Dell® Client Manager 3.2 User Guide

Symantec™

Dell® Client Manager 3.2 User Guide

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

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

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

Symantec's support offerings include the following:

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

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

www.symantec.com/business/support/

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

Contacting Technical Support

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

www.symantec.com/business/support/

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

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

- Product release level

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

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

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

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

Support agreement resources

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

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

Contents

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 13
What you can do with Dell Client Manager 13
Where to get more information 13

Chapter 2 Installing Dell Client Manager 17

System requirements 17
About Dell Client Manager requirements 17
About Dell client computer requirements 18
Installing the Dell Client Manager product 18
Upgrading Dell Client Manager 19
Uninstalling Dell Client Manager 19
Uninstalling the Dell client software from client computers 20
Uninstalling Dell Client Manager from the Notification Server computer 20
Installing licenses 21

Chapter 3 Getting started with Dell Client Manager 23

About the Dell Management Console 23
About the Dell Client Manager home page 24
Dell Client Discovery and Installation Summary web part 24
About managing multiple and single computers 26
About actions that require a client restart 26
About Windows BitLocker Drive Encryption 27
About BIOS password restrictions 27

Chapter 4 Preparing target Dell computers for management 29

Preparing target Dell computers for management 29
Discovering computers 31
Installing the Symantec Management Agent 31
Configuring the Symantec Management Agent settings for evaluation use 32
Discovering Dell computers 33
Installing the Dell Client Plug-in 34
Installing the Power Scheme Agent 35
Restarting Dell client computers awaiting reboot 35
Configuring the Dell Client Plug-in settings 36
Customizing the Dell client patching settings 37

Chapter 5 Using Dell Client Manager 39

Prerequisites for using Dell Client Manager 39
Collecting BIOS, hardware, display, and power scheme settings inventory 40
Collecting BIOS settings and BIOS version inventory data 40
Collecting hardware inventory data 41
Collecting display inventory data 42
Collecting power scheme inventory data 43
Viewing BIOS settings, hardware, and power scheme settings inventory 43
Updating BIOS versions 44
Discovering current Dell BIOS versions 45
Creating a dynamic filter and a BIOS Update Job 45
Viewing the BIOS update job execution status 47
Viewing the BIOS Update Job execution reports 48
Configuring BIOS settings 48
Using reports to configure BIOS settings 50
Collecting BIOS settings inventory 51
Creating a dynamic filter and a BIOS Settings Job 51
Viewing the BIOS settings job execution status 53
Viewing the BIOS settings job execution reports 53
Configuring Dell display settings 54
Changing brightness and contrast settings 54
Restoring display factory default settings 54
Turning off displays 55
Configuring power scheme settings 55
Monitoring the health of a computer 56
Viewing alerts 57

Assessing Microsoft Windows 7 migration readiness 58
Updating the Dell Supported Models database 59

Chapter 6 Applying software patches to Dell computers 61

Applying software patches to Dell computers 61
Downloading the Dell Update Packages catalog 63
Determining patchable Dell client computers 64
Viewing patchable Dell client computers 65
Viewing applicable updates 65
Staging and distributing updates 65
Monitoring update progress 66
Using reports to view patch management data 66

Chapter 7 Managing individual Dell computers 69

About managing individual Dell computers 69
Modifying the connection profile for real-time management 71
Accessing the Real-Time view 71
About the Real-Time Home page 72
Viewing the Dell client computer summary 72
Performing one-to-one BIOS configuration 73
Performing one-to-one boot order configuration 73
Performing one-to-one BIOS or system password change 74
Resetting the chassis intrusion alert 75

Chapter 8 About Dell Client Manager pages 77

Disable BitLocker and Enable BitLocker tasks 77
BIOS Settings Job, BIOS Update Job, and Inventory Job 78
Restart Computer task 78
Update Dell Clients Patch Compliance Inventory task 79
Download Software Update Package task 79
Stage and Distribute job 79
Patch management rollout job 79
Dell Update Applicability Task 80
Dell Update Install Task 80
Patch Management Configuration page 80
Stage and Distribute Wizard 82
Inventory Job 83

Appendix A Troubleshooting Dell Client Manager 85

Troubleshooting the Symantec Management Agent push installation 85
Configuring the firewall to allow push installation 85
Troubleshooting connection through the Real-Time view 86
Configuring the firewall to allow WMI connection 88
Disabling simple file sharing on Windows XP SP2 91
Configuring User Access Control on Windows Vista and Windows 7 92

Appendix B Technical reference 93

Dell client computers that support BIOS updates 93
Dell Update Package error codes 94
About using macros for BIOS settings 95

Index 97

Chapter 1

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 a 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 3.2 release of Dell Client Manager:

- Dell Client Manager installs Dell OpenManage Client Instrumentation (OMCI) 8.0 to the client Dell computers.
- You can use reports to identify computers that need a BIOS update and create a BIOS update job directly from the report.
  See "Updating BIOS versions " on page 44.
- You can use reports to identify computers whose BIOS settings are out of compliance and create a BIOS settings job directly from the report.
  See "Using reports to configure BIOS settings" on page 50.

Products installed with Dell Client Manager

Dell Client Manager installs and uses other Symantec and Altiris management products.

Table 1-1 Products installed with Dell Client Manager

Product	Description
Symantec Management Platform	The base management platform.
Dell Client Manager	Lets you inventory and manage Dell client computers.
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.
Altiris™ Event Console	Lets you receive and view health alerts that Dell client computers send to Notification Server.

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 Plug-in software to these computers. The Dell Client Plug-in works as a link between the OMCI and EnTech software and the Symantec Management 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 Dell Management Console. You can run these tasks immediately or schedule for a later time, on one or many computers at a time.

From Dell Management Console'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 change BIOS settings, BIOS password, 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 (DUPs) 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 about and use this product.

