



Dell® Client Manager User Guide

Version 3.1 SP1

Dell® Client Manager User Guide

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

Documentation version: 3.1 SP1

Legal Notice

Copyright © 2010 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, Altiris, and any Altiris or Symantec trademarks 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.

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, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

<http://www.symantec.com>

Technical Support

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

Symantec's maintenance offerings include the following:

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

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

www.symantec.com/techsupp/

Contacting Technical Support

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

www.symantec.com/techsupp/

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

Customer service

Customer service information is available at the following URL:

www.symantec.com/techsupp/

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

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

Maintenance agreement resources

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

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

Additional enterprise services

Symantec offers a comprehensive set of services that allow you to maximize your investment in Symantec products and to develop your knowledge, expertise, and global insight, which enable you to manage your business risks proactively.

Enterprise services that are available include the following:

Symantec Early Warning Solutions	These solutions provide early warning of cyber attacks, comprehensive threat analysis, and countermeasures to prevent attacks before they occur.
Managed Security Services	These services remove the burden of managing and monitoring security devices and events, ensuring rapid response to real threats.
Consulting Services	Symantec Consulting Services provide on-site technical expertise from Symantec and its trusted partners. Symantec Consulting Services offer a variety of prepackaged and customizable options that include assessment, design, implementation, monitoring, and management capabilities. Each is focused on establishing and maintaining the integrity and availability of your IT resources.
Educational Services	Educational Services provide a full array of technical training, security education, security certification, and awareness communication programs.

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

www.symantec.com

Select your country or language from the site index.

Contents

Technical Support	3
Chapter 1	Introducing Dell Client Manager 11
	About Dell Client Manager 11
	What's new in Dell Client Manager 12
	Products installed with Dell Client Manager 12
	How Dell Client Manager works 12
	What you can do with Dell Client Manager 13
	Where to get more information 13
Chapter 2	Installing Dell Client Manager 15
	System requirements 15
	About Dell Client Manager requirements 15
	About Dell client computer requirements 16
	Installing the Dell Client Manager product 16
	Upgrading Dell Client Manager 17
	Uninstalling Dell Client Manager 17
	Uninstalling the Dell Client Manager Agent from client computers 18
	Uninstalling Dell Client Manager from the Notification Server computer 18
	Installing licenses 19
Chapter 3	Getting started with Dell Client Manager 21
	About the Dell Management Console 21
	About the Dell Client Manager home page 22
	About the Dell Client Discovery and Installation Summary web part 22
	About managing multiple and single computers 24
	About actions that require a client restart 24
	About Windows BitLocker Drive Encryption 25
	About BIOS password restrictions 25

Chapter 4	Preparing target Dell computers for management	27
	Preparing target Dell computers for management	27
	Discovering computers	29
	Installing the Altiris Agent	29
	(Optional) Configuring the Altiris Agent settings for evaluation use	30
	Discovering Dell computers	31
	Installing the Dell Client Manager Agent	32
	Installing the Power Scheme Agent	33
	(Optional) Restarting Dell client computers awaiting reboot	34
	(Optional) Configuring the Dell Client Manager Agent	35
	(Optional) Customizing the Dell client patching settings	36
Chapter 5	Using Dell Client Manager	37
	Prerequisites for using Dell Client Manager	37
	Collecting BIOS, hardware, display, and power scheme settings inventory	38
	Collecting BIOS inventory data	38
	Collecting hardware and BIOS version inventory data	38
	Collecting display inventory data	39
	Collecting power scheme inventory data	39
	Viewing BIOS, hardware, display, and power scheme settings inventory	40
	Updating BIOS versions	41
	Discovering current Dell BIOS versions	42
	Saving computers with older BIOS versions as a filter	42
	Running the BIOS Update Job	43
	Viewing the BIOS Update Job execution reports	45
	Configuring BIOS settings	46
	About using macros for BIOS settings	47
	Configuring Dell display settings	48
	Changing brightness and contrast settings	48
	Restoring display factory default settings	49
	Turning off displays	49
	Configuring power scheme settings	49
	Monitoring computers health	50
	Viewing alerts	51
	Assessing Microsoft Windows 7 migration readiness	52
	Updating the Dell Supported Models database	53

Chapter 6	Applying software patches to Dell computers	55
	Applying software patches to Dell computers	55
	Downloading the Dell Update Packages catalog	57
	Determining patchable Dell client computers	58
	Viewing patchable Dell client computers	59
	Viewing applicable updates	59
	Staging and distributing updates	59
	Monitoring update progress	60
	Using reports to view patch management data	61
Chapter 7	Managing individual Dell computers	63
	About managing individual Dell computers	63
	Accessing the Real-Time view	64
	About the Real-Time Consoles page	65
	Viewing the Dell client computer summary	66
	Performing one-to-one BIOS configuration	66
	Performing one-to-one boot order configuration	67
	Performing one-to-one BIOS password change	67
	Performing one-to-one BIOS update	68
	Resetting chassis intrusion alert	69
Chapter 8	About Dell Client Manager pages	71
	About the Disable BitLocker and Enable BitLocker tasks	71
	About the BIOS Settings and BIOS Update jobs	72
	About power management tasks	72
	About the Update Dell Clients Patch Compliance Inventory task	72
	About the Download Software Update Package task	73
	About the Stage and Distribute job	73
	About the patch management rollout jobs	73
	About the Dell Update Applicability Task	74
	About the Dell Update Install Task	74
	About the Patch Management Configuration page	74
	About the Stage and Distribute Wizard	76
Appendix A	Troubleshooting Dell Client Manager	79
	Troubleshooting the Altiris Agent push installation	79
	Configuring the firewall to allow push installation	79
	Troubleshooting connection through the Real-Time view	80
	Configuring the firewall to allow WMI connection	82
	Disabling simple file sharing on Windows XP SP2	85

	Configuring User Access Control on Windows Vista and Windows 7	85
Appendix B	Technical reference	87
	Dell client computers that support BIOS updates	87
	Dell Update Package error codes	88
	Index	91

Introducing Dell Client Manager

This chapter includes the following topics:

- [About Dell Client Manager](#)
- [What's new in Dell Client Manager](#)
- [Products installed with Dell Client Manager](#)
- [How Dell Client Manager works](#)
- [What you can do with Dell Client Manager](#)
- [Where to get more information](#)

About Dell Client Manager

Dell Client Manager helps make Dell OptiPlex™ desktops, Latitude™ notebooks, and Dell Precision™ workstations some of the easiest and most cost effective client systems you can own. Dell Client Manager lets IT professionals automate common tasks that are associated with owning client systems and perform the tasks from a remote, centralized location. The results are powerful: far fewer desk-side visits and repetitive tasks, greater visibility and control of client inventory and usage, and improved consistency and compliance in the way client systems are configured. Organizations with as few as 50 Dell client systems will benefit, and larger organizations or organizations with distributed workforce will experience even greater advantages from centralized, automated client management.

Dell Client Manager is a suite of integrated tools that are developed by Dell and Symantec. These combined technologies work under the Symantec Management

Platform infrastructure. You manage Dell resources across your network using a single, integrated, and secure Dell Management Console.

What's new in Dell Client Manager

The following new features are introduced in the 3.1 SP1 release of Dell Client Manager:

- Dell Client Manager installs OMCI 7.7 to the client Dell computers.
- Dell Client Manager Agent can be installed on the client Dell computers running Microsoft Windows 7.
- Microsoft Windows 7 migration readiness reports let you determine what computers can be migrated to Windows 7.

Products installed with Dell Client Manager

Dell Client Manager installs and uses other Altiris management products.

Table 1-1 Products installed with Dell Client Manager

Product	Description
Symantec Management Platform	The base management platform.
Altiris™ Out of Band Management Component	Lets you configure computers with DASH, ASF, or Intel AMT for out-of-band management.
Altiris™ Real-Time Console Infrastructure	Provides out-of-band management tasks and the infrastructure for one-to-one management.
Altiris™ Power Scheme Task	This add-on lets you configure the Dell client computer's power-saving options remotely.

How Dell Client Manager works

Dell Client Manager discovers supported Dell computers in your environment and installs the Dell OpenManage Client Instrumentation (OMCI), EnTech SoftOSD, and Dell Client Manager Agent software to these computers. The Dell Client Manager Agent software works as a link between the OMCI and EnTech software and the Altiris Agent.

Dell Client Manager can also connect to a target Dell computer directly through WMI and query OMCI for inventory and configuration information and display

this information in the Symantec Management Console's Resource Manager, in the **Real-Time** view.

Dell Client Manager scans patchable Dell client computers for the required software updates. Then, it creates rollout jobs that install the updates to the appropriate computers.

What you can do with Dell Client Manager

Dell Client Manager lets you collect hardware, BIOS, and Dell display inventory from the client Dell computers. You can update the computer's BIOS and change BIOS settings remotely from the Symantec Management Console. You can run these tasks immediately or schedule for a later time, on one or many computers at a time.

From Dell Client Manager's **Real-Time** view you can also view the target Dell computer's inventory and configuration information in real time. During this live connection you can update BIOS, change BIOS and other settings for the particular Dell computer, and verify your changes.

With Dell Client Manager, you can discover patchable Dell computers and distribute Dell Update Packages to the computers that need an update, all from the centralized Dell Management Console.

Where to get more information

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

Table 1-2 Documentation resources

Document	Description	Location
Release Notes	Information about new features and important issues. This information is available as an article in the knowledge base.	http://kb.altiris.com/ You can search for the product name under Release Notes.

Table 1-2 Documentation resources (*continued*)

Document	Description	Location
User Guide	Information about how to use this product, including detailed technical information and instructions for performing common tasks. This information is available in PDF format.	<ul style="list-style-type: none"> ■ The Documentation Library, which is available in the Symantec Management Console on the Help menu. ■ The Product Support page, which is available at the following URL: http://www.symantec.com/business/support/all_products.jsp When you open your product's support page, look for the Documentation link on the right side of the page.
Help	Information about how to use this product, including detailed technical information and instructions for performing common tasks. Help is available at the solution level and at the suite level. This information is available in HTML help format.	<p>The Documentation Library, which is available in the Symantec Management Console on the Help menu.</p> <p>Context-sensitive help is available for most screens in the Symantec Management Console.</p> <p>You can open context-sensitive help in the following ways:</p> <ul style="list-style-type: none"> ■ The F1 key ■ The Context command, which is available in the Symantec Management Console on the Help menu.

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

Table 1-3 Altiris information resources

Resource	Description	Location
Knowledge base	Articles, incidents, and issues about Altiris products.	http://kb.altiris.com/
Symantec Connect (formerly Altiris Juice)	An online magazine that contains best practices, tips, tricks, forums, and articles for users of this product.	http://www.symantec.com/connect/endpoint-management-virtualization

Installing Dell Client Manager

This chapter includes the following topics:

- [System requirements](#)
- [Installing the Dell Client Manager product](#)
- [Upgrading Dell Client Manager](#)
- [Uninstalling Dell Client Manager](#)
- [Installing licenses](#)

System requirements

Dell Client Manager has the following system requirements:

- Dell Client Manager installation requirements.
See [“About Dell Client Manager requirements”](#) on page 15.
- Dell Client Manager Agent installation requirements.
See [“About Dell client computer requirements”](#) on page 16.

About Dell Client Manager requirements

Dell Client Manager requires the following:

- Symantec Management Platform 7.0 SP3

For more information on Symantec Management Platform prerequisites and installation instructions, see the *Symantec Management Platform Help*.

See [“Where to get more information”](#) on page 13.

When you install Dell Client Manager through Symantec Installation Manager, Symantec Management Platform is installed or upgraded automatically.

Dell Client Manager installs Out of Band Management Component on Notification Server. Dell Client Manager requirements are sufficient for default Out of Band Management Component installation, however more environment prerequisites must be met for advanced features. You can configure your environment before or after installing Out of Band Management Component.

For more information on Out of Band Management Component prerequisites and configuration instructions, see the *Out of Band Management Component Implementation Guide*.

See [“Where to get more information”](#) on page 13.

About Dell client computer requirements

Full feature support is available for most Dell OptiPlex, Latitude, and Dell Precision client computers.

The Dell client patch feature is supported by recent Dell OptiPlex, Latitude, and Precision client computers.

See [“Dell client computers that support BIOS updates”](#) on page 87.

For more information about supported and unsupported models, see the Dell Client Manager Release Notes.

For more information about supported Dell displays, see the Dell Client Manager Release Notes.

Table 2-1 Dell client computer requirements

Requirement	Description
Operating system	Microsoft Windows XP SP2 or later with .NET framework 2.0 installed
Available disk space	20 MB disk space for the Altiris Agent, plus space to install required software
Memory	64 MB RAM

Installing the Dell Client Manager product

Use Symantec Installation Manager to install Dell Client Manager.

For more information on installing products, see Symantec Installation Manager documentation.

See [“Where to get more information”](#) on page 13.

Upgrading Dell Client Manager

Use Symantec Installation Manager to upgrade Dell Client Manager.

For more information on upgrading products, see the Symantec Installation Manager documentation.

See [“Where to get more information”](#) on page 13.

After you upgrade the product, you must upgrade all of the management agents that are installed on the target Dell computers. The agents include:

- Altiris Agent
- Dell Client Manager Agent
- Power Scheme Agent

To upgrade the management agents

- 1 In the Dell Management Console, on the **Actions** menu, click **Agents/Plug-ins > Rollout Agents/Plug-ins**.
- 2 In the left pane, locate and turn on the upgrade policies for each of the agents that you want to upgrade.

