrade is necessary. You can access the filters that are used from the Manage > Filters > Software Filters > Agent and Plug-in Filters menu.

To upgrade Deployment Solution 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 folders.
3. Select one of the following upgrade policies:
   - Deployment Automation Folder for Linux(x86)-Upgrade
   - Deployment Automation Folder for Linux-Upgrade
   - Deployment Plug-in for Linux(x86)-Upgrade
   - Deployment Plug-in for Linux(x64)-Upgrade
   - Deployment Automation folder for Mac-Upgrade
   - Deployment Plug-in for Mac-Upgrade
   - Deployment Automation Folder for Windows(x64)-Upgrade
   - Deployment Plug-in for Windows(x64)-Upgrade
   - Deployment Site Server Component(x64)- Upgrade
   - Deployment Automation Folder for Windows(x86)-Upgrade
   - Deployment Plug-in for Windows(x86)-Upgrade
   - Deployment Site Server Component(x86)- Upgrade
4. On the right-side pane, you can view the details of the selected policy. Symantec recommends that you do not modify the default settings of the policy. If you want to modify the settings, first clone the policy and then modify the cloned policy.

The details of the fields are as follows:
Program Name
Displays the name of the program that is applicable.

Enable Verbose Reporting of Status Events
This option sends the package status events to Notification Server. The Notification Server Event Capture settings in the Global Symantec Management Agent Settings policy take precedence to the Enable Verbose Reporting setting here. Events are sent only if they are enabled in the Global Symantec Management Agent Settings policy.

Applied to
Displays the list of computers to which the policy applies. By default, Deployment Solution lists the targets in the textbox, as per the predefined filter that is set for the SMP. A target is a group of computers that are created as per the set filter.

Package Multicast
This option disables the package download through multicast. Multicast slows down the rollout of a package, so you can turn it off for an urgent patch. Additionally, in some environments multicast does not work. For example, multicast has to be disabled for routers and switches. The Package Multicast settings in the Global Symantec Management Agent Settings policy take precedence to the settings here.

Schedule
The policy schedule is displayed. By default, the options that are configured in the Extra Schedule Options field are applicable. Symantec recommends maintaining these settings. By default, the Run once ASAP and the User can run options are selected.

Extra Schedule Options
The Extra Schedule Options that are selected by default are as follows:
- Run once ASAP
- User can run

5. Click Save changes to save the configuration settings of the policy.
Setting up client computers

This chapter includes the following topics:

- About types of client computers in Deployment Solution
- About predefined computers in Deployment Solution
- About supporting Mac computers
- Prerequisites for Mac computer setup
- Setting up unknown client computers
- Setting up predefined computers
- Redeploying managed computers

About types of client computers in Deployment Solution

The core function of Deployment Solution includes identifying, setting up, and managing different types of client computers. The type of the client computer is categorized based on whether the computer is a bare metal computer, a predefined computer, or a managed computer that is registered with Notification Server.

The types of client computers that Deployment Solution can set up and manage are as follows:

- Unknown computer
  See “Setting up unknown client computers” on page 52.
- Predefined computer
  See “Setting up predefined computers” on page 62.
- Managed computer
  See “Redeploying managed computers” on page 71.
Deployment Solution identifies the computer type, and then boots the client computer to the preboot or pre-OS environment to perform other deployment and maintenance tasks.

**Table 3-1  Types of client computers in Deployment Solution**

<table>
<thead>
<tr>
<th>Type of client computer</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unknown computer</td>
<td>An unknown computer is a bare metal computer that does not have an operating system to boot. The unknown computer when plugged into a network is identified by the Symantec Management Platform (SMP) as an unmanaged computer because it does not have the Symantec Management Agent (SMA) installed on it. After an unknown computer is added to the network, you can boot it to the preboot environment. You can then install an operating system to perform other deployment and maintenance tasks.</td>
</tr>
<tr>
<td>Predefined computer</td>
<td>A predefined computer is a computer for which you add the details such as computer name, MAC address and so on before adding the computer to the network. To create a predefined computer, you can either add the computer details or import the computer details. If you add a predefined computer, then ensure that you specify the computer name, which is mandatory, through the console. Besides the computer name, you can also provide the computer details and the hardware identifiers of the computer that you want to resolve as a predefined computer. You can also import predefined computer details from a CSV file, into Deployment Solution. After a predefined computer is added to a network, Deployment Solution boots the computer to the preboot environment. After the computer boots to the preboot environment, you can perform tasks such as imaging and system configuration.</td>
</tr>
<tr>
<td>Managed computer</td>
<td>A managed computer is a computer on which the SMA is installed. To execute deployment tasks on a managed computer, such as create disk image, deploy disk images, and changing system configuration, then you must install the Deployment plug-in on the computer.</td>
</tr>
</tbody>
</table>

**About predefined computers in Deployment Solution**

Predefined computers in Deployment Solution are computers, the details of which, such as the computer name and MAC address are added even before the computer is connected in the network. You can specify the name, computer details, and hardware identifiers of a computer that you want to resolve as a predefined computer. You specify the computer name and other details through the SMP console to add a computer as a predefined computer.
Deployment Solution lets you either add the predefined computer details or import the list of computer details through the SMP console. You import the predefined computer details through a TEXT (.txt) or CSV (comma-separated values) file. Both addition or import of predefined computer details can be performed through the Settings > Deployment > Predefined Computers dialog box of the console.

To create predefined computer entries through the Settings > Deployment > Predefined Computers dialog box of the console, you must specify a name. The name is a mandatory field to create predefined computer entries in Deployment Solution. Besides, name, you can choose to specify the other details such as computer details and hardware identifier details. The hardware identifier entries, although not mandatory, play an important role in discovering computer of a network as a predefined computer.

If an unknown computer is discovered in a network, Deployment Solution boots the computer with a PXE image that you configure for unknown computers. PXE images are configured through the NBS General Settings dialog box of the console. Before the discovery process, if you have specified entries for predefined computers through the Predefined Computers dialog box, then the specified hardware identifier entries are matched with that of the booting computer. Entries of hardware identifiers such as MAC, SerialNumber, and UUID are matched with those of the booting computer. Based on the matching results, you configure the unknown computer as a predefined computer.

Deployment Solution resolves an unknown computer as a predefined computer based on the following matching criteria:

- If the values for the hardware identifiers, MAC, SerialNumber, and UUID are specified as null in the Predefined Computers dialog box.
  In this case, all the unknown computers that are discovered are potential predefined computers of Deployment Solution. For example, if you do not specify any value for MAC, SerialNumber, and UUID fields in the Predefined Computers dialog box, then all unknown computers are identified as potential predefined computers. In this case, the unknown computer boots with the PXE image that is configured for the predefined computers through the NBS General Settings.

- If one or more values of the hardware identifiers, MAC, SerialNumber, and UUID matches with that of the booting computer.
  In this case, based on the number of hardware identifiers whose values match, the booting computer is identified as a predefined computer. The booting computer whose two or more values match have the highest potential to be a predefined computer. For example, you specify value for MAC as M1 and the values for the identifiers as null, then if booting computer's MAC is M1, this computer has good possibility to be a predefined computer. If two specified identifier values match, for example, MAC as M1 and UUID as 1234 with that of the booting computer, then this computer has higher possibility to be a predefined computer over other computers.
If the hardware identifier values that you specify matches with that of the booting computer then the computer boots with the PXE image that you configured for predefined computers.

See “Adding or importing predefined computers” on page 210.

See "Configuring and filtering computers to boot with PXE " on page 88.

About supporting Mac computers

Deployment Solution supports Mac computers of an enterprise network to set up, execute, and report on the deployment-related tasks that are executed on the computers. Some of the deployment-related tasks of the Deployment Solution for Mac computers are imaging, installing operating system and so on. Similar to Windows and Linux computers, Mac computers too are driven by the Symantec Management Agent and the Deployment Solution plug-in for execution of any deployment-related tasks on the computers.

Deployment Solution supports set up of the Mac computers that can be categorized into unknown, predefined, or managed. A new Mac computer that is added in a network without a computer name or IP address and is unmanaged by the Symantec Management Platform (SMP) is called the unknown computer. A predefined Mac computer is a computer for which you add the details such as computer name, MAC address and so on to the Symantec Management Platform even before the computer is added to the network. You can add the computer name and the hardware identifier through the SMP console and the details are stored in the database. Managed computers are the ones on which the Symantec Management Agent is installed and are managed by the SMP.

The key features that are supported for the Mac computers are as follows:

- Booting Mac computers in preboot environment
- Imaging Mac computers
- Installing the Mac OS
- Performing system configuration after deploying an image.

Deployment Solution leverages these features even without the presence or connection with the Apple Server. Mac computers boot in the preboot environment using a NetBoot image or in an automation environment using an automation folder. An automation environment is installed on the client computer when the Deployment Automation folder for Mac - Install policy is enabled from the SMP. A NetInstall image is required for installing a Mac OS on the client computer. A NetBoot image and a NetInstall image can be created using the Symantec's Mac pre-OS Creation Utility (MOCU) of the Deployment Solution along with the Apple's System Image Utility. Deployment Solution also facilitates creation of jobs and tasks for Mac computers through the Jobs and Tasks page of the console. In the console you can access the Jobs and Tasks page by navigating to Manage > Jobs and Tasks > Deployment.

Deployment Solution lets you perform the following tasks on Mac computers:
Prerequisites for Mac computer setup

Following are the prerequisites that you must comply with before you use Deployment Solution to manage your Macintosh (Mac) client computers:

- Ensure that you add the following services on the site server on which you enable the NBS service before you check Enable Mac Netboot (BSDP) support in the NBS General Settings dialog box:
  - Windows Role Services for Network File System (NFS) in File Services for Windows
  - Windows Services for UNIX (SFU)
- Configure the DHCP server in the network. The Network Boot Server (NBS) and the DHCP server must be on different computers.
- Install the Symantec Management Agent and the Deployment Solution plug-in for Mac on the source volume and ensure that the Deployment Automation folder for Mac - Install policy is installed on the NetBoot image source computer. Symantec recommends that you install the Symantec Management Agent and the Deployment Plug-in for Mac clients as a root user.
  
  You can access the plug-ins through either of the following menus:

  - **Settings > Agent/Plug-ins > All Agent/Plug-ins**
    On the left pane of the window, access Agent/Plug-ins > Deployment > Mac folder.
  - **Settings > All Settings**
    On the left pane of the window, access Agents/Plug-ins > Deployment > Mac folder.
  - **Actions > Deployment > Install Deployment Plug-in > Mac.**

- The Mac preboot image creator must be logged in as the root user of the source computer.
- Ensure that you have at least the same amount of empty space on the booted source volume as occupied by the installed Mac OS.
Ensure that you set the following for the All Linux/Mac Workstations and the All UNIX/Linux/Mac Servers in the Targeted Agent Settings dialog box before adding a Mac client computer in the network:

- Return the following information as computer name as DNS name
- Return the following information as computer domain as DNS name

You can access the Targeted Agent Settings from Settings > Agents/Plug-ins.

See “About Symantec’s Mac pre-OS Creation Utility” on page 171.

See “Launching Symantec’s Mac pre-OS Creation Utility” on page 171.

Setting up unknown client computers

Deployment Solution lets you set up unknown computers or bare metal computers with Windows, Linux, or Mac operating system. An unknown computer is not managed by the Symantec Management Platform (SMP). When you add an unknown computer into the enterprise network and the Symantec Management Agent (SMA) is installed on the computer, the computer becomes managed by the SMP.

To set up the client computer with Windows, Linux, or Mac operating system, you must first boot the client computer in the preboot environment of the OS that you want to install. You can install Windows, Linux, or Mac operation system in any of the following ways:

- Install a operating system on the computer.
- Deploy an image on the computer.

In Deployment Solution, the PXE image is bundled with the OS-specific agent and the Deployment Solution Plug-in. After an unknown computer boots in the preboot environment, you can execute other deployment-related tasks.

This process addresses the steps you must follow to set up an unknown computer with Windows operating system.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Launch the console</td>
<td>Launch the Symantec Management Console. You can launch the console either from the Start menu of the Notification Server computer or from any computer of the network. To access the console from a different computer, you must type the following: http://&lt;IP address of NS&gt; /altiris/console.</td>
</tr>
<tr>
<td>Step</td>
<td>Action</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>---------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Step 2| Prepare an unknown computer to boot with PXE image. | Boot the client computer with the PXE image that is configured from the Manage Preboot Configuration page.  
See “Preparing unknown computers to boot with WinPE image” on page 54.  
See “Preparing unknown computers to boot with LinuxPE” on page 56.  
See “Booting an unknown Mac computer in NetBoot environment” on page 58. |
| Step 3| Install operating system                    | You can install Windows, Linux, or Mac operating system on the client computer by performing either of the following:  
- Install OS task  
  - **Install Windows OS** task  
    You can install Windows operating system on the client computer using the **Install Windows OS** task.  
    See “Installing Windows OS on client computers” on page 146.  
  - **Install Linux/ESX OS** task  
    You can install Linux operating system on the client computer using the **Install Linux/ESX OS** task.  
    See “Installing Linux/ESX OS using Deployment Solution” on page 167.  
  - **Install Mac OS** task  
    You can install Mac operating system on the client computer using the **Install Mac OS** task.  
    See “Installing Mac OS using Deployment Solution” on page 168.  
- **Deploy Image** task  
  You can install Windows, Linux, or Mac operating system by deploying an image of the respective OS on the client computer.  
  See “Creating and Deploying a Windows disk image” on page 107.  
  See “Deploying a Linux image” on page 127.  
  See “Deploying a Mac image” on page 133.  
  See “Deploying a Windows image” on page 116. |
### Setting up unknown client computers with Windows operating system (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 4 (Optional) | (Optional) View the reports on the status of the task execution or the installation of SMA on the client computer | You can view the following reports for client computers:  
- **Status of the client computer**  
  You can check the status of the client computer to view if the SMA is installed on the client computer. You can view the report from Manage > Computers > Installed Agent. The Installed Agent page lists all the computers along with their IP addresses and the Symantec Management Agent installed on them.  
- **Task execution Status**  
  You can view the task execution status of the client computer from Reports > All Reports > Deployment > Computers with Deployment Tasks Execution Status. You can view the status of the executed tasks on the client computers.  
- **Deployment Plug-in Installation Status**  
  You can check if the Deployment Plug-in of the Deployment Solution is installed successfully on the client computer from Reports > All Reports > Deployment > Deployment Plug-in Installation Status |

See “About types of client computers in Deployment Solution” on page 47.  
See “Setting up predefined computers” on page 62.  
See “Redeploying managed computers” on page 71.

### Preparing unknown computers to boot with WinPE image

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

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

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

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

<table>
<thead>
<tr>
<th>Table 3-3</th>
<th>Booting an unknown computer with WinPE image</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Launch the console</td>
</tr>
<tr>
<td></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td></td>
<td>Launch the Symantec Management Console.</td>
</tr>
<tr>
<td></td>
<td>You can launch the console either from the</td>
</tr>
<tr>
<td></td>
<td>Start menu of the Notification Server</td>
</tr>
<tr>
<td></td>
<td>computer or from any computer of the network.</td>
</tr>
<tr>
<td></td>
<td>To access the console from a different</td>
</tr>
<tr>
<td></td>
<td>computer, you must type the following:</td>
</tr>
<tr>
<td></td>
<td>http://&lt;IP address of NS&gt;/altiris/console</td>
</tr>
<tr>
<td>Step 2</td>
<td>Install Network Boot Service on a site server</td>
</tr>
<tr>
<td></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td></td>
<td>You must install the Network Boot Service</td>
</tr>
<tr>
<td></td>
<td>(NBS) on a site server and also enable the</td>
</tr>
<tr>
<td></td>
<td>policy before you configure the unknown</td>
</tr>
<tr>
<td></td>
<td>client computer to boot in the preboot</td>
</tr>
<tr>
<td></td>
<td>environment.</td>
</tr>
<tr>
<td></td>
<td>See “Installing Network Boot Service on site</td>
</tr>
<tr>
<td></td>
<td>server” on page 35.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Create a WinPE image</td>
</tr>
<tr>
<td></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td></td>
<td>You must create a WinPE image through the</td>
</tr>
<tr>
<td></td>
<td>Manage Preboot Configurations dialog box of</td>
</tr>
<tr>
<td></td>
<td>the console.</td>
</tr>
<tr>
<td></td>
<td>See “Creating preboot configuration for</td>
</tr>
<tr>
<td></td>
<td>Windows” on page 96.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Configure NBS settings for unknown computers</td>
</tr>
<tr>
<td></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td></td>
<td>You must configure the NBS settings for the</td>
</tr>
<tr>
<td></td>
<td>unknown client computer from the console.</td>
</tr>
<tr>
<td></td>
<td>See “Configuring Network Boot Service for</td>
</tr>
<tr>
<td></td>
<td>unknown computers ” on page 89.</td>
</tr>
<tr>
<td></td>
<td>For the unknown computer, you configure the</td>
</tr>
<tr>
<td></td>
<td>NBS General Settings that lets you select the</td>
</tr>
<tr>
<td></td>
<td>image to boot the client computer with and</td>
</tr>
<tr>
<td></td>
<td>also configure the boot menu. Besides, you</td>
</tr>
<tr>
<td></td>
<td>can also configure the NBS Global Setting</td>
</tr>
<tr>
<td></td>
<td>that lets you filter computers based on MAC</td>
</tr>
<tr>
<td></td>
<td>address to which the NBS site server must or</td>
</tr>
<tr>
<td></td>
<td>must not respond.</td>
</tr>
<tr>
<td></td>
<td>See “About NBS General Settings ” on page 85.</td>
</tr>
<tr>
<td></td>
<td>See “About filtering computers through NBS</td>
</tr>
<tr>
<td></td>
<td>Global Settings ” on page 86.</td>
</tr>
</tbody>
</table>
### Table 3-3: Booting an unknown computer with WinPE image (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 5</td>
<td>(optional) Set up <strong>Initial Deployment</strong> job to execute tasks on the client computers</td>
<td>You can set up an <strong>Initial Deployment</strong> job for the Windows unknown client computer to execute the deployment tasks that you create. You can perform this step after you create the deployment tasks for the unknown client computer. The <strong>Initial Deployment</strong> job menu is displayed on the client computer after the computer boots to the preboot environment. You can select all or specific tasks from the menu and execute them on the client computer. See “Configuring the initial deployment settings” on page 207.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Add the unknown computer to the network and wait for the client computer to boot to preboot environment</td>
<td>If you have added predefined computer entries through the console with no hardware identifier values, then the Windows unknown client computers boot in the preboot environment using the PXE image that was configured for predefined computers. You configure the PXE image for a predefined computer through the <strong>NBS General Settings</strong> dialog box. After the computer boots to the preboot environment, Deployment Solution provides an option to boot the unknown computer as a predefined computer. See “Performing tasks in preboot environment for Windows computers” on page 60.</td>
</tr>
</tbody>
</table>

See “Booting managed Windows computer with WinPE image” on page 74. See “Preparing predefined computers to boot with WinPE image” on page 64.

---

**Preparing unknown computers to boot with LinuxPE**

After an unknown computer is added to a network, Deployment Solution boots the computer in the preboot environment using a Linux PXE image. You must configure the unknown computer to boot in the preboot environment before you install the Linux operating system (OS) on the computer. The computer boots in the preboot environment with a PXE image. For Linux, a PXE image is known as LinuxPE, which is configurable in Deployment Solution before you boot the unknown computer. The LinuxPE image contains the preboot files, the ULM Agent, and the Deployment Solution Plug-in that are installed on the client computer after the computer boots in the preboot environment. These agents are required for the execution of deployment tasks on the client computer.

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

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

**Table 3-4**  Booting an unknown computer with LinuxPE image

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Launch the console</td>
<td>Launch the Symantec Management Console. You can launch the console either from the Start menu of the Notification Server computer or from any computer of the network. To access the console from a different computer, you must type the following: http://&lt;IP address of NS&gt;/altiris/console</td>
</tr>
<tr>
<td>Step 2</td>
<td>Install Network Boot Service on a site server</td>
<td>You must install the <strong>Network Boot Service</strong> (NBS) on a site server and also enable the policy before you configure the unknown client computer to boot in the preboot environment. See “Installing Network Boot Service on site server” on page 35.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Create a LinuxPE image</td>
<td>You must create a LinuxPE image through the <strong>Manage Preboot Configurations</strong> dialog box of the console. See “Creating preboot configuration for Linux” on page 102.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Configure NBS settings for unknown computers</td>
<td>You must configure the NBS settings for the unknown client computer from the console. See “Configuring Network Boot Service for unknown computers” on page 89. For the unknown computer, you configure the <strong>NBS General Settings</strong> that lets you select the image to boot the client computer with and also configure the boot menu. Besides, you can also configure the <strong>NBS Global Setting</strong> that lets you filter computers based on MAC address to which the NBS site server must or must not respond. See “About NBS General Settings” on page 85. See “About filtering computers through NBS Global Settings” on page 86.</td>
</tr>
</tbody>
</table>
Table 3-4  Booting an unknown computer with LinuxPE image (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 5</td>
<td>Add the unknown computer to the network and wait for the client computer to boot to preboot environment</td>
<td>If you have added predefined computer entries through the console with no hardware identifier values, then the Linux unknown client computers boot in the preboot environment using the PXE image that was configured for predefined computers. You configure the PXE image for a predefined computer through the <strong>NBS General Settings</strong> dialog box. After the computer boots to the preboot environment, Deployment Solution provides an option to boot the unknown computer as a predefined computer.</td>
</tr>
</tbody>
</table>

See "Preparing predefined computer to boot with LinuxPE" on page 67.

Booting an unknown Mac computer in NetBoot environment

Deployment Solution lets you boot an unknown Mac computer in the preboot environment using a NetBoot image. An unknown client computer is not managed by the Symantec Management Platform (SMP).

To boot an unknown client computer with the default NetBoot image, hold the N key of the keyboard while booting the Mac computer that is added in the network.

The following process elaborates the steps that are involved to boot a client computer in NetBoot environment using a NetBoot image when an unknown computer is added in the network:

Table 3-5  Process for booting an unknown Mac computer with NetBoot image

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Launch the Console</td>
<td>Launch the Symantec Management Console. You can launch the console either from the Start menu of the Notification Server computer or from any computer of the network. To access the console from a different computer, you must type the following: http://&lt;IP address of NS&gt;/altiris/console</td>
</tr>
<tr>
<td>Step 2</td>
<td>Install the Network Boot Service on a site server</td>
<td>Install the Network Boot Service (NBS) on a site server before you perform any other configurations. See “Installing Network Boot Service on site server” on page 35.</td>
</tr>
</tbody>
</table>
### Table 3-5  Process for booting an unknown Mac computer with NetBoot image *(continued)*

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 3</td>
<td>Create and modify a NetBoot image using Symantec's Mac pre-OS Creation Utility</td>
<td>Create and modify a NetBoot image that is used to boot the Mac client computer. You can do this using the Symantec's Mac pre-OS Creation Utility. This utility along with Apple's System Image Utility is used to create and modify the NetBoot image to make it compatible for Deployment Solution. See “Creating and modifying NetBoot images” on page 172.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Create preboot environment</td>
<td>Create a preboot environment with the NetBoot image. The preboot environment ensures that the NetBoot image is uploaded on the Notification Server computer. It is then distributed to all the NBS in the network.</td>
</tr>
</tbody>
</table>
| Step 5 | Enable the NBS service to support Boot Service Discovery Protocol       | Enable the following services in the Network Boot Service Configuration pane of the NBS General Settings dialog box:  
  - Enable the NBS service  
  - Enable Mac NetBoot (BSDP) support  
  See “Configuring NBS for Mac computers” on page 178. |
| Step 6 | Configure response for unknown computers                              | In the NBS General Settings, set default response for unknown computers.  
In the Netboot menu (Mac) of Initial Deployment (Unknown Computer) Menu, select the Respond to unknown computers and select the Default Boot image from the list of NetBoot images that are configured from the Manage Preboot Configuration menu of the console.  
See “Configuring NBS for Mac computers” on page 178. |
Table 3-5 Process for booting an unknown Mac computer with NetBoot image (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 7</td>
<td>Boot the client computer in preboot environment</td>
<td>Turn on your Mac client with the DHCP IP enabled and hold the N key of the keyboard. The client computer searches for the Network Boot Server (NBS) by broadcasting Boot Service Discovery Protocol (BSDP) requests. NBS receives and processes this BSDP request. The client then receives and boots the default NetBoot image as set in the NBS in step 6. On booting the unknown computer with the NetBoot image its inventory is added and displayed in SMP as a predefined computer.</td>
</tr>
</tbody>
</table>

See “Booting Mac computers with NetBoot image” on page 176.

Performing tasks in preboot environment for Windows computers

After the client computers boot to the Windows preboot environment (WinPE), you can perform the following:

- Configure an unknown computer as predefined computer through the **Predefined Computer Options**
- Execute tasks and jobs on the unknown computers from the **Initial Deployment** job
- Execute tasks and jobs on the predefined computers from the **Re-deployment (Managed Computer)** option of the **Initial Deployment** job
- Execute tasks and jobs on the managed computers from the **Re-deployment (Managed Computer)** option of the **Initial Deployment** job
To configure unknown computers as predefined computers

1. After a Windows unknown computer boots in the preboot environment, the **Predefined Computer Options** dialog box is displayed.

   Unknown computers boot to this option only if you have configured the **Predefined Computer** settings through the console and the hardware identifier values are null. The hardware identifiers are MAC address, Serial number, and UUID.

2. In the **Predefined Computer Options** dialog box, select the predefined computer name that you want to assign to the unknown computer, and click **OK**.

   If you click **Cancel**, then the **Initial Deployment Settings** job menu that you configured for the unknown computer, is displayed.

3. In the **Predefined Computer Confirmation** dialog box click **Continue** if you want to configure the unknown computer as a predefined computer.

   Click **Initial Deployment** if you do not want to configure the unknown computer as predefined computer. In such case, the initial deployment tasks that you configured for an unknown computer are executed on the client computer.

To select Initial deployment job for unknown Windows computers

1. After an unknown client computer boots to the preboot environment, the **Initial Deployment** job menu is displayed.

   This menu is displayed only if you have set tasks or jobs for **Initial Deployment (Unknown Computer)** menu in the **Initial Deployment** job menu dialog box.

2. In the **Initial Deployment** menu, select the jobs or tasks that you want to execute on the unknown client computer.

3. Check the status of the tasks or jobs in the console that execute on the client computer.

   Ensure that the client computer boots in the production to continue with deployment-related tasks.

To select Initial deployment job for predefined or managed Windows computers

1. After a predefined or managed client computer boots to the preboot environment, the **Initial Deployment** job menu is displayed.

   This menu is displayed only if you have set tasks or jobs for **Re-deployment (Managed Computer)** menu in the **Initial Deployment** job menu dialog box.

2. In the **Initial Deployment** menu, select the jobs or tasks that you want to execute on the client computer.

3. Check the status of the tasks or jobs in the console that execute on the client computer.

   Ensure that the client computer boots in the production to continue with deployment-related tasks.
Setting up predefined computers

Deployment Solution lets you add or import computers as predefined computers through the **Settings > Deployment > Predefined Computers** menu of the console. The import of the predefined computer details can be performed through a TXT file or a CSV file, while you can add a computer details directly through the **Predefined Computers** dialog box. Before a predefined computer is physically added to the network, you must configure the deployment settings through the console. These settings are configured to boot the computers to the preboot environment successfully after they are added to the network. Deployment Solution also let you create the jobs and the tasks that you execute on the predefined computers after they boot in the preboot environment.

See “About predefined computers in Deployment Solution” on page 48.

The process to set up a predefined computer is as follows:

<table>
<thead>
<tr>
<th>Table 3-6</th>
<th>Setting up predefined computers</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step</strong></td>
<td><strong>Action</strong></td>
</tr>
<tr>
<td>Step 1</td>
<td>Launch the console</td>
</tr>
<tr>
<td>Step 2</td>
<td>Add or import predefined computers</td>
</tr>
</tbody>
</table>
Table 3-6  Setting up predefined computers  (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 3| Prepare the predefined computers to boot in the preboot environment    | Configure settings in Deployment Solution that boots the predefined computers to the preboot environment after they are added to the network. You must perform the following configuration:  
  - Create preboot configurations for the specific operating system that you want to install on the predefined computer. You create the preboot configurations through Settings > Deployment > Manage Preboot Configurations menu of the console.  
  - Install and configure Network Boot Service (NBS) for the predefined computers to boot in the preboot environment.  
  See “Configuring Network Boot Service for predefined computers” on page 92. |
| Step 4| Create the tasks or the jobs that you want to execute on the client computers in the preboot environment | After a predefined computer boots to the preboot environment, you can execute the tasks or jobs to perform the following:  
  - Installation of an operating system  
  - Deployment of an image  
  You can schedule the tasks or jobs to execute on the computers or you can add them to the Initial Deployment job and execute the job on the computers. You can access the Initial Deployment job through Settings > Deployment > Initial Deployment menu of the console. |

See “Setting up unknown client computers” on page 52.

See “Redeploying managed computers” on page 71.

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.
You can import predefined computer using the CSV file. For Windows and Linux computers, the computer name field is mandatory in the CSV file. For Mac computers, you must specify the MAC address, which is mandatory.

**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.

**Preparing predefined computers to boot with WinPE image**

If you have provisioned computers before they are added to a network, then Deployment Solution identifies such computers as predefined computers. You can configure the predefined computers to boot in the preboot environment before you install the Windows operating system (OS). The computers boot in the preboot environment with a PXE image.

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

---

**Note:** If you add a predefined computer through the **Settings > Deployment > Predefined Computer** dialog box of the console, then Deployment Solution boots all unknown computers as potential predefined computer based on a criteria. The criteria is that you have not specified any value for the hardware identifier fields such as MAC address, Serial Number, and UUID, in the dialog box.

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

You must perform the following steps to boot a predefined computer with the WinPE image:
### Table 3-7  Booting a predefined computer with WinPE image

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Launch the console</td>
<td>Launch the Symantec Management Console. You can launch the console either from the Start menu of the Notification Server computer or from any computer of the network. To access the console from a different computer, you must type the following: http://&lt;IP address of NS&gt;/altiris/console</td>
</tr>
<tr>
<td>Step 2</td>
<td>Install the <strong>Network Boot Service</strong> on a site server</td>
<td>You must install the <strong>Network Boot Service</strong> (NBS) on a site server and also enable the policy before you configure the client computer to boot in the preboot environment. See “Installing Network Boot Service on site server” on page 35.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Add or import predefined computers</td>
<td>You must add or import one or more predefined computers through the <strong>Predefined Computers</strong> dialog box of the console. See “Adding or importing predefined computers” on page 210.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Create a WinPE image</td>
<td>Create a WinPE image through the <strong>Manage Preboot Configurations</strong> dialog box of the console. See “Creating preboot configuration for Windows” on page 96.</td>
</tr>
</tbody>
</table>
### Table 3-7  Booting a predefined computer with WinPE image (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 5</td>
<td>Configure NBS settings for predefined computer</td>
<td>Configure the NBS settings for the predefined client computer from the console. See “Configuring Network Boot Service for predefined computers” on page 92. For the predefined computer, you configure the NBS General Settings that lets you select the WinPE image to boot the client computer with and also configure the boot menu. Besides, you can also configure the NBS Global Setting that lets you filter computers based on MAC address to which the NBS site server must or must not respond. See “About NBS General Settings ” on page 85. See “About filtering computers through NBS Global Settings ” on page 86.</td>
</tr>
<tr>
<td></td>
<td>(optional) Set up the Re-Deployment (Managed Computer) menu in the Initial Deployment Settings dialog box</td>
<td>In the Initial Deployment Settings dialog box, you can configure the Re-Deployment (Managed Computer) menu to execute jobs or tasks on the predefined computer after the computer boot in the preboot environment. See “Configuring the initial deployment settings” on page 207.</td>
</tr>
</tbody>
</table>
### Table 3-7
Booting a predefined computer with WinPE image *(continued)*

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step7 | Add a predefined computer to the network and wait for the computer to boot in the preboot environment | After a predefined computer is added to the network, the computer boots with the WinPE image that you configured.  
If you have not specified any values for the hardware identifier fields, then, after the computer boots to the preboot environment, you have can execute the Initial deployment tasks that you configured for the unknown computer.  
The hardware identifier fields are, MAC address, Serial number, and UUID that you specify in the **Add Predefined Computer** dialog box.  
See “Performing tasks in preboot environment for Windows computers” on page 60. |

---

See “About predefined computers in Deployment Solution” on page 48.  
See “Booting managed Windows computer with WinPE image” on page 74.  
See “Preparing unknown computers to boot with WinPE image” on page 54.