Table 1-2 Documentation resources

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

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

Table 1-3 Symantec product information resources

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

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

Resource	Description	Location
Symantec Connect	An online resource that contains forums, articles, blogs, downloads, events, videos, groups, and ideas for users of Symantec products.	http://www.symantec.com/connect/endpoint-management

Chapter 2

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 17.
- Dell Client Plug-in installation requirements.
  See "About Dell client computer requirements " on page 18.

About Dell Client Manager requirements

Dell Client Manager requires the following:

- Symantec Management Platform 7.0 SP5

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 93.

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 Symantec Management 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:

- Symantec Management Agent
- Dell Client Plug-in
- 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 software from the client computers.	This step is required if you do not want to reinstall Dell Client Manager later. See "Uninstalling the Dell client software from client computers " on page 20.
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 20.

Uninstalling the Dell client software from client computers

The **Dell Client Software - Uninstall** policy lets you remove Dell Client Plug-in, Dell OMCI and EnTech software from supported client computers. Because the Dell Client Plug-in communicates with the Symantec Management Agent and Notification Server, you cannot run any Dell Client Manager tasks after uninstallation.

Before you uninstall the Dell client software, make sure the **Dell Client Software - Install** policy is turned off.

We recommend that you do not uninstall the Dell Client Manager software from the Notification Server computer until the **Dell Client Software - Uninstall** policy has run on all Dell computers. When Dell Client Manager is uninstalled, there is no automated way to uninstall the Dell client software.

The Dell client software uninstallation process can take some time to start, depending on the intervals that are set between the updates of the Symantec Management Agent.

See "Configuring the Symantec Management Agent settings for evaluation use " on page 32.

To uninstall the Dell Client Plug-in, Dell OMCI and EnTech software

1. In the Dell Management Console, on the **Actions** menu, click **Agents/Plug-ins > Rollout Agents/Plug-ins**.
2. In the left pane, click **Dell Client > Dell Client Software - Uninstall**.
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**.

Uninstalling Dell Client Manager from the Notification Server computer

Before uninstalling Dell Client Manager, make sure you uninstalled the Dell client software from the client computers.

See "Uninstalling the Dell client software from client computers " on page 20.

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.

Chapter 3

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 using 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 that you can perform administration tasks from wherever you are.

The console lets you set security that is specific to each console user. You specify which areas of the console a user has access to and the rights that 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.

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

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

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 the 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 23.

The Dell Client Manager home page displays the following summaries:

Dell Client Discovery and Installation Summary	Displays the Dell computer discovery and Dell Client Plug-in installation information. See "Dell Client Discovery and Installation Summary web part" on page 24.
BIOS Update Task Summary	Displays the **BIOS Update Task** execution summary. See "Updating BIOS versions " on page 44.
BIOS Settings Task Summary	Displays the **BIOS Settings Task** execution summary. See "Configuring BIOS settings " on page 48.
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 61.
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 65.

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 Plug-in 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 33.
Patchable Dell Client Computers	The total number of Dell client computers that support patching. See "Applying software patches to Dell computers " on page 61.
Dell Client Computers with Supported Displays	The total number of Dell client computers with displays that you can manage. See "Configuring Dell display settings " on page 54.
Dell Client Plug-in Installed	The total number of supported computers that successfully installed the Dell Client Plug-in. See "Installing the Dell Client Plug-in " on page 34.
Supported Dell Client Computers Awaiting Reboot to Finish Installation	The total number of supported computers that require reboot after the Dell Client Plug-in installation or upgrade. See " Restarting Dell client computers awaiting reboot " on page 35.
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 40.
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 40.
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 59.

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 40.

See "Updating BIOS versions " on page 44.

See "Configuring BIOS settings " on page 48.

See "Configuring Dell display settings " on page 54.

See "Configuring power scheme settings " on page 55.

See "Monitoring the health of a computer" on page 56.

See "Applying software patches to Dell computers " on page 61.

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 69.

About actions that require a client restart

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

- Dell OMCI software installation and upgrade as part of the Dell client software installation
  See "Installing the Dell Client Plug-in " on page 34.
- BIOS update
  See "Updating BIOS versions " on page 44.
- BIOS settings change

See “Configuring BIOS settings ” on page 48.

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 Update Job** and the **BIOS Settings Job** that are included with Dell Client Manager. These jobs include BitLocker tasks, 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 44.

See “Configuring BIOS settings ” on page 48.

About BIOS password restrictions

The BIOS passwords that 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 setting passwords and verifying passwords.

See “Updating BIOS versions ” on page 44.

See “Configuring BIOS settings ” on page 48.

Chapter 4

Preparing target Dell computers for management

This chapter includes the following topics:

- Preparing target Dell computers for management
- Discovering computers
- Installing the Symantec Management Agent
- Configuring the Symantec Management Agent settings for evaluation use
- Discovering Dell computers
- Installing the Dell Client Plug-in
- Installing the Power Scheme Agent
- Restarting Dell client computers awaiting reboot
- Configuring the Dell Client Plug-in settings
- 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 client computers. The agents include: the Symantec Management Agent, the Dell Client Plug-in, and the optional Altiris Power Scheme Agent.

See "How Dell Client Manager works " on page 13.

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 host names of the computers on which you can install the Symantec Management Agent. See "Discovering computers " on page 31.
Step 2	Install the Symantec Management Agent to the client computers.	The Symantec Management Agent lets Notification Server get information from and interact with the client computers. See "Installing the Symantec Management Agent " on page 31.
Step 3	(Optional) Configure the Symantec Management Agent settings for evaluation use.	For easier configuration and evaluation of Dell Client Manager, make the Symantec Management Agent request configuration from Notification Server more frequently. See "Configuring the Symantec Management Agent settings for evaluation use " on page 32.
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 33.
Step 5	Install the Dell Client Plug-in.	This plug-in works to communicate information between Dell client computers and the Notification Server computer See "Installing the Dell Client Plug-in " on page 34.
Step 6	(Optional) Install the Altiris Power Scheme Agent.	This agent lets you inventory and change power scheme settings. See "Installing the Power Scheme Agent" on page 35.
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 " Restarting Dell client computers awaiting reboot " on page 35.