Uninstalling Dell Client Manager

To uninstall Dell Client Manager perform the following steps:

Table 2-2 Process for uninstalling Dell Client Manager

Step	Action	Description
Step 1	Uninstall the Dell Client Manager Agent from the client computers.	This step is required if you do not want to reinstall Dell Client Manager later. See “Uninstalling the Dell Client Manager Agent from client computers” on page 18.
Step 2	Uninstall Dell Client Manager from the Notification Server computer.	This step removes the product from the Notification Server computer. See “Uninstalling Dell Client Manager from the Notification Server computer” on page 18.

Uninstalling the Dell Client Manager Agent from client computers

The **Dell Client Manager Agent - Uninstall** task lets you remove all Dell Client Manager components from supported client computers. Because the Dell Client Manager Agent communicates with the Altiris Agent and Notification Server, you cannot run any Dell Client Manager tasks after uninstallation.

Before you uninstall the Dell Client Manager Agent, make sure the **Dell Client Manager Agent - Install** policy is turned off.

We recommend that you do not uninstall Dell Client Manager software from the Notification Server until the task has run on all Dell computers. When Dell Client Manager is uninstalled, there is no automated way to uninstall the agents.

The agent uninstallation process can take some time to start, depending on the intervals that are set between the updates of the Altiris Agent.

See [“\(Optional\) Configuring the Altiris Agent settings for evaluation use ”](#) on page 30.

To uninstall the Dell Client Manager Agent, Dell OMCI and EnTech software

- 1 In the Symantec Management Console, on the **Home** menu, click **Dell Client Manager**.
- 2 In the left pane, click **Dell Client Manager Agent Install > Dell Client Manager Agent - Uninstall (32-bit)**.
- 3 Turn on the policy (To turn on the policy, at the upper right of the page, click the colored circle, and then click **On**).
- 4 Click **Save changes**.
- 5 In the left pane, click **Dell Client Manager Agent Install > Dell Client Manager Agent - Uninstall (64-bit)**.
- 6 Turn on the policy (To turn on the policy, at the upper right of the page, click the colored circle, and then click **On**).
- 7 Click **Save changes**.

Uninstalling Dell Client Manager from the Notification Server computer

Use Symantec Installation Manager to uninstall Dell Client Manager.

For more information on uninstalling products, see the Symantec Installation Manager documentation.

See [“Where to get more information”](#) on page 13.

Installing licenses

Dell Client Manager includes a restricted trial license that is valid for 30 days. You can register and receive a free unlimited and permanent license by visiting the following Web site:

<http://www.altiris.com/Partners/AlliancePartners/Dell/DCMLicensing.aspx>

After you register, a new product key will be sent to you through email.

Use Symantec Installation Manager to license Dell Client Manager.

For more information, see the Symantec Installation Manager documentation.

See “[Where to get more information](#)” on page 13.

Getting started with Dell Client Manager

This chapter includes the following topics:

- [About the Dell Management Console](#)
- [About the Dell Client Manager home page](#)
- [About managing multiple and single computers](#)
- [About actions that require a client restart](#)
- [About Windows BitLocker Drive Encryption](#)
- [About BIOS password restrictions](#)

About the Dell Management Console

You perform all Dell Client Manager configuration and administration tasks in the Dell Management Console.

The Dell Management Console is the Web browser based administration console for working with Symantec Management Platform and solutions, including Dell Client Manager. The console lets you perform tasks, schedule events, run reports, perform configuration, configure security, and more. You can run the console from the Notification Server computer (locally) or from a remote computer with a network connection to Notification Server. This means you can perform administration tasks from wherever you are.

The console lets you set security specific to each console user. You specify which areas of the console a user has access to and the rights a user has to perform specific actions. For example, one user can run reports while another user can only view reports that have already been run.

For more information on the console, see the *Symantec Management Platform Help*, which can be accessed through the console's Help menu.

You can start the console remotely by typing the following URL into the Internet Explorer's address bar: `http://<Notification_Server_name>/altiris/console`

About the Dell Client Manager home page

The Dell Client Manager home page shows the number of discovered Dell computers by model and the summary information of tasks that you performed.

You can open the Dell Client Manager home page by clicking **Home > Dell Client Manager** in the Dell Management Console.

See “[About the Dell Management Console](#)” on page 21.

The Dell Client Manager home page displays the following summaries:

Dell Client Discovery and Installation Summary

Displays the Dell computer discovery and Dell Client Manager Agent installation information.

See “[About the Dell Client Discovery and Installation Summary web part](#)” on page 22.

BIOS Update Task Summary

Displays the **BIOS Update Task** execution summary.

See “[Updating BIOS versions](#)” on page 41.

BIOS Settings Task Summary

Displays the **BIOS Settings Task** execution summary.

See “[Configuring BIOS settings](#)” on page 46.

Update compliance of client computers that are ready to receive updates

Lists the number of discovered Dell client computers that support patching and their update status: up to date, or missing an update.

See “[Applying software patches to Dell computers](#)” on page 55.

Status of update jobs

Lists the rollout jobs that you created using the Stage and Distribute Wizard and their status. You can click a job to view its details.

See “[Staging and distributing updates](#)” on page 59.

About the Dell Client Discovery and Installation Summary web part

This web part is located on the Dell Client Manager home page and displays the Dell computer discovery and Dell Client Manager Agent installation information.

Table 3-1 Information in the Dell Client Discovery and Installation Summary web part

Summary	Description
Supported Dell Client Computers	The total number of Dell client computers discovered. Newer Dell models, not yet recognized as supported computers, are also listed. See “Discovering Dell computers” on page 31.
Patchable Dell Client Computers	The total number of Dell client computers that support patching. See “Applying software patches to Dell computers” on page 55.
Dell Client Manager Agent Installed	The total number of supported computers that successfully installed the Dell Client Manager Agent. See “Installing the Dell Client Manager Agent” on page 32.
Supported Dell Client Computers Awaiting Reboot to Finish Installation	The total number of supported computers that require reboot after the Dell Client Manager Agent installation or upgrade. See “(Optional) Restarting Dell client computers awaiting reboot” on page 34.
Systems Reporting Inventory Data	The total number of supported computers that successfully reported inventory data. See “Collecting BIOS, hardware, display, and power scheme settings inventory” on page 38.
Systems Reporting BIOS Settings Data	The total number of supported computers that successfully reported BIOS settings data. See “Collecting BIOS, hardware, display, and power scheme settings inventory” on page 38.
Unsupported Dell Client Computers	The total number of unsupported Dell client computers by product line. Legacy computers include older and unsupported models of OptiPlex, Latitude, and Dell Precision product lines. See “Updating the Dell Supported Models database” on page 53.

About managing multiple and single computers

Dell Client Manager provides the following two methods of managing Dell client computers:

One-to-many One-to-many management is when you assign a task to a collection of computers and schedule it to run at a later time. Dell Client Manager includes several predefined computer collections, called filters. Filters are logical groupings of computers based on any criteria you want. These filters can be based on Dell models, the operating system installed, BIOS version, and so on. You can also create your own filters.

See [“Collecting BIOS, hardware, display, and power scheme settings inventory”](#) on page 38.

See [“Updating BIOS versions”](#) on page 41.

See [“Configuring BIOS settings”](#) on page 46.

See [“Configuring Dell display settings”](#) on page 48.

See [“Configuring power scheme settings”](#) on page 49.

See [“Monitoring computers health”](#) on page 50.

See [“Applying software patches to Dell computers”](#) on page 55.

One-to-one One-to-one management is when you manage a single computer in real time. This method is useful for one-off management and repair. During a one-to-one management session Dell Client Manager connects to the target computer using the Windows Management Instrumentation (WMI). You can then view actual inventory and configuration information in the Dell Management Console. You can run management tasks on the target computer and immediately see the results.

See [“About managing individual Dell computers”](#) on page 63.

About actions that require a client restart

The Dell client computer restart is required when you perform the following actions:

- Dell OMCI software install and upgrade as part of the Dell Client Manager Agent installation
See [“Installing the Dell Client Manager Agent”](#) on page 32.
- BIOS update
See [“Updating BIOS versions”](#) on page 41.
- BIOS settings change

See [“Configuring BIOS settings”](#) on page 46.

You can control the restart options by scheduling, deferring, or allowing the restart to occur immediately after running the task.

About Windows BitLocker Drive Encryption

Windows BitLocker Drive Encryption is a full disk encryption feature included with the Microsoft Windows Vista Ultimate, Windows Vista Enterprise, Windows 7 Ultimate, and Windows Server 2008 operating systems. This feature is designed to protect data by providing encryption for entire volumes.

If you want to use Dell Client Manager to upgrade BIOS or change BIOS settings on computers with Windows BitLocker Drive Encryption enabled, you must disable BitLocker before you make any changes to the BIOS.

Warning: Never run the **BIOS Update Task** or the **BIOS Settings Task** on computers with BitLocker. Instead, use the **BIOS Settings Job** and the **BIOS Update Job**, included with Dell Client Manager. These jobs have BitLocker tasks included, which check the Dell client computers for the BitLocker feature and disable it when necessary. If you try to modify BIOS without disabling BitLocker first, the computer will fail to boot.

See [“Updating BIOS versions”](#) on page 41.

See [“Configuring BIOS settings”](#) on page 46.

About BIOS password restrictions

The BIOS passwords you type when configuring BIOS settings have the following restrictions:

- Only alphanumeric passwords are supported.
- Spaces may not be used. Using spaces results in incorrect passwords. For example, if you specified a BIOS password as "qwe 123", the password is set as "qwe".
- The maximum length is dependent on the computer model. For example, on Dell Latitude notebooks, the maximum is eight characters. When you use the **Real-Time** view to provide a password with more than the maximum characters, the password is truncated to the first number of characters allowed. For example, if the maximum is eight characters, and you provide a 12-character password, only the first eight characters are used. You need to use that truncated password to use or clear the BIOS password.

These restrictions apply to both setting passwords and password verification.

See [“Updating BIOS versions ”](#) on page 41.

See [“Configuring BIOS settings ”](#) on page 46.

Preparing target Dell computers for management

This chapter includes the following topics:

- [Preparing target Dell computers for management](#)
- [Discovering computers](#)
- [Installing the Altiris Agent](#)
- [\(Optional\) Configuring the Altiris Agent settings for evaluation use](#)
- [Discovering Dell computers](#)
- [Installing the Dell Client Manager Agent](#)
- [Installing the Power Scheme Agent](#)
- [\(Optional\) Restarting Dell client computers awaiting reboot](#)
- [\(Optional\) Configuring the Dell Client Manager Agent](#)
- [\(Optional\) Customizing the Dell client patching settings](#)

Preparing target Dell computers for management

Before you can manage Dell client computers with Dell Client Manager, you must install management agents on the computers.

See [“How Dell Client Manager works”](#) on page 12.

Table 4-1 Process for preparing target Dell computers for management

Step	Action	Description
Step 1	Discover manageable computers in your environment.	Discovery helps you find the hostnames of the computers on which you can install the Altiris Agent. See “Discovering computers” on page 29.
Step 2	Install the Altiris Agent to the client computers.	The Altiris Agent lets the Notification Server get information from and interact with the client computers. See “Installing the Altiris Agent” on page 29.
Step 3	(Optional) Configure the Altiris Agent settings for evaluation use.	For easier configuration and evaluation of Dell Client Manager, make the Altiris Agent request configuration from the Notification Server more frequently. See “(Optional) Configuring the Altiris Agent settings for evaluation use” on page 30.
Step 4	Discover Dell computers.	The Dell Client Discovery policy lets you find Dell computers that Dell Client Manager supports. See “Discovering Dell computers” on page 31.
Step 5	Install the Dell Client Manager Agent.	You must install this agent to supported Dell computers in your environment. See “Installing the Dell Client Manager Agent” on page 32.
Step 6	Install the Altiris Power Scheme Agent.	This agent lets you inventory and change power scheme settings. See “Installing the Power Scheme Agent” on page 33.

Table 4-1 Process for preparing target Dell computers for management
(continued)

Step	Action	Description
Step 7	(Optional) Restart the computers awaiting reboot.	Some computers need to be restarted in order for the Dell management software to work. See which computers need to be restarted and run the restart task. See “(Optional) Restarting Dell client computers awaiting reboot” on page 34.
Step 8	(Optional) Configure the Dell Client Manager Agent.	You can configure alerts, logging, and inventory refresh intervals. See “(Optional) Configuring the Dell Client Manager Agent” on page 35.

Discovering computers

Discovery lets you find the hostnames of the computers where you can install the Altiris Agent. You can discover computers on the network using a domain or a workgroup search.

For more information on Resource Discovery, see the *Symantec Management Platform Help*.

See “[Preparing target Dell computers for management](#)” on page 27.

To discover computers

- 1 In the Dell Management Console, on the **Actions** menu, click **Discover > Import Domain Membership/WINS**.
- 2 In the **Add Domain** field, type the domain name and click the **Add** symbol.
- 3 Check **Domain Membership** and click **Discover Now**.
- 4 As the discovery process finishes, click **View discovery reports** to view the list of discovered computers.

Installing the Altiris Agent

The Altiris Agent is the software that establishes communication between Notification Server and the computers in your network. Computers with the Altiris Agent installed on them are called managed computers. Notification Server then interacts with the Altiris Agent to monitor and manage each computer from the Dell Management Console.