### Preparing predefined computer to boot with LinuxPE

If you have provisioned computers before they are added to a network, then Deployment Solution identifies such computers as predefined computers. You can configure the predefined computers to boot in the preboot environment before you install the Linux operating system (OS). The computers boot in the preboot environment with a PXE image.

The PXE image for Linux OS is known as LinuxPE image. For Linux, a PXE image is created using the preboot configuration files, LinuxPE that Deployment Solution supports, the ULM Agent, and the Deployment plug-in for Linux. The Deployment Plug-in is required for the execution of deployment tasks on the client computer.

---

**Note:** If you add a predefined computer through the **Settings > Deployment > Predefined Computer** dialog box of the console, then Deployment Solution boots all unknown computers as potential predefined computer based on a criteria. The criteria is that you have not specified any value for the hardware identifier fields such as MAC address, Serial Number, and UUID, in the dialog box.
The following process addresses how you must configure the settings to boot a predefined Linux computer in the preboot environment. After the computer boots in the preboot environment, the communication with the Notification Server is established and the computer is registered as a managed computer.

You must perform the following steps to boot a predefined computer with the LinuxPE image:

Table 3-8  Booting a predefined computer with LinuxPE image

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Launch the console</td>
<td>Launch the Symantec Management Console.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You can launch the console either from the Start menu of the Notification</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Server computer or from any computer of the network. To access the console</td>
</tr>
<tr>
<td></td>
<td></td>
<td>from a different computer, you must type the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>http://&lt;IP address of NS&gt;/altiris/console</td>
</tr>
<tr>
<td>Step 2</td>
<td>Install the Network Boot Service on a site</td>
<td>You must install the <strong>Network Boot Service</strong> (NBS) on a site server and</td>
</tr>
<tr>
<td></td>
<td>server</td>
<td>also enable the policy before you configure the client computer to boot in</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the preboot environment.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Installing Network Boot Service on site server” on page 35.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Add or import predefined computers</td>
<td>You must add or import one or more predefined computers through the</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Predefined Computers</strong> dialog box of the console.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Adding or importing predefined computers” on page 210.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Create a LinuxPE image</td>
<td>Create a LinuxPE image through the <strong>Manage Preboot Configurations</strong> dialog</td>
</tr>
<tr>
<td></td>
<td></td>
<td>box of the console.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Creating preboot configuration for Linux ” on page 102.</td>
</tr>
</tbody>
</table>
Table 3-8  Booting a predefined computer with LinuxPE image (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 5</td>
<td>Configure NBS settings for predefined computer</td>
<td>Configure the NBS settings for the predefined client computer from the console.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Configuring Network Boot Service for predefined computers” on page 92.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For the predefined computer, you configure the NBS General Settings that lets you select the LinuxPE image to boot the client computer with and also configure the boot menu. Besides, you can also configure the NBS Global Setting that lets you filter computers based on MAC address to which the NBS site server must or must not respond.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “About NBS General Settings” on page 85.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “About filtering computers through NBS Global Settings” on page 86.</td>
</tr>
<tr>
<td>Step 6</td>
<td>(optional) Set up the Re-Deployment (Managed Computer) menu in the Initial Deployment Settings dialog box</td>
<td>In the Initial Deployment Settings dialog box, you can configure the Re-Deployment (Managed Computer) menu to execute jobs or tasks on the predefined computer after the computer boot in the preboot environment.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Configuring the initial deployment settings” on page 207.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Add the predefined computer to the network and wait for the computer to boot in the preboot environment</td>
<td>After a predefined computer is added to the network, the computer boots with the LinuxPE image that you configured.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If you have not specified any values for the hardware identifier fields, then after the computer boots to the preboot environment, you have an option to execute the Initial deployment tasks that you configured for the unknown computer. The hardware identifier fields are, MAC address, Serial number, and UUID that you specify in the Add Predefined Computer dialog box.</td>
</tr>
</tbody>
</table>

See “Preparing predefined computer to boot with LinuxPE” on page 67.

Booting a predefined Mac computer in NetBoot environment

Deployment Solution supports Mac operating system and lets you boot predefined Mac client computer in preboot environment. A predefined computer is a computer whose details are
added in the Symantec Management Platform. You add the predefined computer details or import them from a .txt file or a .csv file.

See “About predefined computers in Deployment Solution” on page 48.

The following process elaborates the steps that are involved to boot a predefined Mac client computer in preboot environment using a NetBoot image:

### Table 3-9 Process for booting a predefined Mac client in preboot environment with NetBoot image

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Launch the console</td>
<td>Launch the Symantec Management Console. You can launch the console either from the Start menu of the Notification Server computer or from any computer of the network. To access the console from a different computer, you must type the following: http://&lt;IP address of NS&gt;/altiris/console</td>
</tr>
<tr>
<td>Step 2</td>
<td>Install the Network Boot service on a site server</td>
<td>Install the Network Boot Service (NBS) on a site server before you perform any other configurations. See “Installing Network Boot Service on site server” on page 35.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Add or import a predefined computer</td>
<td>You can add predefined computers using the Add Predefined Computers Settings dialog box or import predefined computers using a .txt file or a .csv file. See “Adding or importing predefined computers” on page 210.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Create and modify a NetBoot image using Symantec’s Mac pre-OS Creation Utility</td>
<td>Create and modify a NetBoot image to be installed on a Mac client computer. You can do this using the Symantec’s Mac pre-OS Creation Utility. This utility along with the Apple’s System Image Utility is used to create and modify the NetBoot image to make it compatible for Deployment Solution. See “Creating and modifying NetBoot images” on page 172.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Create preboot environment</td>
<td>Create a preboot environment with the NetBoot image. The preboot environment ensures that the NetBoot image is uploaded on the Notification Server computer from where it is distributed to all the NBS in the network.</td>
</tr>
</tbody>
</table>
Table 3-9  Process for booting a predefined Mac client in preboot environment with NetBoot image (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 6| Enable the NBS service to support Boot Service Discovery Protocol | In the Network Boot Service Configuration of the NBS General Settings page enable the following services:  
  ■ Enable the NBS service  
  ■ Enable Mac NetBoot (BSDP) support  
  See “Configuring NBS for Mac computers” on page 178. |
| Step 7| Configure response for predefined computers in NBS          | In the NBS General Settings, set the default response for the predefined computers. Configure the NBS to respond to the predefined Mac computers and set the default image.  
  See “Configuring NBS for Mac computers” on page 178. |
| Step 8| Boot the client computer in preboot environment             | Turn on your Mac client with DHCP IP enabled and hold the N key of the keyboard. The client computer searches for the Network Boot Server (NBS) by broadcasting BSDP requests. NBS receives and processes this BSDP request. The client receives and boots the default NetBoot image as set in the NBS in step 7. |

See “Booting Mac computers with NetBoot image” on page 176.

Redeploying managed computers

Deployment solution lets you redeploy managed computers of an enterprise network that are installed with the Windows, Linux, or Mac operating system. Managed computers are the client computers that have the Symantec Management Agent (SMA) installed on them.

To install the Windows, Linux, or Mac operating system on a managed client computer, you must boot the computer in the preboot environment using the PXE configuration or the automation folder of the operating system that you want to install. An Automation folder contains the PXE image that is required to boot the computer into the automation environment. To install an automation folder on the client computer, enable the Deployment Automation Folder-Install policy for the operation system that you want to install.

See “Booting managed computers in Windows automation environment” on page 80.

This process addresses the steps you must follow to redeploy a managed computer with Windows, Linux, or Mac operating system.
### Table 3-10  Redeploying managed computer with Windows operating system

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Launch the console</td>
<td>Launch the Symantec Management Console. You can launch the console either from the Start menu of the Notification Server computer or from any computer of the network. To access the console from a different computer, you must type the following: http://&lt;IP address of NS&gt;/altiris/console</td>
</tr>
</tbody>
</table>
| Step 2| Boot the managed client computer in preboot environment | Boot the managed client computer in preboot environment using any of the following:  
- PXE image  
  You can boot the client computer using the PXE image of the operating system that you want to install. You can either create a **Boot To** task for the client computer or schedule the task for the client computer.  
  See “Booting managed Windows computer with WinPE image” on page 74.  
  See “Booting managed Linux computer with LinuxPE” on page 76.  
  See “Booting a managed Mac computer in NetBoot environment” on page 77.  
- Automation folder  
  You can boot the client computer using an Automation Folder that is installed on the computer by performing a **Boot To** task using an automation folder. Ensure that an automation folder is installed on the client computer for which you perform the **Boot To** task.  
  See “Booting managed computers in Windows automation environment” on page 80. |
## Redeploying managed computer with Windows operating system (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 3</td>
<td>Install Windows, Linux, or Mac operating system</td>
<td>Install Windows operating system on the client computer by performing either of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Install operating system</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You can install Windows, Linux, or Mac operating system on the client computer using the Install Windows OS task.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Installing Windows OS on client computers” on page 146.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Installing Linux/ESX OS using Deployment Solution” on page 167.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Installing Mac OS using Deployment Solution” on page 168.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Deploy Image task</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You can set up the client computer with Windows, Linux, or Mac operating system by deploying a Windows, Linux, or Mac image on the client computer.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Creating and Deploying a Windows disk image” on page 107.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Creating and deploying Linux disk images” on page 122.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Creating and deploying Mac images” on page 129.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Deploying a Windows image” on page 116.</td>
</tr>
<tr>
<td>Step 4 (Optional)</td>
<td>(Optional) Configure the network setting of managed computer using the Apply system configuration task</td>
<td>Configure the network settings for the managed client computer by using the <strong>Apply System Configuration</strong> task.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You can modify the settings such as the IP address, Domain Name and so on.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Changing system configuration of computers in Deployment Solution” on page 202.</td>
</tr>
</tbody>
</table>
Table 3-10  Redeploying managed computer with Windows operating system (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 5 (Optional) | (Optional) View the reports on the status of the task execution or the installation of the SMA and the Deployment Plug-in on the client computer | You can view the following reports for client computers:  
  ■ Status of the client computer  
  You can check the status of the client computer to view if the SMA is installed on the client computer. You can view the report from Manage > Computers > Installed Agent. The Installed Agent page lists all the computers along with their IP addresses and the Symantec Management Agent that is installed on them.  
  ■ Task execution Status  
  You can view the task execution status of the client computer from Reports > All Reports > Deployment > Computers with Deployment Tasks Execution Status. You can view the status of the executed tasks on the client computers.  
  ■ Deployment Plug-in Installation Status  
  You can check if the Deployment Plug-in of the Deployment Solution is installed successfully on the client computer from Reports > All Reports > Deployment > Deployment Plug-in Installation Status  

See “Setting up unknown client computers” on page 52.  
See “Setting up predefined computers” on page 62.

Booting managed Windows computer with WinPE image

Deployment Solution lets you redeploy a managed computer that is installed with the Windows operating system (OS) to a preboot environment. The managed computer redeploys to the preboot environment using the WinPE image that Deployment Solution supports, after you execute the Boot To deployment task.

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

You must perform the following steps to reboot a managed computer with a WinPE image:
Table 3-11  Booting a managed computer with WinPE image

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Launch the console</td>
<td>Launch the Symantec Management Console. You can launch the console either from the Start menu of the Notification Server computer or from any computer of the network. To access the console from a different computer, you must type the following: http://&lt;IP address of NS&gt;/altiris/console</td>
</tr>
<tr>
<td>Step 2</td>
<td>Install the <strong>Network Boot Service</strong> on a site server</td>
<td>You must install the <strong>Network Boot Service</strong> (NBS) on a site server and also enable the policy before you configure the client computer to boot in the preboot environment. See “Installing Network Boot Service on site server” on page 35.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Create a WinPE image</td>
<td>Create a WinPE image through the <strong>Manage Preboot Configurations</strong> dialog box of the console.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Configure NBS settings for managed computer</td>
<td>Configure the NBS settings for the managed client computer from the console. See “Configuring Network Boot Service for managed computers” on page 94. For the managed computer, you configure the <strong>NBS General Settings</strong> that lets you select the WinPE image to boot the client computer with and also configure the boot menu. Besides, you can also configure the <strong>NBS Global Setting</strong> that lets you filter computers based on MAC address to which the NBS site server must or must not respond. See “About NBS General Settings ” on page 85. See “About filtering computers through NBS Global Settings ” on page 86.</td>
</tr>
<tr>
<td>Step 5</td>
<td>(optional) Set up the <strong>Re-Deployment (Managed Computer) menu</strong> in the <strong>Initial Deployment Settings</strong> dialog box</td>
<td>In the <strong>Initial Deployment Settings</strong> dialog box, you can configure the <strong>Re-Deployment (Managed Computer) menu</strong> to execute jobs or tasks on the managed computer after the computer boots in the preboot environment. See “Configuring the initial deployment settings” on page 207.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Execute <strong>Boot To PXE task</strong></td>
<td>Execute the <strong>Boot To</strong> task and select the <strong>PXE/NetBoot image</strong> option in the <strong>Create New Task</strong> dialog box.</td>
</tr>
</tbody>
</table>
Table 3-11 Booting a managed computer with WinPE image (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 7</td>
<td>Execute tasks or jobs after the client computer boots to preboot environment</td>
<td>After the Windows client computer boots to preboot environment, the Re-Deployment menu for managed computers is displayed. You can select all or specific tasks or jobs that you want to execute. See “Performing tasks in preboot environment for Windows computers” on page 60.</td>
</tr>
</tbody>
</table>

See “Configuring and filtering computers to boot with PXE ” on page 88.
See “Preparing unknown computers to boot with WinPE image ” on page 54.
See “Preparing predefined computers to boot with WinPE image ” on page 64.

### Booting managed Linux computer with LinuxPE

Deployment Solution lets you redeploy a managed computer that is installed with the Linux operating system (OS) to a preboot environment. The managed computer redeploys to the preboot environment using the LinuxPE image that Deployment Solution supports, after you execute the **Boot To** deployment task.

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

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

Table 3-12 Booting a managed computer with LinuxPE image

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Launch the console</td>
<td>Launch the Symantec Management Console. You can launch the console either from the Start menu of the Notification Server computer or from any computer of the network. To access the console from a different computer, you must type the following: http://&lt;IP address of NS&gt;/altiris/console</td>
</tr>
<tr>
<td>Step 2</td>
<td>Install the <strong>Network Boot Service</strong> on a site server</td>
<td>You must install the <strong>Network Boot Service</strong> (NBS) on a site server and also enable the policy before you configure the client computer to boot in the preboot environment. See “Installing Network Boot Service on site server” on page 35.</td>
</tr>
</tbody>
</table>
### Table 3-12  Booting a managed computer with LinuxPE image (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 3 | Create a LinuxPE image | Create a LinuxPE image through the Manage Preboot Configurations dialog box of the console.  
See “Creating preboot configuration for Linux ” on page 102. |
| Step 4 | Configure NBS settings for managed computer | Configure the NBS settings for the managed client computer from the console.  
See “Configuring Network Boot Service for managed computers” on page 94.  
For the managed computer, you configure the NBS General Settings that lets you select the LinuxPE image to boot the client computer with and also configure the boot menu. Besides, you can also configure the NBS Global Setting that lets you filter computers based on MAC address to which the NBS site server must or must not respond.  
See “About NBS General Settings ” on page 85.  
See “About filtering computers through NBS Global Settings ” on page 86.  
See “About NBS General Settings ” on page 85. |
| Step 5 | Set up the Re-Deployment (Managed Computer) menu | Configure the Re-Deployment (Managed Computer) menu to set the default Linux PXE image with which the client computer boots in the preboot environment. |
| Step 6 | Execute Boot To PXE task | Execute the Boot To task and select the PXE/NetBoot image option in the Create New Task dialog box.  
See “Creating a Boot To task” on page 199. |
| Step 7 | Execute tasks or jobs after the client computer boots to preboot environment | After the Linux client computer boots to preboot environment, the Re-Deployment menu for managed computers is displayed. You can select all or specific tasks or jobs that you want to execute. |

See “Creating preboot configuration for Linux ” on page 102.

### Booting a managed Mac computer in NetBoot environment

Deployment Solution lets you boot a managed Mac client computer in preboot environment with NetBoot image. A managed computer is the one that is managed by the Symantec Management Platform.
You can boot a managed Mac client in the preboot environment using a NetBoot image or you can boot a Mac client in automation environment using the DSAutomation volume. The DSAutomation volume is installed on the Mac client computer by enabling the **Deployment Automation folder for Mac - Install** policy.

The following process elaborates the steps that are involved in booting a managed Mac computer in preboot environment:

**Table 3-13** Process for booting a managed Mac client in preboot environment

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Launch the Console</td>
<td>Launch the Symantec Management Console. You can launch the console either from the Start menu of the Notification Server computer or from any computer of the network. To access the console from a different computer, you must type the following: <strong>http://&lt;IP address of NS&gt;/altiris/console</strong></td>
</tr>
<tr>
<td>Step 2</td>
<td>Install the Network Boot Service on a site server</td>
<td>Install the Network Boot Service (NBS) on a site server before you perform any other configurations. See “<strong>Installing Network Boot Service on site server</strong>” on page 35.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Create and modify a NetBoot image using Symantec's Mac pre-OS Creation Utility</td>
<td>Create and modify NetBoot image that is used to boot the Mac client computer. You can do this using the Symantec's Mac pre-OS Creation Utility. This utility along with Apple's System Image Utility is used to create and modify the NetBoot image to make it compatible for Deployment Solution. See “<strong>Creating and modifying NetBoot images</strong>” on page 172.</td>
</tr>
</tbody>
</table>
Table 3-13  Process for booting a managed Mac client in preboot environment *(continued)*

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 4</td>
<td>Create preboot environment</td>
<td>Create a preboot environment with the NetBoot image. The preboot environment ensures that the NetBoot image is uploaded on the Notification Server computer from where it is distributed to all the NBS in the network.</td>
</tr>
</tbody>
</table>
| Step 5 | Enable the NBS service to support Boot Service Discovery Protocol | Enable the following services in the Network Boot Service Configuration from the NBS General Settings dialog box.  
  ■ Enable the NBS service  
  ■ Enable Mac NetBoot (BSDP) support  
  See “About NBS General Settings” on page 85. |
| Step 6 | Configure response for managed computers in NBS or Create a **Boot To** task. | You can do either of the following:  
  ■ In the NBS General Settings set default response for managed computers. Configure NBS to respond to managed Mac computers and set the default image.  
  See “Configuring NBS for Mac computers” on page 178.  
  ■ You can also boot a managed Mac computer using the **Boot To** task.  
  See “Creating a **Boot To** task” on page 199. |
### Process for booting a managed Mac client in preboot environment (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 7</td>
<td>Boot the client computer in preboot environment</td>
<td>Turn on your Mac client and hold the N key. The client computer searches for the NBS by broadcasting BSDP requests. NBS receives and processes this BSDP request. The client then receives and boots the default NetBoot image as set in the NBS in step 6. If you have scheduled a <strong>Boot To</strong> task, the client computer receives the task as scheduled. See “Creating a Boot To task” on page 199.</td>
</tr>
</tbody>
</table>

See “Boot Mac computers with NetBoot image” on page 176.

### Booting managed computers in Windows automation environment

You use Deployment Solution to boot managed computers in automation environment whenever you want to install a different operating system or deploy a new image on the computer. Automation environments are created and activated after you install the operating system (OS) specific Automation Folder plug-in on the client computer. You use the automation folder as an alternative option to boot computer especially when the client computer is disconnected from the Network Boot Service (NBS) server in a network.

An automation folder stores the preboot files of an operating system on the client computer. The client computer uses this functionality to boot in the preboot environment using the preboot OS that is installed locally. The preboot OS for Windows OS is known as WinPE.

This process lets you boot a Windows managed computer in an automation environment.

Before you get started, review the location and size of the Automation Folder that is created on the client computer in the following table:

### Default location and size of Windows automation folder

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Architecture</th>
<th>Default folder location</th>
<th>Approximate folder size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>x86</td>
<td>C:\Boot</td>
<td>214 MB</td>
</tr>
<tr>
<td>Windows</td>
<td>x64</td>
<td>C:\Boot</td>
<td>214 MB</td>
</tr>
</tbody>
</table>
Ensure that proper filters are set while installing the Deployment Automation Folder. Ensure that a 64-bit policy gets installed on a 64-bit computer and a 32-bit policy get installed on a 32-bit client computer.

**Table 3-15** To boot a managed computer in an automation environment

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Launch the console</td>
<td>Launch the Symantec Management Console. You can launch the console either from the Start menu of the Notification Server computer or from any computer of the network. To access the console from a different computer, you must type the following: http://&lt;IP address of NS&gt;/altiris/console</td>
</tr>
<tr>
<td>Step 2</td>
<td>Install the Deployment Automation Folder plug-in for Windows on the client computer</td>
<td>Install the Deployment Automation Folder for Windows plug-in on the client computer. Ensure you install the 64-bit plug-in and the 32-bit plug-in on the appropriate computers. To install the plug-in, you must access the Settings &gt; Agents/Plug-ins &gt; All Agents/Plug-ins menu of the console. Expand the Deployment node in the left pane and select the Windows folder. Inside the folder, select the Deployment Automation Folder for Windows - Install policy. In the right pane, perform the required actions to apply the policy on the client computer that you want. See “Installing and uninstalling Automation Folder on client computers” on page 39.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Configure an automation environment</td>
<td>Create and configure an automation environment through the Manage Preboot Configuration dialog box of the console. By default, the automation environment for Windows is PEInstall, which is listed in the dialog box. If you create custom automation folders through this dialog box, then you must manually copy the automation folders to the computer on which the Notification Server (NS) is installed. Ensure that the automation policy is enabled as performed in step 2 such that NS can replicate the automation folder on the client computer.</td>
</tr>
</tbody>
</table>
Table 3-15  To boot a managed computer in an automation environment *(continued)*

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 4 | (optional) Create Initial Deployment tasks or jobs | You can create and assign initial deployment tasks or jobs to the Windows managed computers through the Initial Deployment job menu. The jobs are executed after the computer boots in the automation environment.  
See “Configuring the initial deployment settings” on page 207. |
| Step 5 | Create a **Boot To** automation task | Create the **Boot To** task in the **Create New Task** dialog box and select the **Automation** option.                                                                                                        |
| Step 6 | Schedule the **Boot To** task to execute on a client computer | Schedule the **Boot To** Automation task that you created for the client computers to boot in the automation environment.  
See “Scheduling a deployment job or task” on page 198.                                                                                       |

See “Booting managed Windows computer with WinPE image” on page 74.
Setting up preboot environment

This chapter includes the following topics:

- About PXE configuration using Network Boot Service
- About Network Boot Service
- About NBS General Settings
- About filtering computers through NBS Global Settings
- Configuring the preboot environment

About PXE configuration using Network Boot Service

A Pre-Boot Execution Environment (PXE) lets you boot computers using network interfaces such as a Network Interface Card (NIC). In Deployment Solution, PXE service, SymantecNetworkBootService(PxeandBSDP) is a part of the Network Boot Service (NBS), which is installed on the Windows site servers. The PXE service is activated and remains in the state only if the NBS is in the enabled state. The NBS is rolled out on the site servers as a policy whose state you can control from the console.

See “About Network Boot Service” on page 84.

The preboot booting options that you can configure through the NBS includes booting using a PXE image for Windows, Linux, and Mac operating systems. Deployment Solution also lets you boot the UEFI computers using a PXE image of Windows (x64) architecture.

A PXE image is required to boot client computers in preboot environment before you install a Windows operating system, a Linux operating system, or a Mac operating system on those computers. Deployment Solution supports and packages the preboot environments, WinPE, and LinuxPE of Windows operating system and Linux operating system, respectively. You
create PXE images specific to the WinPE or LinuxPE architectures. For the Mac client computers, you create NetBoot image to boot the computers with before you install a Mac operating system on them.

Before you configure NBS on the site servers, you must create the PXE images for the Windows or Linux client computers. For the Mac client computers, you must create the NetBoot images.

See “Creating and modifying NetBoot images” on page 172.

You create PXE images using the Settings > Deployment > Manage Preboot Configuration dialog box of the console. After a PXE image is created, the image is sent to the site servers that are installed with NBS.

Deployment Solution has a provision to boot an unknown computer, a predefined computer, or a managed computer in the preboot environment. You can also add drivers for the PXE image of a Linux or Windows client computer to ensure that the PXE image supports the new hardware. The drivers that are added in the preboot environment are stored in the Preboot database of Deployment Solution.

See “Configuring and filtering computers to boot with PXE ” on page 88.

See “Adding drivers to the Preboot database” on page 160.

### About Network Boot Service

Network Boot Service (NBS) is a component of Deployment Solution that you install and run as a service on a site server. This service is independent of the presence of Task service or Package service on a site server and handles all communication with the Symantec Management Platform (SMP) for Deployment Solution.

The NBS comprises of the PXE /BSDP service and the TFTP service that are installed on the site servers. In the Site Management > Site Server > Services pane, click the Add or Removed Services dialog box to install the NBS on the site servers.

See “Installing Network Boot Service on site server” on page 35.

The details of the NBS services are as follows:

- **Symantec Network Boot Service (PXE and BSDP)**
  This service functions as the PXE server and lets you configure client computers to boot them in the preboot environment. It also supports the Boot Service Discovery Protocol (BSDP) used for Mac client computers.

- **Symantec Network Boot Service (TFTP)**
  This service functions as the TFTP server and lets you perform tasks such as copy file.

The NBS configuration settings are accessible through the Settings > Notification Server > Site Server Settings menu of the Symantec Management Console. In the Site Management
tree, on the left pane, click Settings > Network Boot Service folder. This folder displays the Advanced folder and the Settings folder.

The Advanced folder contains predefined filters that help you know the NBS installation details for the site servers of your network.

The filters of the Advanced folder are as follows:

- **Computers with Deleted Network Boot Service entries**
  This filter lists the site servers on which NBS was installed but is removed currently.

- **Computers with NBS Site Service installed**
  This filter lists the site servers on which NBS is installed.

- **NBS Potential Site Servers**
  This filter displays the site servers on which NBS can be installed.

- **NBS Site Service Assigned**
  This filter lists the site servers on which you enabled the NBS policy but is yet to install.

The Settings folder lets you configure NBS after you install the policy on the site servers.

The configurable options of NBS are as follows:

- **NBS General Settings**
  This configurable setting is about configuring client computers to boot in preboot environment using PXE image. You can configure the setting to be applied to one or more site servers. See “About NBS General Settings ” on page 85.
  You can also configure these settings from the Settings > Deployment > NBS General Settings dialog box of the console.

- **NBS Global Settings**
  This configurable setting is applied to all the site servers.
  See “About filtering computers through NBS Global Settings ” on page 86.
  You can also configure these settings from the Settings > Deployment > NBS Global Settings dialog box of the console.

The status of the NBS that is installed on a site server is displayed in the Site Management -> Site Servers -> [Site Server Name] ->Services pane. The red, yellow, and green colors indicate the normal state, warning state, and error state, respectively of the service. Expand Services > Network Boot Service node to view the details about the service.

See “Configuring and filtering computers to boot with PXE ” on page 88.

### About NBS General Settings

The NBS General Settings option of the Network Boot Service (NBS) lets you configure one or more site servers with preboot configuration settings. The preboot configuration settings are required to configure the client computers to boot in the pre-OS or preboot environment.
using a PXE image or NetBoot image. A PXE image is related to the Windows or Linux preboot environments whereas a NetBoot image is related to the Mac environment. Computers of UEFI architecture can boot in the preboot environment using the x64-bit PXE image of Windows. Deployment Solution categorizes preboot configuration settings for unknown computers, managed computers, and predefined computers.

The **NBS General Settings** configuration is applicable only when NBS is installed on the site server and the service is enabled.

See “Installing Network Boot Service on site server” on page 35.

You can access the **NBS General Settings** option from the following menus of the console:

- **Settings > Notification Server > Site Server Settings**
  - In the **Site Management** view pane, access **Settings > Network Boot Service > Settings > NBS General Setting**.

- **Settings > Deployment > NBS General Settings**

See “Configuring and filtering computers to boot with PXE” on page 88.

See “About Network Boot Service” on page 84.

### About filtering computers through NBS Global Settings

Deployment Solution lets you filter client computers based on their MAC addresses for applying the Network Boot Service (NBS) settings on them. The NBS settings when applied on the client computers boot them to the preboot environment using the PXE image. This NBS setting configuration can be performed through the **Settings > Deployment > NBS General Settings** menu, while the filter configuration settings can be performed through the **Settings > Deployment > NBS Global Settings** menu of the console. The NBS Global Settings configuration is applicable to all the NBS site servers.

You can also access the **NBS Global Settings** dialog box from the **Settings > Notification Server > Site Server Settings** menu. In the **Site Management** pane, access **Settings > Network Boot Service > Settings** folder.

The fields and descriptions of the **NBS Global Settings** dialog box are as follows:
Table 4-1  NBS Global Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Apply NBS settings immediately</strong></td>
<td>Check this option if you want to apply the NBS Global Settings policy immediately on all the NBS site servers. By default, this option is unchecked and so this policy runs as per the default time set for the Symantec Management Platform (SMP).</td>
</tr>
<tr>
<td><strong>MAC Address Filter</strong></td>
<td>Lets you filter client computers based on their MAC address and choose whether to configure them with NBS settings or not. Check <strong>Apply MAC Address Filter</strong> if you want to apply the MAC filter for the client computers. If you check this option, you must select either of the following:</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Service Network Boot clients with following MAC addresses only</strong> Lets you filter the client computers based on their MAC addresses to which the NBS site server must respond. The NBS site server is configured to respond to the client computers and boot them either with PXE image or with NetBoot image. The NetBoot image is created for Mac OS computers using the BSDP protocol. You must click <strong>Add</strong> to specify the MAC address of either a single client computer or the range of MAC addresses of the client computers.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Do not service Network Boot clients with following MAC addresses</strong> Lets you filter the client computers based on their MAC addresses for which you do not want the NBS site server to respond. You must click <strong>Add</strong> to specify the MAC address of either a single client computer or the range of MAC addresses of the client computers.</td>
</tr>
<tr>
<td><strong>Save changes</strong></td>
<td>Click this button to save the configuration changes that you made.</td>
</tr>
</tbody>
</table>

See “About NBS General Settings ” on page 85.
See “Configuring and filtering computers to boot with PXE ” on page 88.

Configuring the preboot environment

You configure a preboot environment in which client computers can boot using a PXE image and then execute the deployment tasks that are configured for the computers.

The process for configuring the preboot environment includes the following tasks:
The Preboot eXecution Environment (PXE) configuration setup task is contained in the Network Boot Service (NBS) that you deploy on a site server.

NBS contains the PXE service, SymantecNetworkBootServicePxe for Windows and Linux computers and BSDP for Mac computers. The service runs on the site server after NBS is installed and enabled on the site server computer. This PXE service initiates the Windows and Linux client computers to boot with the PXE image and the Mac computers to boot with the Netboot image. The images are configured through the Manage Preboot Configurations dialog box of the console.

See “Configuring and filtering computers to boot with PXE” on page 88.
See “Configuring NBS for Mac computers” on page 178.

You can create a preboot configuration for creating a PXE image and a preboot installation file.

See “Editing and deleting preboot configurations” on page 106.
See “Configuring the initial deployment settings” on page 207.

### Configuring and filtering computers to boot with PXE

The Network Boot Service (NBS) component of Deployment Solution comprises the PXE/BSDP service, SymantecNetworkBootService(PXE and BSDP), which is used to boot client computers to the preboot environments. The Windows and Linux client computers use the PXE service whereas the Macintosh computers use the Boot Service Discovery Protocol (BSDP) service to boot in the preboot environments. NBS must be installed on the site servers and configured with PXE image of Windows and Linux or Netboot image of Mac to boot the computers to the preboot environment.

You must configure NBS based on the type of computers that you want to boot to the preboot environments. The types of computers that Deployment Solution addresses are unknown computers, predefined computers, or managed computers. Based on the operating system and the type of computer, you must configure the NBS settings. You can also configure to filter the client computers based on their MAC address to which the NBS site servers must respond.

**Note:** The client computer must be installed with Microsoft XML Core Services (MSXML) 6.0 before you install NBS on the site server.
To configure the Network Boot Service settings

1. In the Symantec Management Console, select the Settings > Deployment > NBS General Settings menu.
   
   You can also access this menu from Settings > All Settings. In the All Settings tree pane, select Notification Server > Site Server Settings > Network Boot Service.

2. In the NBS General Settings dialog box, configure the settings for the type of client computers you want.

   You can configure the NBS General Settings for the following types of client computers:
   
   ■ Unknown computers of Windows OS or Linux OS
     See “Configuring Network Boot Service for unknown computers” on page 89.
   
   ■ Predefined computers of Windows OS or Linux OS
     See “Configuring Network Boot Service for predefined computers” on page 92.
   