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

Step	Action	Description
Step 8	(Optional) Configure the Dell Client Plug-in settings.	You can configure alerts, logging, and inventory refresh intervals. See " Configuring the Dell Client Plug-in settings" on page 36.

Discovering computers

Discovery lets you find the host names of the computers where you can install the Symantec Management 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 29.

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 a 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 Symantec Management Agent

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

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

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

See "Preparing target Dell computers for management" on page 29.

To install the Symantec Management Agent

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

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

Configuring the Symantec Management Agent settings for evaluation use

(Optional)

By default, the Symantec Management Agent requests new configuration from Notification Server once per hour. This means that it can take up to one hour for a rollout policy (for example, the **Dell Client Software - 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 Symantec Management 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 29.

To configure the Symantec Management Agent for evaluation use

1. In the Dell Management Console, on the **Settings** menu, click **Agents/Plug-ins > Targeted Agent Settings**.
2. In the left pane, under **Policy Name**, click the policy that applies to the computers that you want to configure. For example, click **All Desktop computers (excluding 'Site Servers')**.
3. On the **General** tab, in the **Download new configuration every** box, change the value 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.

4 In the **Upload basic inventory every** box, change the value to 15 minutes.

This forces inventory data to be sent more frequently.

5 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 Symantec Management Agent.

See “Configuring the Symantec Management Agent settings for evaluation use ” on page 32.

See “Preparing target Dell computers for management” on page 29.

To discover Dell computers

1 In the Dell Management Console, on the **Actions** menu, click **Agents/Plug-ins > Rollout Agents/Plug-ins**.

2 In the left pane, click **Dell Client > 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 Plug-in

The Dell Client Plug-in, combined with the Symantec Management Agent, works to communicate information between Dell client computers and the Notification Server computer. The Dell Client Plug-in, 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, and displays inventory, to the Notification Server computer .

The Dell Client Plug-in 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 Plug-in installed on the Dell computers in your environment, you must upgrade the agents.

See “Upgrading Dell Client Manager ” on page 19.

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

See “Configuring the Symantec Management Agent settings for evaluation use ” on page 32.

See “Preparing target Dell computers for management” on page 29.

To install the Dell Client Plug-in

1. In the Dell Management Console, on the **Actions** menu, click **Agents/Plug-ins > Rollout Agents/Plug-ins**.
2. In the left pane, click **Dell Client > Dell Client Software - Install**.
3. Under **Power Management**, specify if you want to restart the Dell client computer after the Dell Client Plug-in 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 “ Restarting Dell client computers awaiting reboot ” on page 35.
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

(Optional)

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

See "Configuring power scheme settings " on page 55.

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

See "Configuring the Symantec Management Agent settings for evaluation use " on page 32.

See "Preparing target Dell computers for management" on page 29.

To install the Power Scheme Agent

1. In the Dell Management Console, on the **Actions** menu, click **Agents/Plug-ins > Rollout Agents/Plug-ins**.
2. In the left pane, click **Power Scheme > Power Scheme Agent Install**.
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**.

Restarting Dell client computers awaiting reboot

(Optional)

You may be required to restart the Dell client computers after the Dell Client Plug-in 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 24.

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 tasks 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 Symantec Management Agent update interval. Target computers are notified of this task immediately.

See "Preparing target Dell computers for management" on page 29.

To run the restart task that is included in Dell Client Manager

1. In the Dell Management Console, on the **Manage** menu, click **Jobs and Tasks**.
2. In the left pane, click **System Job and Tasks > Dell Client > Common Tasks > Restart Computer**.
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 that 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.

Configuring the Dell Client Plug-in settings

(Optional)

You can configure some of the Dell Client Plug-in and Dell OMCI settings using the **Dell Client Plug-in Settings** policy.

See "Preparing target Dell computers for management" on page 29.

To configure the Dell Client Plug-in

1. In the Dell Management Console, on the **Home** menu, click **Dell Client Manager**.
2. In the left pane, under **Configuration Policies**, click **Dell Client Plug-in Settings**.

3 If you want OMCI to generate alert notifications, check **Notifications**.

OMCI alert notifications duplicate the notifications that are produced by Dell Client Manager, and this option is unchecked by default.

4 If you want to log alerts into the Windows Application Log on the Dell client computer, check **Logging**.

5 Under **Basic Inventory Schedule**, configure when to send Dell client computer 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**.

Customizing the Dell client patching settings

(Optional)

If you want, you can customize the Dell client patching settings to suite your needs. For example, you can change the Dell Update Packages (DUPs) download location. You can also choose to leave the default settings.

See "Preparing target Dell computers for management" on page 29.

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, under **Configuration Policies**, click **Patch Management Configuration**.

3 In the right pane, configure the settings.

See "Patch Management Configuration page " on page 80.

4 Click **Save changes**.

Chapter 5

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 settings, hardware, and power scheme settings inventory
- Updating BIOS versions
- Configuring BIOS settings
- Using reports to configure BIOS settings
- Configuring Dell display settings
- Configuring power scheme settings
- Monitoring the health of a computer
- 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 Symantec Management Agent, Dell Client Plug-in and Altiris Power Scheme Agent on Dell client computers.

See "Preparing target Dell computers for management" on page 29.

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

- See "About managing multiple and single computers " on page 26.
- See "About actions that require a client restart " on page 26.

- See "About Windows BitLocker Drive Encryption " on page 27.
- See "About BIOS password restrictions " on page 27.