You must install the Altiris Agent on the computers you want to manage with Dell Client Manager.

For more information on the Altiris Agent, see the *Symantec Management Platform Help*.

See [“Preparing target Dell computers for management”](#) on page 27.

To install the Altiris Agent

- 1 In the Dell Management Console, on the **Actions** menu, click **Agents/Plug-ins > Push Altiris Agent**.
- 2 On the **Altiris Agent Installation** page, install the Altiris Agent to computers in your environment.

For more information on how to install the Altiris Agent, see the *Symantec Management Platform Help* (Press F1 or click **Help > Context** in the Dell Management Console).

(Optional) Configuring the Altiris Agent settings for evaluation use

By default, the Altiris Agent requests new configuration from the Notification Server once per hour. This means that it can take up to one hour for a rollout policy (for example, **Dell Client Manager Agent - Install** policy) to reach the target Dell computer.

If you are evaluating this solution in a lab environment, you can change the configuration request interval to speed up the evaluation process.

The next time the Altiris Agent downloads configuration information, these settings will take effect. If you were using the default agent configuration values before the change, updates can take up to one hour before these changes are effective.

See [“Preparing target Dell computers for management”](#) on page 27.

To configure the Altiris Agent for evaluation use

- 1 In the Dell Management Console, on the **Settings** menu, click **Agents/Plug-ins > Targeted Agent Settings**.
- 2 In the **Policy Name** field, select the policy that applies to the computers you want to configure, for example: **All Desktop computers (excluding 'Package servers')**.
- 3 Click the **General** tab if it is not already selected.

- 4 Change the value in the **Download new configuration every** field to 5 minutes. This forces the agent to check more frequently for changes so you can see the results of the changes you make more quickly.
- 5 Change the value in the **Upload basic inventory every** field to 15 minutes. This forces inventory data to be sent more frequently.
- 6 Click **Save changes**.

Discovering Dell computers

You can determine if the computer is manufactured by Dell by using the **Dell Client Discovery** policy. This policy collects hardware inventory information and reports it to Notification Server.

When you run Dell client discovery, computers that are identified as Dell computers, appear in the following filters:

- **Supported Dell Client Computers**
- **Unsupported Dell Client Computers**
- **OptiPlex Desktops**
- **Latitude Notebooks**
- **Dell Precision Workstations**
- **Dell Client Computers with Supported Displays**
- **<Model> Computers**

By default, "model" filters are hidden. They appear only for the models that are actually discovered and inventoried in your environment by the Dell Client Discovery policy.

The discovery process can take some time to start, depending on the intervals that are set between updates of the Altiris Agent.

See [“\(Optional\) Configuring the Altiris Agent settings for evaluation use”](#) on page 30.

See [“Preparing target Dell computers for management”](#) on page 27.

To discover Dell computers

- 1 In the Dell Management Console, on the **Home** menu, click **Dell Client Manager**.
- 2 In the left pane, click **Dell Client Manager Agent Install > Dell Client Discovery**.

- 3 Turn on the policy.

To turn on the policy, at the upper right of the page, click the colored circle, and then click **On**.

- 4 Click **Save changes**.

Installing the Dell Client Manager Agent

The Dell Client Manager Agent, combined with the Altiris Agent, work to communicate information between Dell client computers and the Notification Server. The Dell Client Manager Agent, OMCI, and EnTech SoftOSD software that you install on client computers are the mechanisms that interact with Dell hardware. These agent components work together to send client information, such as hardware inventory, BIOS inventory, BIOS settings, displays inventory, to the Notification Server.

The Dell Client Manager Agent install policy installs OMCI and EnTech SoftOSD on the computers that do not have it already installed. If a client computer already has a supported previous version of OMCI installed, the policy also upgrades the OMCI software.

For more information on OMCI version that is included in this release, see the *Dell Client Manager Release Notes*.

If you already have a previous version of the Dell Client Manager Agent installed on the Dell computers in your environment, you must upgrade the agents.

The agent installation and upgrade process can take some time to start, depending on the intervals that are set between updates of the Altiris Agent.

See “(Optional) Configuring the Altiris Agent settings for evaluation use ” on page 30.

See “Preparing target Dell computers for management” on page 27.

To install the Dell Client Manager Agent

- 1 In the Dell Management Console, on the **Home** menu, click **Dell Client Manager**.
- 2 In the left pane, click Dell Client Manager Agent Install > Dell Client Manager Agent - Install (32-bit).
- 3 Under Power Management, specify if you want to restart the Dell client computer after the Dell Client Manager Agent installation. Restart may be required for the OMCI software to work. If you do not want to restart the computer right after the task, you may do it later on a schedule.

See “(Optional) Restarting Dell client computers awaiting reboot ” on page 34.

- 4 Turn on the policy.

To turn on the policy, at the upper right of the page, click the colored circle, and then click **On**.

- 5 Click Save changes.

To upgrade the Dell Client Manager Agent

- 1 In the Dell Management Console, on the **Home** menu, click **Dell Client Manager**.
- 2 In the left pane, click Dell Client Manager Agent Install > Dell Client Manager Agent - Upgrade (32-bit).
- 3 Under Power Management, specify if you want to restart the Dell client computer after the Dell Client Manager Agent installation. Restart may be required for the OMCI software to work. If you do not want to restart the computer right after the task, you may do it later on a schedule.

See “(Optional) Restarting Dell client computers awaiting reboot ” on page 34.

- 4 Turn on the policy.

To turn on the policy, at the upper right of the page, click the colored circle, and then click **On**.

- 5 Click Save changes.

Installing the Power Scheme Agent

The Power Scheme Agent is an add-on to the Altiris Agent that lets you configure power scheme settings of the target Dell computers.

See “[Configuring power scheme settings](#) ” on page 49.

The agent installation process can take some time to start, depending on the intervals that are set between updates of the Altiris Agent.

See “(Optional) [Configuring the Altiris Agent settings for evaluation use](#) ” on page 30.

See “[Preparing target Dell computers for management](#)” on page 27.

To install the Power Scheme Agent

- 1 In the Dell Management Console, on the **Home** menu, click **Dell Client Manager**.
- 2 In the left pane, click **Quick Start > Section 2. Enable Hardware Management > Step 4. Configure Agents for Power Schemes Management**.

- 3 Turn on the policy.

To turn on the policy, at the upper right of the page, click the colored circle, and then click **On**.

- 4 Click **Save changes**.

(Optional) Restarting Dell client computers awaiting reboot

You may be required to restart the Dell client computers after the Dell Client Manager Agent installation or upgrade. You can view if any Dell computers are awaiting reboot on the Dell Client Manager home page.

See [“About the Dell Client Manager home page”](#) on page 22.

To restart the Dell client computers that are awaiting reboot you must run the restart task. You can create a new Power Control task from the Jobs and Tasks Portal (**Manage > Jobs and Tasks**) or use the sample task that are included in Dell Client Manager.

For more information on task management, see the *Symantec Management Platform Help*.

The restart task uses the task server infrastructure to run and does not depend on the Altiris Agent update interval. Target computers are notified of this task immediately.

See [“Preparing target Dell computers for management”](#) on page 27.

To run the sample restart task included in Dell Client Manager

- 1 In the Dell Management Console, on the **Home** menu, click **Dell Client Manager**.
- 2 In the left pane, click **Tasks > Job Samples > Job Tasks > Restart by Power Control**.
- 3 In the right pane, click the **New Schedule** symbol.
- 4 In the **New Schedule** dialog box, configure the scheduling options, and then click **Add > Target**.
- 5 In the **Add Target** dialog box, under **Filtering Rules**, click **Add rule**.

- 6 To create a new rule, select **exclude computers not in**, then **Filter** and then select the **Supported Dell Client Computers Awaiting Reboot to Finish Installation** filter.
 To easily find the filter that you want, type the first letters of the filter's name. This will reduce the number of entries in the drop-down list. In this example, type `Supp`.
- 7 (Optional) To save the target you created, on the toolbar, click the **Save as** symbol.
- 8 In the **Add Target** dialog box, click **OK**.
- 9 In the **New Schedule** dialog box, click **Schedule**.
- 10 Under **Task Status**, on the toolbar, click the **Refresh** symbol to monitor the status of the task.

(Optional) Configuring the Dell Client Manager Agent

You can configure some of the Dell Client Manager Agent and Dell OMCI settings using the **Agent Settings Policy**.

See [“Preparing target Dell computers for management”](#) on page 27.

To configure the Dell Client Manager Agent

- 1 In the Dell Management Console, on the **Home** menu, click **Dell Client Manager**.
- 2 In the left pane, click **Configuration > Agent Settings**.
- 3 Check **Notifications** if you want the OMCI to generate alert notifications.
 OMCI alert notifications duplicate the notifications that are produced by Dell Client Manager, and this option is unchecked by default.
- 4 Check **Logging** to log alerts into the Windows Application Log on the Dell client computer.
- 5 Under **Basic Inventory Schedule**, configure when to send Dell Client Manager discovery and installed components information to Notification Server. Check **Send once ASAP** if you want to send this information once immediately after the next configuration request by the Dell client computers.
- 6 Click **Save changes**.

(Optional) Customizing the Dell client patching settings

If you want, you can customize the Dell client patching settings. You can also choose to use the default settings.

See [“Preparing target Dell computers for management”](#) on page 27.

To customize the Dell client patching settings

- 1 In the Dell Management Console, on the **Home** menu, click **Dell Client Manager**.
- 2 In the left pane, click **Configuration > Patch Management Configuration**.
- 3 In the right pane, configure the settings.
See [“About the Patch Management Configuration page”](#) on page 74.
- 4 Click **Save changes**.

Using Dell Client Manager

This chapter includes the following topics:

- [Prerequisites for using Dell Client Manager](#)
- [Collecting BIOS, hardware, display, and power scheme settings inventory](#)
- [Viewing BIOS, hardware, display, and power scheme settings inventory](#)
- [Updating BIOS versions](#)
- [Configuring BIOS settings](#)
- [Configuring Dell display settings](#)
- [Configuring power scheme settings](#)
- [Monitoring computers health](#)
- [Assessing Microsoft Windows 7 migration readiness](#)
- [Updating the Dell Supported Models database](#)

Prerequisites for using Dell Client Manager

Before using Dell Client Manager, you must install the Altiris Agent, Dell Client Manager Agent and Altiris Power Scheme Agent on Dell client computers.

See [“Preparing target Dell computers for management”](#) on page 27.

Before you start using Dell Client Manager read the following important information:

- See [“About managing multiple and single computers ”](#) on page 24.
- See [“About actions that require a client restart ”](#) on page 24.
- See [“About Windows BitLocker Drive Encryption ”](#) on page 25.

- See [“About BIOS password restrictions”](#) on page 25.

Collecting BIOS, hardware, display, and power scheme settings inventory

You can collect the following inventory information from Dell client computers:

- BIOS settings inventory
See [“Collecting BIOS inventory data”](#) on page 38.
- Hardware and BIOS version inventory
See [“Collecting hardware and BIOS version inventory data”](#) on page 38.
- Display settings inventory
See [“Collecting display inventory data”](#) on page 39.
- Power scheme settings inventory
See [“Collecting power scheme inventory data”](#) on page 39.

Collecting BIOS inventory data

You can collect BIOS settings inventory from the Dell client computers using the **BIOS Inventory Task**.

You can view collected inventory in reports.

See [“Viewing BIOS, hardware, display, and power scheme settings inventory”](#) on page 40.

To collect BIOS inventory data

- 1 In the Dell Management Console, on the **Home** menu, click **Dell Client Manager**.
- 2 In the left pane, click **Quick Start > Section 3. Hardware Management Tasks > Scan for Current BIOS Settings**.
- 3 If you want to report only the inventory that has changed since the last inventory scan, check **Only report inventory if changed**, and click **Save changes**.
- 4 Run the task one time or on a schedule. For more information on running tasks, see the *Symantec Management Platform Help*.

Collecting hardware and BIOS version inventory data

You can collect hardware inventory that is provided by Dell OMCI software that is installed on the Dell client computers using the **Hardware Inventory Task**.

You can view collected inventory in reports.

See [“Viewing BIOS, hardware, display, and power scheme settings inventory”](#) on page 40.

To collect hardware inventory data

- 1 In the Dell Management Console, on the **Home** menu, click **Dell Client Manager**.
- 2 In the left pane, click **Quick Start > Section 3. Hardware Management Tasks > Scan for Inventory Data**.
- 3 If you want to report only inventory that has changed since the last inventory scan, check **Only report inventory if changed**, and click **Save changes**.
- 4 Run the task one time or on a schedule. For more information on running tasks, see the *Symantec Management Platform Help*.

Collecting display inventory data

You can collect configuration inventory for displays, manufactured by Dell, using the **Display Inventory Task**.

You can view collected inventory in reports.

See [“Viewing BIOS, hardware, display, and power scheme settings inventory”](#) on page 40.

To collect display inventory data

- 1 In the Dell Management Console, on the **Home** menu, click **Dell Client Manager**.
- 2 In the left pane, click **Quick Start > Section 3. Hardware Management Tasks > Scan for Display Inventory Data**.
- 3 Run the task one time or on a schedule. For more information on running tasks, see the *Symantec Management Platform Help*.

Collecting power scheme inventory data

You can collect power scheme settings inventory from Dell client computers using the **Power Scheme Inventory Task**.

To perform this task, you must install the Altiris Power Scheme Agent on the target computers.

See [“Installing the Power Scheme Agent”](#) on page 33.