   ■ Managed computers of Windows OS or Linux OS
     See “Configuring Network Boot Service for managed computers” on page 94.
   
   ■ Mac client computers
     See “Configuring NBS for Mac computers” on page 178.

3. Click Save changes.

To filter computers to boot with PXE

1. In the Symantec Management Console, select the Settings > Deployment > NBS Global Settings menu.

   You can also access this menu from Settings > All Settings. In the All Settings tree pane, select Notification Server > Site Server Settings > Network Boot Service.

2. In the NBS Global Settings dialog box, configure the settings to filter the client computers based on the MAC addresses.

   See “About filtering computers through NBS Global Settings” on page 86.

   See “Configuring the initial deployment settings” on page 207.

   See “Installing Network Boot Service on site server” on page 35.

   See “About PXE configuration using Network Boot Service” on page 83.

   See “Configuring NBS for Mac computers” on page 178.

Configuring Network Boot Service for unknown computers

After an unknown computer is added to a network, you must boot the computer in the preboot environment. To boot computers in the preboot environment, you must install the Network
Boot Service (NBS) on a site server and configure the site server with the NBS settings for unknown computers.

To configure site server with NBS settings for unknown computers

1. In the Symantec Management Console, click `Settings > Deployment > NBS General Settings`.

2. In the `NBS General Settings` dialog box, for the `Network Boot Service Configuration`, configure the settings for the unknown client computers.

   - **Network Boot Service Configuration**: Lets you configure the Network Boot Service (NBS) for a site server.

   - To enable or disable the policy, you must select the `Turn On` or `Turn Off` icons on the right side of the dialog box or page.

   - **Apply NBS settings immediately**: Check the option if you want to apply the NBS policy immediately on the site servers.

   - If the option remains unchecked then the NBS configurations changes are applied as per the schedule set in the Symantec Management Agent (SMA) for rolling out policies.

   - **Enable the NBS service**: Check the NBS service to enable the service on the site server.

   By default, this option is checked.

   - **Reset button**: Lets you restore the previous configuration that you performed for the NBS site server.

3. In the `NBS General Settings` dialog box, for the `PXE menu (Windows/Linux)` tab of the `Initial Deployment (Unknown Computer) Menu`, specify the following:

   - **Respond to unknown computers**: Check this option if you want to respond to the unknown computers to configure them to boot in the preboot environment using a PXE image.

   - **PXE boot image**: Select the PXE image that you want to use to boot the unknown client computers in the preboot or automation environment. If you do not want to boot using a PXE image, you can select, `Next Device (BIOS/EFI)` mode of booting option for the client computer. Based on whether the default boot option of the client computer is set to BIOS or EFI, the computer boots to the preboot environment. The potential boot devices of BIOS are CD, disk, and so on. Computers of UEFI architecture can boot in the preboot environment using the x64-bit PXE image of Windows.
For the PXE image, select any of the following architectures from the drop-down list:

- **Auto**
  Select this option if you want to boot the client computer based on the computer's processor architecture. For example, if you have a client computer whose processor type is x64 but the installed operating system is x86 of Windows 7, then the **Auto** option boots the computer in x64 architecture mode and not in x86 mode.
  The **Auto** option can be useful if you have created a common PXE image for both x86 and x64 architectures or want to boot a computer as per the processor architecture irrespective of the OS architecture. You create PXE images through the Manage Preboot Configuration dialog box of the console.

- **x86**
  Select this option if the PXE image that you have created is for the x86 architecture of the operating system.

- **x64**
  Select this option if the PXE image that you have created is for the x64 architecture of the operating system.

Configure the schedule of the network boot menu through the following:

- **Run default boot option immediately**
  Select this option if you want to deploy the PXE boot image immediately after you select the image in the drop-down list.

- **Wait indefinitely for user selection**
  Select this option if you want to manually select and deploy the PXE boot image from the network boot menu. The network boot menu appears on the unknown computer.

- **Run default boot option after**
  Select this option if you want to deploy the PXE boot image after the time period that you specify in the text box. After the time out, the client computer boots to the PXE image that you have selected. Press F8 to invoke the network boot menu to deploy the PXE boot image on the client computer.

4 Click **Save changes**.

5 Again, in the console, click the **Settings >Deployment > NBS Global Settings** menu.
   This is an optional step.
   See "About filtering computers through NBS Global Settings " on page 86.

6 In the **NBS Global Settings** dialog box or pane, click **Save Changes**.
   If you are reading this procedure as a part of a process, return to the process by clicking on the following link:
   See “Preparing unknown computers to boot with WinPE image ” on page 54.
Configuring Network Boot Service for predefined computers

Predefined computers of Deployment Solution are those computers whose details are added to the Notification Server even before the computers are added to the network. The specific computer details that qualify a client computer as predefined computer are, computer name, MAC address, Serial number, UUID and so on. Deployment Solution's filter criteria resolves an unknown computer as a predefined computer based on these computer details that are added to the Notification Server. You can add the computer details through the Settings > Deployment > Predefined Computers menu of the console.

To boot a predefined computer in the preboot environment, you must do the following:

- Create and configure a preboot environment through the Settings > Deployment > Manage Preboot Configurations menu.
- Configure a site server with the Network Boot Service (NBS) settings of predefined computers

For Windows, after the client computers boot to the preboot environment, you can configure the initial deployment job that executes on the computers. The initial deployment job menu contains the tasks that you configure through the Settings > Deployment > Initial Deployment Settings > Redeployment (Managed Computer) Menu menu to execute on the client computers.
To configure NBS settings for predefined computers

1 In the Symantec Management Console, click **Settings >Deployment > NBS General Settings**.

2 In the **NBS General Settings** dialog box, for the **Network Boot Service Configuration**, configure the settings for the predefined client computers.

   - **Network Boot Service Configuration**
     - Lets you configure the Network Boot Service (NBS) for a site server.
     - To enable or disable the policy, you must select the **Turn On** or **Turn Off** icons on the right side of the dialog box or page.

   - **Apply NBS settings immediately**
     - Check the option if you want to apply the NBS settings immediately on the site servers.
     - If the option remains unchecked then the NBS configurations changes are applied as per the schedule set in the Symantec Management Agent (SMA) for rolling out policies.

   - **Enable the NBS service**
     - Lets you start or stop the PXE service on the NBS site servers.
     - By default, this option is checked.

     - For the Mac computers, you can enable or disable the Mac Netboot BSDP service on the NBS site servers through **Enable Mac Netboot (BSDP) support** option.

   - **Reset button**
     - Lets you restore the previous NBS settings that you configured in the dialog box.

3 In the **NBS General Settings** dialog box, for the **Redeployment (Predefined Computer) Menu**, select **PXE menu (Windows/ Linux) tab**.

   Configure the following settings:

   - **Respond to Predefined computers**
     - Check this option if you want to respond to the predefined client computers.

   - **PXE boot image**
     - Select the PXE or preboot image that you have configured to boot the predefined computers in the preboot environment. If you do not want to boot using a PXE image, you can select, **Next Device (BIOS/EFI)**. The potential booting devices of BIOS are CD, hard disk, and so on. Based on whether the default boot option of the client computer is set to BIOS or EFI, the computer boots to the preboot environment. Computers of UEFI architecture can boot in the preboot environment using the x64-bit preboot or PXE image of Windows.

     For the PXE image, select any of the following architectures from the drop-down list:
- **Auto**
  This option is displayed if a preboot configuration is created for both x86 and x64 architectures and selects the appropriate configuration as per the architecture of the client computer. For example, if you have a client computer whose processor type is x64 but the installed operating system is Windows 7 x86, then the **Auto** option boots the computer in x64 architecture.

- **x86**
  Select this option if the PXE image that you have created is for the x86 architecture of the operating system.

- **x64**
  Select this option if the PXE image that you have created is for the x64 architecture of the operating system.

- **Prompt**
  Configure this option to change the default prompt for F8 when booting the computer in the preboot environment. You can enter a message in the textbox that you want to display on the client computer. After the message appears in the client computer, you can press F8 to invoke the network boot menu. Select the option, **Continue immediately** if you want to deploy the PXE boot image immediately after you select the boot image or select, **Continue after** to invoke the boot menu after the time period that you specify.

4. Click **Save changes**.

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

   See “Preparing predefined computers to boot with WinPE image” on page 64.

   See “About predefined computers in Deployment Solution” on page 48.

   See “Configuring NBS for Mac computers” on page 178.

**Configuring Network Boot Service for managed computers**

Deployment Solution has provision to redeploy a Windows, Linux, or Mac managed computer to a preboot environment. Redeployment of a managed computer facilitates you to install a new operating system or a driver on the computer. Before you redeploy the managed computer, you must configure the site server on which the Network Boot Service (NBS) is installed.

See “Installing Network Boot Service on site server” on page 35.

After the Windows client computers boot to the preboot environment, you can configure the initial deployment job to execute on the computers. The initial deployment job menu contains the tasks that you configure through the **Settings > Deployment > Initial Deployment Settings** menu to execute on the client computers.
To configure site server with NBS settings for managed computers

1. In the Symantec Management Console, click **Settings >Deployment > NBS General Settings**.

2. In the **NBS General Settings** dialog box, for the **Network Boot Service Configuration**, configure the settings for the managed client computers.

   **Network Boot Service Configuration**
   - Lets you configure the Network Boot Service (NBS) for a site server.
   - To enable or disable the policy, you must select the **Turn On** or **Turn Off** icons on the right side of the dialog box or page.

   **Apply NBS settings immediately**
   - Check the option if you want to apply the NBS policy immediately on the site servers.
   - If the option remains unchecked then the NBS configurations changes are applied as per the schedule set in the Symantec Management Agent (SMA) for rolling out policies.

   **Enable the NBS service**
   - Check the NBS service to enable the service on the site server.
   - By default, this option is checked.

   **Reset button**
   - Lets you restore the previous configuration that you performed for the NBS site server.

3. In the **NBS General Settings** dialog box, for the **Redeployment (Managed Computer) Menu** configure the following settings:

   This option lets you select the PXE image to deploy on a Windows or Linux managed client computer.

   The various options to configure are as follows:

   - **Respond to Managed computers**
     - Check this option if you want to respond to the managed client computers to configure them to boot in the preboot environment using a PXE image.

   - **PXE image**
     - Select the PXE image that you want to use to boot the predefined client computers in the preboot environment. If you do not want to boot using a PXE image, you can select, **Next Device (BIOS/EFI)** mode of booting option for the client computer. Based on whether the default boot option of the client computer is set to BIOS or EFI, the computer boots to the preboot environment. The potential boot devices of BIOS are CD, disk, and so on. Computers of UEFI architecture can boot in the preboot environment using the x64-bit PXE image of Windows.
     - For the PXE image, select any of the following architectures from the drop-down list:
Auto
Select this option if you want to boot the client computer based on the computer’s processor architecture. For example, if you have a client computer whose processor type is x64 but the installed operating system is x86 of Windows 7, then the **Auto** option boots the computer in x64 architecture mode and not in x86 mode. The **Auto** option can be useful if you have created a common PXE image for both x86 and x64 architectures or want to boot a computer as per the processor architecture irrespective of the OS architecture. You create PXE images through the **Manage Preboot Configuration** dialog box of the console.

x86
Select this option if the PXE image that you have created is for the x86 architecture of the operating system.

x64
Select this option if the PXE image that you have created is for the x64 architecture of the operating system.

Prompt
Configure the option to display the prompt message on the client computer to display the network boot menu. You can enter a message in the textbox that you want to display on the client computer. After the message appears in the client computer, you can press F8 to invoke the network boot menu. Select the option, **Continue immediately** if you want to deploy the PXE boot image immediately after you select the boot image or select, **Continue after** to invoke the boot menu after the time period that you specify.

4 Click **Save changes**.

5 Again, in the console, click the **Settings >Deployment > NBS Global Settings** menu. This step is optional.

   See “About filtering computers through NBS Global Settings” on page 86.

6 In the **NBS Global Settings** dialog box or pane, click **Save Changes**.

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

   See “Booting managed Windows computer with WinPE image” on page 74.

   See “Configuring the initial deployment settings” on page 207.

Creating preboot configuration for Windows

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

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

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

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

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

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

- For WinPE 3.1, you must also download and install the Windows AIK for Windows 7. After you install the Windows AIK for Windows 7, follow the Windows AIK Supplement for Windows 7 SP1 instructions to create the preboot environment for WinPE 3.1.
- For WinPE 4.0, you must download and install the Windows ADK for Windows 8.
- For WinPE 5.1, after you download and install the Windows ADK for Windows 8.1 Update, you must also execute the steps that are mentioned in the article WinPE 5.0 to WinPE 5.1. Follow the following URL:
  If you do not follow the steps then by default the WAIK folder is created for WinPE 5.0.
- For WinPE 10, download and install Windows ADK for Windows 10.
  Remove the older ADK's from the computer by running the older ADK setup file from other ADK's.
Note: Microsoft does not allow multiple ADKs on the same computer.

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

How to change a preboot configuration?

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

To change a preboot configuration

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

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

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

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

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

- Settings > All Settings > Deployment > Preboot Configuration

To create a preboot configuration

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

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

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

- **WinPE 3.1**
  - Download and install the Windows AIK for Windows 7 and Supplement for Windows 7 SP1
    This option is displayed if the Windows Automated Installation Kit (AIK) for Windows 7 is not installed on Notification Server.
    
    **Note:** To use WinPE 3.1 as a preboot environment, you must first download and install the Windows AIK for Windows 7 followed by installing the Windows AIK Supplement for Windows 7 SP1.

- Then import the Windows AIK install into DS
  Lets you modify the BDC package to include the WAIK folder that is installed after you install the Windows Automated Installation Kit (AIK) for Windows 7.

- **WinPE 4.0**
  - Download and install the Windows ADK for Windows 8
    This option is displayed if the Windows Assessment and Deployment Kit (ADK) for Windows 8 is not installed on Notification Server.
    Ensure that you select the following options while installing the ADK for Windows 8:
    - Deployment Tools
    - Windows Preinstallation Environment (Windows PE)

  - Then import the Windows ADK install into DS
    Lets you modify the BDC package to include the WAIK folder that is installed after you install the Windows Assessment and Deployment Kit (ADK) for Windows 8.

- **WinPE 5.x**
  - Download and install the Windows ADK for Windows 8.1 Update
    This option is displayed if the Windows Assessment and Deployment Kit (ADK) for Windows 8.1 is not installed on Notification Server.
    Ensure that you select the following options while installing the ADK for Windows 8.1:
    - Deployment Tools
    - Windows Preinstallation Environment (Windows PE)

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

  - Then import the Windows ADK install into DS
    Lets you modify the BDC package to include the WAIK folder that is installed after you install the Windows Assessment and Deployment Kit (ADK) for Windows 8.1.

- **WinPE 10 (From 8.0 HF2 onwards)**
  - Download and install the Windows ADK for Windows 10 Update
    This option is displayed if the Windows Assessment and Deployment Kit (ADK) for Windows 10 is not installed on Notification Server.

    **Note:** Remove older ADK's from the computer by running the older ADK setup file from other
ADK’s. Microsoft does not allow multiple ADK’s on the same computer.

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

- Deployment Tools
- Windows Preinstallation Environment (Windows PE)

For more information, refer to the following article: Info3561

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

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

   - **Operating System**: Select the WinPE version.
   - **Architecture**: Select x86 or x64 for Windows.
   - **OEMextension**: Select DS Agent as the OEM agent.
   - **Lock the keyboard and mouse**: For Windows, you can select this option to lock the keyboard and mouse while the computer is booted to the preboot environment.
   - **Select which preboot environments to build**: Select the type of preboot environment you want to configure.

   You can select from the following:

   - **PXE**: This preboot configuration can be accessed only from the Network Boot Service (NBS) server. Only the client computers that are configured to boot to and from their network card can access the configuration.
   - **Automation Folder**: This preboot configuration can be installed on the client computers by using policies. You can access these policies from Settings > Agent/Plug-ins > Deployment.
   - **Both PXE and Automation Folder**: This option creates both types of configuration.
4. On the **Add Preboot Configurations** page, click **OK**.

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

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

See “Preparing unknown computers to boot with WinPE image” on page 54.

See “About types of boot environments in Deployment Solution” on page 24.

### Customizing preboot background image manually

Deployment Solution has the provision to customize the preboot background screen image manually. You can now replace the background screen image displayed in WinPE preboot environment.

**To replace the background screen image manually**

1. Create two background graphic images in the .bmp format and of 640x480 or 800x600 pixels in resolution.

   One image must be for the unlocked WinPE preboot environment and the other for the WinPE preboot environment in which the keyboard and mouse are locked.

2. Name the files as `winpe.bmp` and `winpe-lock.bmp` and place them in the following directories:

   - `\bootwiz\oem\ds\winpe2\x86\optional\boot`
   - `\bootwiz\oem\ds\winpe2\x64\optional\boot`

   Ensure that you place the files both on the computer on which Symantec Management Platform is installed and on the site servers.

### Creating preboot configuration for Linux

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

The PXE environment lets you boot a client computer in the preboot environment using a PXE image over a network. A PXE image is saved on the site server on which the Network Boot Service (NBS) is installed. Deployment Solution lets you configure the LinuxPE image using the **Manage Preboot Configurations** option of the console. Ensure that the NBS policy is enabled on the site server before you configure the LinuxPE image. If you configure a LinuxPE image before installing the NBS on a site server, then you have to recreate the environment. Every time a LinuxPE image is configured and saved, the Notification Server (NS) distributes the image to all the NBS site servers of a network.
An automation environment is created when you install an Automation Folder containing the LinuxPE package on a client computer. To install an Automation Folder, you must enable the Deployment Automation folder for Linux -Install policy through the console. By default, Deployment Solution creates LinInstall folder for Linux computers. The automation folder is created on the Notification Server computer and is installed on the client computers after you enable the predefined deployment Automation Folder Plug-in policy through the console.

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

To use the preboot configuration, you must have the administrative rights and the User Account Control (UAC) settings disabled.

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

- Settings > Deployment > Manage Preboot Configuration
- Settings > All Settings > Deployment > Preboot Configuration

To create a preboot configuration

1. Launch the Symantec Management Console.
2. In the Symantec Management Console, on the Settings menu, click Deployment > Manage Preboot Configurations.
3. In the Manage Preboot Configurations dialog box, click Add.
4. In the Add Preboot Configurations dialog box, enter the name and description of the preboot configuration.

- **Operating System**: Select Linux operating system.
- **Architecture**: Select the x86. The x86 Linux preboot configuration can be deployed on both x86-bit client computers as well as x64-bit client computers.
- **OEMextension**: Select DS Agent as the OEM agent.
Select which preboot environments to build

Select the type of preboot environment you want to configure.

You can select from the following:

- **PXE**
  This preboot configuration can be accessed only from the Network Boot Service (NBS) server. Only the client computers that are configured to boot to and from their network card can access the configuration.

- **Automation Folder**
  This preboot configuration can be installed on the client computers by using policies. You can access these policies from Settings > Agent/Plug-ins > Deployment.

- **Both PXE and Automation Folder**
  This option creates both types of configuration.

5 On the Add Preboot Configurations page, click OK.

6 On the Preboot Configurations page, click Save changes.

Creating preboot configuration for Mac

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

For Mac, you create NetBoot environment using the images that are created before creating the preboot environment. The NetBoot environment is used to boot the client computer in preboot environment. You can also create a NetInstall environment to boot client computers in the preboot environment and install Mac OS without manual intervention using the Mac configuration file.

See “Creating and modifying NetBoot images” on page 172.

To use the preboot configuration, you must have the administrative rights and the User Account Control (UAC) settings disabled.

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

- **Settings > Deployment > Manage Preboot Configuration**
- **Settings > All Settings > Deployment > Preboot Configuration**
To create a preboot configuration

1. In the Symantec Management Console, on the Settings menu, click Deployment > Manage Preboot Configurations.
2. In the Manage Preboot Configurations dialog box, click Add.
3. In the Add Preboot Configurations dialog box, enter the name and description of the preboot configuration.
   - Operating system: Select Mac operating system.
   - OEMextention: Select DS Agent as the OEM agent.
   - Select Mac Preboot Environment to upload: These options are available when you select Mac as the operating system.
     - NetBoot: You can create a NetBoot configuration environment by selecting NetBoot.
     - NetInstall: You can create a NetInstall configuration environment by selecting NetInstall.
     Browse and select the NetBoot or NetInstall folder (<name>.nbi) by clicking on the folder icon. To select a folder that is placed on a UNC location, use, \\<ipaddress>\<shared folder> in the File Name.

4. On the Add Preboot Configurations page, click OK.
5. On the Preboot Configurations page, click Save changes.

Creating preboot configuration for Mac
See “Configuring NBS for Mac computers” on page 178.

Customizing background image for Mac automation environment manually
Deployment Solution lets you customize the background screen image that is displayed in the automation environment manually. By default, the background image displays the Deployment Solution automation background image.

To change the desktop background image, refer to support.apple.com.
Editing and deleting preboot configurations

Deployment Solution lets you edit or delete the preboot configurations that you have created. You cannot edit the default preboot configurations, LinInstall, and PEInstall of Linux and Windows operating systems respectively. If you create a preboot configuration for WinPE, then you can edit only the architecture and can switch the environments. If you create a preboot environment for Linux, then you can edit the OEM extensions, and can switch to different environments. If you create a preboot configuration for Mac, then you can edit to upload a different NetBoot image.

To edit preboot configurations

1. In the Symantec Management Console, on the Settings menu, click Settings > Deployment > Manage 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 > Manage 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 “Configuring the preboot environment” on page 87.
Creating and Deploying a Windows disk image

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

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

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

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

- Creating a Windows image of a client computer
  See Table 5-1 on page 108.

- Deploying a Windows image on a client computer
  See Table 5-2 on page 110.

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

**Table 5-1**  Process for creating an image of a Windows client computer

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Launch the Console</td>
<td>Launch the Symantec Management Console. You can launch the console either from the Start menu of the Notification Server computer or from any computer of the network. To access the console from a different computer, you must type the following: http://&lt;IP address of NS&gt;/altiris/console</td>
</tr>
<tr>
<td>Step 2</td>
<td>Prepare a reference computer for imaging.</td>
<td>Prepare the reference computer that contains the core software and settings that you want to be replicated on other computers. For Windows XP and Windows 2003, install the Sysprep files on the reference computer. Copy the support\tools\deploy.cab file from your Windows XP installation disk or service pack. See &quot;Configuring the Sysprep imaging&quot; on page 112.</td>
</tr>
<tr>
<td>Step</td>
<td>Action</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Step 3</td>
<td>Create a client job for the deployment tasks in the console</td>
<td>To create a client job, right-click on the Deployment folder and select New &gt; Client Job menu. By default, a job of the name New Client Job is created that you can rename appropriately. Navigate to the Manage &gt; Jobs and Tasks menu of the console and create a client job for the Deployment folder. To create a client job, right-click on the Deployment folder and select New &gt; Client Job menu. By default, a job of the name New Client Job is created that you can rename appropriately.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Execute the <strong>Prepare for Image capture</strong> task</td>
<td>Run the <strong>Prepare for Image capture</strong> task if you want to perform Sysprep imaging and use the <strong>Include DeployAnywhere for hardware independent imaging</strong> option for the <strong>Deploy Image</strong> task. The <strong>Prepare for Image capture</strong> task ensures that the captured image does not contain any hardware-dependent data. You can then deploy a hardware independent image on other computers. <strong>Note</strong>: If you deploy a disk image using the <strong>Include DeployAnywhere for hardware independent imaging</strong> option and you have not performed the <strong>Prepare for Image capture</strong> task, the client computer image gets corrupted. See “<strong>Configuring the Sysprep imaging</strong>” on page 112. See “<strong>Preparing to capture an image</strong>” on page 138.</td>
</tr>
<tr>
<td>Step</td>
<td>Action</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>---------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Step 5</td>
<td>Create an image of the client computer</td>
<td>Run the <strong>Create Image</strong> task to create the disk image of the reference computer.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You can either run the task immediately by using the <strong>Quick Run</strong> option of the task that you have saved or you can schedule the task to run later on the reference computer.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Creating a Windows image” on page 113.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Scheduling a deployment job or task” on page 198.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Launch the Console</td>
<td>Launch the Symantec Management Console.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You can launch the console either from the Start menu of the Notification Server computer or from any computer of the network. To access the console from a different computer, you must type the following: http://&lt;IP address of NS&gt;/altiris/console</td>
</tr>
<tr>
<td>Step 2</td>
<td>Boot the client computer to Automation environment</td>
<td>Boot the client computer to Automation environment using the <strong>Boot To</strong> task.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Creating a Boot To task” on page 199.</td>
</tr>
</tbody>
</table>
### Table 5-2  Process for deploying an image of a Windows client computer *(continued)*

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 3 | Create a client job for the deployment tasks in the console | To create a client job, right-click on the Deployment folder and select **New > Client Job** menu. By default, a job of the name **New Client Job** is created that you can rename appropriately.  
**Navigate to the Manage > Jobs and Tasks menu of the console and create a client job for the Deployment folder.**  
To create a client job, right-click on the Deployment folder and select **New > Client Job** menu. By default, a job of the name **New Client Job** is created that you can rename appropriately. |
| Step 4 | Deploy the image on the client computer | Create a **Deploy Image** task for the target client computers.  
You can specify the Sysprep-enabled image that you captured to be deployed on the target client computers.  
You can either execute the task immediately by using the **Quick Run** option of the task that you have saved or you can schedule the task to be executed later on the reference computer.  
See “Deploying a Windows image” on page 116.  
See “Scheduling a deployment job or task” on page 198. |
| Step 5 | Boot the client computer to Production environment | Boot the client computer to production environment using the **Boot To** task.  
See “Creating a Boot To task” on page 199. |

See “Configuring the Sysprep imaging” on page 112.

See “Restoring a backup image” on page 141.
Configuring the Sysprep imaging

The System Preparation Tool (Sysprep) is a Microsoft utility that prepares computers for Windows OS deployments. All versions of Windows OS that are released after Windows XP and Windows 2003 include Sysprep files as part of the OS installation. The **Sysprep Imaging Configuration** dialog box lets you configure Deployment Solution to use the sysprep files to execute the **Prepare for Image capture** task. For this task to work on Windows XP computers, you must upload the deploy.cab file to Deployment Solution. The Sysprep imaging is supported for Windows x86 and x64 only.

When you work with Microsoft domains, each computer must use a unique Windows SID. SIDs are security IDs that are used with Windows NT or later operating systems. Before you deploy Windows images, you must 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.

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

To configure Sysprep imaging

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

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

   The fields and their descriptions are as follows:

   - **x86 Deploy.cab**
     
     Lets you upload the deploy.cab file for the 32-bit Windows computers.
     
     You must download the x86 deploy.cab file, which is required for the Sysprep imaging tasks, from the Microsoft website.

   - **x64 Deploy.cab**

     Lets you upload the deploy.cab file for the 64-bit Windows computers.
     
     You must download the x64 deploy.cab file, which is required for the Sysprep imaging tasks, from the Microsoft website.

3. Click **Save changes**.
Creating a Windows image

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

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

To create a Windows image

1. In the Symantec Management Console, from the Manage menu select Jobs and tasks.

2. In the left pane, do either of the following:
   - Right-click System Jobs and Tasks and select New > Task.
   - Expand the System Jobs and Tasks and right-click Deployment to select New > Task.

3. In the Create New Task dialog box, select Deployment > Create Image option.

4. The fields and their descriptions are as follows:

   **Task name**
   - Displays the default task name as Create Image.
   - You can edit the default task name to specify a relevant task name. For example, Create Image_Windows XP.

   **Image name**
   - Enter a name for the image to be created.
   - Image name supports only ASCII characters. If you use a token for image name, ensure that it is a valid predefined token. Otherwise, an image package with a blank name is created, which is difficult to locate when you want to deploy the image.

   See “About predefined tokens in Deployment Solution” on page 217.
<table>
<thead>
<tr>
<th>Description</th>
<th>Lets you enter a description, if required.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Imaging tool</td>
<td>You can create disk image and backup image of Windows client computers using the Ghost tool. The Ghost imaging tool creates disk images with the default option <strong>Balanced for size and speed</strong> mode.</td>
</tr>
<tr>
<td>Image type</td>
<td>Lets you select the type of image that you want to capture. Select from the following types of computer images:</td>
</tr>
</tbody>
</table>

- **Disk Image**
  - The **Disk Image** can be deployed on multiple computers. These images are saved in a package on the package server and can be distributed to other package servers.
  - If you intend to deploy a disk image using the option **Include DeployAnywhere for hardware independent imaging**, ensure that the **Prepare for Image capture** task is executed before the image is created. Otherwise, the client computer on which this disk image is deployed might get corrupted.
  - See “Configuring the Sysprep imaging” on page 112.

- **Back-Up image**
  - A **Back-Up Image** contains a snapshot of the hard disk of a computer. The backup images retain the data and software of a specific computer. A backup image can be restored only to the computer from which the image was captured. You can restore the image name same as the computer name if you use %COMPNAME% token as the image name.
  - The images cannot be deployed on multiple computers and cannot be saved in a package and distributed to other package servers through the replication process. Back-up images are created if you want to image only a data disk, which is a disk without an operating system or a partition of a data disk.
  - See “About predefined tokens in Deployment Solution” on page 217.
5 On the **Create Image** page, you can set the **Advanced** imaging options. Following are the options that you can set with the description:

**Media**

Determines at what point an image file is split into multiple files.

When you use Ghost imaging tool to create image over network such as HTTP or mapped path of Package Server or SMP, the maximum span size is 1.99 GB that refers to the 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.

For UEFI enabled Dell Precision T7600 computer, you must use the `-fngcc` switch to create an image.

See “About command-line switches” on page 236.
HTTP

Lets you upload and download images through 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 task fails and returns a message that the file cannot be created.

Deployment Solution supports both Anonymous Authentication and Basic Authentication.

For Ghost tool you must add MIME types to the IIS Manager.

To add the MIME types, navigate to the Internet Information Services (IIS) Manager and add the MIME Types for the folder where images are stored. For the MIME types, enter the File name extension and the MIME Type.

For the Ghost tool, you must add the following MIME types:

- **File name extension**: .gho and **MIME Type**: application/octet-stream
- **File name extension**: .ghs and **MIME Type**: application/octet-stream

Ghost tool supports the HTTP Web server that is configured on Windows 2008 IIS 7.5 and on Windows 2003 server IIS 6.0.

6  Click OK.

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

See “Creating and Deploying a Windows disk image” on page 107.

See “Deploying a Windows image” on page 116.

See “Restoring a backup image” on page 141.

Deploying a Windows image

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

Before you perform the **Deploy Image** task, you must know the following:

- 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.
- 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.
- If the computer is a member of a domain, supply the appropriate credentials to rejoin the domain.
- Ensure that you deploy a BIOS-based image on a BIOS-based computer and an EFI-based computer image on an EFI-based computer. If you deploy a BIOS-based image on an EFI-based computer, the EFI-based computer does not boot to automation environment from production environment.
- Ensure that you run the `x:/bcdedit.exe` after deploying a UEFI enabled image on the virtual machine that has ESX 5.0 and then boot the virtual machine into the production environment.

To create a deploy image task

1. In the Symantec Management Console, navigate to the **Manage** menu and select **Jobs and tasks**.
2. On the right pane, right-click **Jobs and tasks** and select **New > Task**.
3. On the **Create new task** page, select **Deploy Image**.
   The **Create or Deploy image** task can only be executed in the Automation environment.
4. Specify a name for the task on the first field.
5 Enter the following of the Imaging section:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image Name</td>
<td>Enter the name of the image file to deploy.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> For Linux, only the Name and Image Name fields are necessary. All of the other fields are optional.</td>
</tr>
<tr>
<td>Product Key</td>
<td>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.</td>
</tr>
</tbody>
</table>

6 In the DeployAnywhere section, check Include DeployAnywhere for hardware independent imaging to deploy the drivers that you added to the DeployAnywhere database.

The DeployAnywhere database works only for the WinPE preboot operating system. After you select the option, the DeployAnywhere database executes once you deploy the image. The database runs even when the computer is running the WinPE preboot operating system. This option discovers what type of hardware is on the destination client computer and creates a new HAL. The HAL and the required drivers that Sysprep removed are then deployed to help the computer boot successfully.

You can skip validation of missing critical drivers that are added in DeployAnywhere database by checking Skip missing critical drivers option. Check this option if you do not want the drivers that you add to pass through the validation that is performed by Deployment Solution. The system file and the .inf file validations are bypassed for the drivers that you add if you select this option.

After you check this option, select either of the options from the Bypass Driver Validation drop-down list:

- **None**
  - By default, this value is selected, which means that for no drivers the validation is bypassed.