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

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

- BIOS settings and BIOS version inventory
  See "Collecting BIOS settings and BIOS version inventory data " on page 40.
- Hardware inventory
  See "Collecting hardware inventory data " on page 41.
- Display settings inventory
  See "Collecting display inventory data " on page 42.
- Power scheme settings inventory
  See "Collecting power scheme inventory data " on page 43.

Collecting BIOS settings and BIOS version inventory data

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

Then you can view collected inventory in reports.

The **BIOS Inventory Task** lets you collect inventory based on the server schedule. This means that if the target computer is offline at the scheduled time, the task will not run on that computer. To collect inventory from the computers that may be offline, use the **BIOS Inventory Policy**, which uses the client task schedule.

For more information, see topics about client task schedule in the *Symantec Management Platform Help*.

See "Viewing BIOS settings, hardware, and power scheme settings inventory " on page 43.

To collect BIOS inventory data

1. In the Dell Management Console, on the **Home** menu, click **Dell Client Manager**.
2. In the left pane, under **Tasks**, click **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 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*.

To collect BIOS inventory data on the client schedule

1 In the Dell Management Console, on the **Manage** menu, click **Policies**.

2 In the left pane, click **Dell Client > Inventory Policies > BIOS Inventory Policy**.

3 Configure and turn on the policy. For more information about client task schedule, see the *Symantec Management Platform Help*.

Collecting hardware inventory data

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

Then you can view collected inventory in reports.

The **Hardware Inventory Task** lets you collect inventory based on the server schedule. This means that if the target computer is offline at the scheduled time, the task will not run on that computer. To collect inventory from the computers that may be offline, use the **Hardware Inventory Policy**, which uses the client task schedule.

For more information, see topics about client task schedule in the *Symantec Management Platform Help*.

See "Viewing BIOS settings, hardware, and power scheme settings inventory " on page 43.

To collect hardware inventory data

1 In the Dell Management Console, on the **Home** menu, click **Dell Client Manager**.

2 In the left pane, under **Tasks**, click **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*.

To collect hardware inventory data on the client schedule

1. In the Dell Management Console, on the **Manage** menu, click **Policies**.
2. In the left pane, click **Dell Client > Inventory Policies > Hardware Inventory Policy**.
3. Configure and turn on the policy. For more information, see the *Symantec Management Platform Help*.

Collecting display inventory data

You can collect configuration inventory for supported Dell displays using the **Display Inventory Task**.

Then you can view collected inventory in reports.

The **Display Inventory Task** lets you collect inventory based on the server schedule. This means that if the target computer is offline at the scheduled time, the task will not run on that computer. To collect inventory from the computers that may be offline, use the **Display Inventory Policy**, which uses the client task schedule.

For more information, see topics about client task schedule in the *Symantec Management Platform Help*.

See "Viewing BIOS settings, hardware, and power scheme settings inventory " on page 43.

To collect display inventory data

1. In the Dell Management Console, on the **Home** menu, click **Dell Client Manager**.
2. In the left pane, under **Tasks**, click **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*.

To collect display inventory data on the client schedule

1. In the Dell Management Console, on the **Manage** menu, click **Policies**.
2. In the left pane, click **Dell Client > Inventory Policies > Display Inventory Policy**.
3. Configure and turn on the policy. For more information, 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 35.

Then you can view collected inventory in reports.

See "Viewing BIOS settings, hardware, and power scheme settings inventory " on page 43.

To collect power scheme settings inventory data

1. In the Dell Management Console, on the **Home** menu, click **Dell Client Manager**.
2. In the left pane, under **Tasks**, click **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 settings, hardware, and power scheme settings inventory

You can view collected inventory in reports or in the Resource Manager. Reports show you information about all Dell computers that you have inventoried. In 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 40.

To view collected BIOS or hardware inventory in reports

1. In the Dell Management Console, on the **Reports** menu, click **All Reports**.
2. To view BIOS settings inventory, in the left pane, click **Dell Client > BIOS > Systems with Specific BIOS Setting**.
3. To view BIOS version inventory, in the left pane, click **Dell Client > BIOS > Systems with Specific BIOS Version**.
4. To view hardware inventory, in the left pane, click **Dell Client > Hardware Inventory > Systems with Specific 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 in the Resource Manager

1. In the Dell Management Console, on the **Manage** menu, click **Filters**.
2. In the left pane, click a filter, for example, click **Dell Client > Supported Dell Client Computers**.
3. In the right pane, double-click the computer for which you want to view the inventory.
4. In the Resource Manager, on the **View** menu, click **Inventory**.
5. To view the BIOS settings or hardware inventory, in the tree view pane, expand the **Dell Client Inventory** folder, and then click the node you want to get information about: for example, click **Dell Client BIOS Settings > Boot Sequence**.
6. To view the power scheme settings inventory, in the tree view 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 27.

You can use the **BIOS Update Job** to update the BIOS on most pre-2008 Dell Precision, OptiPlex, and Latitude models. For the Dell client 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 93.

See “Applying software patches to Dell computers ” on page 61.

Table 5-1 Recommended process for updating BIOS versions with the **BIOS Update Job**

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 **BIOS Inventory Task** lets you collect current BIOS versions inventory. See "Discovering current Dell BIOS versions" on page 45.
Step 3	Create a dynamic filter and a BIOS update job for the computers that you want to update.	From the **Systems with Specific BIOS Version** report you can find the computers of the specific model that need a BIOS update. Directly from the report, you can create a filter and a BIOS update job. See "Creating a dynamic filter and a BIOS Update Job" on page 45.
Step 5	(Optional) View the BIOS update job execution status.	You can view the BIOS update job that you created and its execution status. See "Viewing the BIOS update job execution status" on page 47.
Step 6	(Optional) 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 48.