You can view collected inventory in reports.

See [“Viewing BIOS, hardware, display, and power scheme settings inventory”](#) on page 40.

To collect power saving inventory data

- 1 In the Dell Management Console, on the **Home** menu, click **Dell Client Manager**.
- 2 In the left pane, click **Quick Start > Section 5. Power Scheme Tasks > Power Scheme Inventory**.
- 3 Run the task one time or on a schedule. For more information on running tasks, see the *Symantec Management Platform Help*.

Viewing BIOS, hardware, display, and power scheme settings inventory

You can view collected inventory from reports or from the Resource Manager. Reports show you information about all Dell computers that you have inventoried. From the Resource Manager, you can view full inventory information for a particular Dell computer.

See [“Collecting BIOS, hardware, display, and power scheme settings inventory”](#) on page 38.

To view collected BIOS, hardware, or display inventory in reports

- 1 In the Dell Management Console, on the **Home** menu, click **Dell Client Manager**.
- 2 To view BIOS settings inventory, in the left pane, click **Reports > BIOS > Systems with Specified BIOS Setting**.
- 3 To view hardware inventory, in the left pane, click **Reports > Hardware Inventory > Systems with Specified Hardware Value**.

To view collected power scheme inventory in reports

- 1 In the Dell Management Console, on the **Reports** menu, click **All Reports**.
- 2 In the left pane, click **Power Scheme > Power Scheme Settings**.

To view collected inventory from the Resource Manager

- 1 In the Dell Management Console, on the **Home** menu, click **Dell Client Manager**.
- 2 Click **Filters**.
- 3 Click a filter, for example, **Supported Dell Client Computers**.

- 4 In the right pane, double-click the computer for which you want to view the inventory.
- 5 In the Resource Manager, on the **View** menu, click **Inventory**.
- 6 To view the BIOS, hardware, or display inventory, in the treeview pane, expand the **Dell Client Manager Inventory** folder, and then click the node you want to get information about. For example, click **Dell Client BIOS Settings > Boot Sequence**.
- 7 To view the power scheme settings inventory, in the treeview pane, click **Power Scheme > Power Scheme Settings**.

Updating BIOS versions

From time to time, IT organizations need to upgrade the BIOS on client computers across the network. Often times, this task is done before an organization-wide operating system installation. Company-wide BIOS upgrades do not occur frequently but, when they are necessary, the process can be time consuming and labor intensive. Dell Client Manager lets you automate the BIOS update process.

You can update the BIOS on the Dell client computers using the **BIOS Update Job**.

Warning: Never run the **BIOS Update Task** on computers with BitLocker. Instead, use the **BIOS Update Job**.

See [“About Windows BitLocker Drive Encryption”](#) on page 25.

You can also update BIOS versions for a single computer in real time from the Resource Manager.

See [“Performing one-to-one BIOS update”](#) on page 68.

You can use the **BIOS Update Job** to update BIOS on most Dell Precision, OptiPlex, and Latitude client computers. For the Dell computers that are procured after 2008, use the patch management functionality of Dell Client Manager to perform a BIOS update.

See [“Dell client computers that support BIOS updates”](#) on page 87.

See [“Applying software patches to Dell computers”](#) on page 55.

Table 5-1 Recommended process for updating BIOS versions with Dell Client Manager

Step	Action	Description
Step 1	Get the latest BIOS package.	You can download the latest BIOS update package for a specific Dell model from the following Web site: support.dell.com .
Step 2	Discover current BIOS versions.	The Hardware Inventory Task lets you collect current BIOS versions inventory. See “ Discovering current Dell BIOS versions ” on page 42.
Step 3	Save the computers you want to update as a static filter.	From the Systems with Specified BIOS Version report you can find the computers of the specific model that need a BIOS update. Then you can save this list of computers as a static filter. See “ Saving computers with older BIOS versions as a filter ” on page 42.
Step 4	Update the BIOS	Now you must run the BIOS Update Job on the computers that are listed in the static filter that you saved. See “ Running the BIOS Update Job ” on page 43.
Step 5	View the BIOS update reports.	If you want, you can view the BIOS update statistics in the reports. See “ Viewing the BIOS Update Job execution reports ” on page 45.

Discovering current Dell BIOS versions

To gather an inventory of BIOS versions that are used in Dell client computers in your environment, you must run the **Hardware Inventory Task**.

See “[Collecting hardware and BIOS version inventory data](#)” on page 38.

See “[Updating BIOS versions](#)” on page 41.

Saving computers with older BIOS versions as a filter

You can find Dell computers with the BIOS versions that require an update using the **Systems with Specified BIOS Version** report.

You can save the list of computers that is displayed in this report as a static filter. Then you can run the **BIOS Update Job** on the computers that are listed in the filter.

Note: As an example, we will update the BIOS for all Dell OptiPlex 745C computers to version 1.2.2.

See “[Updating BIOS versions](#)” on page 41.

To save computers with older BIOS versions as a filter

- 1 In the Dell Management Console, on the **Home** menu, click **Dell Client Manager**.
- 2 In the left pane, click **Reports > BIOS > Systems with Specified BIOS Version**.
- 3 In the report, under **Parameters**, select the product line and the model you want to update the BIOS for.

In this example, select **OptiPlex Desktops** and **745C** accordingly.

- 4 In the report, under **Parameters**, in the **Operator** drop-down list, click **Older Than**.
- 5 In the **BIOS Version** box, type the BIOS version to which you want to update.
In this example, type 1.2.2
- 6 On the toolbar, click **Refresh**. Computers that need a BIOS update appear in the list.
- 7 In the list, click the computers on which you want to update the BIOS version.
- 8 On the toolbar, click **Save As**, and then click **Static Filter**.
- 9 In the **Save as static filter** dialog box, type the name of the new filter that you are creating.

In this example, type `My OptiPlex 745C computers with BIOS older than 1.2.2`

- 10 Click **Save**.

Running the BIOS Update Job

You can upgrade the BIOS on multiple computers using the **BIOS Update Job**.

To create and save another BIOS update job to run on a different group of computers, clone the existing **BIOS Update Job** (you can do this by right-clicking on the job and then clicking **Clone**) or create a new one.

For more information on tasks and jobs, see the *Symantec Management Platform Help*.

Warning: Never run the **BIOS Update Task** alone on computers with BitLocker. Instead, use the sample **BIOS Update Job** that is included with Dell Client Manager. See [“About Windows BitLocker Drive Encryption”](#) on page 25.

Warning: After performing a BIOS update, the computer must be restarted rather than shut down. If a user shuts down the computer after the **BIOS Update Task** has run, the BIOS update will not take effect and it can cause the computer to not start properly. We recommend that you never run the **BIOS Update Task** alone without a follow-up **Restart by Power Control** task. Instead, use the sample **BIOS Update Job** that is included with Dell Client Manager.

Note: Dell Client Manager can extract the .hdr file only from the Windows type .exe BIOS upgrade files. For DOS type .exe BIOS upgrade files, you must extract the .hdr file manually. You can do this by typing the following in the command-line interface: `filename.exe -writehdrfile`

See [“Updating BIOS versions”](#) on page 41.

To run the BIOS Update Job

- 1 In the Dell Management Console, on the **Home** menu, click **Dell Client Manager**.
- 2 In the left pane, click **Quick Start > Section 3. Hardware Management Tasks > Update BIOS Version**.
- 3 On the **BIOS Update Job** page, click **Run "BIOS Update Task"**.
- 4 On the toolbar, click the **Edit the selected item** symbol.
- 5 On the **BIOS Update Task** page, click **Browse** and navigate to the location of the BIOS upgrade .exe (or extracted .hdr) file.

In this example, browse to the `0745C-010202.EXE` file — a BIOS update package for Dell OptiPlex 745C computers.
- 6 If you want to rewrite the BIOS even if the Dell client computer's BIOS version is higher than the one that you uploaded, check **Allow version downgrades**.
- 7 Type the BIOS setup password if needed.
- 8 Click **Save changes**.
- 9 Click **Close**.

- 10 On the **BIOS Update Job** page, click **Save changes**.
- 11 Under **Task Status**, on the toolbar, click **New Schedule**.
- 12 On the **New Schedule** page, select a schedule to run this job on and, if you want, configure **Run Options**.
- 13 Under **Input**, click **Add > Target**.
- 14 In the **Add Target** dialog box, under **Filtering Rules**, click **Add rule**.
- 15 To create a new rule, select **exclude computers not in**, then **Filter**, and then select the filter on which you want to run the **BIOS Update Job**.

In this example, select the **My OptiPlex 745C computers with BIOS older than 1.2.2** filter that you previously created. To easily find the filter that you want, type the first letters of the filter's name. This will reduce the number of entries in the drop-down list. In this example, type `My Opti.`

- 16 (Optional) To save the target that you created, on the toolbar, click the **Save as** symbol.
- 17 In the **Add Target** dialog box, click **OK**.
- 18 In the **New Schedule** dialog box, click **Schedule**.
- 19 Under **Task Status**, on the toolbar, click the **Refresh** symbol to monitor the status of the job.

The job will be executed according to the schedule that you specified. You can double-click the job instance in the **Task Status** section to see run details of the job. On the **Run Details** page, you can double-click each computer in the grid and see the details of each task included into the job, their execution status, output, and error codes.

Viewing the BIOS Update Job execution reports

You can view the status of the BIOS update jobs that you ran by viewing the Dell Client Manager reports.

The summary information is also displayed on the Dell Client Manager home page.

See [“About the Dell Client Manager home page”](#) on page 22.

See [“Updating BIOS versions”](#) on page 41.

To view the job execution progress reports

- 1 In the Dell Management Console, on the **Home** menu, click **Dell Client Manager**.
- 2 In the left pane, click **Reports > BIOS**.

3 Click BIOS Upgrade Task Execution Report.

This report lists the computers that are associated with the task and reports their status.

4 Click BIOS Upgrade Task Execution Summary.

This report shows how many computers successfully upgraded, the number of computers yet to run the policy, and those that failed.

Configuring BIOS settings

With Dell Client Manager you can remotely update BIOS settings for Dell client computers, targeting specific product lines or models, one or more computers, and reducing the cost of maintenance.

Use the **BIOS Settings Job** to change BIOS settings on the Dell client computers.

Warning: Never run the **BIOS Settings Task** alone on computers with BitLocker. Instead, use the sample **BIOS Settings Job** that is included with Dell Client Manager.

See [“About Windows BitLocker Drive Encryption”](#) on page 25.

You can specify new BIOS settings within the job, or you can import BIOS settings from another Dell computer's BIOS inventory that you previously collected with the **BIOS Inventory Task**.

See [“Collecting BIOS inventory data”](#) on page 38.

To create and save different sets of BIOS settings to run on a different group of computers, clone the existing **BIOS Settings Task** (you can do this by right-clicking on the task and then clicking **Clone**) or create a new one.

For more information on tasks and jobs, see the *Symantec Management Platform Help*.

You can also change BIOS settings for a single computer in real time by using the Resource Manager.

See [“Performing one-to-one BIOS configuration”](#) on page 66.

To configure BIOS settings using the sample BIOS Settings Job

- 1 In the Dell Management Console, on the **Home** menu, click **Dell Client Manager**.
- 2 In the left pane, click **Tasks > Job Samples > Job Tasks > BIOS Settings Job: BIOS Settings Task**.

- 3 On the **BIOS Settings Job: BIOS Settings Task** page, under **Software Settings**, check the BIOS settings that you want to change on the target Dell computers, and select a value.
See [“About using macros for BIOS settings”](#) on page 47.
- 4 If you want to import BIOS settings from another Dell computer that has run the **BIOS Inventory Task**, click **Import settings from collected BIOS inventory**, and then select the Dell computer from which to import the settings from. This is useful when you want to use a Dell computer's BIOS settings as a sample and have other Dell computers configured similarly.
See [“Collecting BIOS inventory data”](#) on page 38.
- 5 Type the BIOS setup password if needed.
See [“About BIOS password restrictions”](#) on page 25.
- 6 If you want the target Dell computers to send BIOS inventory after they run the task, check **Refresh inventory on settings change**.
- 7 Click **Save changes**.
- 8 In the left pane, click **Tasks > Job Samples > BIOS Settings Job**.
- 9 Run the job one time or on a schedule. For more information on running tasks, see the *Symantec Management Platform Help*.

About using macros for BIOS settings

Dell Client Manager lets you use macros when configuring BIOS settings.

See [“Configuring BIOS settings”](#) on page 46.

Macros, or variables, use data that is stored on client computers to populate BIOS settings based on the client-specific data. For example, you can use macros for the AssetTag property. You can use several different macros in one BIOS setting.

You can use any system environment variable that exists on a client computer, such as %ComputerName%. Many environment variables are provided by default with Windows operating systems. You can also create your own custom variables.

Most BIOS settings have limitations on their length. If you use macros that will result in a string longer than is supported for that BIOS setting, the task will fail.

Table 5-2 Macros that Dell Client Manager supports

Macro	Description
%username%	The logged on user name

Table 5-2 Macros that Dell Client Manager supports (*continued*)

Macro	Description
%systemname%	The client computer name (similar to what the %ComputerName% environment variable provides).
%macaddress%	The MAC address is used for the first enumerated physical adapter. If a computer has more than one physical adapter, the first enumerated adapter is selected.
%macaddress:w%	The MAC address of the wireless adapter.
%macaddress:n%	The MAC address of the physical NIC (not wireless) adapter.