- **All**
  - You can select if you want to bypass validation for all the drivers.
**Note:** If a driver does not pass the validation checks and if you did not check the **Bypass Driver Validation** option, then the driver will not be installed on the computer after you execute the **Install Windows OS** task.

7. In the **DeployAnywhere** section, select the debug log level in **Debug Log Level** for the installation of the drivers.

The debug log levels are as follows:

- **None**
  This log level captures the logs of all the failures of a task.

- **Driver Match**
  The log level is 5 and it retrieves log information about the drivers that match.

- **Function Start**
  The log level is 10 and the log is created when a function is entered.

- **Function Ends**
  The log level is 11 and the log is created when the function exits.

- **Device Details**
  The log level is 20 and it prints information about the devices.

- **INF Parsing**
  The log level is 30 and it logs information about inf parsing.

- **No matching Device for inf**
  The log level is 40 and it logs information about infs if they do not match with devices of the client computer.

- **All**
  The log level is 255 and it logs information on all the points that are listed for this field.

8. Select **Enable tagging of the drivers** option to add tags to the **Tags** field. Drivers that are tagged are deployed forcefully on the client computers.
1. Select one of the following options from the **Sysprep Configuration** section:

- **Generate Sysprep configuration file using inventory data**
  - The required information is obtained from the CMDB.

- **Custom Sysprep configuration file**
  - Click **Browse** to select the custom Sysprep file that you created.
2. Click the **Advanced** tab to set the following:

**Partition**

Lets you decide the partitions on which you deploy the image. You can change the destination partition size by clicking the partition number.

**Note:** For Data Partition or System reserve partition deployment do not use **DeployAnywhere**.

For Linux, only Data Partition deployment is supported.

To deploy Windows 7 with system reserved partition, create a job to run deploy system reserved partition and system partition in the same preboot environment.

In case of Mac Deploy image task, if empty disk space is present on the client computer then it is merged with the last partition of the client computer.

**Note:** For Mac Deploy image task ensure that the client computer partition capacity is more than the partition capacity of the image source computer.

**Command-line**

Lets you add command-line options for the imaging tool.

For Ghost partition deployment, following command lines must not be used:

MODE, Size, SRC and DST values should not be used for command line.

If you want to deploy an image of a Windows 2012 computer of BIOS type which does not have a system reserve partition on a UEFI computer, then you must use the following Ghost switch `-cesp`

**Note:** Ensure that you do not specify the switch `-SZEE` and select the Resize partition option simultaneously for the deploy image task.
Multicasting

Lets you configure the number of computers on which you want to multicast the image. You can override the default multicast settings that were set in Settings > Deployment > Image Multicasting.

There must be at least one computer over the threshold value that you specify for multicasting. For example, if the threshold count is 2, there must be at least two client computers and one master computer, which is 3 in total, before multicasting is used in the session.

Deployment Solution does not support Multicast and Unicast options simultaneously if you use the Ghost imaging tool.

File Preservation

Lets you specify the files and folders that you want to preserve when the image is restored.

This option is not supported if the client computer is installed with Linux operating system.

HTTP

Lets you add the credentials that are required to deploy an image, which was obtained from an HTTP site.

3 Click OK.

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

See “Creating and Deploying a Windows disk image” on page 107.

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

Creating and deploying Linux disk images

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

For Linux operating system, deploying disk images and back-up images does not support the ReiserFS file system. Image deployment supports only the SUSE Ext3 file system. If you have a ReiserFS partition, you must use the -raw switch when you image the partition to preserve
its structure. Linux IDE images must be deployed on computers that have the Linux IDE disk. SCSI disk images must also be deployed on computers having the SCSI disk image.

The following process lists the steps that you must follow to create an image of a Linux client computer and to deploy the Linux image on other client computers.

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

Table 5-3  Process for creating an image of a Linux client computer

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Launch the Console</td>
<td>Launch the Symantec Management Console. You can launch the console either from the Start menu of the Notification Server computer or from any computer of the network. To access the console from a different computer, you must type the following: http://&lt;IP address of NS&gt; /altiris/console</td>
</tr>
<tr>
<td>Step 2</td>
<td>Prepare a reference computer for imaging.</td>
<td>Prepare the reference computer that contains the core software and settings that you want to be replicated on other computers.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Create a client job for the deployment tasks in the console</td>
<td>To create a client job, right-click on the Deployment folder and select New &gt; Client Job menu. By default, a job of the name New Client Job is created that you can rename appropriately. Navigate to the Manage &gt; Jobs and Tasks menu of the console and create a client job for the Deployment folder. To create a client job, right-click on the Deployment folder and select New &gt; Client Job menu. By default, a job of the name New Client Job is created that you can rename appropriately.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Execute the Prepare for Image capture task</td>
<td>Execute the Prepare for Image capture task to ensure that the captured image does not contain any hardware-dependent data. You can then deploy a hardware independent image on other computers. See &quot;Preparing to capture an image&quot; on page 138.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Create an image of the client computer</td>
<td>Execute the Create Image task to create the disk image of the reference computer. You can either execute the task immediately by using the Quick Run option of the task that you have saved or you can schedule the task to be executed later on the reference computer. See &quot;Creating a Linux image&quot; on page 124. See &quot;Scheduling a deployment job or task&quot; on page 198.</td>
</tr>
</tbody>
</table>
Following are the steps that you must follow to deploy an image of a Linux client computer on client computers:

**Table 5-4** Process for deploying an image of a Linux client computer

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Launch the Console</td>
<td>Launch the Symantec Management Console. You can launch the console either from the Start menu of the Notification Server computer or from any computer of the network. To access the console from a different computer, you must type the following: http://&lt;IP address of NS&gt; /altiris/console</td>
</tr>
<tr>
<td>Step 2</td>
<td>Create a client job for the deployment tasks in the console</td>
<td>To create a client job, right-click on the Deployment folder and select New &gt; Client Job menu. By default, a job of the name <strong>New Client Job</strong> is created that you can rename appropriately. Navigate to the Manage &gt; Jobs and Tasks menu of the console and create a client job for the Deployment folder. To create a client job, right-click on the Deployment folder and select New &gt; Client Job menu. By default, a job of the name <strong>New Client Job</strong> is created that you can rename appropriately.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Boot the client computer in Automation environment</td>
<td>Create a Boot To task and add the task to the client job to boot the client computer to Automation environment. See “Creating a Boot To task” on page 199.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Deploy the image on the client computer</td>
<td>Create a Deploy Image task for the target client computers. You can either execute the task immediately by using the Quick Run option of the task that you have saved or you can schedule the task to be executed later on the reference computer. See “Deploying a Linux image” on page 127. See “Scheduling a deployment job or task” on page 198.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Boot the client computer to production</td>
<td>Boot the client computer to production using the Boot To task. See “Creating a Boot To task” on page 199.</td>
</tr>
</tbody>
</table>

**Creating a Linux image**

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

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

To create an image

1. Launch the Symantec Management Console.
2. In the Symantec Management Console, from the Manage menu select Jobs and tasks.
3. In the left pane, right-click System Jobs and Tasks and click New > Task.
4. The fields and their descriptions are as follows:

   **Task name** icon 
   Displays the default task name as Create Image. You can edit the default task name to specify a relevant task name. For example, Create Image_LINUX.

   **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. In case you use an invalid token, then either an error is displayed on the task or the image package is created with the task name.
   See “About predefined tokens in Deployment Solution” on page 217.

   **Description** 
   Enter a description, if required.

   **Imaging tool** 
   You can create disk image and backup image of Linux client computers using the Ghost imaging tool. By default, the Ghost imaging tool creates disk images with the default option Balanced for size and speed mode.
Select from the following two types of computer images:

- **Disk Image**
  A disk image can be deployed to multiple computers. These images are saved in a package on the package server and are replicated to other package servers. Ensure that the Prepare for Image capture task is executed before the image is created.

- **Backup image**
  A backup image is used to back up a single computer. These images must be deployed only to the same computer where they were created from. They must 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 that is a disk without an operating system or partition of a data disk, select the backup image option.

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

**Media**
When you use Ghost imaging tool to create image over network such as HTTP or mapped path of Package Server or SMP, the maximum span size is 1.99 GB that refers to the 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.

See “About command-line switches” on page 236.
HTTP

Lets you upload and download images through 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 cannot be created.

For the Ghost imaging tool, you must add MIME type to the IIS Manager.

To add the MIME types, navigate to the Internet Information Services (IIS) Manager and add the MIME Types for the folder where images are stored. For the MIME types, enter the File name extension and the MIME Type.

For the Ghost tool, you must add the following MIME types:

- File name extension: .gho and MIME Type: application/octet-stream
- File name extension: .ghs and MIME Type: application/octet-stream

Ghost tool supports the HTTP Web server that is configured on Windows 2008 IIS 7.5 and on Windows 2003 server IIS 6.0.

6 Click OK.

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

See “Creating and deploying Linux disk images” on page 122.

Deploying a Linux image

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

Before you perform the Deploy Image task, you must know the following:

- 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.
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.

**To deploy a Linux image**

1. Launch the Symantec Management Console.
2. In the Symantec Management Console, select Manage > Jobs and Tasks.
3. In the left pane, right-click System Jobs and Tasks folder and select New > Task.
4. Enter the following:

   **Task name icon**
   
   Displays the default task name as Deploy Image. You can edit the default task name to specify a relevant task name. For example, Deploy Image/Linux.

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

   **Note:** For Linux, only the Name and Image Name fields are necessary. All of the other fields are optional.
5 Click the **Advanced** tab to set the following:

**Partition**

Lets you decide the partitions on which you deploy the image. You can change the destination partition size by clicking the partition number.

For Linux, only Data Partition deployment is supported.

**Command-line**

Lets you add command-line options for the imaging tool.

For Ghost partition deployment, following command lines must not be used:

MODE, Size, SRC and DST values should not be used for command line.

**Note:** Ensure that you do not specify the switch -SZEE and select the Resize partition option simultaneously for the deploy image task.

**Multicasting**

Lets you configure the number of computers on which you want to multicast the image. You can override the default multicast settings that were set in Settings > Deployment > Image Multicasting. 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**

Lets you specify the files and folders that you want to preserve when the image is restored.

This option is not supported if the client computer is installed with Linux operating system.

**HTTP**

Lets you add the credentials that are required to deploy an image, which was obtained from an HTTP site.

6 Click **OK**.

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

See “Creating and deploying Linux disk images” on page 122.

### Creating and deploying Mac images

Deployment Solution lets you create and deploy Mac images. Imaging of a client computer involves copying the applications and settings of a computer into an image which is then deployed on other computers.
To create Mac images use the **Create Image** task and to deploy an image use the **Deploy Image** task in any preboot mode of the client. The client computer can be booted in preboot environment using a NetBoot image or in the automation environment using the DSAutomation volume. You can access the **Create Image** task and the **Deploy Image** task from the **Manage > Jobs and Tasks** menu.

**Note:** Mac imaging is not supported on HTTP or HTTPS. You must have the **Publish UNC codebase** check box checked in the **Package Server Settings** page.

See "Installing and uninstlling Automation Folder on client computers" on page 39.

The following process elaborates the steps that are involved in creating and deploying Mac images on client computer:

**Table 5-5  Creating and deploying Mac image**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Launch the console</td>
<td>Launch the Symantec Management Console. You can launch the console either from the Start menu of the Notification Server computer or from any computer of the network. To access the console from a different computer, you must type the following: http://&lt;IP address of NS&gt;/altiris/console</td>
</tr>
</tbody>
</table>
| Step 2   | Boot the image source client computer to preboot environment | You must boot the image source client computer to preboot environment using one of the following:  
  ■ NetBoot image  
  ■ Automation folder  
  See "Booting Mac computers with NetBoot image" on page 176. |
### Table 5-5 Creating and deploying Mac image (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 3</td>
<td>Create image of the source Mac computer</td>
<td>You use the <strong>Create Image</strong> task to create an image of the source computer after you boot the computer in the preboot environment or automation environment. See “Creating a Mac image” on page 131.</td>
</tr>
</tbody>
</table>
| Step 4 | Boot the target client computer to preboot environment | You must boot the target client computer to preboot environment on which you want to deploy the image using one of the following:  
- NetBoot image  
- Automation folder  
See “Booting Mac computers with NetBoot image” on page 176. |
| Step 5 | Deploy image on the target computer | Deploy the image on Mac computers using the **Deploy Image** task. See “Deploying a Mac image” on page 133. |

### Creating a Mac image

Deployment Solution lets you create the Mac images that you can use to deploy on client computers. You can use predefined tokens to image Mac client computers.

See “About predefined tokens in Deployment Solution” on page 217.

Before you create a Mac image ensure to comply with the following:

- The Mac image source computer is booted in preboot or automation environment.
  Sometimes, the Symantec Management Agent crashes when the computer is booted in the Netboot environment. The issue arises due to Spotlight running in the background. To resolve the issue, you must disable spotlight before you capture the Netboot.
  Move the following files to another location and then reboot the Mac computer:
  /System/Library/LaunchAgents/com.apple.Spotlight.plist
  /System/Library/LaunchDaemons/com.apple.metadata.mds.plist
  For more information, refer to the following URL:
The Mac image source client computer has its IP configured as dynamic and receives it from the DHCP server in the network.

To create a Mac image

1. In the Symantec Management Console, select Manage > Jobs and Tasks.
2. In the left pane, do either of the following:
   - Right-click System Jobs and Tasks folder and select New > Task.
   - Expand the System Jobs and Tasks folder and right-click Deployment folder to select New > Task.
3. In the Create New Task dialog box, under the Deployment folder select the Create Image task.
4. In the Create Image dialog box, specify the details for the following:
   - Task name icon: Displays the default task name as Create Image. You can edit the default task name to specify a relevant task name. For example, Create Image_Mac10.7.
   - Image Name: Enter the name of the image that you want to create.
   - Description: Enter the details of the image that you want to create.
   - Imaging tool: Select the imaging tool as symDeploMac to image the Mac computer.
5. In the Create Image task pane, click the Advanced... button.
6. In the Advanced dialog box, in the Command line tab, set the Source disk (-SRC).

You must enter the details of the disk name and the partition or the volume number of the image source of the Mac client computer. The format to enter the Source disk (-SRC) is diskname:partition or volume number.

For example 1:2, here 1 is the disk name and 2 is the partition number or volume number of the Mac client computer. To know the Mac disk name and partition details of the Mac client computer, navigate to Go > Utilities > Terminal and enter the command diskutil list.

On executing the command, the details of the Mac client computer are displayed. For example, disk0s1, disk0s2, disk2s1 and so on. Here for disk0s1, disk0 is the disk name and 1 is the partition number or the volume number.
In Deployment Solution, the **Source disk (-SRC)** field starts with 1, here 1 corresponds to the disk 0 of the Mac computer. Similarly 2 corresponds to disk 1 of the Mac computers and so on.

Following are few examples of the disk name and partition number format that should be entered in the **Source disk (-SRC)** field:

- For disk0s2 specify the value as 1:2, where 1 is the disk name and 2 is the partition number.
- For disk1s2 specify the value as 2:2, where 1 is the disk name and 2 is the partition number.
- For disk2s1 specify the value as 3:1, where 3 is the disk name and 1 is the partition number.
- For disk2s2 specify the value as 3:2, where 3 is the disk name and 2 is the partition number.

See “Creating and deploying Mac images” on page 129.

See “Deploying a Mac image” on page 133.

**Deploying a Mac image**

Deployment Solution lets you deploy Mac disk images on one or more Mac computers. If you plan to deploy disk images across different models of computers of the same make, ensure to update the operating system of the source computer with the Combo update.

For Mac client computers, following settings must be done to ensure that correct inventory details are displayed on the Notification Server computer:

- In the Symantec Management Console, go to **Settings > Agents/Plug-ins > Targeted Agent Settings**.
  
  In the left pane of the **Targeted Agent Settings** page, select **All Linux/Mac Workstations** option.

  In the **All Linux/Mac Workstations** page, select the **UNIX/Linux/Mac** tab and set the following in the **Computer information**:

  - **Return the following information as computer name** as DNS name
  - **Return the following information as computer domain** as DNS name.

- In the Symantec Management Console, go to **Settings > Agents/Plug-ins > Targeted Agent Settings**.

  In the left pane of the **Targeted Agent Settings** page, select **All Linux/Mac Servers** option.

  In the **All Linux/Mac Servers** page, select the **UNIX/Linux/Mac** tab and set the following in the **Computer information**:
Return the following information as computer name as DNS name

Return the following information as computer domain as DNS name.

To deploy a Mac image

1. In the Symantec Management Console, select Manage > Jobs and Tasks.
2. In the left pane, do either of the following:
   - Right-click System Jobs and Tasks folder and select New > Task.
   - Expand the System Jobs and Tasks folder and right-click Deployment folder to select New > Task.
3. In the Create New Task dialog box, under the Deployment folder select the Deploy Image task.

   In the Deploy Image task pane, specify the following details:

   **Task name** icon
   
   Displays the default task name as Deploy Image.
   You can edit the default task name to specify a relevant task name. For example, Deploy Image_Mac10.7.

   **Imaging**
   
   Select or browse the Mac image with a .mac extension that is to be deployed on the client computer.
Deploy Image Options
Lets you enter the details about deploying the image on the client computer.

Click the **Advanced** button.

In the **Advanced** dialog box, enter details for the following:

- **Partition**
  
  In the **Partition** tab, select the **Resize partition proportionately** to resize disk partitions.

  **Note:** If there is empty disk space present on the computer then it is merged with the last partition of the Mac computer.

- **Command-line**
  
  In the **Command-line** tab, enter the **Destination disk (-DST)**.
  
  You must enter the details of the destination of the Mac client computer where the image is to be deployed. The format to enter the destination is **diskname:partition or volume number**.

  To know the disk name and partition details of the Mac source computer, navigate to **Go > Utilities > Terminal** and enter the command `diskutil list`.

  On executing the command, the details of the Mac client computer are displayed. For example, disk0s1, disk0s2, disk2s1 and so on. Here for disk0s1, disk0 is the disk name and 1 is the partition number or the volume number.

  In Deployment Solution, the **Destination disk (-DST)** field starts with 1, here 1 corresponds to the disk 0 of the Mac computer. Similarly 2 corresponds to disk 1 of the Mac computers and so on.

  Following are few examples of the disk name and partition number format that should be entered in the **Destination disk (-DST)** field.

  - For disk0s2 specify the value as 1:2, where 1 is the disk name and 2 is the partition number.
  - For disk1s2 specify the value as 2:2, where 1 is the disk name and 2 is the partition number.
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 the images.

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 233.

See "Preparing to capture an image" on page 138.

About disk image packages

A Symantec Management Platform package is created for all disk images when you run the Create Image task with Disk Image as the option. You can then use this package to distribute the image to other Package Servers.

Disk images are stored on the Deployment share of the site server on which the Package Service runs. 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 > 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 pre-staging.

You can also delete packages.

See “Deleting an image package” on page 233.

See “About image resources” on page 137.

Prepare to capture an image

The Prepare for Image capture task prepares a client computer before you create an image.

For Windows, the Prepare for Capture Image task uses Sysprep utility to remove the computer name, Security Identifier (SID), the operating system license, GUID of the agent, and some hardware-dependent drivers. You must always run this task before creating a disk image. Sysprep also disables the built-in administrator account and clears the admin password.

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

See “Configuring the Sysprep imaging” on page 112.

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

To prepare for image capture

1. In the Symantec Management Console, select Manage > Jobs and Tasks.
2. In the left pane, do either of the following:
   - Right-click System Jobs and Tasks folder and select New > Task.
- Expand the **System Jobs and Tasks** folder and right-click **Deployment** folder to select **New > Task**.

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

The fields and their descriptions are as follows:

### Task name icon
Displays the default task name as Prepare for Image capture. You can edit the default task name to specify a relevant task name. For example, Prepare for image capture_Linux.

### Pre-imaging
Lets you select the operating system for which you want to create a **Prepare for image capture** task.

For Windows, you can select from the following:

- **OS type**
  Select the version of Windows operating system.

- **Product key**
  Select an operating system license that you use to restore the computer back to its original state after the task runs. For Windows Vista and higher versions, you can select the Current Key option that is displayed in the list. If you select the Current Key option, then the product key is retained with the image. When you select the Current Key option in the Deploy image task, then the key that is captured is used on deploying the Windows image on the client computer.

  If the license is not added to Deployment Solution, you can add one by clicking **New**. In the **Add OS License Key** dialog box, add the product key for the operating system that you select.

---

**Enter credentials to rejoin a domain after capture is complete**
Lets you join back the client computer to the domain after the task executes.

Specify the credentials to join the domain in the **User name**, **Password**, and the **Confirm password** fields.

This option is applicable for the Windows operating system only.
**Boot to**

Lets you select the environment to which you want to boot the client computer before you start the image creation process.

In case of Linux, only x86 architecture type is supported.

You can either select from either of the following options:

- **Automation**
  
  Select this option to boot the client computer in the Automation environment. Automation environment is created on the client computers on which the automation folder is installed. Automation folders are specific to operating systems.

- **PXE**
  
  Select this option if you want to boot the client computer in the preboot environment.

For the PXE image, select any of the following architectures from the drop-down list:

- **Auto**
  
  Select this option if you want to boot the client computer based on the computer's processor architecture. For example, if you have a client computer whose processor type is x64 but the installed operating system is x86 of Windows 7, then the Auto option boots the computer in x64 architecture mode and not in x86 mode.
  
  The Auto option can be useful if you have created a common PXE image for both x86 and x64 architectures or want to boot a computer as per the processor architecture irrespective of the OS architecture. You create PXE images through the Manage Preboot Configuration dialog box of the console.

- **x86**
  
  Select this option if the PXE image that you have created is for the x86 architecture of the operating system.

- **x64**
  
  Select this option if the PXE image that you have created is for the x64 architecture of the operating system.

See “Creating preboot configuration for Windows” on page 96.

See “Creating preboot configuration for Linux” on page 102.

**Registration Period**

The registration time period is the time period during which the client computer is un-enrolled from the Notification Server’s registration policy. This happens only when the client computer tries to boot from one environment to another. Within the specified registration time, the client computer must again register back to the registration policy, failing which, the computer must be registered manually.

The default registration time that is displayed is the registration time that is set in the Global Settings page.

See “About deployment tasks and jobs” on page 191.
Restoring a backup image

In Deployment Solution you can restore the backup image of a client computer. You can restore a backup image only to the client computer from which it is captured. Deployment Solution lets use the %Computername% as the default name for the backup image. You can also preserve any files that you want to retain on the client computer after deploying the backup image.

To restore a backup image

1. In the Symantec Management Console, on the Manage menu, click Jobs and Tasks.
2. On the left pane, right-click Jobs and tasks and select New > Task.
4. Select the image name to restore.

The fields and descriptions are as follows:

<table>
<thead>
<tr>
<th>Task name</th>
<th>icon</th>
<th>Lets you specify the name of the restore backup image task in the text field.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image name</td>
<td></td>
<td>Lets you browse to the backup image that you want to restore.</td>
</tr>
<tr>
<td>Path</td>
<td></td>
<td>Lets you view the path and description of the backup image that you want to restore.</td>
</tr>
</tbody>
</table>

5. (Optional) Click Advanced to specify additional parameters.

The tabs and their descriptions are as follows:

<table>
<thead>
<tr>
<th>Partition</th>
<th>Lets you configure the disk partitions for the backup image that you want to restore.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Check the checkbox, Resize Partition to partition the disks.</td>
</tr>
<tr>
<td></td>
<td>For resizing the disk, you can select any of the following options:</td>
</tr>
<tr>
<td></td>
<td>■ Proportionately</td>
</tr>
<tr>
<td></td>
<td>■ First partition will use available disk space</td>
</tr>
<tr>
<td></td>
<td>■ Last partition will use available disk space</td>
</tr>
<tr>
<td></td>
<td>■ As follows</td>
</tr>
<tr>
<td></td>
<td>This option lets you select the disk partition whose properties you want to configure.</td>
</tr>
</tbody>
</table>
**File Preservation**

Lets you preserve the files and folders of a disk during image restoration.

Use the following options:

- **Preservation partition**
  Select the number of partitions of the disk in which you want to preserve the files and folders that you select in the table. You can select the drives or volumes whose files or folders you want to preserve.

- **Add**
  Click this option to add files and folders of the disk that you want to preserve. You add the options in the **Add File Preservation** dialog box.
  In the **Add File Preservation** dialog box select the drive whose files or folders you want to preserve. Provide the source path of the file or folder and the destination path where the file or folder must be preserved.

- **Edit** icon
  Lets you edit the properties of the drive or volume that you select in the table.

- **Delete** icon
  Lets you delete the drives or volumes that you select in the table.

**Command -line**

You can specify the following:

- **Base command -line**
- **Destination disk (-DTK)**
- **Command-line options**

**HTTP**

Lets you deploy an image from the HTTP server location after you specify the HTTP credentials.

On the Advanced options page, click **OK** to save your options.

6. On the **Restore BackUp Image** task page, click **OK**.

See “About deployment tasks and jobs” on page 191.

---

**Importing images using Resource Import tool**

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

You can also import OS packages using the **Deployment Solution Resource Import Tool**.
To import an existing image

1. Browse to \Install Directory\Program Files\Altiris\Deployment\Tools and execute the ResourceImporterTool.exe. You can execute this tool 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.

How to image a Windows 10 (1607) Anniversary update computer?

The following procedure lists the steps to create and deploy a Sysprep image of a Windows 10 (1607) Anniversary update computer.

To create and deploy a Sysprep image of a computer with Windows 10 Anniversary update operating system

1. Disable the Windows update on the source computer.

   To disable Windows update, run the following commands:
   
   ```
   net stop wuauserv
   sc config wuauserv start= disabled
   ```

   **Note:** If the Windows updates are already installed on the source computer, then Sysprep image task fails.

2. Run Prepare for Image capture task on the source computer.

3. Create an image of the source computer.

4. Deploy image on the target computer.
5 Run the following commands to enable Windows Update services on the computer on which the Windows 10 Anniversary (1607) update is deployed:

```
sc config wuauserv start= auto
net start wuauserv
```

6 Download and install all the updates from Microsoft site on the client computer.
Installing an operating system

This chapter includes the following topics:

- About supported OS installed using Deployment Solution
- Installing Windows OS on client computers
- Installing Linux/ESX OS on client computers
- Installing Mac OS using Deployment Solution
- Sample scripted OS job

About supported OS installed using Deployment Solution

You can use Deployment Solution to install an operating system (OS) on a client computer. To install an OS, Deployment Solution contains predefined tasks that you can configure and schedule on the client computers. Deployment Solution supports installation of Windows, UNIX, ESX, and Mac operating systems on client computers.

The deployment task, **Install Windows OS** lets you install the Windows operating system on a client computer, while **Install Linux/ESX OS** task lets you install Linux and ESX operating systems. The **Install Mac OS** task lets you install Mac operating system on client computers.

For the list of supported Windows, Linux and Mac OS versions and architecture, refer to the following article:

HOWTO9965
Installing Windows OS on client computers

Deployment Solution lets you install a Windows operating system (OS) on an unknown, a predefined, or a managed computer in an enterprise network. Windows OS installation lets you remotely install the Windows OS on any desktop, laptop, or on a server that is independent of the computer's hardware configuration. Besides, you can create a Windows OS package with the required source files, and decide what source files are included in that package.

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

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

**Table 6-1 Installing Windows OS on a client computer**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Launch the Symantec Management Console</td>
<td>Launch the Symantec Management Console. You can launch the console either from the Start menu of the Notification Server computer or from any computer of the network. To access the console from a different computer, you must type the following: http://&lt;IP address of NS&gt;/altiris/console</td>
</tr>
<tr>
<td>Step 2</td>
<td>Install and enable the Network Boot Service on a site server</td>
<td>Install the Network Boot Service (NBS) on a site server before you perform any other configurations. NBS is a component of Deployment Solution that you install and run as a service on a site server. NBS, once installed on a site server, handles all the communication with the Symantec Management Platform for Deployment Solution. See “Installing Network Boot Service on site server” on page 35.</td>
</tr>
</tbody>
</table>
## Table 6-1 Installing Windows OS on a client computer (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Create and configure a Windows preboot environment using a PXE image. The PXE image is used to boot the client computer in a network in the preboot environment or the pre-OS state. A PXE image is saved on the site server on which NBS is configured. Therefore, ensure that NBS is running on the site server before you create the PXE image. See “Preparing unknown computers to boot with WinPE image” on page 54. See “Preparing predefined computers to boot with WinPE image” on page 64. See “Booting managed Windows computer with WinPE image” on page 74.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Create Windows preboot environment</td>
<td>Configure Network Boot Service (NBS) for the type of client computer that you want to boot in the preboot environment. The NBS settings are configured through Settings &gt; Deployment &gt; NBS General Settings menu of the console. See “Configuring Network Boot Service for unknown computers” on page 89. See “Configuring Network Boot Service for predefined computers” on page 92. See “Configuring Network Boot Service for managed computers” on page 94.</td>
</tr>
</tbody>
</table>
### Table 6-1 Installing Windows OS on a client computer (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 5 | Add or import OS files for OS installation package | Add or import OS package to manage the Windows OS source files. You can configure the import parameters for your package.

To add OS package for Windows OS installation, from the Symantec Management Console, click **Settings > Deployment > OS Files > Add files**.

To import the OS files to a Windows OS installation package, you can also use the **Deployment Solution Resource Import Tool**. This tool is located in the `<install_directory>/Altiris/Deployment/Tools` folder of the Notification Server computer.

**Note:** You can add or import OS files to a Windows OS installation package before executing the **Install Windows OS** task. Alternatively, you can specify the files to be added or imported to the installation package at run-time while executing the **Install Windows OS** task.

See “Adding or importing OS files” on page 159.

| Step 6 | Add a Windows OS license to install Windows OS on the client computer | Add the Windows OS license for the corresponding OS through the Symantec Management Console so that you can track the OS licenses later.

**Note:** You can add Windows OS license before executing the **Install Windows OS** task. Alternatively, you can specify the Windows OS license for the corresponding OS at run-time while executing the **Install Windows OS** task.

See “Adding OS licenses” on page 158.

| Step 7 | (optional) Erase disk of client computer | Perform the **Erase Disk** task to erase the disks on the client computer. This action ensures that any preexisting data and partitions are removed from the computer. When you reallocate hardware, you can use this task to ensure that none of the old data can be retrieved.

You can execute this step only when you want to wipe the client computer’s disk clean of any preexisting data or disk partitions.

See “Erasing a Disk” on page 154. |
## Table 6-1 Installing Windows OS on a client computer *(continued)*

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 8</td>
<td>Create disk partition on client computer</td>
<td>Execute the <strong>Partition Disk</strong> task to create partitions on the client computer’s hard drive before you install the Windows OS.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To install Windows OS on UEFI/EFI computers, the computer must have partitions created with GPT partition table type. The GPT partition is required because the <strong>Partition disk</strong> task of Deployment Solution is not applicable for the UEFI computers. See “Creating disk partitions” on page 156.</td>
</tr>
<tr>
<td>Step 9</td>
<td>Install a Windows OS on the client computer</td>
<td>After you execute the <strong>Install Windows OS</strong> task on the computer, verify that the Windows OS is installed and the computer is in production environment.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To boot the client computer in the production environment, use the <strong>Boot To</strong> task in a job after the <strong>Install Windows OS</strong> task.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You can install Windows OS on UEFI/EFI computers using the default answer file or a custom answer file.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Installing a Windows OS using Deployment Solution ” on page 150.</td>
</tr>
<tr>
<td>Step 10</td>
<td>Perform Quick Run or schedule the <strong>Install Windows OS</strong> task</td>
<td>After a task is created, you can choose to either perform Quick Run or schedule the <strong>Install Windows OS</strong> task to run immediately or at a time that you want to execute on the client computer. You can specify the computer that the task runs on.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Alternatively, you can choose to add the tasks in steps 7, 8, and 9 to the <strong>Initial Deployment Job</strong>. You can also create a job that contains the tasks and add the job to the <strong>Initial Deployment Job</strong> menu .</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Scheduling a deployment job or task” on page 198.</td>
</tr>
<tr>
<td>Step 11</td>
<td>Verify that the computer boots in the production environment</td>
<td>After you execute the <strong>Install Windows OS</strong> task on the computer, verify that the Windows OS is installed and the computer is in production environment.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To boot the client computer in the production environment, use the <strong>Boot To</strong> task in a job after the <strong>Install Windows OS</strong> task.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To verify, from the Symantec Management Console, click <strong>Manage</strong> menu &gt; <strong>Computers</strong> &gt; select the computer name from the list of available computers. The details of the selected computer appear in the <strong>General</strong> pane. Verify the operating system that is installed on the computer. You can also view the status of the <strong>Install Windows OS</strong> task in the <strong>Jobs/Tasks</strong> list.</td>
</tr>
</tbody>
</table>
Installing a Windows OS using Deployment Solution

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

See “Creating disk partitions” on page 156.