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 **BIOS Inventory Task**.

See "Collecting BIOS settings and BIOS version inventory data " on page 40.

See "Updating BIOS versions " on page 44.

Creating a dynamic filter and a BIOS Update Job

You can use the **Systems with Specific BIOS Version** report to find Dell computers with the BIOS versions that require an update.

Directly from the report, you can create a dynamic filter and a BIOS update job. The dynamic filter lists the computers that require a BIOS update, based on the

criteria that you specify. Then you can run the BIOS update job on the computers that are listed in the filter.

The filter is dynamically updated – if later other Dell client computers require a BIOS update, they appear in the filter and you can run the BIOS update job using the same filter again. You don't have to update the filter manually.

The jobs that you create are located at **Manage > Job and Tasks > System Job and Tasks > Dell Client > Report Based Jobs**.

The filters that you create are located at **Manage > Filters > Dell Client > Report Based Filters**.

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 Computer** task. That is why we strongly recommend that you always use a BIOS update job to update BIOS. The BIOS update jobs are comprised of the tasks that are required for a successful BIOS update.

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 44.

To create a filter and a BIOS update job from the report

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

   For example, to update the BIOS on all Dell OptiPlex 745C computers, select **OptiPlex Desktops** and **745C**.
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.

   For example, to update the BIOS on all Dell OptiPlex 745C computers to version 1.2.2, type `1.2.2`

6 On the toolbar, click **Refresh**. Computers that need a BIOS update appear in the list.

7 Click **Create BIOS Update Job**.

8 In the **BIOS Update Job Wizard**, type a name for the new BIOS update job.

For example, if you want to update the BIOS on all Dell OptiPlex 745C computers to version 1.2.2 , type `BIOS Update Job: OptiPlex 745C to 1.2.2`

9 Click **Browse** and navigate to the location of the BIOS upgrade .exe (or extracted .hdr) file.

For example, if you want to update the BIOS on Dell OptiPlex 745C computers to version 1.2.2, browse to the `O745C-010202.EXE` file.

10 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 downgrade**.

11 Type the BIOS setup password if needed.

12 Click **Next**.

13 Type a name for the new filter that will be created.

For example, if you want to update the BIOS on all Dell OptiPlex 745C computers to version 1.2.2 , type `BIOS Update Filter: OptiPlex 745C to 1.2.2`

14 Click **Import filter**.

15 Click **Next**.

16 Configure a schedule for the BIOS update job that you created and then click **Finish**.

Viewing the BIOS update job execution status

You can view the status of the BIOS update jobs that you created using the **BIOS Update Job Wizard**.

See “Updating BIOS versions ” on page 44.

To view the BIOS update job execution status

1. In the Dell Management Console, on the **Manage** menu, click **Jobs and Tasks**.
2. In the left pane, click **System Jobs and Tasks > Dell Client > Report Based Jobs** and then click the job that you want to view.

   For example, click **BIOS Update Job: OptiPlex 745C to 1.2.2**.
3. In the right pane, under **Task Status**, double-click the job instance that you want to view. On the job status 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 24.

See "Updating BIOS versions " on page 44.

To view the job execution progress reports

1. In the Dell Management Console, on the **Reports** menu, click **All Reports**.
2. In the left pane, click **Dell Client > BIOS**.
3. Click **BIOS Update Task Execution History**.

   This report lists the computers that are associated with the task and reports their status.
4. Click **BIOS Update Task Execution Summary**.

   This report shows how many computers successfully upgraded, the number of computers yet to run the task, 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 27.

You can also create a new BIOS settings job directly from the **Systems with Specific BIOS Settings** report.

See "Using reports to configure BIOS settings" on page 50.

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 using the **BIOS Inventory Task**.

See "Collecting BIOS settings and BIOS version inventory data " on page 40.

To create and save different sets of BIOS settings to run on a different group of computers you can clone the existing **BIOS Settings Job**. You can do this by right-clicking on the task and then clicking **Clone**. When you clone a job, all its tasks are also cloned. You can also create a new **BIOS Settings Job**.

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 73.

To configure BIOS settings using the sample BIOS Settings Job

1. In the Dell Management Console, on the **Manage** menu, click **Jobs and Tasks**.
2. In the left pane, click **System Jobs and Tasks > Dell Client > BIOS Management > BIOS Settings Job**.
3. On the **BIOS Settings Job** page, double-click **Run "BIOS Settings Task Intermediate Job"**.
4. On the **BIOS Settings Task Intermediate Job** page, double-click **Run "BIOS Settings Task"**.

5 On the **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 95.

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 settings and BIOS version inventory data ” on page 40.

6 Type the BIOS setup password if needed.

See “About BIOS password restrictions ” on page 27.

7 If you want the target Dell computers to send BIOS inventory after they run the task, check **Refresh inventory on settings change**.

8 Click **Save changes**.

9 Click **Close**.

10 Click **Save changes**.

11 Click **Close**.

12 Click **Save changes**.

13 Run the job one time or on a schedule. For more information on running tasks, see the *Symantec Management Platform Help*.

Using reports to configure BIOS settings

You can create a new BIOS settings job directly from the **Systems with Specific BIOS Settings** report.

You can use this report to identify computers that have BIOS settings that you want to change. Then you can click **Create BIOS Settings Job** to create a dynamic filter and a new BIOS settings job.

The dynamic filter lists the computers that have the BIOS settings that you specified. The filter is dynamically updated – if some time later other Dell client computers are identified as requiring a change of the BIOS settings, they appear in the filter. You can re-run the same BIOS update job using the same filter again. You don't have to update the filter manually.