Configuring Dell display settings

You can inventory, change brightness and contrast settings, restore factory default settings, and turn off Dell displays remotely from the Dell Management Console using the Dell display tasks.

See [“Collecting display inventory data ”](#) on page 39.

See [“Changing brightness and contrast settings ”](#) on page 48.

See [“Restoring display factory default settings ”](#) on page 49.

See [“Turning off displays ”](#) on page 49.

Changing brightness and contrast settings

You can change brightness and contrast settings of the displays that are manufactured by Dell.

See [“Configuring Dell display settings ”](#) on page 48.

To change brightness and contrast settings

- 1 In the Dell Management Console, on the **Home** menu, click **Dell Client Manager**.
- 2 In the left pane, click **Tasks > Display Tasks > Change brightness and contrast settings**.
- 3 If you want to change the brightness, check **Brightness** and set the desired brightness level.
- 4 If you want to change the contrast, check **Contrast** and set the desired contrast level.

- 5 Click **Save changes**.
- 6 Run the task one time or on a schedule.

For more information on running tasks, see the *Symantec Management Platform Help*.

Restoring display factory default settings

You can restore factory default settings on the displays that are manufactured by Dell.

See “[Configuring Dell display settings](#)” on page 48.

To restore display factory default settings

- 1 In the Dell Management Console, on the **Home** menu, click **Dell Client Manager**.
- 2 In the left pane, click **Tasks > Display Tasks > Restore factory defaults**.
- 3 Select the settings that you want to restore.
- 4 Click **Save changes**.
- 5 Run the task one time or on a schedule.

For more information on running tasks, see the *Symantec Management Platform Help*.

Turning off displays

You can turn off the displays that are manufactured by Dell.

See “[Configuring Dell display settings](#)” on page 48.

To turn off displays

- 1 In the Dell Management Console, on the **Home** menu, click **Dell Client Manager**.
- 2 In the left pane, click **Tasks > Display Tasks > Turn off display**.
- 3 Run the task one time or on a schedule.

For more information on running tasks, see the *Symantec Management Platform Help*.

Configuring power scheme settings

Dell Client Manager lets you inventory and change the target computer's power scheme settings remotely from the Dell Management Console.

See “[Collecting power scheme inventory data](#)” on page 39.

To perform this task, you must install the Altiris Power Scheme Agent on the target computers.

See “[Installing the Power Scheme Agent](#)” on page 33.

To configure power scheme settings

- 1 In the Dell Management Console, on the **Home** menu, click **Dell Client Manager**.
- 2 In the left pane, click **Quick Start > Section 5. Power Scheme Tasks** and click **a power scheme, for example, Minimal Power Management Scheme**.
- 3 (Optional) Under **Altiris Power Scheme Task settings**, configure the settings, and then click **Save changes**.
- 4 Run the task one time or on a schedule.

For more information on running tasks, see the *Symantec Management Platform Help*.

Monitoring computers health

Dell Client Manager lets you use health monitoring and alerts to inform administrators and users when client computers do not meet the criteria that you set. You can configure alerts for only administrators, only users, or both. You can also configure different kinds of alerts for administrators and users.

For example, if you are responsible for maintenance on computers that are critical to your business operation, you can create a Dell Client Monitoring Policy to alert you when the status of the computer's hard disk is not OK. Then, set the policy to send an email to you.

If you enable an alert to display on a client computer, a balloon dialog appears on the client computer with a brief description of the alert. The user can click the balloon dialog that opens the Dell Client Manager Alerts dialog. This dialog displays the description, the policy name, and the occurrence time. A mouse-over tool tip is provided to the user. The user can dismiss the alert or configure a reminder. If the user does not click the balloon dialog or does not dismiss the alert, a reminder will appear at the next logon.

Health monitoring is performed by the OMCI and the Dell Client Manager Agent software that is installed on the Dell client computers.

See “[Viewing alerts](#)” on page 51.

To enable health monitoring

- 1 In the Dell Management Console, on the **Home** menu, click **Dell Client Manager**.
- 2 In the left pane, click Policies > Dell Client Monitoring Policies > Dell Client Monitoring Policy.
- 3 If required, type the BIOS setup password. Some Dell models require a BIOS setup password to perform some monitoring tasks (such as chassis intrusion alert).

See [“About BIOS password restrictions”](#) on page 25.

- 4 Under Monitored Items, check the items you want to monitor and specify the rule. For example, check Disk count, and then click Any in the Rule drop-down list.
- 5 Under Actions, configure the alert rule that you want Dell Client Manager to perform.

By default, when an alert occurs, the Dell Client Manager Alert Notification task rule runs. This rule executes the Dell Client Manager Monitoring Policy - Send E-mail task. This task sends an email to the administrator with the alert description. You can configure the alert rule to run other tasks.

For more information on alert rules, see the topics on alert management in the *Symantec Management Platform Help*.

- 6 (Optional) To write an alert to the Windows application log on the Dell client computer that triggers an alert, under Client actions, check Log events. For more information, see the tooltip help.
- 7 (Optional) To display a popup message to the logged in user on the Dell client computer that triggers an alert, under Client actions, check Display alert notification. For more information, see the tooltip help.
- 8 Under Applied to, click Apply to and select the computers on which you want the policy to run.

Viewing alerts

To help you analyze your client computer's health, Dell Client Manager provides the Systems Triggering Alerts report, which details a list of client computers that triggered an alert based on the Dell Client Monitoring Policy that it ran.

Dell Client Manager alerts are also displayed in the Event Console in real time.

If you use the default Event Console settings, the alerts that have severity Informational are automatically resolved after 3 minutes. You can view these alerts later in reports or in the computer's Resource Manager.

The alerts are also sent to the administrator by email.

See “[Monitoring computers health](#)” on page 50.

To view the Systems Triggering Alerts report

- 1 In the Dell Management Console, on the **Home** menu, click **Dell Client Manager**.
- 2 In the left pane, click Reports > Hardware Status > Systems Triggering Alerts.

To view the alerts in the Event Console

- 1 In the Dell Management Console, on the Manage menu, click Events and Alerts.
- 2 In the Event Console window, view the alerts.

For more information on Event Console, see the topics on alert management in the *Symantec Management Platform Help* or press F1.

To view the alerts for a particular Dell computer

- 1 In Dell Management Console, open a report or a filter, and double-click the computer for which you want to view the alerts.
- 2 In the Resource Manager, on the View menu, click Events.
- 3 In the tree pane, click Dell Client Manager Events > Dell Client Manager Alerts.

Assessing Microsoft Windows 7 migration readiness

You can run reports to determine which computers are or are not ready for Microsoft Windows 7. To determine Windows 7 readiness, Dell Client Manager checks the processor, memory, and hard drive.

These reports list the computers that are capable of running Windows 7 with core functionality experience. For Aero experience capability, additional RAM and advanced graphics hardware may be required.

For more information, see www.windows7.com.

Microsoft Windows 7 has not been tested on all user configurations, and drivers may not be available for some hardware devices and software applications.

For more information on the latest driver availability, see support.dell.com.

To populate the reports with data, run the **Hardware Inventory Task**.

See “[Collecting hardware and BIOS version inventory data](#)” on page 38.

Table 5-3 Windows 7 migration readiness reports in Dell Client Manager

Report	Description
Systems Not Windows 7 Capable	These are computers that do not have the minimum hardware required to run Microsoft Windows 7. You can expand the Parameters section and filter by Dell product line or by component. For example, you can filter for OptiPlex desktops that do not have enough memory.
Systems with Windows 7-capable Hardware Profile	These are computers that have the minimum hardware required to run Microsoft Windows 7. You can expand the Parameters section and filter by a Dell product line and model.
Windows 7 Readiness Summary	This report provides a graph view of the Windows 7 readiness data.

To view the Microsoft Windows 7 migration readiness reports

- 1 In the Dell Management Console, on the **Home** menu, click **Dell Client Manager**.
- 2 Click **Reports > Microsoft Windows 7 Migration Readiness**.

Updating the Dell Supported Models database

Dell Client Manager supports all OptiPlex (desktops), Latitude (notebooks), and Dell Precision (workstations) product line computers, including new models that are not listed on the **Supported Models Manager** page. Only models that are listed as unsupported cannot be managed with Dell Client Manager.

Dell Client Manager comes with the latest supported models XML file so you don't need to import it separately. Symantec may release a new supported models XML file and make it available in the predefined location. On the **Supported Models Manager** page, you can configure Dell Client Manager to automatically download updated supported model files from the Symantec support Web site. You can manually download the files from the Dell support Web site and save them to a local directory.

To import the supported models list

- 1 In the Dell Management Console, on the **Home** menu, click **Dell Client Manager**.
- 2 In the left pane, click **Configuration > Supported Models Manager**.

- 3** On the **Supported Models Manager** page, modify the URL if needed, and then click **Import now**.
- 4** If you want to update the supported models list on a schedule, select a schedule, turn on the policy, and then click **Save changes**.
- 5** If you want to import the supported models list from a file, click **Browse**, choose the file, click **Import**, and then click **Save changes**.

Applying software patches to Dell computers

This chapter includes the following topics:

- [Applying software patches to Dell computers](#)
- [Downloading the Dell Update Packages catalog](#)
- [Determining patchable Dell client computers](#)
- [Viewing patchable Dell client computers](#)
- [Viewing applicable updates](#)
- [Staging and distributing updates](#)
- [Monitoring update progress](#)
- [Using reports to view patch management data](#)

Applying software patches to Dell computers

The Dell OptiPlex, Latitude, and Precision client computers that are procured after 2008 support patching. Dell Client Manager can detect patchable Dell computers in your environment and check if they require any updates.

A Dell Update Package (DUP) is an individual driver or firmware update that is designed to update certain system components of a Dell computer.

The Dell Update Packages catalog lists all of the DUPs that are available for download. You can view the list of available DUPs on the Manage Dell Client Hardware Updates page. When you choose to stage and distribute an update, the update package is downloaded (staged) to the Notification Server computer and then sent to the Dell client computers by DUP Rollout Jobs.

DUPs can be downloaded from the Dell Web site or from a local storage media (for example, Dell CD). When a DUP is downloaded it is marked as **Downloaded** on the **Manage Dell Client Hardware Updates** page. The DUP is then ready to be distributed by DUP Rollout Jobs.

A DUP rollout job is created automatically when you distribute an update. The rollout jobs are stored in the **Home > Dell Client Manager > Tasks > Patch Management > Rollout Jobs** folder.

Before you can use the Dell client computer patching functionality, you must prepare Dell client computers for management.

See [“Preparing target Dell computers for management”](#) on page 27.

Table 6-1 Process for Dell client computer patching

Step	Action	Description
Step 1	Download the Dell Update Packages catalog.	The catalog lists all of the available updates. See “Downloading the Dell Update Packages catalog” on page 57.
Step 2	Determine which Dell computers support patching.	The patch compliance inventory task can detect the computers that support patching and the updates that they require. See “Determining patchable Dell client computers” on page 58.
Step 3	View patchable Dell client computers.	The computers appear in the Patchable Dell Client Computers filter. See “Viewing patchable Dell client computers” on page 59.
Step 4	View the updates that need to be installed.	You can use reports to view the updates. See “Viewing applicable updates” on page 59.
Step 5	Stage and distribute the updates.	The Stage and Distribute Wizard helps you download and deploy Dell Update Packages to patchable Dell client computers. See “Staging and distributing updates” on page 59.

Table 6-1 Process for Dell client computer patching (*continued*)

Step	Action	Description
Step 6	Monitor the update progress.	You can watch the rollout jobs that are running and their status. See “Monitoring update progress” on page 60.
Step 7	View detailed patch management data.	You can view detailed information in the reports. See “Using reports to view patch management data” on page 61.

Downloading the Dell Update Packages catalog

You must download the Dell Update Package (DUP) catalog before you can create any DUP rollout jobs.

The **Dell Client Update Packages Catalog Import** task lets you download and import the catalog. You can download the DUP catalog from the ftp.dell.com Web site or you can copy it from a Dell CD.

To ensure that you always have the latest DUPs released by Dell, you can configure this task to run on a schedule.

See [“Applying software patches to Dell computers”](#) on page 55.

To download the Dell Update Catalog

- 1 In the Dell Management Console, on the **Home** menu, click **Dell Client Manager**.
- 2 In the left pane, click **Quick Start > Section 4. Patch Management > Step 2. Import Dell Client Update Packages Catalog**.
- 3 (Optional) In the right pane, configure the **Import Options** and then click **Save changes**.
- 4 By default, the catalog is downloaded from the Dell Web site. If you want to use another source (for example, a Dell CD), click **Custom location** and type the path to the storage media.
- 5 **Only if modified** is checked by default to ensure that only new or updated files are downloaded. This option avoids unnecessary downloads.
- 6 If you want to retry downloading the catalog in case it has failed, check **Retry failed downloads** and type the number of times to retry.

- 7 Click **New Schedule**.
- 8 In the **New Schedule** dialog box, click **Now**.
- 9 Click **Schedule**.

The task downloads the Dell Client Update Packages Catalog immediately.

- 10 (Optional) We recommend that you also configure this task to run on a schedule, for example, weekly. Scheduling ensures that you have the list of latest DUPs released by Dell. To schedule the task, click **New Schedule**, and then configure a schedule.

For more information on scheduling tasks, see the *Symantec Management Platform Help*.

Determining patchable Dell client computers

After you download the Dell Client Update Packages catalog for the first time, the **Determine Patchable Dell Clients** policy automatically becomes enabled. The policy runs once on all discovered Dell computers that are known to Dell Client Manager.