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

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

**To install Windows OS on client computers**

1. In the Symantec Management Console, from the **Manage** menu select **Jobs and tasks**.
2. On the right pane, right-click **Jobs and tasks** and select **New > Task**.
3. On the **Create new task** page, select **Install Windows OS**.
4. Enter values for the following fields:

   **Task name** icon
   
   Displays the default task name as Install Windows OS. You can edit the default task name to specify a relevant task name. For example, Install Windows_XP.

   **System Files - OS source**
   
   Lets you select the source of the previously installed operating system files from the drop-down list.
   
   Click **Add** to add a new OS package in the **Add OS Packages** dialog box.

   **System Files - Product Key**
   
   Lets you select a previously added license from the drop-down list.
   
   Click **Add** to add licenses in the **Add OS License**.
Install drivers
Check **Install drivers from Driver Database during OS installation** to install the missing drivers that are required for a successful installation.

**Note:** If you select this option and if you use the unattended configuration file to install the Windows OS, then ensure that you do not add partitions in the configuration file. This is so because DeployAnywhere requires the partition to be created before the **Install Windows OS** task executes. If you create a partition in the configuration file then DeployAnywhere fails to add the driver to the client computer.

After you select this option, you can select the following:

- **Bypass Driver Validation**
  Check this option if you do not want the drivers that you add to pass through the validation that is performed by Deployment Solution. The system file and the .inf file validations are bypassed for the drivers that you add if you select this option. By default, the value **None** is selected, which means that for no drivers the validation is bypassed. You can select **All** if you want to bypass validation for all the drivers.

  **Note:** If a driver does not pass the validation checks and if you did not check the **Bypass Driver Validation** option, then the driver will not be installed on the computer after you execute the **Install Windows OS**.

- **Debug Log Level**
  Select the debug log level for the installation of drivers from the driver database operation.
  The following are the log levels:
  - **None**
    This log level captures the logs of all the failures of a task.
  - **Driver Match**
    The log level is 5 and it retrieves log information about the drivers that match.
  - **Function Start**
    The log level is 10 and the log is created when a function is entered.
  - **Function Ends**
    The log level is 11 and the log is created when the function exits.
  - **Device Details**
    The log level is 20 and it prints information about the devices.
  - **INF Parsing**
    The log level is 30 and it logs information about inf parsing.
  - **No matching Device for inf**
    The log level is 40 and it logs information about infs if they do not match with devices of the client computer.
  - **All**
    The log level is 255 and it logs information on all the points that are listed for this field.
Enable tagging of the drivers
Select this option to add tags in the Tags field. You can add only comma separated values for the tags.
Tagged drivers are forced to install on the target computer.

Configuration
Lets you configure the settings to install the Windows OS.
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.

  **Note:** Symantec recommends that you use the Apply System Configuration task to join the client computer to the domain.

- **Use default configuration settings**
  Uses the default settings.

- **Configuration file**
  Uses a custom answer file.
  If you use a custom answer file that creates disk partitions then, the following is observed:
  - OS is installed successfully on the client computer
  - DeployAnywhere fails to add drivers on the client computer
    If you select the **Install drivers from Driver Database during OS installation** option, the partition configuration that you specify in the configuration file overwrites the partition that stores the drivers on the client computer.
    If you want to use DeployAnywhere, then you must create partitions using the **Partition Disk** task from the console.
  - SMA fails to get installed on the client computer
    You must install the SMA manually on the client computer.

The user name and password that is specified in the answer file is displayed in the plain text format when the client computer is booted in the preboot environment.

Drive
Lets you specify the following:

- **Disk number**
  Select the disk number from the drop-down list.

- **Partition**
  Select the disk partition from the drop-down list.
Regional

<table>
<thead>
<tr>
<th>Let you specify the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Language</td>
</tr>
<tr>
<td>Select the language of the operating system.</td>
</tr>
<tr>
<td>Keyboard</td>
</tr>
<tr>
<td>Select the keyboard language support for the operating system.</td>
</tr>
</tbody>
</table>

Video

<table>
<thead>
<tr>
<th>Let you specify the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Screen resolution</td>
</tr>
<tr>
<td>Select the keyboard resolution.</td>
</tr>
<tr>
<td>Color quality</td>
</tr>
<tr>
<td>Select the color quality type from the drop-down list.</td>
</tr>
</tbody>
</table>

5 Click OK.

See “Erasing a Disk” on page 154.

Erasing a Disk

You can use the Erase Disk task to wipe a disk clean. Hence, the partitions along with data are removed from the client computer. When you reallocate hardware, you can use this task to ensure that none of the old data can be retrieved. You can either delete the partitions of the disk, erase the system disk, or configure the task to erase all the disks. You cannot perform an Erase Disk task for a disk that is connected through a USB or FireWire interface.

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

To erase a disk

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

   **Task name icon**
   
   Lets you specify the name of the erase disk task.

   **Disk selection**
   
   Lets you select the disk partition from the drop-down list. You can select the disk number from the range 1 to 8, All disk, and System disk. In case, you select the System disk option, the remove partition section is disabled.
Remove partitions

Lets you remove the selected partitions of the disk.

Select the disk partition from the drop-down list of the Disk selection option and check the Erase data check box.

Erase disk

Lets you select from the following options to erase disk:

- **Secure erase**
  
  Select this option to erase data more than once.

  The following group of operations is performed on the hard drive six times:
  
  - All addressable locations are overwritten with 0x35.
  - All addressable locations are overwritten with 0xCA.
  - All addressable locations are overwritten with a pseudo-random character.
  - All addressable locations are verified in hardware using the Verify Sectors command to the disk.

- **Convert To**

  Select this option to erase the selected disk and convert the partition of the client computer to the following type:

  - **GPT**
    
    Converts the client computer partition to GPT partition type.

  - **MBR**
    
    Converts the client computer partition type to MBR partition type.

**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.

6 Click Ok.

See "Creating disk partitions" on page 156.
Creating disk partitions

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

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

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

The partitions that you must create for BIOS based and UEFI/EFI based client computers are as follows:

<table>
<thead>
<tr>
<th>BIOS</th>
<th>NTFS</th>
<th>Align must not be set</th>
<th>Mark as Active option must be selected</th>
</tr>
</thead>
<tbody>
<tr>
<td>UEFI/EFI</td>
<td>EFI</td>
<td>Align must be set to 1MB</td>
<td>(optional) Mark as Active option must be selected</td>
</tr>
<tr>
<td>UEFI/EFI</td>
<td>MSR</td>
<td>Align must be set to 1MB</td>
<td>(optional) Mark as Active option must be selected</td>
</tr>
<tr>
<td>UEFI/EFI</td>
<td>NTFS</td>
<td>Align must not be set</td>
<td>Mark as Active option must not be selected</td>
</tr>
</tbody>
</table>

See “Erasing a Disk” on page 154.

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.

Is Secondary disk
Select this option if you want to partition the disk as a secondary disk.

Disk Number
Select the disk drive for which the partition is created.
GPT Partitioning

Select the type of partition from either of the following:

- **EFI**
  In EFI-based GPT partition, the computer boots to the EFI partition.

- **MSR**
  The Microsoft reserved partition (MSR) is used for UEFI/GPT partition system and must be located before the partition on which you want to install the Windows operating system.

If you select the **GPT partitioning** option, then the **Format**, **Partition**, and the **Size** options are disabled.

**Format**
Select the format of the partition as **Fat32**, **NTFS**, and **EXT**.

**Partition**
Select the type of partition to create such as **Extended**, **Logical**, and **Primary**. By default, **Primary** is selected.

**Mark Partition as 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.

If you create a single NTFS partition for a BIOS-based computer then, you must select the **Mark Partition as Active** option. If you create the NTFS partition for UEFI/EFI based computer then you should not select this option.

**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.
**Align**

Lets you override the way in which the partitions are aligned when an individual partition or disk full of partitions is restored. By default it is set to 1MB. You must use this option only for creating a GPT partition.

You must not select the **Align** option for the following:

- Creating an operating system or data partition
- For UEFI/EFI based computers with last partition as NTFS

**Is Secondary disk**

Select this option if you want to partition the disk as a secondary disk.

Select the following settings if you select this option:

- **Disk Number**
  Select the disk drive for which the partition is created.

- **Format**
  Select the format of the partition as Fat32, NTFS, and EXT.

- **Partition**
  Select the type of partition to create such as Extended, Logical, and Primary. By default, **Extended** is selected.

- **Mark Partition as 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.

7 Click **OK**

8 On the **Create New Task** page, click **OK**.

**Adding OS licenses**

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

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

   The new license is displayed in the OS Licenses list.

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

See “Configuring the Sysprep imaging” on page 112.

Adding or importing OS files

Deployment Solution lets you add or import operating system (OS) files to include them in the Windows OS installation package. When you add or import the OS files to an installation package, you are customizing the Windows OS installation package for executing the scripted Windows OS task successfully.

You can do the following with the OS installation packages:

- Add files to the installation package through the Symantec Management Console
  After you add the OS Files from the Symantec Management Console, the files are added to the following location on which Notification Server is installed:
  <install_directory>\Altiris\Notification Server\NSCap\bin\Deployment\Packages\SOI
  The package is created on the computer on which Symantec Management Platform is installed, which is later replicated to the Package Server, which is configured for Deployment Solution.
  See “To add OS files” on page 160.

- Import files to the installation package through the Deployment Solution Resource Import Tool
  To import OS files from the OS sources, you must use the Deployment Solution Resource Import Tool.
  See “To import OS files” on page 160.
Note: If you have performed the **Copy File** task before and have copied the OS files, ensure that you add or import the copied OS source files to the Windows OS package for Windows OS installation. The OS source files are added at the following location on the Notification Server:

```text
<install_directory>\Altiris\Notification Server\NSCap\bin\Deployment\Packages\SOI.
```

To add OS files

1. In the Symantec Management Console, navigate to the **Settings** menu and 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 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.

To import OS files

1. Navigate to the location `<install_directory>\Altiris\Deployment\Tools` of the computer on which Symantec Management Platform is installed and execute `ResourceImportTool.exe`.
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**.

**Adding drivers to the Preboot database**

Deployment Solution lets you add drivers to the Preboot driver database, which is required when you boot a computer to the preboot configurations. If a preboot configuration that you
already created requires a new driver, you must add the driver to the preboot driver database and then recreate the preboot configuration.

After you add the drivers to the Preboot database, the preboot images can then support mass storage devices (MSDs) and network interface cards (NICs). These critical drivers are added to the preboot images and are then deployed through the preboot environment. It ensures that you can boot the client computers successfully to preboot environment. The Preboot driver database supports the Windows and Linux operating systems. You cannot add non-critical drivers to preboot database.

To add a new driver to an existing preboot configuration, you must recreate that preboot configuration with the newly-added driver using the **Recreate Preboot Environment** option. If you create a preboot image before Network Boot Service (NBS) is installed and enabled on a remote site server, then it is not registered with the site server. In such case, you must either recreate that preboot environment for the selected image or create a new image to be registered with the new remote site server.

To update the automation folder that is installed on the client computer immediately after you recreate the automation folder package, you must disable the automation folder upgrade policy first and then recreate the preboot configuration. After recreating the preboot configuration, update the following tasks from the Windows Task Scheduler and then enable the automation folder upgrade policy on the client computer

- NS.Package distribution Point Update Schedule
- NS.Package Server Status Event Capture Item
- NS.Package Refresh

**To add drivers to the Preboot database**

1. In the Symantec Management Console, on the **Settings** menu, click **Deployment > Driver Management**.
2. In the **Driver Database Management** dialog box 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. In the **Add Driver** dialog box, specify the values of the fields.

The fields and their descriptions are as follows:

- **Location**
  - Lets you browse to the driver folder, which contains the drivers that you want to add.
  - Deployment Solution creates auto-generated names for the drivers that you add.
Select the operating system for which you want to add the drivers.

Select one of the following operating systems for the preboot environment:

- **WinPE**
  
  *Note:* If you select WinPE, then ensure that you manually add the network driver of WinPE 3.0 for Windows XP 32-bit in VMware computer, to successfully boot the client computer in the preboot environment.

- **Linux**

**Architecture**

Select the hardware architecture of the computer for which you want to add the driver.

Select one of the following architectures:

- **x86**
- **x64**

6 Click **OK**.

The new driver is used when you create a new configuration or recreate an existing preboot configuration.

See “Adding drivers to the DeployAnywhere database” on page 162.

### Adding drivers to the DeployAnywhere database

Deployment Solution lets you to add drivers to the DeployAnywhere driver database that are required for client computers on which you want to install Windows OS or deploy a Windows image. All the device drivers are stored at one central location in the DeployAnywhere driver database. The drivers in DeployAnywhere database are located at `C:\Program Files\Altiris\Deployment\DriversDB` folder. This location also consists of the `drivers.manifest.txt` file, that includes the information about what DeployAnywhere drivers are available to Deployment Solution.

After adding drivers to the DeployAnywhere driver database, the task of imaging and Windows OS installation are rendered hardware independent. Hence, deploying of image to client computers and performing an OS installation do not fail due to hardware dependencies. You can add drivers to the DeployAnywhere driver database while executing either an **Install Windows OS** task or a **Deploy Image** task. The DeployAnywhere driver database supports only the Windows operating system.
For example, you can add device drivers to the DeployAnywhere database in the following situations:

- While deploying an image that is compatible for different hardware sets, such as, to deploy images across dissimilar hardware.
- While adding any missing critical drivers required for successful execution of deployment tasks on the remotely-managed computers.
- While supporting new devices that are added to the system or the environment.

In all the above mentioned cases, you must add the additionally required drivers to the DeployAnywhere database.

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

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. In the Driver Database Management dialog box, click the DeployAnywhere tab.
3. To view details of a driver, select the driver from the list and click More Info.
4. Click Add.
5 In the Add Driver dialog box, for the Location field, browse to the driver folder, which contains the drivers that you want to add. Deployment Solution creates auto-generated names for the drivers that you add.

6 Add tags in the Tags field. You can add comma separated values in the Tags field. The tagged drivers are installed forcefully on the target computer.

7 Click OK.

See “Adding drivers to the Preboot database” on page 160.

Installing Linux/ESX OS on client computers

Deployment Solution lets you install a Linux operating system (OS) on an unknown, a predefined, or a managed computer in an enterprise network. Linux OS installation lets you remotely install the Linux OS on any desktop, laptop, or on a server that is independent of the computer's hardware configuration. Besides, you can create a Linux OS package with the required source files, and decide what source files are included in that package.

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

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

Table 6-2 Installing Linux OS on a client computer

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Launch the Symantec Management Console</td>
<td>Launch the Symantec Management Console.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You can launch the console either from the Start menu of the Notification Server computer or from any computer of the network. To access the console from a different computer, you must type the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>http://&lt;IP address of NS&gt;/altiris/console</td>
</tr>
</tbody>
</table>
Table 6-2 Installing Linux OS on a client computer (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 2 | Install and enable the Network Boot Service on a site server | Install the Network Boot Service (NBS) on a site server before you perform any other configurations. NBS is a component of Deployment Solution that you install and run as a service on a site server. NBS, once installed on a site server, handles all the communication with the Symantec Management Platform for Deployment Solution. 
See "Installing Network Boot Service on site server" on page 35. |
| Step 3 | Create a Linux preboot environment using a PXE image | Create and configure a Linux preboot environment using a PXE image. The PXE image is used to boot the client computer in a network in the preboot environment or the pre-OS state. A PXE image is saved on the site server on which NBS is configured. Therefore, ensure that NBS is running on the site server before you create the PXE image. 
See "Creating preboot configuration for Linux " on page 102. |
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 4</td>
<td>Configure types of computers with PXE</td>
<td>Configure different types of computers, such as unknown, predefined, or managed computer from the <strong>NBS General Settings</strong> page.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Configuring Network Boot Service for unknown computers” on page 89.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Configuring Network Boot Service for predefined computers” on page 92.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Configuring Network Boot Service for managed computers” on page 94.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Install a Linux OS on the client computer</td>
<td>Execute the <strong>Install Linux/ESX OS</strong> task to install the Linux OS on the client computer after the computer boots in the preboot environment.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>After a task is created, you can choose to either perform Quick Run or schedule the <strong>Install Linux/EX OS</strong> task to run immediately or at a time that you want to execute on the client computer. You can specify the computer that the task runs on.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Scheduling a deployment job or task” on page 198.</td>
</tr>
</tbody>
</table>
Table 6-2 Installing Linux OS on a client computer (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 6</td>
<td>Boot the client computer in production environment</td>
<td>After you execute the <strong>Install Linux/ESX OS</strong> task on the computer, execute the <strong>Boot To task</strong> to boot the client computer to production environment. See “Creating a Boot To task” on page 199. See “Scheduling a deployment job or task” on page 198.</td>
</tr>
</tbody>
</table>

Installing Linux/ESX OS using Deployment Solution

Deployment Solution lets you install the Linux or ESX operating system on the client computer. You must ensure to execute the **Install Linux/ESX OS** task on the client computers in the Linux preboot environment.

For this task, the OS packages are fetched and retrieved from the anonymous HTTP server or the FTP server. You must ensure that the anonymous HTTP server or FTP server is accessible and is set up with the OS packages to fetch them for the client computers that are in the Linux preboot environment.

After performing the OS installation task, if the package server is configured on HTTPS, you must download and install the package server certificate on the client computer by running the `aex-getsscert <IP> yes` command.

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

**Note:** If you are installing ESXi 5.1 version, ensure that you add the respective drivers in the OS source that you are installing before running the Install Linux/ESX OS task

If you use IDE disks and try to install old kernel versions of Linux OS on the client computer then do either of the following to successfully install the OS:

- Replace `%DISK%` token by actual device name in the configuration or answer file. The Linux configuration file is located in, `<installdir>\Program Files\Altiris\Notification Server\NSCap\bin\UNIX\Deployment\Linux\x86\SOI\AnswerFile path.`
- Remove `%DISK%` token
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.

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

See “Installing a Windows OS using Deployment Solution” on page 150.

Installing Mac OS using Deployment Solution

Deployment Solution lets you install Mac operating system on client computers. You can perform OS installation using the Install Mac OS task.

You can access the Install Mac OS task from the console's Manage > Jobs and Tasks > Create New Task > Install Mac OS.

You can execute Mac OS installation for the following:

- Unknown computers
  See "Installing Mac OS on an unknown computer" on page 181.

- Predefined computers
  See "Installing Mac OS on a predefined Mac computer" on page 183.

- Managed computers in automation or NetBoot environment
  See "Installing Mac OS on a managed computer" on page 187.

Ensure that the client computer hard drive has proper partitions and the target volume is correctly mentioned in the configuration file before you perform the Install Mac OS task on the client computers.

You can access the Mac configuration file from the following location:

<installdir>\Program Files\Altiris\Notification\Server\NSCap\bin\UNIX\Deployment\Mac\NetInstall\AnswerFile\n
After performing the operating system installation, if the client computer is not able to connect to Symantec Management Platform, then you must manually install the Symantec Management Agent.

To view the logs, go to

<instal.Volume>/var/tmp/AltirisAgentInstallStartup/ and click AltirisAgentInstallStartupLog.txt.

If you want to install Mac OS on multiple client computers, you must do the following settings to ensure that correct inventory details are displayed on the Notification Server computer:

- Go to Settings > Agents/Plug-ins > Targeted Agent Settings > All Linux/Mac Workstations. In the UNIX/Linux/Mac tab, set the following in the Computer information:
Return the following information as computer name as DNS name.
Return the following information as computer domain as DNS name.

- Go to Settings > Agents/Plug-ins > Targeted Agent Settings > All UNIX/Linux/Mac Servers. In the UNIX/Linux/Mac tab, set the following in the Computer information:
  Return the following information as computer name as DNS name.
  Return the following information as computer domain as DNS name.

To perform Mac OS installation

1. In the Symantec Management Console, from Manage menu select Jobs and tasks.
2. Right-click Jobs and tasks and select New Task.
3. On the Create new task page, select Install Mac OS.
4 In the **Install Mac OS** task page, you must specify the values for the fields. The fields and descriptions are as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Task name</strong> icon</td>
<td>Lets you specify the Install Mac OS task name.</td>
</tr>
<tr>
<td><strong>OS Flavor</strong></td>
<td>Lets you select the OS version for Mac from the drop-down list.</td>
</tr>
<tr>
<td><strong>OS NetInstall Image</strong></td>
<td>Lets you select the NetInstall image.</td>
</tr>
<tr>
<td></td>
<td>Ensure that you have modified the NetInstall image using the Symantec's Mac pre-OS Creation Utility and uploaded the image to Notification Server computer. You can upload the NetInstall image by creating a preboot configuration for the NetInstall image.</td>
</tr>
<tr>
<td></td>
<td>See &quot;Creating and modifying NetInstall images&quot; on page 175.</td>
</tr>
<tr>
<td><strong>Configuration File</strong></td>
<td>Lets you browse for the configuration file that you want to use for the installation. The configuration file stores answers for the required parameters during installation of the operating system.</td>
</tr>
<tr>
<td></td>
<td>The configuration file is placed at <code>&lt;installdir&gt;\NSCap\bin \UNIX\Deployment\Mac\NetInstall\AnswerFile\</code></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Symantec recommends that you set the ShouldErase parameter as False. If you set it as True, then you must select the drive, on which the Mac operating system must be installed and install the Symantec Management Agent and Deployment Plug-in manually on the client computer.</td>
</tr>
<tr>
<td></td>
<td>See &quot;About Mac configuration file&quot; on page 258.</td>
</tr>
</tbody>
</table>

5 Click **OK**.

See “Installing Mac OS on an unknown computer” on page 181.

See “Installing Mac OS on a predefined Mac computer” on page 183.

See “Installing Mac OS on a managed computer” on page 187.
Launching Symantec's Mac pre-OS Creation Utility

The Symantec's Mac pre-OS Creation Utility of Deployment Solution lets you create and modify the Mac NetBoot image and the NetInstall image. The NetBoot image is used as a preboot image to boot client computers in preboot environment. The NetInstall image is a type of preboot image that is used along with the configuration file to install Mac operating system on client computers. After you create a NetBoot image or a NetInstall image ensure that you modify the image using the Mac pre-OS Creation Utility and upload the image to the Notification Server computer. The NetBoot image and the NetInstall image are then distributed from the Notification Server computer to all the site servers with Network Boot Service (NBS) installed. The NBS supports only .dmg images that are shared over the Network File System (NFS). The HTTP protocol is not supported for sharing images.

Before you use the Mac pre-OS Creation Utility ensure that you comply with the prerequisites for using Mac computers for deployment-related tasks.

See "Prerequisites for Mac computer setup " on page 51.

Note: Ensure that you do not access the Automation folder and the Agent folder that is placed in the <install_dir>/Program Files/Altiris/Notification Server/NSCap/bin/UNIX/Deployment/Mac/universal/ path from a Mac client computer using the Server Message Block (SMB) shares.

To launch Symantec's Mac pre-OS Creation Utility

1. On the Notification Server computer, navigate to the <install_dir>/Program Files/Altiris/Notification Server/NSCap/bin/UNIX/Deployment/Mac/universal/MocuAppInstaller path and download the MOCUInstaller.pkg utility on the source computer.
2. Install the MOCUInstaller.pkg on the volume of the source computer, which is installed with the Symantec Management Agent, the Deployment plug-in for Mac, and the policies. You use the utility to create and modify the NetBoot image and the NetInstall image.
3. To launch the application on your Mac source computer, navigate through Finder > Go > Applications and double-click on the MOCU.app.

See “Creating and modifying NetBoot images” on page 172.

See “Creating and modifying NetInstall images” on page 175.


About Symantec's Mac pre-OS Creation Utility

The Symantec's Mac pre-OS Creation Utility of Deployment Solution lets you create and modify Mac NetBoot image and NetInstall images. This utility along with Apple’s System Image Utility...
lets you create the Mac NetBoot image either from a booted volume or from a bootable volume of the source computer. Ensure that the booted volume or the bootable volume is installed with the Symantec Management Agent and the Deployment Solution plug-in for creating the NetBoot image. The NetInstall image is used to install Mac OS on the client computers.

A NetBoot image is used to boot Mac clients into diskless mode and is used in the Create Image, Deploy Image, and Boot To tasks. The modified NetBoot image that is prepared using the Mac pre-OS Creation Utility contains bootable OS files, Symantec Management Agent, and the Deployment Solution plug-in. The NetBoot image does not contain Mac OS files and therefore cannot be used for installing the Mac operating system. The NetBoot image is used to boot the client computers in the preboot environment.

A NetInstall image is a type of preboot image that is used to install Mac operating system on the client computers. The NetInstall image contains the required Mac operating system files that are available in the Mac OS distribution media. In Deployment Solution, you use the Install Mac OS task to install Mac OS on client computers. The Install Mac OS task uses the modified NetInstall image and the configuration file to carry out the installation of Mac operating system without human assistance.

After you create a NetBoot image or a NetInstall image ensure that you modify the image using the Mac pre-OS Creation Utility and upload the image to the Notification Server computer. The NetBoot image and the NetInstall image are then distributed from the Notification Server computer to all the site servers with Network Boot Service (NBS) installed. The NBS supports only .dmg images that are shared over the Network File System (NFS). The HTTP protocol is not supported for sharing images.

See “Launching Symantec’s Mac pre-OS Creation Utility” on page 171.


See “Creating and modifying NetBoot images” on page 172.

See “Creating and modifying NetInstall images” on page 175.

Creating and modifying NetBoot images

Deployment Solution lets you create and modify Mac NetBoot images using the Symantec’s Mac pre-OS Creation Utility and the Apple’s System Image Utility. These images are then used to boot Mac clients in preboot environment. Ensure that you modify the NetBoot image using the Mac pre-OS Creation Utility so that the image is compatible with Deployment Solution. Symantec recommends that the NetBoot source is booted with the combo update of the supported operating system.

After you modify the NetBoot image, you must upload the NetBoot image to the Notification Server computer. You can do this using the Add Preboot Configuration dialog box. The NetBoot image is then distributed to all the Network Boot Servers in the network.

See “Creating preboot configuration for Mac” on page 104.
Before you create the NetBoot image, ensure the following:

- Symantec Management Agent, and Deployment Solution plug-in for Mac are installed on the NetBoot image source volume.
- Deployment Automation folder for Mac- Install policy is installed on the source computer.
- Rename the NetBoot source volume with a unique name before you launch the Symantec's Mac pre-OS Creation Utility.
  After you create the Mac NetBoot image, you can rename the NetBoot source volume name to its original name.

If you face an error, it can be verified in the Console’s application. To access the application go to Finder > Utilities and launch console.app application.

To view logs of Apple’s System Image Utility, go to Menu > View > Show Log.

You can create and modify Mac NetBoot images from the following sources:

- Mac booted volume
  The Mac booted volume of the source computer is the current volume in which the client computer is booted.

  **Note:** For Mac OS X 10.10 and higher, you cannot create a NetBoot image from a booted volume.

- Mac bootable volume
  The Mac bootable volume of the source computer is any volume other than the booted volume on which Mac operating system is installed and is used to create a NetBoot image.

  **Note:** For Mac OS X 10.10 and higher, you can create a NetBoot image only of the production volume on which the Symantec Management Agent and the Deployment Solution plug-in for Mac are installed.

To create and modify Mac NetBoot image from Mac booted volume

1. Launch the Symantec's Mac pre-OS Creation Utility.
2. In the Mac pre-OS Creation Utility, select NetBoot from Create and Update image.
3. Click Next.
4. Enter the Temporary Volume Name.
   You can estimate the size of the temporary volume by clicking the Estimate Size.
5 Click **Prepare Temporary Volume**.
   Ensure that you have emptied the **Trash** before creating the temporary volume.

6 Click **Next**.

7 Click **Launch System Image Utility**.

8 In the Apple's System Image Utility, enter the **Type**, **Installed Volume**, **Save To**, **Image name**, and **Description**. The **Network disk** and the **Image Index** must be left as default. A message is displayed if the NetBoot image (.nbi) is created successfully.

9 In the Symantec's Mac pre-OS Creation Utility, click **Choose...** from **Select image to update**. To modify a NetBoot image select the NetBoot.dmg.

10 Click **Update Image** to modify the image (.dmg file) and make it suitable to be used for Deployment Solution tasks.

   Save the modified image on your computer and then upload it to the Notification Server computer.

To create and modify Mac NetBoot image from bootable volume

1 Launch the Mac pre-OS Creation Utility.

2 In the Mac pre-OS Creation Utility, select **NetBoot** from **Create and Update image**.

3 Click **Next**.

4 Click **Next** again.

5 Click **Launch System Image Utility**.

6 In the Apple's System Image Utility, enter the **Type**, **Installed Volume**, **Save To**, **Image name**, and **Description**. The **Network disk** and the **Image Index** must be left as default. A message is displayed if the NetBoot image (.nbi) is created successfully.

7 In the Symantec's Mac pre-OS Creation Utility, click **Choose...** from **Select image to update** and select the image (.dmg) to modify.

8 Click **Update Image** to modify the image (.dmg) and make it suitable to be used for Deployment Solution tasks.

   For Mac OS X 10.10 and higher NetBoot image, you must add more files to the .nbi folder. Browse and select the **Target .nbi folder** and the **Source Volume of the NetBoot image**. Click on **OK**.

   Save the modified image and then upload it to the Notification Server computer.

See “About Symantec's Mac pre-OS Creation Utility” on page 171.

See “Launching Symantec's Mac pre-OS Creation Utility” on page 171.
Creating and modifying NetInstall images

A NetInstall image along with the Mac configuration file is used to install Mac OS on a client computer. The Symantec’s Mac pre-OS Creation Utility and the Apple’s System Image Utility lets you create and modify NetInstall image. You must modify a NetInstall image to make it compatible with Deployment Solution. If you modify an existing NetInstall image, ensure that it is created using the latest version of Deployment Solution. After modifying the NetInstall image, you must upload the image to the Notification Server computer. From the Notification Server computer the image is then distributed to all the Network Boot Servers (NBS) present in the network.

If you check any any errors, you can check the following logs:

- **System.log file**
  To view Symantec’s Mac pre-OS Creation Utility logs, view the log in the System.log file.

- **Console.app**
  To access the console application's logs, go to Finder > Utilities and open Console.app.

- **Show log**
  To view the Apple’s system Image Utility logs, go to Menu > View > Show Log of the utility.

To create and modify NetInstall image

1. Launch the Symantec's Mac pre-OS Creation Utility.
2. In the Mac pre-OS Creation Utility, select NetInstall from Create and Update Image.
3. Click Next.
4. On the page that is displayed, click Launch System Image Utility. Save the NetInstall image on your computer.
   
   Ensure that the Enable Automated Installation is included after the Define Image Source in the workflow while creating a NetInstall image using the Apple's System Image Utility.

5. In the Apple's System Image Utility, enter the Type, Installed Volume, Save To, Image name, and Description. The Network disk and the Image Index must be left as default.
6. In the Mac pre-OS Creation Utility, click Choose... from Select image to update. Browse and select the NetInstall.dmg image.
7. Click Update Image.

To modify NetInstall image

1. Launch the Symantec's Mac pre-OS Creation Utility application.
2. In the Mac pre-OS Creation Utility, select NetInstall from Create and Update Image.
3. Click Next.
On the page that is displayed, click **Choose...** from **Select image to update**. Browse and select the NetInstall.dmg image.

Click **Update Image**.

See “About Symantec's Mac pre-OS Creation Utility” on page 171.

See “Launching Symantec's Mac pre-OS Creation Utility” on page 171.

See “About Mac configuration file” on page 258.

**Booting Mac computers with NetBoot image**

Deployment Solution lets you boot different types of Mac computers such as unknown or bare metal computers, predefined computers, or managed computers in the preboot environment or the automation environment using a NetBoot image. A NetBoot image is created using the Apple's System Image Utility and must be modified before you use it in Deployment Solution. You can create and modify a NetBoot image using the Symantec's Mac pre-OS Creation Utility.

See “Launching Symantec's Mac pre-OS Creation Utility” on page 171.

To boot a Mac computer, besides the NetBoot image, you also require to configure the site server on which the Network Boot Service (NBS) is installed.

See “About Network Boot Service” on page 84.

The NBS settings let you configure the default response setting for unknown, predefined, and managed Mac computers. The default response of the Mac client computer is set based on the NetBoot image that you configure for the type of client computer. The client computer then boots in the preboot environment using the NetBoot image. You must hold the N key of the keyboard while booting the Mac computer that is added into the network to receive the default NetBoot image.