Table 5-2 Recommended process for using reports to configure BIOS settings

Step	Action	Description
Step 1	Get BIOS settings inventory.	The **BIOS Inventory Task** lets you collect current BIOS settings inventory. See "Collecting BIOS settings inventory" on page 51.
Step 2	Create a dynamic filter and a BIOS settings job for the computers that you want to configure.	From the **Systems with Specific BIOS Setting** report you can find the computers with the BIOS settings that you want to change. Directly from the report, you can create a filter and a BIOS settings job. See "Creating a dynamic filter and a BIOS Settings Job" on page 51.
Step 4	(Optional) View the BIOS settings job execution details.	You can view the BIOS settings job that you created and its execution status. See "Viewing the BIOS settings job execution status" on page 53.
Step 5	(Optional) View the BIOS settings job execution reports.	If you want, you can view the job execution status in the reports. See "Viewing the BIOS settings job execution reports" on page 53.

Collecting BIOS settings inventory

To gather BIOS settings inventory from the Dell client computers in your environment, you must run the **BIOS Inventory Task**.

See "Collecting BIOS settings and BIOS version inventory data " on page 40.

See "Using reports to configure BIOS settings" on page 50.

Creating a dynamic filter and a BIOS Settings Job

You can use the **Systems with Specific BIOS Setting** report to find Dell computers with the BIOS settings that are out of compliance.

Directly from this report, you can create a dynamic filter and a BIOS settings job. The dynamic filter lists the computers that have the BIOS settings that you specified in the report. Then you can run the BIOS settings job on the computers that are listed in the filter and change BIOS settings. Using this dynamic filter ensures that the BIOS settings job runs only on the computers that need a change.

The filter is dynamically updated – if later other Dell client computers require a BIOS settings change, they appear in the filter. You can run the same BIOS settings job using the same filter again. You don't have to update the filter manually.

See "Using reports to configure BIOS settings" on page 50.

To create a filter and a BIOS settings job from the report

1. In the Dell Management Console, on the **Reports** menu, click **All Reports**.
2. In the left pane, click **Dell Client > BIOS > Systems with Specific BIOS Setting**.
3. In the report, under **Parameters**, select the product line and the model for which you want to change BIOS settings.

   For example, to update BIOS settings on all Dell OptiPlex 745C computers, select **OptiPlex Desktops** and **745C**.
4. Click **Change parameters**.
5. In the **Select Settings** dialog, select the settings that you want to modify.

   For example, if you want to find computers that have IDE controller disabled, under **Drives**, in the **IDE controller** drop-down list, click **Disable**.
6. Click **OK**.
7. On the toolbar, click **Refresh**. Computers that need a change in the BIOS settings appear in the list.
8. Click **Create BIOS Settings Job**.
9. In the **BIOS Settings Job Wizard**, type a name for the new BIOS settings job.

   For example, if you want to change the IDE controller settings on all Dell OptiPlex 745C computers, type `BIOS Settings Job: OptiPlex 745C, Enable IDE`
10. Configure the settings that you want to apply to target Dell client computers.

    For example, if you want to enable the IDE controller, change the **IDE controller** property to **Auto**.
11. Type the BIOS setup password if needed.
12. Click **Next**.
13. Type a name for the new filter.

    For example, if you want to change the IDE controller settings on all Dell OptiPlex 745C computers, type `BIOS Settings Filter: OptiPlex 745C with IDE disabled`
14. Click **Import filter**.

15 Click **Next**.

16 Configure a schedule for the BIOS update job that you created and then click **Finish**.

Viewing the BIOS settings job execution status

You can view the status of the BIOS settings jobs that you created using the **BIOS Settings Job Wizard**.

See "Using reports to configure BIOS settings" on page 50.

To view the BIOS update job execution status

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

2 In the left pane, click **System Jobs and Tasks > Dell Client > Report Based Jobs** and then click the job that you want to view.

For example, click **BIOS Settings Job: OptiPlex 745C, Enable IDE**.

3 In the right pane, under **Task Status**, double-click the job instance that you want to view. On the job status 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 settings job execution reports

You can view the status of the BIOS settings 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 24.

See "Using reports to configure BIOS settings" on page 50.

To view the job execution progress reports

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

2 In the left pane, click **Dell Client > BIOS**.

3 Click **BIOS Settings Task Execution History**.

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

4 Click **BIOS Settings Task Execution Summary**.

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

Configuring Dell display settings

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

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

See "Collecting display inventory data " on page 42.

See "Changing brightness and contrast settings " on page 54.

See "Restoring display factory default settings " on page 54.

See "Turning off displays " on page 55.

Changing brightness and contrast settings

You can change brightness and contrast settings of supported Dell displays.

See "Configuring Dell display settings " on page 54.

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, under **Tasks**, click **Change Display 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 supported Dell displays.

See "Configuring Dell display settings " on page 54.

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, under **Tasks**, click **Restore Display 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 supported Dell displays.

See "Configuring Dell display settings " on page 54.

To turn off displays

1. In the Dell Management Console, on the **Home** menu, click **Dell Client Manager**.
2. In the left pane, under **Tasks**, click **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 43.

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

See "Installing the Power Scheme Agent" on page 35.

To configure power scheme settings

1. In the Dell Management Console, on the **Home** menu, click **Dell Client Manager**.
2. In the left pane, under **Tasks**, click a power scheme. For example, click **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 the health of a computer

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 Plug-in 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 Plug-in software that is installed on the Dell client computers.

See "Viewing alerts" on page 57.

To enable health monitoring

1 In the Dell Management Console, on the **Home** menu, click **Dell Client Manager**.

2 In the left pane, under **Configuration Policies**, click **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 27.

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 Alert Notification** task rule runs. This rule executes the **Dell Client 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 tool tip help.

7 (Optional) To display a pop-up 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 tool tip 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 the health of a computer" on page 56.

To view the Systems Triggering Alerts report

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

2 In the left pane, click **Dell Client > 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 Events > Dell Client 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 inventory data ” on page 41.