See “[Discovering Dell computers](#)” on page 31.

The **Determine Patchable Dell Clients** policy stays enabled so that it runs on every Dell computer that is discovered later.

For evaluation, you can also determine patchable Dell computers manually, using the **Update Dell Clients Patch Compliance Inventory Task**.

See “[Applying software patches to Dell computers](#)” on page 55.

To determine patchable Dell computers manually

- 1 In the Dell Management Console, on the **Home** menu, click **Dell Client Manager**.
- 2 In the left pane, click **Quick Start > Section 4. Patch Management > Step 3. Determine Patchable Dell Client Systems**.
- 3 Run the task one time or on a schedule. For example, you can run this task on the All Supported Dell Client Systems target.

For more information on running tasks, see the *Symantec Management Platform Help*.

To view the Determine Patchable Dell Clients Policy

- 1 In the Dell Management Console, on the **Home** menu, click **Dell Client Manager**.
- 2 In the left pane, click **Policies > Patch Management > Determine Patchable Dell Clients Policy**.
- 3 (Optional) To see the list of computers on which the policy has run, under **Policy Status**, in the **View** drop-down list, click **Computers and Users**.

Viewing patchable Dell client computers

After the **Determine Patchable Dell Clients** policy runs, the list of patchable Dell computers appears in the **Patchable Dell Client Computers** filter.

See “[Applying software patches to Dell computers](#)” on page 55.

To view patchable Dell client computers

- 1 In the Dell Management Console, on the **Home** menu, click **Dell Client Manager**.
- 2 In the left pane, click **Quick Start > Section 4. Patch Management > Step 4. View Patchable Dell Client Systems**.

Viewing applicable updates

You can view any applicable updates and computers that require an update in the Dell Client Manager reports.

See “[Applying software patches to Dell computers](#)” on page 55.

To view applicable updates

- 1 In the Dell Management Console, on the **Home** menu, click **Dell Client Manager**.
- 2 In the left pane, click **Quick Start > Section 4. Patch Management > Step 5. View Applicable Updates**.
- 3 Click a report.

Staging and distributing updates

You can stage and distribute Dell Update Packages (DUPs) on the **Manage Dell Hardware Updates** page. This page displays all of the DUPs that are listed in the Dell Update Packages catalog.

See [“Downloading the Dell Update Packages catalog”](#) on page 57.

When you stage an update, the required software is downloaded to the Notification Server computer from the Dell Web site. DUPs can also be downloaded from a local storage media (for example, a Dell CD).

Staged updates are marked **Downloaded** on the **Manage Dell Client Hardware Updates** page.

Updates are distributed to the client Dell computers using DUP rollout jobs. If you distribute multiple DUPs, a separate rollout job is created for each DUP.

You can stage and distribute all of the visible DUPs in one process. You can filter DUPs by client model, device name, operating system, severity, and date.

See [“Applying software patches to Dell computers”](#) on page 55.

To stage and distribute updates

- 1 In the Dell Management Console, on the **Home** menu, click **Dell Client Manager**.
- 2 In the left pane, click **Quick Start > Section 4. Patch Management > Step 6. Stage and Distribute Updates**.
- 3 In the right pane, use filters to display the updates that you want.
- 4 Stage and distribute updates in one of the following ways:
 - Click the updates that you want to roll out and then, on the toolbar, click **Stage and Distribute Selected Updates**.
 - If you want to stage and distribute all of the updates that are currently displayed in the list, on the toolbar, click **Stage and Distribute All Updates**.
- 5 (Optional) In the **Stage and Distribute Wizard**, configure the settings.
See [“About the Stage and Distribute Wizard”](#) on page 76.
- 6 Click **Create**.

Monitoring update progress

You can view the list of the DUP rollout jobs that are currently running and their status.

See [“Applying software patches to Dell computers”](#) on page 55.

To view the status of DUP Rollout Jobs

- 1 In the Dell Management Console, on the **Home** menu, click **Dell Client Manager**.
- 2 In the left pane, click **Quick Start > Section 4. Patch Management > Step 7. Monitor Update Progress**.
- 3 In the right pane, click the job whose progress you want to view.

Using reports to view patch management data

You can view and manage your Patch Management data through reports. These reports give you information that is specific to the Patch Management functionality of Dell Client Manager. For example, you can use compliance reports to determine how many urgent software updates your managed computers require.

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

Also, you can view results from commonly used reports on the Patch Management home page.

See [“About the Dell Client Manager home page”](#) on page 22.

See [“Applying software patches to Dell computers”](#) on page 55.

To view Dell Client Patch Management reports

- 1 In the Dell Management Console, on the **Home** menu, click **Dell Client Manager**.
- 2 In the left pane, click **Reports > Patch Management**.
- 3 Click the folder that contains the reports that you want to view.
- 4 Click the report that you want to see.

Managing individual Dell computers

This chapter includes the following topics:

- [About managing individual Dell computers](#)
- [Accessing the Real-Time view](#)
- [About the Real-Time Consoles page](#)
- [Viewing the Dell client computer summary](#)
- [Performing one-to-one BIOS configuration](#)
- [Performing one-to-one boot order configuration](#)
- [Performing one-to-one BIOS password change](#)
- [Performing one-to-one BIOS update](#)
- [Resetting chassis intrusion alert](#)

About managing individual Dell computers

You can manage many Dell client computers at a time using tasks and jobs. You can also manage a single computer in real time using the Resource Manager 's Real-Time view.

See “[Accessing the Real-Time view](#)” on page 64.

In the **Real-Time** view, the following real-time information about the target Dell client computer is displayed:

- Computer summary
See “[Viewing the Dell client computer summary](#)” on page 66.

- Basic computer information including computer name, model, and service and asset tag numbers
- BIOS configuration information
- Power management settings
- Management software information
- Basic operating system information
- Network information, including IP address, network adapter details, and connectivity status
- Processor information
- Memory and storage information
- OS Services information
- Basic utilization information for CPU/Disk/Memory
- Status information (with critical, warning, normal icon) in a prominent location on the summary page plus text descriptions for the status (for example, Chassis Intrusion detected) in a prominent location on the summary page
- Probe information, for example, temperature, and voltage sensors for workstations from the Dell namespace

From the Real-Time view you can run the following management tasks:

- Change the target Dell computer's BIOS settings, power management settings, warranty information, and so on
See [“Performing one-to-one BIOS configuration ”](#) on page 66.
- Change boot order
See [“Performing one-to-one boot order configuration ”](#) on page 67.
- Change BIOS password
See [“Performing one-to-one BIOS password change ”](#) on page 67.
- Update BIOS version
See [“Performing one-to-one BIOS update ”](#) on page 68.

Accessing the Real-Time view

The **Real-Time** view is located in the Resource Manager and displays live computer information obtained through the WMI interface. Dell Client Manager displays its information under the Dell Client Manager node.

To open the Real-Time view from computer filters or reports

- 1 In the Dell Management Console, on the **Home** menu, click **Dell Client Manager**.
- 2 Click **Filters**.
- 3 Click a filter.
For example, click **Supported Dell Client Computers**.
- 4 In the right pane, double-click the computer you want to manage.
- 5 In the Resource Manager, on the **View** menu, click **Real-Time**.
- 6 In the treeview pane, click **Real-Time Consoles**.

See [“About the Real-Time Consoles page”](#) on page 65.

To open the Real-Time view directly

- 1 In the Dell Management Console, on the **Actions** menu, click **Remote Management > Real-Time Management**.
- 2 On the **Manage** page, type the host name or the IP of the computer to which you want to connect, and click **Connect**.
- 3 In the Resource Manager, on the **View** menu, click **Real-Time**.
- 4 In the treeview pane, click **Real-Time Consoles**.

See [“About the Real-Time Consoles page”](#) on page 65.

About the Real-Time Consoles page

The Real-Time Consoles page is the first page in the Resource Manager's Real-Time view tree. It displays the connection information for the computer, the list of protocols, supported by the target computer (WMI, ASF, DASH, Intel AMT, SNMP, IPMI), and if the connection credentials that you configured are accepted by the target computer.

If credentials are displayed as invalid, verify that your connection profile is using the correct credentials. If the technologies that you want to use are not displayed on this page, open the connection profile and make sure they are turned on.

For more information, see topics about credential manager and connection profiles in the *Symantec Management Platform Help*.

See [“Troubleshooting connection through the Real-Time view”](#) on page 80.

Viewing the Dell client computer summary

You can view the summary information about a resource on the **Dell Client Manager Summary** page. This information includes the target Dell computer's model, BIOS version, and the status of the most important software and hardware components.

To open the Dell Client Manager Summary page

- 1 Open the Resource Manager.
See [“Accessing the Real-Time view”](#) on page 64.
- 2 In the Resource Manager, on the **Summaries** menu, click **Dell Client Manager Summary**.

Performing one-to-one BIOS configuration

You can use the **Real-Time** view to change a BIOS setting for a single Dell client computer.

The behavior is similar to the task-based BIOS configuration capability in Dell Client Manager except that it will occur in real time through the live WMI connection.

See [“Configuring BIOS settings”](#) on page 46.

Warning: Never run this task on computers with BitLocker enabled.

See [“About Windows BitLocker Drive Encryption”](#) on page 25.

See [“About managing individual Dell computers”](#) on page 63.

To configure BIOS settings one-to-one

- 1 Open the **Real-Time** view for the computer that you want to manage.
See [“Accessing the Real-Time view”](#) on page 64.
- 2 In the treeview pane, click **Real-Time Consoles > Dell Client Manager > General Configuration > BIOS Settings**.
- 3 If the client computer requires a BIOS setup password, type it.
See [“About BIOS password restrictions”](#) on page 25.
- 4 If you want to restart the target Dell computer after changing the settings, in the **Reboot After Change** drop-down list click **True**.

- 5 Configure the other settings and options.
- 6 Click **Apply**.

Performing one-to-one boot order configuration

You can use the **Real-Time** view to configure the boot order of the target Dell computer.

Warning: Never run this task on computers with BitLocker enabled.

See [“About Windows BitLocker Drive Encryption”](#) on page 25.

See [“About managing individual Dell computers”](#) on page 63.

To change boot order one-to-one

- 1 Open the **Real-Time** view for the computer that you want to manage.
See [“Accessing the Real-Time view”](#) on page 64.
- 2 In the treeview pane, click **Real-Time Consoles > Dell Client Manager > General Configuration > Boot Order**.
- 3 If you want to restart the target Dell computer after changing the settings, in the **Reboot After Change** drop-down list click **True**.
- 4 Set the boot order for each of the bootable devices.
- 5 You can also enable or disable the boot status of a device.
- 6 Click **Apply**.

Performing one-to-one BIOS password change

You can use the **Real-Time** view to change the BIOS management password.

See [“About BIOS password restrictions”](#) on page 25.

Warning: Never run this task on computers with BitLocker enabled.

See [“About Windows BitLocker Drive Encryption”](#) on page 25.

See [“About managing individual Dell computers”](#) on page 63.

To change a BIOS password one-to-one

- 1 Open the **Real-Time** view for the computer that you want to manage.
See [“Accessing the Real-Time view ”](#) on page 64.
- 2 In the treeview pane, click **Real-Time Consoles > Dell Client Manager > Management Tasks > Change BIOS Password**.
- 3 Type the current and the new BIOS passwords.
- 4 Click **Accept**.

Performing one-to-one BIOS update

You can use the **Real-Time** view to upgrade or downgrade a BIOS by supplying a Dell .exe or .hdr BIOS update to a single client computer.

Note: Dell Client Manager can extract the .hdr file only from the Windows-type .exe BIOS upgrade files. For DOS-type .exe BIOS upgrade files, you must extract the .hdr file manually. You can do this by typing the following in the command interface: `filename.exe -writehdrfile`

The behavior is similar to the task-based BIOS update capability in Dell Client Manager except that it will occur real time through the live WMI connection.

See [“Updating BIOS versions ”](#) on page 41.

You can use the **Real-Time** view to update BIOS on most Dell Precision, OptiPlex, and Latitude client computers. For the Dell computers that are procured after 2008, use the patch management functionality of Dell Client Manager to perform a BIOS update.

See [“Dell client computers that support BIOS updates ”](#) on page 87.

See [“Applying software patches to Dell computers ”](#) on page 55.

Warning: After you click **Accept**, the target Dell computer will restart within 60 seconds closing all programs and losing any unsaved data.

Warning: Never run this task on computers with BitLocker enabled.

See [“About Windows BitLocker Drive Encryption ”](#) on page 25.

See [“About managing individual Dell computers ”](#) on page 63.

To upgrade/downgrade a BIOS one-to-one

- 1 Open the **Real-Time** view for the computer that you want to manage.
See [“Accessing the Real-Time view ”](#) on page 64.
- 2 In the treeview pane, click **Real-Time Consoles > Dell Client Manager > Management Tasks > BIOS Upgrade**.
- 3 Click **Browse** and navigate to the location of the BIOS upgrade .exe (or extracted .hdr) file.
- 4 If the client computer requires a BIOS setup password, type it.
See [“About BIOS password restrictions ”](#) on page 25.
- 5 Click **Accept**.

Resetting chassis intrusion alert

If a chassis intrusion has been detected, you can clear the alert so that the status is returned to **Not Detected**.

Warning: Never run this task on computers with BitLocker enabled.

See [“About Windows BitLocker Drive Encryption ”](#) on page 25.