The basic steps that you must execute to prepare the environment for booting Mac computers with NetBoot images are as follows:
### Table 6-3  Boooting Mac clients in preboot environment

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Launch the console</td>
<td>Launch the Symantec Management Console. You can launch the console either from the Start menu of the Notification Server computer or from any computer of the network. To access the console from a different computer, you must type the following: http://&lt;IP address of NS&gt;/altiris/console</td>
</tr>
</tbody>
</table>
| Step 2 | Install the Network Boot Service on a site server | Install the Network Boot Service on the site server.  
See "Installing Network Boot Service on site server" on page 35. |
| Step 3 | Create and modify a NetBoot image | Create and Modify a NetBoot image using the Symantec's Mac-preOS Creation Utility.  
See "Creating and modifying NetBoot images" on page 172. |
| Step 4 | Create preboot environment | Create the preboot environment with the NetBoot image. |
| Step 5 | Enable the NBS service to support Boot Service Discovery Protocol (BSDP) | Enable the BSDP support from the NBS general settings.  
See "Configuring NBS for Mac computers" on page 178. |
Table 6-3  Booting Mac clients in preboot environment (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 6</td>
<td>Configure response for unknown, predefined, and managed computers</td>
<td>From the NBS General Settings page, set response for unknown, predefined, and managed Mac computers.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You can boot the following types of Mac clients:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Unknown Mac clients</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Booting an unknown Mac computer in NetBoot environment” on page 58.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Predefined Mac clients</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Booting a predefined Mac computer in NetBoot environment” on page 69.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Managed Mac clients</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Booting a managed Mac computer in NetBoot environment” on page 77.</td>
</tr>
</tbody>
</table>

See “Booting an unknown Mac computer in NetBoot environment” on page 58.
See “Booting a predefined Mac computer in NetBoot environment” on page 69.
See “Booting a managed Mac computer in NetBoot environment” on page 77.

Configuring NBS for Mac computers

The NBS General Settings option of the Network Boot Service (NBS) lets you configure one or more site servers with the preboot configuration settings. For Mac, the preboot configuration setting is used to configure the client computers to boot in the pre-OS or the preboot environment using a NetBoot image. The preboot configurations are applicable for the unknown computers, managed computers, and predefined computers of an enterprise network.

You can access the NBS General Settings option from the following menu of the console:

- Settings > Notification Server > Site Server Settings
  In the Site Management view pane, access Settings > Network Boot Service > Settings > NBS General Setting
- Settings > Deployment > NBS General Settings
To configure the NBS settings

1. In the Symantec Management Platform (SMP) console, click **Settings > Deployment > NBS General Settings**.

2. In the **NBS General Settings** dialog box, configure the following **Network Boot Service Configuration** settings:

   - **Network Boot Service Configuration**: Lets you configure the Network Boot Service (NBS) for a site server.
     - To enable or disable the policy, you must select the **Turn On** or **Turn Off** icons on the right side of the dialog box or page.

   - **Apply NBS settings immediately**: Check the option if you want to apply the NBS policy immediately on the site servers.
     - If the option remains unchecked then the NBS configurations changes are applied as scheduled in the Symantec Management Agent (SMA) for rolling out policies.

   - **Enable the NBS service**: Check the NBS service to enable the service on the site server.
     - By default, this option is checked.

   - **Enable Mac Netboot (BSDP) support**: Check the Netboot (BSDP) support to enable Mac client computers to boot using the Mac NetBoot images.
     - Ensure that you add the following services on the site server on which you enable the NBS service before you check **Enable Mac Netboot (BSDP) support**:
       - Windows Role Services for Network File System (NFS) for Windows
       - Windows Services for UNIX (SFU) for UNIX

   - **Reset button**: Lets you restore the previous configuration that you performed for the NBS site server.

3. In the **NBS General Settings** dialog box, for the **Initial Deployment (Unknown Computer) Menu** configure the following settings:
Netboot menu (Mac) tab  Set these options to respond to the unknown computers that are added in the network.

- **Respond to unknown computers**
  Check this option if you want to respond to the unknown computers to configure them to NetBoot environment.

- **Default Boot image**
  Select the default NetBoot image with which you want to boot the client computers.

4 In the **NBS General Settings** dialog box, for the **Redeployment (Predefined Computer) Menu** configure the following settings:

Netboot menu (Mac) tab  Set these options to respond to predefined computers added in the network.

- **Respond to Predefined computers**
  Check this option if you want to respond to the predefined computers to configure them to NetBoot environment.

- **Default Boot image**
  Select the default NetBoot image with which you want to boot the client computers.

5 In the **NBS General Settings** dialog box, for the **Redeployment (Managed Computer) Menu** configure the following settings:

Netboot menu (Mac) tab  Set these options to respond to the managed computers.

- **Respond to Managed computers**
  Check this option if you want to respond to the managed computers to configure them to NetBoot environment.

- **Default Boot image**
  Select the default NetBoot image with which you want to boot the client computers.

6 Click **Save changes**.

7 Again, in the console, click the **Settings > Deployment > NBS Global Settings** menu. See “About filtering computers through NBS Global Settings” on page 86.

8 In the **NBS Global Settings** dialog box or pane, turn on the Netboot Service configuration.

9 In the **NBS Global Settings** dialog box, select the **Apply NBS settings immediately** check box and click **Save Changes**.

See “About NBS General Settings” on page 85.
Installing Mac OS on an unknown computer

Deployment Solution lets you install Mac operating system on an unknown Mac computer. An unknown computer is not managed by the Symantec Management Platform (SMP). For Mac computers, you must first boot the computer in preboot environment and then install the Mac operating system.

Following process elaborates the steps that are involved in installing Mac operating system on an unknown Mac computer:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 1 | Launch the Console | Launch the Symantec Management Console.  
You can launch the console either from the Start menu of the Notification Server computer or from any computer of the network.  
To access the console from a different computer, you must type the following:  
http://<IP address of NS>/altiris/console |
| Step 2 | Install the Network Boot service on a Site Server | Install the Network Boot Service (NBS) on a site server before you perform any other configurations.  
See “Installing Network Boot Service on site server” on page 35. |
| Step 3 | Create and modify NetBoot image and NetInstall image using Symantec's Mac pre-OS Creation Utility | Create and modify NetBoot and NetInstall image to be installed on Mac client computer. You can do this using the Symantec’s Mac pre-OS Creation Utility.  
See “Creating and modifying NetBoot images” on page 172.  
See “Creating and modifying NetInstall images” on page 175. |
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 4</td>
<td>Create preboot environment</td>
<td>Create a preboot environment with the NetBoot image. The preboot environment ensures that the NetBoot image is uploaded on the Notification Server from where it is distributed to all the NBS in the network.</td>
</tr>
</tbody>
</table>
| Step 5 | Enable the NBS service to support BSDP and configure response for unknown computer in NBS | Enable **Enable the NBS service** and **Enable Mac NetBoot (BSDP) support** in Network Boot Service Configuration from the NBS General Settings dialog box.  
In the NBS General Settings page, configure NBS to respond to unknown Mac computers and set the default image.  
**Note:** Ensure that the NetBoot image is modified using the Symantec's Mac pre-OS Creation Utility to make it suitable for Deployment Solution.  
See “Configuring NBS for Mac computers” on page 178. |
| Step 6 | Boot the client computer in preboot environment | Turn on your Mac client and hold the N key. The client computer searches for the NBS by broadcasting BSDP requests. NBS receives and processes this BSDP request and the client receives and boots the default NetBoot image as set in the NBS in step 5. |
Table 6-4  Process for installing Mac operating system on unknown Mac client (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 7| Create an **Install Mac OS** task and schedule it for the client computer | Create an **Install Mac OS** task to install the Mac operating system. Specify the details of the target volume in the configuration file on which you want to install the operating system.  
If you want to clean the disk and partition it, do it before running the task. You must manually erase and partition the disk for Mac computers.  
To run the task immediately, use the **Quick Run** option. You can also schedule the task for the client computer.  
See “Installing Mac OS using Deployment Solution” on page 168.  
See “Scheduling a deployment job or task” on page 198. |

See “Installing Mac OS using Deployment Solution” on page 168.

**Installing Mac OS on a predefined Mac computer**

Deployment Solution lets you add predefined computers to a network and also install a Mac operating system on them. You can either add the details of predefined computers using the **Add Predefined Computers Settings** or import them using a .txt file or a .csv file. For Mac predefined computers, you must specify the MAC address of the computer. You must first boot the Mac predefined computer in the preboot environment and then install the Mac operating system on the client computer.

The following process elaborates the steps that are involved to install the Mac operating system on a predefined Mac computer using a NetInstall image:
Table 6-5  Process for installing Mac operating system on a predefined Mac computer

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Launch console</td>
<td>Launch the Symantec Management Console. You can launch the console either from the Start menu of the Notification Server computer or from any computer of the network. To access the console from a different computer, you must type the following: http://&lt;IP address of NS&gt;/altiris/console</td>
</tr>
<tr>
<td>Step 2</td>
<td>Install the Network Boot service on a site server</td>
<td>Install the Network Boot Service (NBS) on a site server before you perform any other configurations. See &quot;Installing Network Boot Service on site server&quot; on page 35.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Add or import a predefined computer</td>
<td>You can add predefined computers using the Add Predefined Computers Settings dialog box or import predefined computers using a .txt file or a .csv file. See &quot;Adding or importing predefined computers&quot; on page 210.</td>
</tr>
</tbody>
</table>
Table 6-5  Process for installing Mac operating system on a predefined Mac computer  
(continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 4 | Create and modify NetBoot image and NetInstall image using Symantec's Mac pre-OS Creation Utility | Create and modify the NetBoot and NetInstall images before you install the Mac OS on a Mac client computer.  
Create and modify the NetBoot image and the NetInstall image to be installed on a Mac client computer. You can do this using the Symantec's Mac pre-OS Creation Utility. This utility along with the Apple's System Image Utility is used to create and modify the NetBoot image and the NetInstall image to make them compatible for deployment-related tasks  
See “Creating and modifying NetBoot images” on page 172.  
See “Creating and modifying NetInstall images” on page 175. |
| Step 5 | Create preboot environment.                                            | Create a preboot environment with the NetBoot image. The preboot environment ensures that the NetBoot image is uploaded on the Notification Server computer from where it is distributed to all the NBS in the network. |
Table 6-5  Process for installing Mac operating system on a predefined Mac computer (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 6</td>
<td>Enable the NBS service to support Boot Service Discovery Protocol and configure response for predefined computers</td>
<td>Turn on the <strong>Enable the NBS service</strong> and <strong>Enable Mac NetBoot (BSDP) support</strong> in <strong>Network Boot Service Configuration</strong> from the <strong>NBS General Settings</strong> page. In the <strong>NBS General Settings</strong> page, set the default response for the predefined computers. Configure the NBS to respond to the predefined Mac computers and set the default image. See “Configuring NBS for Mac computers” on page 178.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Boot the client computer in preboot environment</td>
<td>Turn on your Mac client and hold the N key. The client computer searches for the NBS by broadcasting BSDP requests. NBS receives and processes this BSDP request and the client receives and boots the default NetBoot image as set in the NBS in step 6.</td>
</tr>
</tbody>
</table>
Table 6-5 Process for installing Mac operating system on a predefined Mac computer (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 8 | Create an Install Mac OS task and schedule it for the client computer. | Create an Install Mac OS task to install the Mac operating system. Specify the details of the target volume in the configuration file on which you want to install the new operating system. If you want to clean the disk and partition it, do it before running the task. You must manually erase and partition the disk for Mac computers. To schedule, you can either use the Quick Run option or schedule the task for the client computer. See “Installing Mac OS using Deployment Solution” on page 168. See “Scheduling a deployment job or task” on page 198.

See “Installing Mac OS using Deployment Solution” on page 168.

Installing Mac OS on a managed computer

Deployment solution lets you install the Mac operating system on a managed computer. A managed computer is managed by the Symantec Management Platform (SMP) and is installed with the Symantec Management Agent (SMA). Deployment Solution lets you install the Mac operating system on a specific volume of the managed client computer.

Following process elaborates the steps that are involved in installing the Mac operating system on a managed Mac computer:
Table 6-6  Process for installing Mac operating system on a managed Mac client

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Launch the Console</td>
<td>Launch the Symantec Management Console. You can launch the console either from the Start menu of the Notification Server computer or from any computer of the network. To access the console from a different computer, you must type the following: http://&lt;IP address of NS&gt;/altiris/console</td>
</tr>
<tr>
<td>Step 2</td>
<td>Create and modify the NetInstall image using Symantec's Mac pre-OS Creation Utility</td>
<td>Create and modify NetInstall image to be installed on Mac client computer. You can do this using the Symantec's Mac pre-OS Creation Utility. See &quot;Creating and modifying NetInstall images&quot; on page 175.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Create preboot environment.</td>
<td>Create a preboot environment with the NetInstall image. The preboot environment ensures that the NetInstall image is uploaded on the Notification Server from where it is distributed to all the NBS in the network.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Enable the NBS service to support Boot Service Discovery Protocol</td>
<td>Enable the Enable the NBS service and Enable Mac NetBoot (BSPD) support in Network Boot Service Configuration pane of the NBS General Settings dialog box. See “Configuring NBS for Mac computers” on page 178.</td>
</tr>
</tbody>
</table>
Table 6-6  Process for installing Mac operating system on a managed Mac client (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 5</td>
<td>Create and schedule an Install Mac OS task</td>
<td>Create an <strong>Install Mac OS</strong> task, to install the Mac operating system. Specify the details of the target volume in the configuration file on which you want to install the new operating system.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If you want to clean the disk and create new partitions, do it before running the task, you must manually erase the disk and create new partitions on the disk for Mac computers.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To schedule, you can either use the <strong>Quick Run</strong> option or schedule the task for the client computer.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Installing Mac OS using Deployment Solution” on page 168.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Scheduling a deployment job or task” on page 198.</td>
</tr>
</tbody>
</table>

See “Installing Mac OS using Deployment Solution” on page 168.

**Sample scripted OS job**

You can create an OS installation job, which contains one or more deployment tasks.

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

- **Boot To PXE**
  Loads a preboot operating system so that other tasks can run.

- **Erase Disk**
  Wipes the disk clean, ensuring that all data and all partitions are erased.  
  See “Erasing a Disk” on page 154.

- **Partition Disk**
  Configures the clean drive with a partition.

- **Install Windows OS or Install Linux OS or Install Mac OS**
Runs the scripted install for the Windows or Linux or Mac operating system. In case of Mac operating system you must erase and partition disk manually as these tasks are not supported for Mac installation.

- See “Installing Mac OS using Deployment Solution” on page 168.
Managing tasks and jobs

This chapter includes the following topics:

- About deployment tasks and jobs
- Deployment Solution task support matrix
- Creating a deployment task
- Combining tasks into a job
- Scheduling a deployment job or task
- Verifying the task status
- Creating a Boot To task
- Changing system configuration of computers in Deployment Solution
- Copying files and folders
- Adding drivers to the Preboot driver database
- Configuring the initial deployment settings
- Adding or importing predefined computers
- Creating system configuration settings
- Creating or modifying tokens in Deployment Solution
- Configuring multicast options to deploy image

About deployment tasks and jobs

Deployment Solution lets you manage client computers using jobs and tasks. Tasks are individual activities such as creating a computer image, installing Windows operating system,
and so on. You can create and customize these tasks for the activities that you perform frequently.

For example, if you frequently boot computers using a PXE image, then you can create a task from the Boot To task with the PXE/Netboot image that you want to boot the client computer with. After the deployment task is created, it is added in the task list under the Deployment folder. You can view the tasks by navigating in the console through Manage > Jobs and Tasks > Deployment. You can right-click and select properties on a task to view the properties of the task.

Jobs are a combination of tasks that are scheduled and executed in an orderly manner on specific computers.

For example, if you want to boot the client computers in pre-OS state and install Windows OS, you can create tasks such as Boot to PXE, Install Windows 2003 OS and club both these tasks into a Job and schedule them or run them when required.

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 “Adding or importing predefined computers” on page 210.

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>
<thead>
<tr>
<th>Table 7-1</th>
<th>Predefined deployment tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task</td>
<td>Description</td>
</tr>
<tr>
<td>Apply System Configuration</td>
<td>Applies the new configurations to a computer. See “Creating system configuration settings” on page 213.</td>
</tr>
<tr>
<td>Boot To</td>
<td>Instructs a computer to boot to the production OS, PXE, or automation folder. See “Creating a Boot To task” on page 199.</td>
</tr>
<tr>
<td>Capture Personality</td>
<td>Captures the personality of the computer. See “Capturing a computer’s personality” on page 229.</td>
</tr>
<tr>
<td>Task</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Copy File</td>
<td>Copies the specified files and folders to a destination computer.</td>
</tr>
<tr>
<td></td>
<td>See “Copying files and folders” on page 204.</td>
</tr>
<tr>
<td>Create Image</td>
<td>Creates the disk images and backup images.</td>
</tr>
<tr>
<td></td>
<td>See “Creating a Windows image” on page 113.</td>
</tr>
<tr>
<td></td>
<td>See “Creating a Linux image” on page 124.</td>
</tr>
<tr>
<td></td>
<td>See “Creating a Mac image” on page 131.</td>
</tr>
<tr>
<td>Deploy Image</td>
<td>Deploys the disk image files (not the backup image files).</td>
</tr>
<tr>
<td></td>
<td>See “Deploying a Windows image” on page 116.</td>
</tr>
<tr>
<td></td>
<td>See “Deploying a Linux image” on page 127.</td>
</tr>
<tr>
<td></td>
<td>See “Deploying a Mac image” on page 133.</td>
</tr>
<tr>
<td>Distribute Personality</td>
<td>Installs a previously captured computer personality.</td>
</tr>
<tr>
<td></td>
<td>See “Distributing a computer's personality” on page 230.</td>
</tr>
<tr>
<td>Erase Disk</td>
<td>Cleans a disk. You can configure this task to meet DoD standards.</td>
</tr>
<tr>
<td></td>
<td>See “Erasing a Disk” on page 154.</td>
</tr>
<tr>
<td>Install Linux/ESX OS</td>
<td>Performs a scripted OS install of Linux and ESX operating systems.</td>
</tr>
<tr>
<td></td>
<td>See “Installing Linux/ESX OS using Deployment Solution” on page 167.</td>
</tr>
<tr>
<td>Install Mac OS</td>
<td>Performs a scripted OS install of Mac operating system</td>
</tr>
<tr>
<td></td>
<td>See “Installing Mac OS using Deployment Solution” on page 168.</td>
</tr>
<tr>
<td>Install Windows OS</td>
<td>Performs a scripted OS install of Windows.</td>
</tr>
<tr>
<td></td>
<td>See “Installing a Windows OS using Deployment Solution” on page 150.</td>
</tr>
<tr>
<td>Partition Disk</td>
<td>Creates the disk partitions on a hard drive.</td>
</tr>
<tr>
<td></td>
<td>See “Creating disk partitions” on page 156.</td>
</tr>
</tbody>
</table>
Table 7-1 Predefined deployment tasks (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prepare for Image capture</td>
<td>Runs Microsoft Sysprep.</td>
</tr>
<tr>
<td></td>
<td>See “Configuring the Sysprep imaging” on page 112.</td>
</tr>
<tr>
<td></td>
<td>See “Preparing to capture an image” on page 138.</td>
</tr>
<tr>
<td>Restore BackUp Image</td>
<td>Deploys the backup image files (not the disk image files).</td>
</tr>
<tr>
<td></td>
<td>See “Restoring a backup image” on page 141.</td>
</tr>
</tbody>
</table>

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*.

See “Creating a deployment task” on page 197.
See “Combining tasks into a job” on page 197.
See “Scheduling a deployment job or task” on page 198.
See “Verifying the task status” on page 199.

### Deployment Solution task support matrix

Deployment Solution lets you manage 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. For Windows and Mac both x86 and x64 architectures are supported for Linux only x86 architecture is supported.

Following table lists the tasks that are supported by Windows architecture:

**Table 7-2** Support matrix for Deployment Solution tasks for Windows

<table>
<thead>
<tr>
<th>Task</th>
<th>Production OS x86</th>
<th>Production OSx64</th>
<th>WinPE x86</th>
<th>WinPE x64</th>
<th>PXE x86</th>
<th>PXE x64</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apply System</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Configuration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Boot To</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Copy File</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Capture Personality</td>
<td>Yes - Not Supported on Server Class OS</td>
<td>Yes - Not Supported on Server Class OS</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Create Image</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Deploy Image</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Distribute Personality</td>
<td>Yes - Not Supported on Server Class OS</td>
<td>Yes - Not Supported on Server Class OS</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Erase Disk</td>
<td>Yes - Not Supported on Server Class OS</td>
<td>Yes - Only on Secondary Disk</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Install Windows OS</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Partition Disk</td>
<td>Yes - Not Supported on Server Class OS</td>
<td>Yes - Only on Secondary Disk</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Prepare for Image</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Capture</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Restore Backup Image</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Following table elaborates the tasks that are supported by Linux operating system:

**Table 7-3** Support matrix for Deployment Solution tasks for Linux

<table>
<thead>
<tr>
<th>Task</th>
<th>Production OS x86</th>
<th>LinPE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apply System</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Configuration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Boot To</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Copy File</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>
Table 7-3  Support matrix for Deployment Solution tasks for Linux (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Production OS x86</th>
<th>LinPE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capture Personality</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Create Image</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Deploy Image</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Distribute Personality</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Erase Disk</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Install Linux OS</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Partition Disk</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Prepare for Image Capture</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Restore Back up Image</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Following table elaborates the tasks that are supported by Mac operating system:

Table 7-4  Support matrix for Deployment Solution tasks for Mac

<table>
<thead>
<tr>
<th>Task</th>
<th>Production OS</th>
<th>NetBoot</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apply System Configuration</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Boot To</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Copy File</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Capture Personality</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Create Image</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Deploy Image</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Distribute Personality</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Erase Disk</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Install Mac OS</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Partition Disk</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Prepare for Image Capture</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Restore Back up Image</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
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 191.

A task cannot be deleted if it is currently in use by a job or policy. You can view the tasks that are used by the policies in the Jobs and Tasks view of the console. Tasks can be renamed, deleted, cloned, moved, and scheduled by right-clicking the task and selecting the corresponding option.

To create a deployment task

1. In the Symantec Management Console, on the Manage menu, click Jobs and Tasks.
2. In the left pane, select Deployment folder.
3. In the Jobs/Tasks pane, right-click on the Deployment folder and select New.
4. In the Create New Task page, select a deployment task.
5. Add the required information, select the options that you want and enter a meaningful name to the task.
   For example, Boot To Windows 2003 PXE.
6. In the selected task page, select OK
7. Schedule the task.
   See “Scheduling a deployment job or task” on page 198.

See “Combining tasks into a job” on page 197.

Combining tasks into a job

A job is a combination of tasks to be performed in a specific order. You can combine deployment-related tasks with other types of tasks in a job. You can create folders and organize jobs and tasks that you have created. You can also drag and drop jobs from one folder to another folder.

You can do the following with Jobs:

- Add condition statements to define the tasks to be performed when the condition is satisfied and when the condition is not satisfied.
- Rename a job.
- Delete a job.
- Clone a job.
Move a job.

Schedule a job.

See “Creating a deployment task” on page 197.

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

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 197.

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.

See “About deployment tasks and jobs” on page 191.

Scheduling a deployment job or task

Deployment Solution lets you schedule a task that you have created. You can schedule the task to run immediately or a specific time. You can also select the computer on which the task is executed.

To schedule a task

1. In the Symantec Management Console, on the Manage menu, click Jobs and Tasks.
2. In the left pane, select the task that you want to schedule.
3. (Optional) If you want to execute the task 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.

4. If you want to schedule the task to run at a later time or you want to schedule multiple computers, click New Schedule.
5 Select the date and time that you want to schedule for the task to execute.
You can also select the task to run at specific intervals.

6 Select the computers that you want the task to run on.

7 Click Schedule.
See “Creating a deployment task” on page 197.

Verifying the task status

You can check the state of any tasks that previously ran.
See “About deployment tasks and jobs” on page 191.
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 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.
See “Creating a deployment task” on page 197.
See “Scheduling a deployment job or task” on page 198.

Creating a Boot To task

You can start computers in an automation environment to run tasks, else boot to a PXE environment or a production environment based on the requirement.
You can use either PXE environment or automation environment but not both environments together. Assign this task only if you want to perform a custom automation task.

To create a Boot to task

1 In the Symantec Management Console, select Manage > Jobs and Tasks.
2 In the left pane, do either of the following:
- Right-click **System Jobs and Tasks** folder and select **New > Task**.
- Expand the **System Jobs and Tasks** folder and right-click **Deployment** folder to select **New > Task**.

3. In the **Create New Task** dialog box, under **Deployment** folder, select the **Boot to** task.

4. The fields and the descriptions are as follows:

<table>
<thead>
<tr>
<th>Task name icon</th>
<th>Displays the default task name as Boot To. You can edit the default task name to specify a relevant task name. For example, Boot To_Automation.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automation</td>
<td>Lets you select the automation environment to boot the client computers. Automation environment is created on the client computers on which the automation folder is installed.</td>
</tr>
<tr>
<td>Production</td>
<td>Lets you select the production environment to the boot the computer either from the preboot environment or automation environment. You boot a computer into the production environment to resume regular tasks such as report generation or so.</td>
</tr>
</tbody>
</table>
Let's you select the PXE image for the WinPE or LinuxPE environments or the NetBoot image for the Mac environment from the drop-down list.

For the PXE image, select any of the following architectures from the drop-down list:

- **Auto**
  Select this option if you want to boot the client computer based on the computer’s processor architecture. For example, if you have a client computer whose processor type is x64 but the installed operating system is x86 of Windows 7, then the Auto option boots the computer in x64 architecture mode and not in x86 mode.
  The Auto option can be useful if you have created a common PXE image for both x86 and x64 architectures or want to boot a computer as per the processor architecture irrespective of the OS architecture. You create PXE images through the **Manage Preboot Configuration** dialog box of the console.

- **x86**
  Select this option if the PXE image that you have created is for the x86 architecture of the operating system.

- **x64**
  Select this option if the PXE image that you have created is for the x64 architecture of the operating system.

**Note:** Before you boot to PXE, ensure that you have started the Windows firewall service and opened the ports 4011 and 69. Otherwise, booting to PXE might fail.

**Registration Period**

The registration time period is the time period during which the client computers are unrolled from Notification Server registration policy. This happens only when the client computer tries to boot from one environment to another. Within the specified registration time, the client computer must again register back to the registration policy, failing which, the computer must be registered manually.

The default registration time that is displayed is the registration time that is set in the **Global Settings** page.
5 Click **OK**.

6 Schedule the task.

See “Scheduling a deployment job or task” on page 198.

See “Preparing predefined computers to boot with WinPE image” on page 64.

### Changing system configuration of computers in Deployment Solution

Deployment Solution lets you apply and change the system configuration of computers. For example, if you want to change the domain settings of computers after an image is deployed. You can create and schedule an **Apply System Configuration** task and change the domain settings for the computers on which you have deployed an image.

In Deployment Solution you can create system configuration by accessing the following:

- **Settings > Deployment > System Configurations**
  
  You create system configurations and apply these system configurations by creating and scheduling an **Apply System Configuration** task.

- **Manage > Jobs and Tasks > Deployment**
  
  On the **Deployment** folder, right-click and select **new > Task**.
  
  In the **Create New Task** page, in the **Deployment** folder, select the **Apply System Configuration** task. You can run and schedule the task individually or in a job with other tasks.

For computer names and host name you can also use tokens. For example, `%CustomerToken%`, `%SERIALNUMBER%`.

**To create an Apply System Configuration task**

1 In the Symantec Management Console, from the **Manage** menu select **Jobs and tasks**.

2 In the left pane, do either of the following:

   - Right-click **System Jobs and Tasks** and select **New > Task**.
   
   - Expand the **System Jobs and Tasks** and right-click **Deployment** to select **New > Task**.

3 In the **Create new task** dialog box, select **Deployment > Apply System Configuration** option.

4 Select one of the following options:
### Task name icon
Displays the default task name as Apply System Configuration. You can edit the default task name to specify a relevant task name. For example, System Config_restorefrominventory.

### Use a predefined system configuration
Select the relevant system configuration settings that you have created from the drop-down list.

You can also click **New** to create a new configuration.

See “Creating system configuration settings” on page 213.

You can also edit the existing system configuration by clicking **Edit**. The system configuration details are displayed in the **Computer name** tab and the **Network adapters** tab.

### Restore system configuration using inventory data
Select this option if you want to restore the system configuration settings for a client computer using the inventory data. For example, if you have specified an IP address for the system configuration setting and later decide to update it. In this case, you can use this option to restore the setting for the client computer provided the specific criteria are met.

You can restore the system configuration settings if the following criteria are met:

- The time interval set for the inventory data update to the SMP agent does not lapse.
- You do not log in to the client computer after the computer boots.

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
  - The credentials are either of a local administrator account or of a domain account if you join the computer to a domain.
- Confirm Password

5 Click **OK**.

6 Schedule the task.

See “Scheduling a deployment job or task” on page 198.

If you execute this task on a Linux or Mac 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.

See “Creating system configuration settings” on page 213.
Copying files and folders

Deployment Solution lets you copy files and folders from one client computer to another computer that is in the same network. You can also copy files and folders from the local computer on which Symantec Management Platform (SMP) is installed. Deployment Solution uses either HTTP protocol or UNC to copy a file from the local computer to the client computer.

Note: For Windows, you can copy files over both HTTP and UNC whereas for Linux computers, you can copy files only over HTTP.

When you copy a file that already exists on a client computer, the earlier version of the file is overwritten. Deployment Solution also provides you the option to install an executable using the command-line switch option.

You can use the Copy File task to copy files of installable that you want to install on a different computer. You can copy installation files such as MSI or EXE. After the task executes, you can install the application by using the command-line switches.

To copy files and folders

1. Launch the Symantec Management Console.
2. In the Symantec Management Console, on the Manage menu select Jobs and Tasks.
3. In the left pane, do either of the following:
   - Right-click System Jobs and Tasks and select New > Task.
   - Expand the System Jobs and Tasks and right-click Deployment to select New > Task.
4. The fields and their descriptions are as follows:

   **Task name icon**
   Lets you specify a name for the Copy File task that you create.

   **Copy file**
   Select this option if you want to copy a file.

   **Copy folder**
   Select this option if you want to copy a folder. Ensure that all the subfolders are included and are compressed into a .ZIP file.
Source

Select the source of the file or the folder from where you want to copy.

Select from either of the source options:

- **Access from UNC location**
  You can access a shared path of the client computer to copy the file or folder. If you want to copy a file that is not on the Symantec Management Platform computer ensure 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.

- **Upload from local system**
  You can upload a file or folder from a local computer on which SMP is installed.

  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

Browse to the location of the files to upload or to the UNC path to copy the files or folder files.

Specify the credentials in the **User name** and **Password** fields to retrieve the files from the selected location.

Destination

The location of the client computer where the files are to be copied.

**File Execute > Command Line**

Specify the command-line instruction to execute the copied file on the client computer.


Provide the required credentials to execute the command-line instructions in the **User name** and **Password** fields.

5 Click **OK**.

6 Schedule the task.

See “Scheduling a deployment job or task” on page 198.
Adding drivers to the Preboot driver database

Deployment Solution lets you add drivers to the Preboot driver database, which is required when you boot a computer to the preboot configurations. If a preboot configuration that you already created requires a new driver, you must regenerate that preboot configuration.

After adding drivers to the Preboot database, the preboot images can then support mass storage devices (MSDs) and network interface cards (NICs). These critical 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.

To add new driver to an existing preboot configuration, you must recreate that preboot configuration with the newly-added driver using the Recreate environment option. If you create a preboot image before Network Boot Service (NBS) is installed and enabled on a remote site server, then it is not registered with the site server. In such case, you must either recreate that preboot environment for the selected image or create a new image to be registered with the new remote site server.

This use case addresses how you must install the NBS on a site server, add drivers to the Preboot driver database, and then boot an unknown computer in the preboot environment using a WinPE image. After the computer boots in the preboot environment, the communication with Notification server is established.

You must perform the following steps to add drivers to the Preboot driver database and then execute a scripted Windows OS installation on a computer:

Table 7-5 Adding drivers to the Preboot driver database

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Launch the Symantec Management Console</td>
<td>Launch the Symantec Management Console. You can launch the console either from the Start menu of the computer or you can launch the Web console if you know the IP address of the Notification Server. For example: http://&lt;IP address&gt;/altiris/console.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Install and enable the Network Boot Service on a site server</td>
<td>Install the Network Boot Service (NBS) on a site server before you perform any other configurations. NBS is a component of Deployment Solution that you install and run as a service on a site server. NBS service, once installed on a site server, handles all the communication with the Symantec Management Platform for Deployment Solution. See “Installing Network Boot Service on site server” on page 35.</td>
</tr>
</tbody>
</table>
### Configuring the initial deployment settings

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

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

**Note:** In case of configuring an Initial Deployment job to deploy an image using multicast option, ensure to add `-mp -clients=3 -threshold=2 -connecttimeout=10` in the command line options of the deploy image task that you want to add in the Initial Deployment job.