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.

Table 5-3 Windows 7 migration readiness reports in Dell Client Manager *(continued)*

Report	Description
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 **Reports** menu, click **All Reports**.
2. Click **Dell Client > 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, under **Configuration Policies**, click **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**.

Chapter 6

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.

See "Dell client computers that support BIOS updates" on page 93.

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 **Manage > Jobs and Tasks > System Jobs and Tasks > Dell Client > 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 29.

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 63.
Step 2	Determine which Dell computers support patching.	The **Determine Patchable Dell Clients** policy can detect the computers that support patching and the updates that they require. See "Determining patchable Dell client computers" on page 64.
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 65.
Step 4	View the updates that need to be installed.	You can use reports to view the updates. See "Viewing applicable updates" on page 65.
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 65.
Step 6	Monitor the update progress.	You can watch the rollout jobs that are running and their status. See "Monitoring update progress " on page 66.

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

Step	Action	Description
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 66.

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 61.

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, under **Getting Started**, click **Enable 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 client computers that are known to Dell Client Manager.

See "Discovering Dell computers " on page 33.

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 61.

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, under **Getting Started**, click **Enable Patch Management > Step 3. Determine Patchable Dell Clients**.

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 **Manage** menu, click **Policies**.

2 In the left pane, click **Dell Client > 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 61.

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, under **Getting Started**, click **Enable Patch Management > Step 4. View Patchable Dell Clients**.

Viewing applicable updates

You can view any applicable updates and computers that require an update in reports.

See "Applying software patches to Dell computers " on page 61.

To view applicable updates

1. In the Dell Management Console, on the **Home** menu, click **Dell Client Manager**.
2. In the left pane, under **Getting Started**, click **Enable 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 Client 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 63.

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 61.

To stage and distribute updates

1. In the Dell Management Console, on the **Home** menu, click **Dell Client Manager**.
2. In the left pane, under **Getting Started**, click **Enable 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 "Stage and Distribute Wizard " on page 82.
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 61.

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, under **Getting Started**, click **Enable 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 Dell Client Manager home page.

See "About the Dell Client Manager home page " on page 24.

See "Applying software patches to Dell computers " on page 61.

To view Dell client patch management reports

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

Chapter 7

Managing individual Dell computers

This chapter includes the following topics:

- About managing individual Dell computers
- Modifying the connection profile for real-time management
- Accessing the Real-Time view
- About the Real-Time Home 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 or system password change
- Resetting the 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 71.

If you want to manage a computer that is running Microsoft Windows Vista or Windows 7, we recommend that you modify the connection profile before you open the **Real-Time** view.

See “Modifying the connection profile for real-time management” on page 71.

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 72.
- 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 73.
- Change boot order
  See "Performing one-to-one boot order configuration " on page 73.
- Change BIOS password
  See "Performing one-to-one BIOS or system password change " on page 74.

Modifying the connection profile for real-time management

If you want to manage Dell client computers with Microsoft Windows Vista or Windows 7, you must enable the packet privacy authentication in the connection profile.

To enable the packet privacy authentication

1. In the Dell Management Console, on the **Settings** menu, click **All Settings**.
2. In the left pane, click **Monitoring and Alerting > Protocol Management > Connection Profiles > Manage Connection Profiles.**.
3. In the right page, click the profile that you want to use.
4. On the toolbar, click the **Edit selected connection profile** symbol.
5. In the **Define Group Settings** dialog, in the **WMI** section, check **Use authentication level**, and then in the **Authentication level** drop-down click **Packet Privacy**.
6. Click **OK**.

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 **Manage** menu, click **Filters**.
2. Click a filter.

   For example, click **Dell Client > Supported Dell Client Computers**.
3. In the right pane, double-click the computer that you want to manage.
4. In the Resource Manager, on the **View** menu, click **Real-Time**.
5. In the tree view pane, click **Real-Time Consoles**.

   See "About the Real-Time Home page" on page 72.

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 tree view pane, click **Real-Time Consoles**.

   See "About the Real-Time Home page" on page 72.

About the Real-Time Home page

The **Real-Time Home** page is the first page in the Resource Manager's **Real-Time** view tree. It displays the connection information for the computer. This page displays the list of protocols that the target computer supports, and if the target computer accepts the connection credentials that you provided. The protocols include WMI, ASF, DASH, Intel AMT, IPMI, and SNMP. Only the protocols that are turned on in the connection profile are displayed.

If credentials are displayed as invalid, verify that your connection profile is configured to use the correct credentials.

Under **Supported protocols**, you can select, add, or modify the connection profile that you want to use when connecting to the target computer.

For more information, view topics about connection profiles in the *Symantec Management Platform Help*.

See "Troubleshooting connection through the Real-Time view" on page 86.

Viewing the Dell client computer summary

You can view the summary information about a resource on the **Dell Client 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 Summary page

1. Open the Resource Manager.

   See "Accessing the Real-Time view " on page 71.

2. In the Resource Manager, on the **Summaries** menu, click **Dell Client 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 48.

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

See "About Windows BitLocker Drive Encryption " on page 27.

See "About managing individual Dell computers " on page 69.

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 71.

2. In the tree view pane, click **Real-Time Consoles > Dell Client > General Configuration > BIOS Settings**.
3. If the client computer requires a BIOS setup password, type it.

   See "About BIOS password restrictions " on page 27.

4. If you want to restart the target Dell computer after changing the settings, check **Choose if you would like to reboot client after successful settings change**.
5. Configure BIOS settings.
6. Click **Accept**.

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 27.

See "About managing individual Dell computers " on page 69.

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 71.
2. In the tree view pane, click **Real-Time Consoles > Dell Client > General Configuration > Boot Order**.
3. Set the boot order for each of the bootable devices.
4. Click **Accept**.