See [“About managing individual Dell computers ”](#) on page 63.

To reset the chassis intrusion alert

- 1 Open the **Real-Time** view for the computer that you want to manage.
See [“Accessing the Real-Time view ”](#) on page 64.
- 2 In the treeview pane, click **Real-Time Consoles > Dell Client Manager > General Configuration > BIOS Settings**.
- 3 If a chassis intrusion alert has been activated, the **Chassis Intrusion Status** property value displays **Detected**. Clear the alert by changing it to **Clear**.
- 4 Click **Apply**.

About Dell Client Manager pages

This chapter includes the following topics:

- [About the Disable BitLocker and Enable BitLocker tasks](#)
- [About the BIOS Settings and BIOS Update jobs](#)
- [About power management tasks](#)
- [About the Update Dell Clients Patch Compliance Inventory task](#)
- [About the Download Software Update Package task](#)
- [About the Stage and Distribute job](#)
- [About the patch management rollout jobs](#)
- [About the Dell Update Applicability Task](#)
- [About the Dell Update Install Task](#)
- [About the Patch Management Configuration page](#)
- [About the Stage and Distribute Wizard](#)

About the Disable BitLocker and Enable BitLocker tasks

This task is an internal client task that is used by the DUP rollout jobs and the BIOS management jobs. This task disables Windows BitLocker Drive Encryption when you are performing a BIOS update. We recommend that you do not modify this task.

See [“About Windows BitLocker Drive Encryption”](#) on page 25.

See [“Updating BIOS versions”](#) on page 41.

See [“Configuring BIOS settings”](#) on page 46.

See [“Applying software patches to Dell computers”](#) on page 55.

About the BIOS Settings and BIOS Update jobs

The **BIOS Settings** job lets you configure BIOS settings on the client Dell computers.

See [“Configuring BIOS settings”](#) on page 46.

The **BIOS Update** job lets you upgrade/downgrade a BIOS on the client Dell computers.

See [“Updating BIOS versions”](#) on page 41.

About power management tasks

This task is an internal client task that is used by the DUP rollout jobs. Dell Client Manager uses this task when rolling out BIOS update packages to patchable Dell computers.

See [“Applying software patches to Dell computers”](#) on page 55.

This task is also used by the BIOS update job and the BIOS settings job.

See [“Updating BIOS versions”](#) on page 41.

See [“Configuring BIOS settings”](#) on page 46.

We recommend that you do not modify this task. If you want to power on, power off, or restart a computer, you can create a new power management task.

For more information on running tasks, see the *Symantec Management Platform Help*.

About the Update Dell Clients Patch Compliance Inventory task

This task is an internal client task that determines the Dell client computers in your environment that can receive Dell updates. The task reports on applicable DUPs and installed firmware. The task targets the **Supported Dell Client Computers** filter and is run by the **Determine Patchable Dell Clients** policy.

See [“Determining patchable Dell client computers”](#) on page 58.

You can also run this task manually. You can schedule this task to periodically check if any computers need updates.

For more information on running tasks, see the *Symantec Management Platform Help*.

See [“Applying software patches to Dell computers”](#) on page 55.

About the Download Software Update Package task

This task is an internal server task that runs when you stage a DUP. This task downloads (stages) the update packages from the Web to local storage. On this page, you can view the download status. You can also re-run a task that has failed.

See [“About the Stage and Distribute job”](#) on page 73.

See [“Applying software patches to Dell computers”](#) on page 55.

About the Stage and Distribute job

This job is an internal server job that is used by the **Stage and Distribute Wizard**. This job is read-only. On this page, you can view the status of the Stage and Distribute jobs. You can view the details of each task by double-clicking a job. You can also re-run a job that has failed.

See [“Staging and distributing updates”](#) on page 59.

See [“Applying software patches to Dell computers”](#) on page 55.

About the patch management rollout jobs

This job is an internal client job that distributes and installs DUPs to patchable Dell computers. This job automatically runs on specific models of Dell computers. It runs only on the computers that needed an update at the time that you staged and distributed the update.

See [“Staging and distributing updates”](#) on page 59.

You can also run this job manually. For example, you can run this job on a particular computer or you can re-run the job that has failed.

See [“Applying software patches to Dell computers”](#) on page 55.

About the Dell Update Applicability Task

This task is an internal client task that is used by the DUP rollout jobs to check if an update is applicable to the target computer.

See [“Applying software patches to Dell computers”](#) on page 55.

About the Dell Update Install Task

This task is an internal client task that is used by the DUP rollout jobs to install the update on the target computer.

See [“Applying software patches to Dell computers”](#) on page 55.

About the Patch Management Configuration page

This page lets you set up how you want to distribute Dell Update Packages (DUPs). Some of the settings on this page are used as default values in the DUP rollout job. Any subsequent DUPs that are downloaded then use these settings. If you change the settings, the existing Software Update tasks and packages are not updated with these default settings. You can force them to update by recreating packages from the **Manage Dell Client Hardware Updates** page.

See [“Applying software patches to Dell computers”](#) on page 55.

Table 8-1 Options on the General tab

Option	Description
Verify authenticity of downloaded Dell Packages	Check to ensure that all DUPs are Dell-certified. Default: checked.
Download from	Select where to download the DUPs from. The options are as follows: <ul style="list-style-type: none">■ Dell site DUPs are downloaded directly from Dell's Web site. This is the default option.■ Local storage DUPs are downloaded from a local storage media, for example a Dell CD. The Browse button is visible only when the Dell Management Console is opened on the Notification Server computer.

Table 8-1 Options on the General tab (*continued*)

Option	Description
To location	<p>Specify the path to the location where downloaded DUPs are stored.</p> <p>Type a path that the Notification Server computer can access.</p> <p>Default: C:\Program Files\Altiris\Notification Server\NSCap\bin\Win32\X86\Dell Client Manager\DUP</p> <p>The Browse button is visible only when the Dell Management Console is opened on the Notification Server computer.</p>
Only download if modified	<p>Check if you want to download only the DUPs that have changed or that have not yet been downloaded to the local storage.</p> <p>Default: checked.</p>
Retry failed downloads	<p>Specify the number of times Dell Client Manager should retry downloading DUPs.</p> <p>Default: 2 times.</p>

Table 8-2 Options on the Advanced tab

Option	Description
Delete packages after	<p>Lets you determine how often to delete downloaded software update packages.</p>
Allow Package Server distribution	<p>Ensures that package servers process all of the software update packages.</p> <p>For more information, see the <i>Symantec Management Platform Help</i>.</p> <p>Default: checked.</p>
Use alternate download location on Package Server	<p>Lets you specify a different location for packages on a package server.</p>
Use alternate download location on client	<p>Lets you specify a different location for packages on managed computers.</p>

Table 8-3 Options on the Programs tab

Option	Description
Run with rights	<p>Specifies whether the program runs with the System Account, Logged in User, or Specified User account. If you select Specified User, you must specify the user's domain in the field.</p> <p>Default: System Account.</p>
Program can run	<p>Specify the conditions under which the program can run.</p> <p>Default: Whether or not a user is logged on.</p>
Minimum connection speed	<p>Specify the minimum connection speed that is needed to execute software delivery programs.</p> <p>Before a program is run, the connection speed from the Altiris Agent to Notification Server is tested. If the connection speed is less than the specified minimum speed, the program does not run. This setting does not affect downloading of software delivery packages.</p>
Terminate after	<p>Specifies the time to terminate software update tasks at.</p> <p>Default: 20 minutes</p>
Agent Events	<p>Lets you choose to send the relevant events from managed computers to Notification Server.</p>

About the Stage and Distribute Wizard

This wizard creates rollout jobs. Rollout jobs distribute Dell Update Packages (DUPs) to managed computers. The **Stage and Distribute Wizard** automatically filters targets to install DUPs only on applicable computers.

See “[Applying software patches to Dell computers](#)” on page 55.

Table 8-4 Options on the Stage and Distribute Wizard page

Option	Description
Reboot if required	<p>Lets you choose to restart the target computer after installing DUPs.</p>
Allow downgrade	<p>Lets you choose to install a DUP that has been superseded.</p>

Table 8-4 Options on the Stage and Distribute Wizard page (*continued*)

Option	Description
Disable and Enable BitLocker for BIOS Updates	<p>Specifies to include BitLocker detection tasks into the update rollout job.</p> <p>If you update BIOS on a computer that has BitLocker drive encryption enabled on it, the computer fails to boot. We recommend that you always check this option when updating BIOS. If the computer does not have BitLocker, the tasks are skipped.</p> <p>See “About Windows BitLocker Drive Encryption” on page 25.</p>
Schedule	Specifies a schedule to install DUPs.
Windows Targets	Specifies the target to which to apply the rollout job. Only the applicable computers in the specified target receive DUPs from the rollout job.
Distribute Selected Updates	Displays a list of DUP bundles that the rollout job distributes.

Troubleshooting Dell Client Manager

This appendix includes the following topics:

- [Troubleshooting the Altiris Agent push installation](#)
- [Troubleshooting connection through the Real-Time view](#)

Troubleshooting the Altiris Agent push installation

If you receive a "No network provider accepted the given network path" error when push installing the Altiris Agent to a Windows XP SP2 or Windows Vista computer, the following issues can be causing the error:

- Windows firewall
See ["Configuring the firewall to allow push installation"](#) on page 79.
- Simple file sharing enabled (Windows XP SP2)
See ["Disabling simple file sharing on Windows XP SP2"](#) on page 85.
- User Account Control is enabled (Windows Vista)
See ["Configuring User Access Control on Windows Vista and Windows 7"](#) on page 85.

Configuring the firewall to allow push installation

To push the Altiris Agent you must configure the firewall on the client computers to allow file and printer sharing exceptions (TCP ports 139, 445 and UDP ports 137, 138).

See ["Troubleshooting the Altiris Agent push installation"](#) on page 79.

To configure the firewall for the Altiris Agent push installation

- 1 On the client computer, from the **Start** menu, open **Control Panel > Windows Firewall**.
- 2 On the **Exceptions** tab, check **File and Printer Sharing**, and then click **OK**.

Troubleshooting connection through the Real-Time view

The following table can help you troubleshoot connection problems.

Table A-1 Possible reasons of connection errors

Technology	Possible reasons
WMI	<p>The connection credentials are incorrect.</p> <p>The computer is turned off .</p> <p>The operating system is not loaded.</p> <p>The computer is not connected to the network.</p> <p>The firewall does not allow incoming WMI connections.</p> <p>See “Configuring the firewall to allow WMI connection” on page 82.</p> <p>Simple file sharing is enabled.</p> <p>See “Disabling simple file sharing on Windows XP SP2” on page 85.</p> <p>User Access Control is turned on.</p> <p>See “Configuring User Access Control on Windows Vista and Windows 7” on page 85.</p> <p>You are connecting to Microsoft Windows XP Home Edition, where WMI remote connection is not available.</p> <p>You are connecting with a user that has an empty password.</p>
ASF	<p>The connection credentials are incorrect.</p> <p>ASF is turned on in the BIOS but not configured.</p> <p>For more information on configuring computers with ASF, see the <i>Out of Band Management Component Implementation Guide</i>.</p> <p>ASF is turned off in the BIOS.</p> <p>The computer is not connected to the network.</p> <p>The target computer is not ASF capable.</p>

Table A-1 Possible reasons of connection errors (*continued*)

Technology	Possible reasons
Intel AMT	<p>The connection credentials are incorrect.</p> <p>The Intel AMT device is not configured.</p> <p>For more information on configuring computers with Intel AMT, see the <i>Out of Band Management Component Implementation Guide</i>.</p> <p>The Intel AMT device is in secure mode, but the connection profile is not configured to use the correct certificates, and vice versa.</p> <p>For more information on configuring connection profiles, see the <i>Symantec Management Platform Help</i>.</p> <p>Intel AMT is turned off in the BIOS.</p> <p>The computer is not connected to the network.</p> <p>The computer is not Intel AMT capable.</p>
DASH	<p>The connection credentials are incorrect.</p> <p>DASH is turned on in the BIOS but not configured.</p> <p>For more information on configuring computers with DASH, see the <i>Out of Band Management Component Implementation Guide</i>.</p> <p>DASH is turned off in the BIOS.</p> <p>The computer is not connected to the network.</p> <p>The target computer is not DASH capable.</p>
IPMI	<p>The connection credentials are incorrect.</p> <p>The IPMI device is not configured.</p> <p>The IPMI device is in secure mode, but the connection profile is not configured to use the correct certificates.</p> <p>IPMI is turned off in the BIOS.</p> <p>The computer is not connected to the network.</p> <p>The target computer is not IPMI capable.</p>
SNMP	<p>The SNMP community string is incorrect.</p> <p>SNMP is not installed on the target computer.</p> <p>The SNMP service is not running on the target computer.</p> <p>The Notification Server computer is not in the list of hosts to accept the SNMP packets from. Check SNMP service properties.</p>

Configuring the firewall to allow WMI connection

WMI connection through the **Real-Time** view can fail when you try to connect to a computer with Microsoft Windows XP Service Pack 2, Windows Vista, or Windows 7 operating system.

This issue can occur when the default configuration of the Windows Firewall program blocks incoming network traffic for Windows Management Instrumentation (WMI) connection. For the connection to succeed, the remote computer must permit incoming network traffic on TCP ports 135, 445, and additional dynamically-assigned ports, typically in the range of 1024 to 1034.