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

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

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

To configure the initial deployment settings

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

2. In the **Initial Deployment Settings** dialog box, specify the values for the fields.

3. In the **Initial Deployment Settings** dialog box, click **Add** to add the tasks that you want to display in the job menu of the computer.

The fields and the descriptions of the dialog box are as follows:

**Network Boot Services Settings**  Lets you browse to the **NBS General Settings** dialog box of the console to configure the Network Boot Service that is installed on a site server.

See “About NBS General Settings” on page 85.
Initial Deployment (Unknown Computer) Menu

Lets you configure the job menu that must display for the unknown computer after the computer boots in the preboot environment.

Click Add to launch the Add Existing Tasks/Jobs dialog box to add the tasks or jobs that you want to display in the job menu. By default, the first task or job is listed as the default task in the table. You can select a different task or job by selecting the corresponding radio button.

Select any one of the following options to configure the schedule of the job:

- **Run default job immediately**
  Select this option to run the default job immediately after you create.

- **Wait indefinitely for user selection**
  Select this option if you want to select the job from the job menu that is displayed on the unknown computer.

- **Run default job after [ ] seconds**
  Select this option if you want to run the default job after the time that you specify in seconds.

- **Shutdown the computer after [ ] seconds**
  Select this option if you want the unknown computer to shut down after the time that you specify in seconds.

You can delete an already configured job by selecting the job and then click the delete icon.
Re-Deployment (Managed Computer) Menu

Lets you configure the job menu that displays for the Windows managed computer after the computer boots in the automation environment.

Click Add to launch the Add Existing Tasks/Jobs dialog box to add the tasks or jobs that you want to display in the job menu. By default, the first task or job is listed as the default task in the table. You can select a different task or job by selecting the corresponding radio button.

Select any one of the following options to configure the schedule of the job:

- **Run default job immediately**
  Select this option to run the default job immediately.

- **Wait indefinitely for user selection**
  Select this option if you want to select the job from the job menu that is displayed on the managed computer.

- **Run default job after [ ] seconds**
  Select this option if you want to run the default job after the time that you specify in seconds.

- **Shutdown the computer after [ ] seconds**
  Select this option if you want the managed computer to shut down after the time that you specify in seconds.

You can delete an already configured job by selecting the job and then click the delete icon.

4. Select the default task for the initial deployment menu.

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

5. Click Save changes.

   See “Booting managed Windows computer with WinPE image” on page 74.

   See “Preparing site servers for Deployment Solution” on page 30.

---

**Adding or importing predefined computers**

Deployment Solution lets you provision client computers even before they are added to the network as predefined computers. You add the predefined computer details or import them from a .txt file or a .csv file. Both addition and import of predefined computer details can be performed through the Symantec Management Platform (SMP) console.

See “About predefined computers in Deployment Solution” on page 48.
To add a predefined computer

1. In the Symantec Management Console, on the Settings menu, click Deployment > Predefined Computers.

2. In the Predefined Computer dialog box, click Add.

3. In the Add Predefined Computer Settings page, specify the values for the fields that are as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Lets you specify a name for the predefined computer. This field is mandatory.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>Lets you specify the serial number of the computer. The value of this hardware identifier is used by Deployment Solution as a matching criteria to identify unknown client computers of a network as potential predefined computers.</td>
</tr>
<tr>
<td>Asset Tag</td>
<td>Lets you specify the asset tag of the computer.</td>
</tr>
<tr>
<td>UUID</td>
<td>Lets you specify the Universal Unique Identifier (UUID) of the computer.</td>
</tr>
<tr>
<td>Host Name</td>
<td>Lets you specify the host name of the computer.</td>
</tr>
<tr>
<td>Domain/Workgroup</td>
<td>Lets you specify the domain of the computer.</td>
</tr>
</tbody>
</table>
Network Adapters

Lets you select the type of network adapter that you want to add as predefined computer. Click Add if you want to add more than one adapters.

The options to select from are as follows:

- **Use DHCP to obtain IP address**
  By default, this option is selected.
  Select this option if you want to select the IP address of computers using DHCP. Specify the values for the required fields that appear after you select this option.
  The fields that you can specify are as follows:
  - MAC Address
    The value of this hardware identifier is used by Deployment Solution as a matching criteria to identify unknown client computers of a network as potential predefined computers.
  - DNS 1, DNS2, DNS3
  - Primary DNS Suffix
  - Primary WINS Server
  - Secondary WINS Server

- **Assign static IP address**
  Select this option if you want to specify a static IP address of the computers. Specify the values for the required fields that appear after you select this option.
  The fields that you can specify are as follows:
  - MAC Address
    The value of this hardware identifier is used by Deployment Solution as a matching criteria to identify unknown client computers of a network as potential predefined computers.
  - IP Address
  - Default Gateway
  - Subnet Mask
  - DNS 1, DNS2, DNS3
  - Primary DNS Suffix
  - Primary WINS Server
  - Secondary WINS Server

**Note:** The MAC address is mandatory for the Mac client computers.

4 Click OK.
To import predefined computer

1. In the Symantec Management Console, on the Settings menu, click Deployment > Predefined Computers.
2. In the Predefined Computer dialog box, click Import Computers.
3. In the Open File dialog box, navigate to the .txt or the .csv file that contains 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.
   
   See “Referencing a sample CSV file” on page 63.
4. From the Manage menu, select Computers to view the details of imported predefined computers.

Creating system configuration settings

The system configuration setting of a client computer comprises of the network setting, domain name, computer name, IP address, and so on. Deployment Solution lets you create system configurations to apply on the client computers after they boot to the production environment from the preboot environment or automation environment. For example, after you boot 50 client computers to the production environment, you might want the computer names to be modified and also join a common domain. This task can be performed through the system configuration that you create and apply on the client computers.

You either create a new system configuration setting for the client computers or update an existing system configuration. Deployment Solution lets you apply system configurations on the managed client computers that are already imaged or on which a Deploy Image task is executed.

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. In the Create System Configuration dialog box, select the appropriate option and specify the values.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Lets you specify a name for the system configuration task that you create.</td>
</tr>
<tr>
<td>Description</td>
<td>Lets you specify a description for the task that you create.</td>
</tr>
</tbody>
</table>
4 On the **Computer Information** tab of the dialog box, select the appropriate option and specify the values.

**Computer name**

Select **Computer name** and enter a computer name. 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.

**Name range**

Select this option to provide a name range for the client computers and click **Define range**.

The **Name range** option lets you use the same configuration for multiple computers. The **Define range** option lets you specify the **Fixed text** and the **Range start** in the **Computer Name Range** dialog box.

In the **Computer Name Range** dialog box, computers are named using a fixed text appended with the range value that you specify. The range is appended to the name only if you check the **Append** textbox. The range is the number that you want to start with. This string increment is by 1 for each computer that receives the configuration.

You can specify a range of 6-digit number. For example, if you specify fixed text as ABC and range start as 123456, then the names of the client computers will be as, ABC123456, ABC 123457 and so on.

Additionally, if you use a name range with a static IP address on this tab, the IP address you specify is incremented as well.

**Workgroup**

Select **Workgroup** and enter a workgroup name for the new configuration. or
Domain
Select Domain and enter the domain name.
If you select Domain, you must specify the administrative domain user name and password.
The credentials are either of a local administrator account or of a domain account if you connect the computer to a domain.
Organizational unit
The organization unit lets you add the computer at different organizational unit levels. If you have only the domain level, then specify the domain level and leave the organizational unit as empty. All the client computers are then added to the domain level of the Active Directory.
You can add the computers to the following organizational units:
- One level under the domain
  For example, If you have an organizational unit name OU1 enter OU1 in the Organizational unit field.
- Multiple level organizational units under the domain
  For example, If you have multiple levels of organizational units such as OU3 under OU2 which is under OU1 and so on, enter OU1/OU2/OU3 in the Organizational unit field to add the client computer to the OU3 level under the domain.

5 In the Network Adapters tab of the dialog box, select and specify the required information.

Connection-specific DNS suffix
Lets you specify the domain suffix of the network.
Select Leave existing if you want to retain the existing domain suffix.
Network adapter

Lets you select a network adapter from the drop-down list.

Click **Add** to add a network adapter to the configuration.

Click **Remove** to remove a network adapter from the configuration.

Select one of the following options:

- **Leave existing**
  Select this option if you want to use the existing default DHCP or IP address.

- **Use DHCP to obtain IP address**
  Select this option if you want to use the DHCP server to assign IP address to the client computers.

- **Assign a static IP address**
  Select this option to assign a static IP address.
  Specify the following after you select this option:
  - **IP address**
  - **Use as range**
  - **Subnet mask**
  - **Default gateway**
  - **DNS1**
  - **DNS2**

Click **Advanced** to create the IP interfaces, gateway, and DNS.

If you change an IP address from DHCP to static, you must supply the subnet mask and gateway. Even if they are the same as they were when you use DHCP, you must supply these numbers. These values are not stored when you use DHCP.

You can add multiple NIC, but it is not supported for SUSE client computers.

6 Click **OK**.

See “Changing system configuration of computers in Deployment Solution” on page 202.

---

**Creating or modifying tokens in Deployment Solution**

In Deployment Solution, a system token is a type of variable, which is replaced with unique deployment-related data that is retrieved from the database. You can insert these variable tokens in scripts or answer files to extract information from the database. Deployment Solution provides you with the option to create tokenized scripts through the console as well as has predefined tokens to use.
See "About predefined tokens in Deployment Solution" on page 217.

You can add or create a new token, edit the SQL query of an existing token, or delete a token that you have created. You are not recommended to modify an existing token name.

To create new tokens through the console

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

To modify an existing token

1. In the Symantec Management Console, on the Settings menu, click Deployment > Tokens.
2. Select an existing token that is listed in the table and double-click it.
3. In the SQL statement field, modify the SQL query of the token.

About predefined tokens in Deployment Solution

In Deployment Solution, a system token is a type of variable that can be replaced with unique deployment-related data that are retrieved from the database. You can insert these variable tokens in scripts or answer files to extract information from the database. Each managed computer can have its own unique value for each token. For example, the %COMPNAME% token stores the NetBios computer name while the %DOMAIN% token stores the Microsoft Domain or Workgroup a computer is a member. Depending on the individual computer, there may not be a value stored in the database for every possible token. The names for the Deployment Solution system tokens are case sensitive and must have a percent sign at the beginning and end of the token name.

There are tokens that you can add through the Symantec Management Console and also through the unattended or answer configuration file.

You can access the tokens from either of the following menus of the console:

- Settings > All Settings menu > Settings pane > Notification Server > Task Settings > Tokens
- Settings > Deployment > Tokens

You can add or create a new token, edit the SQL query of an existing token, or delete a token that you have created. You are not recommended to modify an existing token name.
Deployment Solution supports usage of tokens for the following tasks:

- Prepare for Image capture
- Create Image
- Deploy Image
- Install Windows OS
- Install Linux/ESX OS
- Apply System Configuration
- Capture Personality

Tokens that are supported for the **Create Image** task of Windows operating system are as follows:

<table>
<thead>
<tr>
<th>Table 7-6</th>
<th>Tokens for Windows imaging task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Token</td>
<td>Description</td>
</tr>
<tr>
<td>%COMPNAME%</td>
<td>Actual computer name used by the OS</td>
</tr>
<tr>
<td>%MODELNUMBER%</td>
<td>Model number of the computer</td>
</tr>
<tr>
<td>%OS%</td>
<td>Specific operating system (Win98, Win2K, WinXP, Linux )</td>
</tr>
<tr>
<td>%SERIALNUMBER%</td>
<td>Serial number from SMBIOS</td>
</tr>
<tr>
<td>%TRIMSERIALNUMBER%</td>
<td>Serial number from SMBIOS without black spaces</td>
</tr>
</tbody>
</table>

Tokens that are supported for the **Create Image** task of Linux operating system are as follows:

<table>
<thead>
<tr>
<th>Table 7-7</th>
<th>Tokens for Linux imaging task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Token</td>
<td>Description</td>
</tr>
<tr>
<td>%COMPNAME%</td>
<td>Actual computer name used by the OS</td>
</tr>
<tr>
<td>%NICyIPADDR%</td>
<td>IP Address for NIC y (y = 1-8). For example, the first NIC would be %NIC1IPADDR% , second %NIC2IPADDR%</td>
</tr>
<tr>
<td>%NICyIPHOST%</td>
<td>IP Host for NIC y (y = 1-8). For example, the first NIC would be %NIC1IPHOST%; the second would be %NIC2IPHOST%</td>
</tr>
<tr>
<td>%NICyIPDNSx%</td>
<td>DNS entry x for NIC y, for example: the second NIC fourth DNS entry would be %NIC2IPDNS4%.</td>
</tr>
<tr>
<td>%NICyIPGATEWAY</td>
<td>Default gateway for NIC y (y = 1-8). For example, the first NIC would be %NIC1IPGATEWAY%, second %NIC2IPGATEWAY%</td>
</tr>
</tbody>
</table>
### Table 7-7  Tokens for Linux imaging task (continued)

<table>
<thead>
<tr>
<th>Token</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>%NICyIPNETMASK%</td>
<td>Netmask for NIC y. For example, the first NIC would be %NIC1IPNETMASK%, second %NIC2IPNETMASK%</td>
</tr>
<tr>
<td>%NICyIPWINSx%</td>
<td>WINS entry x for NIC y. For example, the third NIC first WINS entry would be %NIC3IPDNS1%</td>
</tr>
<tr>
<td>%NICyMACADDR%</td>
<td>MAC for NIC y (y = 1-8). For example, the first NIC would be %NIC1MACADDR%, second %NIC2MACADDR%</td>
</tr>
<tr>
<td>%OS%</td>
<td>Specific operating system (Win98, Win2K, WinXP, Linux)</td>
</tr>
<tr>
<td>%OSTYPE%</td>
<td>Operating system type (Win9x, WinNT, Linux)</td>
</tr>
<tr>
<td>%SERIALNUMBER%</td>
<td>Serial number from SMBIOS</td>
</tr>
</tbody>
</table>

Tokens that are supported for the **Create Image** task of Mac operating system are as follows:

### Table 7-8  Tokens for Mac imaging task

<table>
<thead>
<tr>
<th>Token</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>%COMPNAME%</td>
<td>Actual computer name used by the OS</td>
</tr>
<tr>
<td>%NICyIPADDR%</td>
<td>IP Address for NIC y (y = 1-8). For example: the first NIC would be %NIC1IPADDR%, second %NIC2IPADDR%</td>
</tr>
<tr>
<td>%NICyIPHOST%</td>
<td>IP HOST for NIC y (y = 1-8). For example, the first NIC would be %NIC1IPHOST%; the second would be %NIC2IPHOST%</td>
</tr>
<tr>
<td>%NICyIPGATEWAY%</td>
<td>Default gateway for NIC y (y = 1-8). For example: the first NIC would be %NIC1IPGATEWAY%, second %NIC2IPGATEWAY%...</td>
</tr>
<tr>
<td>%NICyIPNETMASK%</td>
<td>Netmask for NIC y. For example: the first NIC would be %NIC1IPNETMASK%, second %NIC2IPNETMASK% ...</td>
</tr>
<tr>
<td>%NICyMACADDR%</td>
<td>MAC for NIC y (y = 1-8). For example: the first NIC would be %NIC1MACADDR%, second %NIC2MACADDR%</td>
</tr>
<tr>
<td>%SERIALNUMBER%</td>
<td>Serial number from SMBIOS</td>
</tr>
<tr>
<td>%OS%</td>
<td>Specify operating system</td>
</tr>
</tbody>
</table>
Table 7-8  Tokens for Mac imaging task (continued)

<table>
<thead>
<tr>
<th>Token</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>%OSTYPE%</td>
<td>Operating system type</td>
</tr>
</tbody>
</table>

Tokens that are supported for the **Apply System Configuration** task of Windows operating system are as follows:

Table 7-9  Tokens for **Apply System Configuration** task of Windows

<table>
<thead>
<tr>
<th>Token</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>%COMPNAME%</td>
<td>Actual computer name used by the OS</td>
</tr>
<tr>
<td>%DOMAIN%</td>
<td>MS Workgroup or domain name</td>
</tr>
<tr>
<td>%DSSERVER%</td>
<td>The NetBios name of the computer where the Deployment Server is installed</td>
</tr>
<tr>
<td>%MANUFACTURERNAME%</td>
<td>Computer manufacturer from SMBIOS</td>
</tr>
<tr>
<td>%MODELNUMBER%</td>
<td>Model number of the computer</td>
</tr>
<tr>
<td>%SERIALNUM%</td>
<td>Serial number from SMBIOS</td>
</tr>
<tr>
<td>%TRIMSERIALNUMBER%</td>
<td>Serial number from SMBIOS without black spaces</td>
</tr>
</tbody>
</table>

Note: Tokens are not supported for **Apply System Configuration** task of Linux operating system.

Tokens that are supported for the **Personality Capture** task are as follows:

Table 7-10  Tokens for **Personality Capture**

<table>
<thead>
<tr>
<th>Token</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>%COMPNAME%</td>
<td>Actual computer name used by the OS</td>
</tr>
</tbody>
</table>

The list of tokens that you can add to the unattended.xml or answer file for installing OS tasks are as follows:

- @timezone
- @userName
- @domainou
- @compName
Adding tokens for deployment tasks

You can add tokens either through the console or through the answer files for specific deployment-related tasks. Addition of tokens in tasks help you retrieve the actual data of the computer that can be useful. For example, if you use a token %COMPNAME% for the Image name field of a Create Image task, then the image is created using the actual name of the computer. You can specify more than one token in a field with no space as separator. You can also specify tokens in the answer files of the deployment tasks. In case of Mac, the tokens are supported for imaging task only and can be added only through the console.

Deployment Solution supports usage of tokens for the following tasks:

- Prepare for Image capture
- Create Image
- Deploy Image
- Install Windows OS
- Install Linux/ESX OS
- Apply System Configuration
- Capture Personality

To add tokens in answer file for the Prepare for Image capture task

1. Launch the Symantec Management Platform console and select Settings > Deployment > Tokens menu.
2. In the Tokens dialog box, create a new token.

See “Creating or modifying tokens in Deployment Solution” on page 216.
3 Place the token that you created either in the answer file for Prepare for Image capture task or in the sysprep.inf file.

   The answer file is located in [install_directory]\Program Files\Altiris\Notification Server\NSCap\bin\Win32\x86\Deployment\unattend.xml and the sysprep.inf file is in NSCap\bin\Win32\x86\Deployment\ location

4 Create a task and schedule it.

To add tokens in answer file for the Deploy Image task

1 Launch the Symantec Management Platform console and select Settings > Deployment > Tokens menu.

2 In the Tokens dialog box, create a new token.

   See “Creating or modifying tokens in Deployment Solution” on page 216.

3 Place the token that you created either in the answer file for Deploy Image task or in the sysprep.inf file.

   The answer file is located in [installation_directory]\Program Files\Altiris\Notification Server\NSCap\bin\Win32\x86\Deployment\unattend.xml and the sysprep.inf file is in \NSCap\bin\Win32\x86\Deployment\ location.

4 Create a task with the option, Custom Sysprep configuration file selected in the Deploy Image dialog box and schedule it.

To add tokens in answer file for the Install Windows OS task

1 Launch the Symantec Management Platform console and select Settings > Deployment > Tokens menu.

2 In the Tokens dialog box, create a new token.

   See “Creating or modifying tokens in Deployment Solution” on page 216.

3 Place the token that you created either in the answer file for Install Windows OS task.

   The answer file is located in [installation_directory]\Program Files\Altiris\Notification Server\NSCap\bin\Win32\x86\Deployment\SOI\AnswerFile location.

4 Create a task with the option, Configuration file selected in the Install Windows OS dialog box and schedule it.

To add tokens in answer file for the Install Linux/ESX OS task

1 Launch the Symantec Management Platform console and select Settings > Deployment > Tokens menu.

2 In the Tokens dialog box, create a new token.

   See “Creating or modifying tokens in Deployment Solution” on page 216.
3. Place the token that you created either in the answer file for Install Linux/ESX OS task. The answer file is located in [installation_directory]\Program Files\Altiris\Notification Server\NSCap\bin\UNIX\Deployment\Linux\x86\SOI\AnswerFile location.

4. Create a task with the option, Configuration file selected in the Install Linux/ESX OS dialog box and schedule it.

See “About predefined tokens in Deployment Solution” on page 217.

Configuring multicast options to deploy image

You can configure the image multicasting settings through the following options:

- **Settings > Deployment > Image Multicasting** menu
- **Settings > All Settings > Deployment > Image Multicasting** option

To configure multicast options

1. In the Symantec Management Console, on the **Settings** menu, click **Deployment > Image Multicasting**.

2. Specify values for the following fields:

   - **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 minutes to wait for the specified number of clients to join the group. If this number is reached, your images are deployed separately.

3. Click **Restore defaults** to use the default configuration settings.

4. Click **Save changes**.
Capturing and distributing computer personalities

This chapter includes the following topics:

- Capturing and distributing personality
- About capturing and distributing personalities
- About personality templates
- About migration settings
- Capturing a computer's personality
- Distributing a computer's personality

Capturing and distributing personality

Deployment Solution lets you capture and distribute computer personalities. Computer personalities contain the documents, the registry settings, and the configuration files that are associated with applications. Deployment Solution supports capturing and distributing of personalities for Windows XP, Windows Vista, and Windows 7.

See “About capturing and distributing personalities” on page 226.

Personalities are usually captured as part of an operating system migration or as a backup. The captured personalities are stored in Personality Packages that are placed in the <install_directory>\Program Files\Altiris\Deployment\PCT folder.

You must use a template while creating a capture personality task. If you haven’t created a template yet, you can use one of the default templates that are included with Deployment Solution. You can create templates using either of the following tools that are in the <install_directory>\Program Files\Altiris\Deployment\PCT folder:
The Template.exe launches the Altiris PCTransplant Template Builder tool that lets you create a Personality Build Template.

The PCTEdit.exe launches the Altiris PC Transplant Package Editor tool. You can launch the PCTransplant Template Builder from the Tools > Template Builder.

The following tables list the steps to capture a computer's personality and distribute the computer's personality:

- Capturing a computer's personality
  - See **Table 8-1** on page 225.

- Distributing a computer's personality
  - See **Table 8-2** on page 226.

The following table lists the steps to capture a computer's personality:

<table>
<thead>
<tr>
<th>Table 8-1 Capturing a computer's personality</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step</strong></td>
</tr>
<tr>
<td>----------</td>
</tr>
<tr>
<td>Step 1</td>
</tr>
<tr>
<td>Step 2</td>
</tr>
<tr>
<td>Step 3</td>
</tr>
</tbody>
</table>
The following table lists the steps to distribute a computer's personality:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Launch the console</td>
<td>Launch the Symantec Management Console. You can launch the console either from the Start menu of the computer or you can launch the Web console if you know the IP address of the Notification Server. For example: http://&lt;IP address&gt;/altiris/console.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Distribute the personality</td>
<td>Create and schedule a Distribute Personality task to distribute the personality of the client computer. See “Distributing a computer’s personality” on page 230.</td>
</tr>
</tbody>
</table>

**About capturing and distributing personalities**

Deployment Solution lets 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 the applications. Personalities are usually captured as part of an operating system migration or as a backup. Deployment Solution supports capturing and distributing personalities for Windows XP, Windows Vista, and Windows 7. Both 64-bit operating system and 32-bit operating system are supported.

The captured personality of a computer is stored in a self extracting executable file that is known as a Personality Package. The 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, files, and options that you want for your Personality Packages. A Personality Package can include the desktop, printer, network, application settings (such as favorites and contacts), and entire directory structures of the client computer. You can create Personality 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 install a specific Personality Package on a computer. After the user completes 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.

See “About migration settings” on page 228.

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.

See “About personality templates” on page 227.

See “Capturing a computer’s personality” on page 229.

See “Distributing a computer’s personality” on page 230.

About personality templates

In Deployment Solution, to create a Personality Package, you must specify the type of information that is to be captured in the package. A personality template file is used to specify all the information that is to be captured in a Personality Package. A personality template file contains information about the settings and files that you want to migrate from the client computer. A personality template reduces errors and allows the deployment job to automatically create packages.

See “About capturing and distributing personalities” on page 226.

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

- **Template.exe**
  
  The Template.exe launches the Altiris PCTransplant Template Builder tool that lets you create a Personality Build Template. The Template.exe is located at \Program Files\Altiris\Deployment\PCT folder.

- **PCTEdit.exe**
  
  The PCTEdit.exe lets you view and change an existing Personality Package. The PCTEdit.exe is located at \Program Files\Altiris\Deployment\PCT folder. In the Altiris PC Transplant Package Editor, select the **Tools > Template Builder** option to create a template or edit an existing template.

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 191.
About migration settings

You can set the settings that you want to capture in a personality. These settings are set in template file.

You can create a template by using either of the following:

- **PCTEdit.exe**
  Navigate to `<Install_directory>\ProgramFiles\Altiris\Deployment\PCT` folder to access the executable file.

- **TEMPLATE.exe**
  Navigate to `<Install_directory>\ProgramFiles\Altiris\Deployment\PCT` folder to access the executable file.

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.

You can choose to migrate settings from the following categories:

- **Computer desktop settings**
  These settings include Control Panel settings, Display properties including desktop colors, and background information.

- **Network settings**
  These settings include the computer, domain name, folder, 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.

- **Individual files and folders**

- **Specific file types**

See “About personality templates” on page 227.

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 `Desktop*.ini` and `Ntwrk*.ini` files.

See “About capturing and distributing personalities” on page 226.
Capturing a computer's personality

Deployment Solution lets you capture a computer's personality. A computer personality includes user data and application settings. Personality Packages are stored in the (install_directory)\Altiris\NSCap\bin\Deployment\Packages\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. You can capture a computer's personality by executing the Capture Personality task.

See “About capturing and distributing personalities” on page 226.

You must use a template to specify the details that are to be captured in a computer's personality. Deployment Solution includes templates for many common applications and provides the tools that help you create and modify templates for new and custom applications.

See “About deployment tasks and jobs” on page 191.

To capture user settings

1. In the Symantec Management Console, navigate to either of the following:
   - From the Actions menu, select Deployment > Capture Personality.
   - Select the Manage > Jobs and Tasks menu
     In the left pane do either of the following:
     - Right-click System Jobs and Tasks folder and select New > Task.
     - Expand the System Jobs and Tasks folder and right-click Deployment folder to select New > Task.

2. In the Create New Task dialog box, from the left pane select Deployment > Capture Personality task.
The fields and the descriptions are as follows:

<table>
<thead>
<tr>
<th>Task name</th>
<th>Displays the default task name as Capture Personality. You can edit the default task name to specify a relevant task name. For example, Personality_WinXP.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personality name</td>
<td>Lets you specify a unique personality name. You can specify a description for the personality that you capture. 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.</td>
</tr>
<tr>
<td>Select template</td>
<td>Lets you browse and select a template for the personality that you want to capture. Select the Create Vista compatible file (pkg) check box if you want to distribute personality to a computer with Windows Vista and above operating system. See “About personality templates” on page 227.</td>
</tr>
<tr>
<td>Personality Credentials</td>
<td>Lets you specify the credentials to secure the personality.</td>
</tr>
</tbody>
</table>

4. Click **OK**.

5. Schedule the task.

See “Scheduling a deployment job or task” on page 198.

See “Distributing a computer’s personality” on page 230.

### Distributing a computer's personality

Deployment Solution lets you restore or distribute computer personality to client computers. The **Distribute Personality** task distributes a personality through a self-extracting executable file that is called a Personality Package. Personality packages are stored in the `<install_directory>\Program Files\Altiris\Deployment\PCT` folder.

See “About capturing and distributing personalities” on page 226.

See “About deployment tasks and jobs” on page 191.
To restore user settings

1. In the Symantec Management Console, you can do either of the following:
   - From the Actions menu, select Deployment > Distribute Personality.
   - From the Manage menu, select Jobs and Tasks.
     In the left pane, do either of the following:
     - Right-click System Jobs and Tasks and select New > Task.
     - Expand the System Jobs and Tasks and right-click Deployment to select New > Task.

2. In the Create New Task dialog box, select Deployment > Distribute Personality.

3. The fields and their descriptions are as follows:

   - **Task name** icon
     Lets you specify the name of the distribute personality task that you create.

   - **Personality name**
     Lets you type the name of the personality or select the name of the personality from the drop-down list 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.

   - **Description**
     Lets you type a description for the personality that you want to use.

   - **Distribute options > Command-line options**
     Type the command-line to distribute the personality to.

   - **Personality Credentials > Password**
     Type the password if the personality is password protected.

4. Click OK.

5. Schedule the task.
   
   See “Scheduling a deployment job or task” on page 198.

See “Capturing a computer's personality” on page 229.
Removing unwanted packages/resources

This chapter includes the following topics:

■ About removing unwanted packages and resources
■ Deleting an image package
■ Deleting an image resource
■ Deleting a scripted install package
■ Deleting a copy file contents package

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 233.

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

See “Deleting a scripted install package” on page 234.

See “Deleting a copy file contents package” on page 234.
See “Deleting an image resource” on page 233.

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 137.

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 233.

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 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.

See “About removing unwanted packages and resources” on page 232.

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 233.

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.

See “About removing unwanted packages and resources” on page 232.

### 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 > 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 234.

See “About removing unwanted packages and resources” on page 232.

### 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 > 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 234.

See "About removing unwanted packages and resources" on page 232.
Command-line switches

This appendix includes the following topics:

- About command-line switches
- About command-line switches for DeployAnywhere.exe

About command-line switches

Table A-1  Ghost command line switches

<table>
<thead>
<tr>
<th>Command-line switch</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-align = chs</td>
<td>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:</td>
</tr>
<tr>
<td>-align = 1mb</td>
<td>1 CHS: Aligns to a track or cylinder boundary</td>
</tr>
<tr>
<td></td>
<td>2 1MB: Aligns with a boundary of 1 MB</td>
</tr>
<tr>
<td></td>
<td>By default, a partition is aligned on the destination computer as it was on the source computer.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The 1MB alignment option supports Windows Vista.</td>
</tr>
<tr>
<td>-bfc</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>This option may slow Symantec Ghost operation substantially.</td>
</tr>
<tr>
<td>Command-line switch</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>-cns</td>
<td>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. <strong>Note:</strong> Symantec Ghost supports long file names.</td>
</tr>
<tr>
<td>-fdsp</td>
<td>Preserves the signature bytes on the destination disk when performing a disk-to-disk or image-to-disk cloning operation</td>
</tr>
<tr>
<td>-fdsz</td>
<td>Clears the signature bytes on the destination disk. This is the default for disk-to-disk and image-to-disk operations.</td>
</tr>
<tr>
<td>-fis</td>
<td>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.</td>
</tr>
<tr>
<td>-fmb</td>
<td>Forces the disk to restore to a MBR-based disk.</td>
</tr>
<tr>
<td>-fro</td>
<td>Forces Symantec Ghost to continue cloning even if the source contains bad clusters</td>
</tr>
<tr>
<td>-ia</td>
<td>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.</td>
</tr>
<tr>
<td>-ial</td>
<td>Forces a sector-by-sector copy of Linux partitions. Other partitions are copied normally</td>
</tr>
</tbody>
</table>
### Table A-1  Ghost command line switches *(continued)*

<table>
<thead>
<tr>
<th>Command-line switch</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>-ib</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>-id</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>-ir</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>-limitswap</strong></td>
<td>Limits the Linux swap space to 2GB.</td>
</tr>
<tr>
<td><strong>-locktype= Type</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>-noindex</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>-noOSlayout</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>-ntc-</strong></td>
<td>Disables NTFS contiguous run allocation.</td>
</tr>
<tr>
<td>Command-line switch</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>-ntchkdsk</td>
<td>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.</td>
</tr>
<tr>
<td>-ntexact</td>
<td>Attempts to arrange the restored NTFS volume in the same way as the source volume.</td>
</tr>
<tr>
<td>-pmbr</td>
<td>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.</td>
</tr>
<tr>
<td>-preserveifexists</td>
<td>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.</td>
</tr>
<tr>
<td>-pwd and -pwd=x</td>
<td>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.</td>
</tr>
<tr>
<td>-split=x</td>
<td>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.</td>
</tr>
<tr>
<td>-sze</td>
<td>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.</td>
</tr>
<tr>
<td>-szee</td>
<td>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.</td>
</tr>
</tbody>
</table>
Table A-1  Ghost command line switches (continued)

<table>
<thead>
<tr>
<th>Command-line switch</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-szef</td>
<td>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.</td>
</tr>
<tr>
<td>-szel</td>
<td>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.</td>
</tr>
<tr>
<td>-z</td>
<td>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)</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>With-CNS</th>
<th>Without -CNS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filename .gho</td>
<td>Filename .gho.</td>
</tr>
<tr>
<td>Filename .001</td>
<td>Filen001.ghs</td>
</tr>
<tr>
<td>Filename .002</td>
<td>Filen002.ghs</td>
</tr>
</tbody>
</table>

About command-line switches for DeployAnywhere.exe

The command-line switches for DeployAnywhere lets you troubleshoot the drivers of the DeployAnywhere database.

The command-line switches for DeployAnywhere.exe are as follows:

Table A-3  Switches for DeployAnywhere.exe

<table>
<thead>
<tr>
<th>Switch</th>
<th>Usages</th>
</tr>
</thead>
<tbody>
<tr>
<td>/target</td>
<td>The usage of this switch is as follows: /target=&lt;path to target windows dir&gt;</td>
</tr>
</tbody>
</table>
**Table A-3**  
Switches for DeployAnywhere.exe (continued)

<table>
<thead>
<tr>
<th>Switch</th>
<th>Usages</th>
</tr>
</thead>
<tbody>
<tr>
<td>/ddb</td>
<td>The usage of this switch is as follows: /ddb=&lt;path to driver database&gt;</td>
</tr>
<tr>
<td>/bypassDrvVali</td>
<td>The usage of this switch is as follows: /byPassDrvVali=[All</td>
</tr>
<tr>
<td>/Loglevel</td>
<td>The usage of this switch is as follows: /Loglevel=[1-255]</td>
</tr>
<tr>
<td>/eval</td>
<td>This switch runs DeployAnywhere in evaluation mode. It can be used with or without /ddb.</td>
</tr>
<tr>
<td></td>
<td>If /ddb is not specified then /eval will report all critical drivers missing from the target. If /ddb is specified then /eval will report all critical drivers missing from the target that are not in the driver database.</td>
</tr>
<tr>
<td>/skipMissingCriticalDrivers</td>
<td>The usage of this switch is that DeployAnywhere executes even when drivers for critical devices are missing.</td>
</tr>
<tr>
<td>/handleNonCriticalDrivers</td>
<td>The usage of this switch is that it turns on non-critical device handling, the switch lets you find and retarget matching non critical drivers. You can provide 3 inputs that are as follows:</td>
</tr>
</tbody>
</table>
|                         | ■ miniSetup  
|                         | non-critical driver installation and upgrading occurs during mini-setup                                                               |
|                         | ■ adminLogon  
|                         | non-critical driver installation and upgrading occurs at first admin logon. This may require a further reboot after driver installation |
|                         | ■ user  
|                         | non-critical driver installation and upgrading occurs when the user runs c:\drivers\symantec\non-critical\run_dpinst.bat. This may require a further reboot after driver installation [requires admin privileges to succeed]. |
| /logPath                | The usage of this switch is as follows: /logPath=<directory for log output>                                                            |
| /logId                  | /logId=<id prepended to log files >                                                                                                  |
| /managed                | The usage of this switch is that it specifies that DeployAnywhere is run in managed mode.                                                |
### Table A-3  
Switches for DeployAnywhere.exe (continued)

<table>
<thead>
<tr>
<th>Switch</th>
<th>Usages</th>
</tr>
</thead>
<tbody>
<tr>
<td>/precheck</td>
<td>-</td>
</tr>
<tr>
<td>/targetOS</td>
<td>The usage of this switch is as follows:</td>
</tr>
<tr>
<td></td>
<td>/targetOS=[ 2000</td>
</tr>
<tr>
<td>/reportNonCriticalDevices</td>
<td>The usage of this switch is that it forces DeployAnywhere to report all non-critical devices.</td>
</tr>
<tr>
<td>/p2v</td>
<td>The usage of this switch is as follows:</td>
</tr>
<tr>
<td></td>
<td>/p2v=[vmdk</td>
</tr>
<tr>
<td>/pathToVirtualDisk</td>
<td>The usage of this switch is as follows:</td>
</tr>
<tr>
<td></td>
<td>/pathToVirtualDisk=&lt;path to the virtual disk&gt;</td>
</tr>
<tr>
<td>/loglevel</td>
<td>The usage of this switch is as follows:</td>
</tr>
<tr>
<td></td>
<td>/loglevel=[1-255]</td>
</tr>
<tr>
<td>/setupApiLogLevel</td>
<td>The usage of this switch is as follows:</td>
</tr>
<tr>
<td></td>
<td>/setupApiLogLevel=&lt;logLevel&gt;</td>
</tr>
<tr>
<td>/ExportDevicesIntoFile</td>
<td>The usage of this switch is as follows:</td>
</tr>
<tr>
<td></td>
<td>/ExportDevicesIntoFile=&lt;path&gt;</td>
</tr>
<tr>
<td></td>
<td>If Path is empty, then device_file.xml that contains information about the devices to perform DeployAnywhere operation, is generated in the current working directory.</td>
</tr>
</tbody>
</table>
Location of tools and packages

This appendix includes the following topics:

- About location of Deployment Solution tools
- About location of Deployment Solution packages

About location of Deployment Solution tools

Deployment Solution includes several tools that you can use for various tasks. The tools are installed on the computer on which Symantec Management Platform is installed.

The default locations of the tools are as follows:

- **PC Transplant Editor**
  `<Install Directory>\Program Files\Altiris\Deployment\PCT\PCTEdit.exe`

- **PC Transplant Wizard**
  `<Install Directory>\Program Files\Altiris\Deployment\PCT\Client\PCTWiz.exe`

- **Boot Disk Creator**
  `<Install Directory>\Program Files\Altiris\Deployment\BDC\Bootwiz\bootwiz.exe`

- **Ghost Image Explorer**
  Explorer `<Install Directory>\Program Files\Altiris\Deployment\Imaging\ghost\x86\Ghostexp.exe`
  `<Install Directory>\Program Files\Altiris\Deployment\Imaging\ghost\x64\Ghostexp64.exe`

- **Image Importer**
  `<Install Directory>\Program Files\Altiris\Deployment\Tools\ResourceImporterTool.exe`
About location of Deployment Solution packages

The images, PCT packages, installation packages, copy file packages and other packages that are created in Deployment Solution are stored on the computer on which the Symantec Management Platform is installed.

The default location of the packages that are created in Deployment Solution are as follows:

<table>
<thead>
<tr>
<th>Package</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deployment .CAB files</td>
<td>&lt;Install_Dir&gt;\Program Files\Altiris\NotificationServer\NSCap\bin\Deployment\Packages\Sysprep\Deploy_Cab</td>
</tr>
<tr>
<td>Image packages</td>
<td>&lt;Install_Dir&gt;:\Program Files\Altiris\NotificationServer\NSCap\bin\Deployment\Packages\Images</td>
</tr>
<tr>
<td>PCT packages</td>
<td>&lt;Install_Dir&gt;:\Program Files\Altiris\NotificationServer\NSCap\bin\Deployment\Packages\PCT</td>
</tr>
<tr>
<td>SOI packages</td>
<td>&lt;Install_Dir&gt;:\Program Files\Altiris\NotificationServer\NSCap\bin\Deployment\Packages\SOI</td>
</tr>
<tr>
<td>Custom answer files</td>
<td>&lt;Install_Dir&gt;:\Program Files\Altiris\NotificationServer\NSCap\bin\Win32\X86\Deployment\SOI\AnswerFile</td>
</tr>
<tr>
<td>Copy File packages</td>
<td>&lt;Install_Dir&gt;:\Program Files\Altiris\NotificationServer\NSCap\bin\Deployment\Packages\CopyFile</td>
</tr>
<tr>
<td>Any drivers that you added to</td>
<td>&lt;Install_Dir&gt;:\Program Files\Altiris\NotificationServer\NSCap\bin\Deployment\DriversDB</td>
</tr>
<tr>
<td>the drivers database</td>
<td>&lt;Install_Dir&gt;:\Program Files\Altiris\NotificationServer\NSCap\bin\Deployment\BDC\bootwiz\Platforms</td>
</tr>
<tr>
<td>Any drivers that you added for</td>
<td>Operating system-specific drivers are stored in an applicable operating system folder under the Platforms folder.</td>
</tr>
<tr>
<td>bootwiz</td>
<td></td>
</tr>
<tr>
<td>Any .PBT files that you added</td>
<td>&lt;install_Dir&gt;:\Program Files\Altiris\Deployment\PCT</td>
</tr>
<tr>
<td>to the Deployment folder</td>
<td></td>
</tr>
</tbody>
</table>
You must create a backup of the images in their existing HTTP location. You must recreate the same HTTP location on your new server and move the backup of your images to the new server computer.

You must create a backup of the UNC location and folder structure. You must recreate the same location and folder structure on your new server computer.
Troubleshooting

This appendix includes the following topics:

- **Troubleshooting Tip: General installation and configuration**
- **Troubleshooting Tip: Imaging and Install OS task**
- **Troubleshooting Tip: PXE and automation environment**
- **Troubleshooting Tip: Driver database management**
- **Troubleshooting Tip: Client Communication and Package Download Issues**
- **Troubleshooting Tip: Upgrade issues**

**Troubleshooting Tip: General installation and configuration**

The troubleshooting tips related to the installation of the Deployment Solution components and its configuration are as follows:

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
<th>Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td>You cannot install the Deployment Solution plug-in in a maintenance window by using the Run once ASAP in maintenance window only option.</td>
<td>You are required to create a schedule using the Add Schedule option.</td>
</tr>
</tbody>
</table>
### General installation and configuration (continued)

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
<th>Workaroud</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deployment folder in IIS gets deleted from the package server.</td>
<td>The Deployment folder that is present in the IIS gets removed if you install the Deployment Solution package server component and then enable the Network Boot Service (NBS) on the site server that is configured with both package server component and the NBS.</td>
<td>Launch the Create_DeploymentDir.bat file that is present on the following path of the package server: &lt;install_dir&gt;/Altiris/Altiris Agent/Package Delivery/{76D113DE-16D4-4A31-826F-A4DACCEAC8AB}/cache/ To verify if the Deployment folder is created under the Altiris\PS in IIS on the package server, refresh the default website.</td>
</tr>
</tbody>
</table>

### Troubleshooting Tip: Imaging and Install OS task

The troubleshooting tips related to the imaging and install OS tasks of Deployment Solution are as follows:

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
<th>Workaroud</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td>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.</td>
<td>• Use -split switch when you create image, where -split size is less than 2GB. • Configure HTTP on 64-Bit Windows.</td>
</tr>
<tr>
<td>An error occurs when you join a Vista computer to a domain</td>
<td>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</td>
<td>Join the computer to a domain using a different task after the Clone task.</td>
</tr>
<tr>
<td>Issue</td>
<td>Description</td>
<td>Workaround</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
<td>------------</td>
</tr>
<tr>
<td>Preserved files on Vista computers have incorrect names</td>
<td>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.</td>
<td>Find and delete the hidden file named desktop.ini inside the affected folders. Windows Explorer should then correctly display the folder name.</td>
</tr>
<tr>
<td>CRC files created by Symantec Ghost return a false result</td>
<td>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</td>
<td>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.</td>
</tr>
</tbody>
</table>
### Table C-2  Imaging and Install OS task (continued)

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
<th>Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td>In IE8 native mode, if a user types the credentials on Deploy image task, and clicks on <strong>Advanced</strong> tab, the credentials on Deploy image task does not appear</td>
<td>Use the IE7 compatibility view in an IE8 web browser. The credentials appear even after you click Advanced.</td>
</tr>
<tr>
<td>The Deploy Image task gets error during the XP GHO image import when the Windows XP operating system boots with DeployAnywhere</td>
<td>When you execute the <strong>Deploy Image</strong> task with the <strong>DeployAnywhere</strong> 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</td>
<td>You are required to connect to a different USB keyboard to continue with the installation.</td>
</tr>
<tr>
<td>Any of the following errors are displayed during execution of Install Linux/ESX OS task:</td>
<td>This issue occurs if the Linux OS's Linux kernel version is older than version 2.6.27 and you use IDE disks. For example, this issue can occur in RHEL 5 and on versions earlier than SUSE 10.2.</td>
<td>You can perform either of the following to successfully install the Linux OS:</td>
</tr>
<tr>
<td>- 'DISK NOT FOUND' with error code 101 when computer is in the automation</td>
<td></td>
<td>- Replace %DISK% token by actual device name in the configuration or answer file.</td>
</tr>
<tr>
<td>- 'Error 15 : File not found' when computer boots into production</td>
<td></td>
<td>The Linux configuration file is located in, <code>&lt;installdir&gt;\Program Files\Altiris\Notification Server\NSCap\bin\UNIX\Deployment\Linux\x86\SOI\AnswerFile</code> path.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Remove %DISK% token from the answer file.</td>
</tr>
<tr>
<td><strong>Deploy Image</strong> task fails on unknown client computers when configured in an Initial Deployment job</td>
<td>If <strong>Deploy Image</strong> task is configured in the <strong>Initial Deployment</strong> job, then it fails for some client computers.</td>
<td>You must add the following command in the <strong>Command-line options</strong> field of the <strong>Command-line</strong> tab of the <strong>Advanced</strong> option of the <strong>Deploy Image</strong> task:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>-mp -clients=3 -threshold=2 -connectimeout=10</code></td>
</tr>
<tr>
<td>Windows 8 client computer fail to join the domain that is specified in the <strong>Deploy Image</strong> task.</td>
<td>After you execute the <strong>Deploy Image</strong> task on a Windows 8 client computer, the computer is not able to join the domain that is specified in the <strong>Deploy Image</strong> task.</td>
<td>You must execute the <strong>Apply System Configuration</strong> task on the Windows 8 client computer after executing the <strong>Deploy Image</strong> task to join the domain.</td>
</tr>
<tr>
<td>Issue</td>
<td>Description</td>
<td>Workaround</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
<td>------------</td>
</tr>
<tr>
<td>The Deploy Image task fails to deploy an image of Windows 12 BIOS type client computer on a UEFI enabled client computer.</td>
<td>This issue occurs when you deploy an image of Windows 12 BIOS type client computer on a UEFI enabled client computer.</td>
<td>You must add the following command in the Command-line options field of the Command-line tab of the Advanced option of the Deploy Image task: <code>-cesp</code></td>
</tr>
<tr>
<td>The Create Image task fails when you create an image of a client computer</td>
<td>The Create Image task fails for a package server that is configured with IIS, as the Deployment folder is missing from the following path in the IIS: Sites\Default Web Site\Altiris\PS\ This issue occurs if you install the Deployment Solution package server component and then enable the Network Boot Service (NBS) on the site server that is configured with both package server component and the NBS.</td>
<td>You must execute the Create_DeploymentDir.bat command that is placed in the following location: <code>&lt;install_dir&gt;/Altiris/Altiris Agent/Package Delivery/76D113DE-16D4-4A31-826F-A4DACCEAC8AB}/cache/</code></td>
</tr>
<tr>
<td>An error is displayed when you execute the Install Windows OS task that is accessed from the console and is launched from a computer other than the Notification Server computer</td>
<td>When you execute the Install Windows OS task with a custom answer file that is accessed from the console and is launched from a computer other than the Notification Server computer Unattended upgrades using setup /unattend with no answer file are not supported when running Windows PE</td>
<td>You must install the Java SE Runtime Environment 7u25 on the Notification Server computer.</td>
</tr>
<tr>
<td>The Prepare For Image Capture task fails for Windows 8 client computer</td>
<td>The Prepare For Image Capture task fails for Windows 8 client computer that is not restarted after installing a Windows update.</td>
<td>You must restart the Windows 8 client computer after installing the Windows updates.</td>
</tr>
</tbody>
</table>
Table C-2  Imaging and Install OS task (continued)

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
<th>Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>A client computer does not join the domain after the <strong>Deploy Image</strong> task is performed.</td>
<td>A client computer does not join the domain after the <strong>Deploy Image</strong> task is performed if the image deployed on the client computer is not prepared using the Sysprep utility.</td>
<td>You must deploy an image that is prepared using the Sysprep utility.</td>
</tr>
</tbody>
</table>

**Troubleshooting Tip: PXE and automation environment**

The troubleshooting tips related to PXE environment and automation environment are as follows:
<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
<th>Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>WHOAMI does not get overwritten and PXE listens on the IP addresses that it picks up at startup.</td>
<td>PXE is not binding to the given IP address when the Symantec Boot Services server has two NIC cards installed on it.</td>
<td>This workaround is based on the following conditions:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Symantec boot services server is running on win2k8R2.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Symantec boot services server has two active NICs.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ DHCP server and Symantec boot services server are bound on the same NIC.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Assuming that the two NICs are A and B, perform the following to make the Symantec boot services server operational:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ 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:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Go to Network &gt; Properties &gt; Change Adapter Settings</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Both A and B NICs are present here.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ On this window (network connections), press Alt (keyboard option). Then the file menu options are visible.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You have changed the binding order of the NIC on your computer.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Now check the binding of the DHCP server and clicking the DHCP server by Start &gt; Run &gt; dhcpmgmt.msc.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Click on the + option in the 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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

### Troubleshooting Tip: Driver database management

The troubleshooting tips related to Deployment Solution drivers and driver database management are as follows:
Driver database management

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
<th>Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device in the Device Manager shows an exclamation mark after</td>
<td>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</td>
<td>If the unsigned drivers show an exclamation mark for the devices, use the following tag entry in the unattended answer file: DriverSigningPolicy</td>
</tr>
<tr>
<td>performing a scripted OS installation for DeployAnywhere</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multiple deletion of drivers from the console is not possible</td>
<td>You cannot delete multiple drivers of DeployAnywhere database through the Driver Database Management dialog box.</td>
<td>You can delete the drivers from DriverDB database.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> Even after the drivers are deleted from the DriverDB database, the Driver Database Management dialog box displays the drivers.</td>
</tr>
<tr>
<td>Drivers not replicated on Package Server if a large number of drivers</td>
<td>When you add a large number of drivers through the Driver Database Management dialog box, the Package Server is not replicated with all the drivers that you add.</td>
<td>This issue occurs because the driver database operation times out. You can perform the following steps to replicate the drivers on the Package Servers:</td>
</tr>
<tr>
<td>are added at a time</td>
<td></td>
<td>- In the console, navigate to Settings &gt; All Settings</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Browse to Settings &gt; Deployment &gt; Packages &gt; DriversDB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- In the Package tab, click Update Distribution Points</td>
</tr>
</tbody>
</table>

Troubleshooting Tip: Client Communication and Package Download Issues

The troubleshooting tips related to client communication and package download of Deployment Solution plug-ins are as follows:
### Table C-5

<table>
<thead>
<tr>
<th>Issue</th>
</tr>
</thead>
<tbody>
<tr>
<td>Error Failed to find available codebase for download error is displayed on installing deployment and automation plug-ins.</td>
</tr>
<tr>
<td>On installing deployment plug-ins using aex-swadapm commands, if the IIS (Internet Informational Services) is not installed on the Package server, the installation fails.</td>
</tr>
<tr>
<td>All ULM client communication is done using HTTP or HTTPS. Therefore, a Web server is required. You should install IIS on Package server to facilitate codebase download. For more information on related issues, refer to the following article: <a href="http://www.symantec.com/docs/TECH46185">http://www.symantec.com/docs/TECH46185</a></td>
</tr>
<tr>
<td>Downloading DS Automation folder and Plug-in fails for Mac clients using SMB (Server Message Block) share.</td>
</tr>
<tr>
<td>Whenever a Mac client accesses any folder using SMB share a .DS_Store hidden file is created which does not allow the Mac client to download DS automation folders and Plug-ins.</td>
</tr>
<tr>
<td>You should unhide the .DS_Store file and run the policy again to download automation folder and Plug-ins.</td>
</tr>
<tr>
<td>Error Package download failed because package was removed is displayed for clients.</td>
</tr>
<tr>
<td>An error is displayed on the client machines on downloading a package</td>
</tr>
<tr>
<td>You should disable the Windows authentication in IIS for the package.</td>
</tr>
<tr>
<td>Issue arises when client codebase files contain an invalid Notification server name.</td>
</tr>
<tr>
<td>The setting called Preferred NSHost lets you specify a preferred Notification Server hostname for SWD (Serial Wire Debug) codebase and snapshot URLs that point to the Notification Server. With Notification Server 7 there is a registry key that controls this information. The CoreSettings.config file has the record for the registry key but it is just a reference of this registry key. If you modify the registry value in the coreSettings.config you will break its functionality.</td>
</tr>
<tr>
<td>Check the registry on the Notification Server for the PreferredNNSHost value. The entry in the coreSettings.config for Notification Server 7 should be &lt;customSetting key=&quot;PreferredNNSHost&quot; type=&quot;registry&quot; regkey=&quot;Notification Server&quot; regvalue=&quot;PreferredNNSHost&quot; /&gt;, For more information on this issue read the following article: <a href="http://www.symantec.com/docs/HOWTO10091">http://www.symantec.com/docs/HOWTO10091</a></td>
</tr>
</tbody>
</table>

## Troubleshooting Tip: Upgrade issues

The troubleshooting tips related to upgrade of Deployment Solution are as follows:
**Table C-6**  Upgrade issues of Deployment Solution

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
<th>Work around</th>
</tr>
</thead>
<tbody>
<tr>
<td>Error Exception has occurred in File SMPPackage.cpp at Line No 599. Type of exception is GeneralError. Error is Default Message: Exception in CSMPPackageException. Error Description is &quot;util::CSMPPackage::GetFileFromHTTP&quot;. Value of Windows error code = 183 and message is &quot;Cannot create a file when that file already exists.</td>
<td>After installation of fresh ITMS or upgrading to ITMS 7.5 or later, the default Driver Manifest file is not generated, and the Deploy Anywhere fails.</td>
<td>You must access the Driver Manager Console after you install and upgrade ITMS 7.5 or later.</td>
</tr>
</tbody>
</table>
Answer files

This appendix includes the following topics:

- About Windows and Linux answer files
- About Mac configuration file

About Windows and Linux answer files

In Deployment Solution, a configuration file is also known as the answer file and stores parameters for operating system (OS) installation. You can customize a configuration file to perform an unattended OS installation.

The configuration files for Windows, and Linux operating system are in the following locations of the computer on which SMP is installed:

- Linux
  `<instaldir>\Program Files\Altiris\Notification Server\NSCap\bin\UNIX\Deployment\Linux\x86\SOI\AnswerFile`
- Windows
  `<instaldir>\Program Files\Altiris\Notification Server\NScap\bin\Win32\X86\Deployment\SOI\AnswerFile`

Following are the parameters that you can customize in a Windows configuration file:

<table>
<thead>
<tr>
<th>Table D-1</th>
<th>Parameters for Windows configuration file</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>Password</td>
<td>You can specify the password that you want to specify for all the client computers.</td>
</tr>
<tr>
<td>License</td>
<td>You can specify the applicable license.</td>
</tr>
<tr>
<td>Display</td>
<td>You can specify the screen resolution.</td>
</tr>
</tbody>
</table>
Table D-1  Parameters for Windows configuration file (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Language</td>
<td>You can set the preferred language of operation.</td>
</tr>
<tr>
<td>ProcessArchitecture</td>
<td>You can set the architecture of the processor, x86, and x32.</td>
</tr>
<tr>
<td>DiskID</td>
<td>You can specify the disk ID for installation of operating system.</td>
</tr>
<tr>
<td>OSFlavorName</td>
<td>You can specify the disk ID for installation of operating system.</td>
</tr>
<tr>
<td>timezone</td>
<td>You can specify the timezone for the target client computers.</td>
</tr>
</tbody>
</table>

Following are the parameters that you can customize for a Linux configuration file:

Table D-2  Parameters for Linux configuration file

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>You can specify the password for the client computers</td>
</tr>
<tr>
<td>IPAddress</td>
<td>You can specify the IP address if you carry out installation of operating system for a single client computer. If you carry out mass operating system installation then do not specify the IP address.</td>
</tr>
<tr>
<td>Hostname</td>
<td>You can specify the host name if you carry out installation of operating system for a single client computer. If you carry out mass operating system installation then do not specify the hostname.</td>
</tr>
<tr>
<td>Static configuration</td>
<td>You can specify the static configuration if you carry out installation of operating system for a single client computer. If you carry out mass operating system installation then do not specify the static configuration.</td>
</tr>
</tbody>
</table>

See “Installing a Windows OS using Deployment Solution” on page 150.
See “Installing Linux/ESX OS using Deployment Solution” on page 167.
See “Installing Mac OS using Deployment Solution” on page 168.
See “About Mac configuration file” on page 258.
About Mac configuration file

In Deployment Solution, a configuration file is also known as the answer file and stores parameters for an operating system (OS) installation. You can customize a configuration file to perform an unattended OS installation.

The configuration file for Mac operating system is in the following location of the computer on which SMP is installed:

<installdir>\Program Files\Altiris\Notification Server\NSCap\bin\UNIX\Deployment\Mac\NetInstall\AnswerFile\n
Refer to Apple’s support documentation to know more about the parameters.

http://www.apple.com/support/

---

**Note:** For mass installation of Mac operating system, do not specify the **TargetUUID** parameter. The **TargetUUID** parameter is unique for every client computer and interrupts mass operating system installation.

---

Following are the parameters that you can customize in a Mac configuration file:

### Table D-3 Parameters for Mac configuration file

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InstallType</td>
<td>You can set the type of installation as automated. You can set the type of installation as automated if the workflow in the Apple’s System Image Utility includes Enable Automated Installation while creating the NetInstall image</td>
</tr>
<tr>
<td>Language</td>
<td>You can set the preferred language of operation.</td>
</tr>
<tr>
<td>Package</td>
<td>Set the Package name with the folder location. By default it is set as &gt;/System/Installation/Packages/OSInstall.mpkg</td>
</tr>
<tr>
<td>ShouldErase</td>
<td>Symantec recommends setting the <strong>ShouldErase</strong> parameter as <strong>False</strong>. If you set it as <strong>True</strong>, then you must select the drive, on which the Mac operating system must be installed and install the Symantec Management Agent and Deployment Plug-in manually on the client computer.</td>
</tr>
</tbody>
</table>
Table D-3  Parameters for Mac configuration file (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target</td>
<td>Set the target volume where the operating system has to be installed. By default it is set to Volumes/Macintosh HD.</td>
</tr>
</tbody>
</table>

See “About Windows and Linux answer files” on page 256.
See “Installing Mac OS using Deployment Solution” on page 168.
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>automation environment</td>
<td>A preboot environment in which the client computers boot using the automation folder.</td>
</tr>
<tr>
<td>automation folder</td>
<td>A storage for the preboot operating system on the client computers.</td>
</tr>
<tr>
<td>BDC (Boot Disk Creator)</td>
<td>A component of Deployment Solution that creates a boot disk using the Windows or Linux preboot operating systems.</td>
</tr>
<tr>
<td>DeployAnywhere</td>
<td>A component of Deployment Solution that is used to deploy the Windows operating system image to dissimilar hardware and perform a Windows-scripted installation on a bare metal computer.</td>
</tr>
<tr>
<td>Deployment Package Server component</td>
<td>A component of Deployment Solution that is deployed on a site server on which the Package Service functions, and which is assigned to Deployment Solution to store product-specific packages of files.</td>
</tr>
<tr>
<td>Deployment Plug-in</td>
<td>A component of Deployment Solution that is installed on the client computers on which the deployment tasks need to be executed. The Deployment Plug-in allows the user to create and deploy disk images, perform remote operating system installation, change system settings, and migrate the personality settings.</td>
</tr>
<tr>
<td>deployment task</td>
<td>An individual activity, such as creating a computer image, installing an operating system, etc.</td>
</tr>
<tr>
<td>Deployment Task Server component</td>
<td>A component of Deployment Solution that is deployed on a site server on which the Task Service functions and which performs tasks specific to Deployment Solution.</td>
</tr>
<tr>
<td>Driver Manager</td>
<td>A component of Deployment Solution that provides the interface to perform driver operations such as adding and deleting data from the DeployAnywhere driver database and the Preboot driver database.</td>
</tr>
<tr>
<td>image resource</td>
<td>A component of Deployment Solution that is created when an image is created. This component is used to build tasks to deploy the images.</td>
</tr>
<tr>
<td>imaging tools</td>
<td>Components of the Deployment Solution. The imaging tools are Ghost and symDeploMac disk imaging tools.</td>
</tr>
<tr>
<td>Initial Deployment Settings</td>
<td>A job that is used to set up the initial set of tasks or jobs for unknown computers or client computers after they boot to the preboot environment or the automation environment.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>job</td>
<td>A sequence of tasks that are executed on a target. Jobs can include the conditions that specify when the task runs.</td>
</tr>
<tr>
<td>NBS (Network Boot Service server)</td>
<td>A component of Deployment Solution that is installed on a site server and comprises PXE service, Boot Service Discovery Protocol service, and TFTP service. NBS provides configuration of the TFTP service, logging levels for PXE image deployment, and configuration of the network settings.</td>
</tr>
<tr>
<td>predefined computer</td>
<td>A computer the details of which, such as the computer name and MAC address are added to the Deployment Solution even before the computer is connected to the network.</td>
</tr>
<tr>
<td>Resource Import tool</td>
<td>A component of Deployment Solution that is used to import the existing Windows and Linux images and to add Windows-scripted OS installation files.</td>
</tr>
</tbody>
</table>
A
About
  remove packages and resources 232
about
  automation folder 20
delete packages and resources 232
image resources 137
initial deployment 207
add
  drivers for preboot configuration 161
add drivers
  DeployAnywhere 162
adding
  licenses 158
  system configuration 213
align switch 236
align partitions 236
automation folder
  about 20

B
bad sectors 236
bfc switch 236
Boot Disk Creator
  adding drivers 161

C
capture
  preparing a disk image 138
cns switch 237
configuration driver
  adding 161
configure
  preboot environment 87
context-sensitive help 26
Copy File
  task 204
copy file contents package
  delete 234
  remove 234

D
copy files and folder
  procedure 204
Create Image
  task options 113, 125
creating
  deployment task 197

display
  copy file contents package 234
disk image 233
image package 233
resource 233
delete packages and resources
  about 232
deploy
  disk image 116, 127
Deploy Image
  task options 116, 127
DeployAnywhere
  add drivers 162
DeployAnywhere driver database
  add 162
deployment
  settings 30
Deployment plug-in
  upgrading 45
Deployment settings
  configuring 208
Deployment Solution
  about 17
    about Automation Folder 18
    about Deployment Plug-in component 18
    about site server components 18
    about task server handler 18
    installer components 18
    installing plug-in 36
    policy for upgrading plug-in 45
    preinstallation requirements 29
    settings 30
    upgrading plug-in 45
deployment task
creating 197
disk image
deleting 233
deploying 116, 127
Preparing for Image Capture 138
preparing to capture 138
documentation 26
driver
adding with Boot Disk Creator 161
settings 161
driver database
DeployAnywhere 162

e
erase
disk 154
Erase Disk
task 154
ESX OS
scripted installation 167

F
FAT
clusters 236

H
help
context-sensitive 26

I
image
deploying a disk image 116, 127
for multiple computers 116, 127
preparing to capture 138
image file
spanned 237
image package
deleting 233
image resource
about 137
deleting 233
initial deployment
about 207
settings 208
Initial Deployment menu
adding tasks to 208
install
Windows scripted OS 150, 167
installation
Deployment plug-in 36
Windows scripted OS 150, 167
installation prerequisites
Deployment Solution 29

L
license
adding 158
settings 158
Linux OS
scripted installation 167

O
Operating system license
adding 158
options
Create Image task 113, 125
Deploy Image task 116, 127
OS license
adding 158

P
partition
aligning 236
Partition Disk
task 156
personality resource
deleting 233
policy
Deployment Solution
upgrading plug-in 45
for upgrading Deployment plug-in 45
preboot configuration driver
adding 161
preboot environment
configure 87
predefined computers
about 48
reference sample file 63
preinstallation requirements
Deployment Solution 29
prepare
capturing a disk image 138
procedure
copy files and folder 204
R
Release Notes 26
remove
copy file contents package 234
remove packages and resources
about 232
resource
about image 137
deleting 233

S
sample csv file
reference 63
sector
bad 236
settings
DeployAnywhere driver 161
drivers 161
initial deployment 208
licenses 158
OS licenses 158
site server 30
task list 208
spanning
naming 237
state
checking a task 199
System configuration
adding 213
settings 213

T
task
checking the state of a 199
Copy File 204
Create Image options 113, 125
creating a deployment 197
Deploy Image options 116, 127
Erase Disk 154
Partition Disk 156
task options
Create Image 113, 125
Deploy Image 116, 127

V
Vista
support 236