You can resolve this issue in one of the following ways:

- Configure the firewall on the computer you want to connect to.
See [“Configuring the firewall on a single computer”](#) on page 82.
- Configure the firewall on all computers in the domain using group policy.
See [“Configuring the firewall on multiple domain computers with a group policy”](#) on page 83.
- Temporarily disable the firewall.

See [“Troubleshooting connection through the Real-Time view”](#) on page 80.

Configuring the firewall on a single computer

For evaluation, you can configure the firewall using the computer’s local settings.

See [“Configuring the firewall to allow WMI connection”](#) on page 82.

To configure the firewall on Windows XP SP2

- 1 Log on to the target computer as the administrator.
- 2 Click **Start > Run**, type `gpedit.msc` in the **Open** dialog box, and then click **OK**.
- 3 In the **Group Policy** window, click **Local Computer Policy > Computer Configuration > Administrative Templates > Network > Network Connections > Windows Firewall**.
- 4 If the computer is in a domain, click **Domain Profile**. If the computer is not in a domain, click **Standard Profile**.
- 5 Double-click **Windows Firewall: Allow remote administration exception**, click **Enable**, and then click **OK**.

To configure the firewall on Windows Vista

- 1 Log on to the target computer as the administrator.
- 2 From the **Control Panel**, open the **Windows Firewall Settings** dialog box.
- 3 On the **Exceptions** tab, check **Windows Management Instrumentation (WMI)**.

To configure the firewall on Windows 7

- 1 Log on to the target computer as the administrator.
- 2 From the **Control Panel**, locate and open the Windows Firewall configuration dialog.
- 3 Click **Allow a program or feature through Windows Firewall**.
- 4 Check **Windows Management Instrumentation (WMI)**.

Configuring the firewall on multiple domain computers with a group policy

These steps assume that all the computers that you want to manage by using this policy are in the same organizational unit.

For more information about how to use a group policy, visit the following Microsoft Web site:

<http://technet.microsoft.com/en-us/windowsserver/grouppolicy/default.aspx>

These steps assume that Windows Firewall is configured to use the domain profile. The domain profile is the most typical scenario.

For more information about Windows Firewall profiles and about how Windows selects the profile to load, see the *Deploying Windows Firewall Settings for Microsoft Windows XP with Service Pack 2* guide.

To obtain this guide, visit the following Microsoft Web site:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=4454e0e1-61fa-447a-bdcd-499f73a637d1&DisplayLang=en>

See “[Configuring the firewall to allow WMI connection](#)” on page 82.

To configure the firewall on multiple domain computers with a group policy

- 1 Create a group policy object for the organizational unit that contains the Windows XP SP2 computers that you want to manage:
 - Log on to a domain controller.
 - Click **Start > Run**, type `dsa.msc` in the **Open** dialog box, and then click **OK**.

- Expand your domain, right-click the organizational unit in which you want to create the group policy, and then click **Properties**.
 - On the **Group Policy** tab, click **New**.
 - Type a name for the group policy object, and then press **Enter**.
 - Click **Close**.
- 2 Log on to a domain-member computer that is running Windows XP SP2. Log on with a user account that is a member of one or more of the following security groups:
 - **Domain Admins**
 - **Enterprise Admins**
 - **Group Policy Creator Owners**
 - 3 Click **Start > Run**, type `mmc` in the **Open** dialog box, and then click **OK**.
 - 4 On the **File** menu, click **Add/Remove Snap-in**.
 - 5 On the **Standalone** tab, click **Add**.
 - 6 In the **Add Standalone Snap-in** dialog box, click **Group Policy**, and then click **Add**.
 - 7 In the **Select Group Policy Object** dialog box, click **Browse**.
 - 8 Click the group policy object that you want to update with the new Windows Firewall settings.

For example, click the organizational unit that contains the Windows XP SP2 computers, click **OK**, and then click the group policy object that you created in step 1.
 - 9 Click **OK**, and then click **Finish**.
 - 10 Click **Close**, and then click **OK**.
 - 11 Under **Console Root**, expand the group policy object that you selected in step 8, and then click **Computer Configuration > Administrative Templates > Network > Network Connections > Windows Firewall > Domain Profile**.
 - 12 In the right pane, double-click **Windows Firewall: Allow remote administration exception**.

- 13** Click **Enabled**, and then specify the administrative scope in the **Allow unsolicited incoming messages from** dialog box.

For example, to permit remote administration from a particular IP address, type that IP address in the **Allow unsolicited incoming messages from** dialog box. To permit remote administration from a particular subnet, type that subnet by using the Classless Internet Domain Routing (CIDR) format. In this scenario, type 192.168.1.0/24 to specify the network 192.168.1.0 with a 24-bit subnet mask of 255.255.255.0.

For more information on how to specify a valid administrative scope, see the **Syntax** area of the **Setting** tab in this policy.

- 14** Click **OK**, and then click **Exit** on the **File** menu.

Disabling simple file sharing on Windows XP SP2

This is a Windows XP limitation caused by the “ForceGuest” option that is enabled by default on all Windows XP computers that are members of a workgroup (in contrast to domain members). All users who log onto such computers over the network are forced to use the Guest account.

See “[Troubleshooting connection through the Real-Time view](#)” on page 80.

To disable simple file sharing

- ◆ Do one of the following steps:
 - Uncheck **Use simple file sharing** under the **Control Panel > Folder Options > View** tab.
 - Set the “ForceGuest” DWORD value equal to 0 (zero) under the [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa] key in the Windows registry on the client computer.
 For more information, see Microsoft knowledge base articles :
<http://support.microsoft.com/default.aspx?scid=KB;EN-US;180548>
<http://support.microsoft.com/default.aspx?scid=kb;en-us;290403>

Configuring User Access Control on Windows Vista and Windows 7

You can turn off the User Access Control (UAC) from the **Control Panel**. This applies only to the computers that are not in a domain.

For more information, see Microsoft article <http://technet.microsoft.com/en-us/windowsvista/aa905108.aspx>.

See “[Troubleshooting connection through the Real-Time view](#)” on page 80.

To configure User Access Control on Windows Vista

- 1 On the client computer with the Microsoft Windows Vista operating system, open the **Control Panel**.
- 2 Double-click **User Accounts**.
- 3 In the **User Accounts** dialog box, click **Turn User Account Control on or off**.
- 4 Uncheck **Use User Account Control (UAC) to help protect your computer**, and then click **OK**.

To configure User Access Control on Windows 7

- 1 On the client computer with the Microsoft Windows 7 operating system, open the **Control Panel**.
- 2 Click **User Accounts**.
- 3 Click **Change User Account Control settings**.
- 4 Move the slider to **Never notify**, and then click **OK**.

Technical reference

This appendix includes the following topics:

- [Dell client computers that support BIOS updates](#)
- [Dell Update Package error codes](#)

Dell client computers that support BIOS updates

You can use the **BIOS Update Job** or the **Real-Time** view to update BIOS on most Dell Precision, OptiPlex, and Latitude client computers.

See [“Updating BIOS versions”](#) on page 41.

See [“Performing one-to-one BIOS update”](#) on page 68.

For the Dell computers that are procured after 2008 and not listed in the following table, use the patch management functionality of Dell Client Manager to perform a BIOS update.

See [“Applying software patches to Dell computers”](#) on page 55.

Table B-1 Dell client computers that support BIOS updates

Precision	OptiPlex	Latitude
360	160L	X1
370	170L	XT
380	210L	110L
390	GX270	120L
450	GX280	130L
470	GX520	131L

Table B-1 Dell client computers that support BIOS updates (*continued*)

Precision	OptiPlex	Latitude
490	GX620	D400
650	320	D410
670	330	D420
690	360	D430
M20	740	D500
M50	740 Enhanced	D505
M60	745	D510
M65a	745C	D520
M70	755	D530
M90	SX270	D531
M2300	SX280	D600
M4300		D610
M6300		D620
M6400		D630
T3400		D630C
T5400		D631
T7400		D800
		D810
		D820
		D830

Dell Update Package error codes

After running Update Packages, error codes are generated. They appear in the **Dell Update Execution Details** report. The error codes help you determine and analyze the execution results after you run Update Packages.

Table B-2 Dell Update Packages error codes

Error code	Message	Description
0	SUCCESS	The update was successful.
1	UNSUCCESSFUL	An error has occurred during the update process; the update was unsuccessful.
2	REBOOT_REQUIRED	You must restart the system to apply the updates.
3	DEP_SOFT_ERROR	<p>Possible explanations are as follows:</p> <ul style="list-style-type: none"> ■ You attempted to update to the same version of the software ■ You tried to downgrade to a previous version of the software
4	DEP_HARD_ERROR	The required prerequisite software was not found on your system.
5	QUAL_HARD_ERROR	<p>The Update Package is not applicable.</p> <p>Possible explanations are as follows:</p> <ul style="list-style-type: none"> ■ The Update Package does not support the operating system. ■ The Update Package is not compatible with the devices found in your system
6	REBOOTING_SYSTEM	Restarting system.

Index

A

- alerts
 - configuring 50
 - resetting chassis intrusion alert 69
- Altiris Agent
 - about 29
 - configuring for evaluation 30
 - installing 29
 - troubleshooting installation 79
- ASF 80

B

- BIOS
 - changing password 67
 - collecting inventory 38
 - configuring settings 46, 66
 - password restrictions 25
 - updating version 41, 68
 - upgrading 41, 68
- BIOS inventory
 - collecting 38
- BIOS version inventory
 - collecting 38
- BitLocker
 - about 25
- boot order
 - configuring 67

C

- chassis intrusion alert
 - resetting 69
- collecting
 - BIOS inventory 38
 - BIOS version inventory 38
 - display inventory 39
 - hardware inventory 38
 - inventory 38
 - power scheme inventory 39
- computers
 - Dell computer summary 66

- computers (*continued*)
 - discovering 29
 - discovering Dell systems 31
 - installing Altiris Agent 29
 - installing Dell Client Manager Agent 32
 - installing Power Scheme Agent 33
 - managing one-to-many 24
 - managing one-to-one 24
 - preparing for management 27
 - restarting 34
- configuring
 - alerts 50
 - BIOS settings 46, 66
 - boot order 67
 - Dell Client Manager Agent 35
 - Dell displays settings 48
 - patch management settings 36
 - power scheme settings 49
- context-sensitive help 13

D

- DASH 80
- Dell Client Manager
 - about 11
 - how it works 12
 - installing 16
 - licensing 19
 - requirements 15
 - uninstalling 17
 - upgrading 17
- Dell Client Manager Agent
 - configuring 35
 - installing 32
 - uninstalling 18
- Dell Client Manager home page
 - about 22
- Dell Client Manager web parts 22
- Dell Management Console
 - about 21
 - viewing 21
- Dell OMCI. *See* OMCI

- Dell Update Package. *See* DUP
- discovering Dell systems 31
- discovering manageable computers 29
- display inventory
 - collecting 39
- displays
 - configuring settings 48
- documentation 13
- DUP 57
 - error codes 88

E

- EnTech SoftOSD software 12
 - installing 32

F

- filters 31
- firewall
 - configuring 82

H

- hardware inventory
 - collecting 38
- health monitoring 50
- help
 - context-sensitive 13

I

- installing
 - Dell Client Manager 16
 - Dell Client Manager Agent 32
 - Power Scheme Agent 33
- Intel AMT 80
- inventory
 - collecting 38
 - viewing 40
- IPMI 80

L

- Latitude 16, 31
- licensing
 - Dell Client Manager 19

M

- macros 47
- managing
 - multiple computers 24

- managing (*continued*)
 - single computers 24
- Microsoft Windows 7
 - viewing capable computers 52

N

- Notification Server 21

O

- OMCI 12
 - installing 32
- one-to-many
 - configuring BIOS settings 46
 - updating BIOS version 41
- one-to-many management 24
- one-to-one
 - changing BIOS password 67
 - configuring BIOS settings 66
 - configuring boot order 67
 - resetting chassis intrusion alert 69
 - updating BIOS version 68
- one-to-one management 24, 63
- OpenManage Client Instrumentation. *See* OMCI
- OptiPlex 16, 31
- Out of Band Management Component 12, 15

P

- password
 - changing BIOS password 67
- password restrictions 25
- patch management
 - configuring settings 36
 - determining patchable computers 58
 - downloading update catalog 57
 - monitoring progress 60
 - reports 61
 - staging and distributing updates 59
 - updating computers 55
 - viewing applicable updates 59
 - viewing patchable computers 59
- power scheme
 - collecting inventory 39
 - configuring settings 49
- Power Scheme Agent
 - installing 33
- Precision 16, 31
- product key 19

R

- Real-Time Console Infrastructure 12
- Real-Time view 12, 63
 - opening 64
 - troubleshooting connection via 80
- Release Notes 13
- requirements
 - Dell client computer 16
 - Dell Client Manager 15
- restarting
 - computers awaiting reboot 34
 - when restart is needed 24

S

- SNMP 80
- supported Dell computers 53
- Supported Models database 53
- Symantec Installation Manager 16–19
- Symantec Management Platform 12, 15

T

- trial license 19

U

- uninstalling
 - Dell Client Manager 17
 - Dell Client Manager Agent 18
- unsupported Dell computers 53
- updating
 - BIOS version 41, 68
- upgrading
 - BIOS 41, 68
 - Dell Client Manager 17

V

- viewing
 - Dell computer summary 66
 - inventory results 40

W

- Windows 7. *See* Microsoft Windows 7
- WMI 12, 80, 82