Performing one-to-one BIOS or system password change

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

See "About BIOS password restrictions " on page 27.

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

See "About Windows BitLocker Drive Encryption " on page 27.

See "About managing individual Dell computers " on page 69.

To change the 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 71.
2. In the tree view pane, click **Real-Time Consoles > Dell Client > Management Tasks > Change BIOS Password**.
3. Type the current and the new BIOS passwords.
4. Click **Accept**.

To change the system 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 71.
2. In the tree view pane, click **Real-Time Consoles > Dell Client > Management Tasks > Change System Password**.
3. Type the current and the new system passwords.
4. Click **Accept**.

Resetting the 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 27.

See "About managing individual Dell computers " on page 69.

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 71.

2. In the tree view pane, click **Real-Time Consoles > Dell Client > General Configuration > BIOS Settings**.
3. If a chassis intrusion alert has been activated, the **Chassis Intrusion Status** property value displays **Tripped**. Clear the alert by changing it to **Trip reset**.
4. Click **Accept**.

Chapter 8

About Dell Client Manager pages

This chapter includes the following topics:

- Disable BitLocker and Enable BitLocker tasks
- BIOS Settings Job, BIOS Update Job, and Inventory Job
- Restart Computer task
- Update Dell Clients Patch Compliance Inventory task
- Download Software Update Package task
- Stage and Distribute job
- Patch management rollout job
- Dell Update Applicability Task
- Dell Update Install Task
- Patch Management Configuration page
- Stage and Distribute Wizard
- Inventory Job

Disable BitLocker and Enable BitLocker tasks

This task is an internal client task that is used by the Dell Update Package (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 27.

See “Updating BIOS versions ” on page 44.

See “Configuring BIOS settings ” on page 48.

See “Applying software patches to Dell computers ” on page 61.

BIOS Settings Job, BIOS Update Job, and Inventory Job

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

See “Configuring BIOS settings ” on page 48.

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

See “Updating BIOS versions ” on page 44.

The **Inventory Job** lets you collect BIOS, hardware, display, and patch compliance inventory.

See “Inventory Job” on page 83.

Restart Computer task

This task is an internal client task that is used by the Dell Update Package (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 61.

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

See “Updating BIOS versions ” on page 44.

See “Configuring BIOS settings ” on page 48.

We recommend that you do not modify this task. If you want to turn on , turn 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*.

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 Dell Update Packages (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 64.

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 61.

Download Software Update Package task

This task is an internal server task that runs when you stage a Dell Update Package (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 "Stage and Distribute job " on page 79.

See "Applying software patches to Dell computers " on page 61.

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 65.

See "Applying software patches to Dell computers " on page 61.

Patch management rollout job

This job is an internal client job that distributes and installs Dell Update Packages (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 65.

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 61.

Dell Update Applicability Task

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

See "Applying software patches to Dell computers " on page 61.

Dell Update Install Task

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

See "Applying software patches to Dell computers " on page 61.

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 61.

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.

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

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

Table 8-2 Options on the Advanced tab

Option	Description
Delete packages after	Lets you specify when to delete software update packages that are no longer needed.

Table 8-2 Options on the Advanced tab *(continued)*

Option	Description
Allow Package Server distribution	Ensures that package servers process all of the software update packages. For more information, see the *Symantec Management Platform Help*. Default: checked.
Use alternate download location on Package Server	Lets you specify a different location for packages on a package server.
Use alternate download location on client	Lets you specify a different location for packages on managed computers.

Table 8-3 Options on the Programs tab

Option	Description
Run with rights	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. Default: **System Account**.
Program can run	Specify the conditions under which the program can run. Default: **Whether or not a user is logged on**.
Terminate after	Specifies the time to terminate software update tasks at. Default: 20 minutes
Agent Events	Lets you choose to send the relevant events from managed computers to Notification Server.

Stage and Distribute Wizard

This wizard lets you create 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 61.

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

Option	Description
Reboot if required	Lets you choose to restart the target computer after installing DUPs.
Allow downgrade	Lets you choose to install a DUP that has been superseded.
Disable and Enable BitLocker for BIOS Updates	Specifies to include BitLocker detection tasks into the update rollout job. 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. See "About Windows BitLocker Drive Encryption " on page 27.
Schedule	Specifies a schedule on which 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.

Inventory Job

This job lets you collect BIOS settings, display settings, and hardware inventory from the Dell client computers. This job also includes a task that lets you determine if the target Dell client computer supports automated patching.

See "Collecting BIOS, hardware, display, and power scheme settings inventory " on page 40.

See "Applying software patches to Dell computers " on page 61.

Appendix A

Troubleshooting Dell Client Manager

This appendix includes the following topics:

- Troubleshooting the Symantec Management Agent push installation
- Troubleshooting connection through the Real-Time view

Troubleshooting the Symantec Management Agent push installation

If you receive a "No network provider accepted the given network path" error when push installing the Symantec Management Agent to a Microsoft Windows XP SP2, Windows Vista, or Windows 7 computer, the following issues can be causing the error:

- Windows firewall
  See "Configuring the firewall to allow push installation" on page 85.
- Simple file sharing enabled (Windows XP SP2)
  See "Disabling simple file sharing on Windows XP SP2" on page 91.
- User Account Control is enabled (Windows Vista, Windows 7)
  See "Configuring User Access Control on Windows Vista and Windows 7" on page 92.

Configuring the firewall to allow push installation

To push the Symantec Management 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 Symantec Management Agent push installation " on page 85.

To configure the firewall for the Symantec Management 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

Some of the reasons why Dell Client Manager cannot establish a real-time connection with the target computer are listed in the following table.

Table A-1 Possible reasons of real-time connection errors

Technology	Possible reasons
WMI	The connection credentials are incorrect. The computer is turned off . The operating system is not loaded. The computer is not connected to the network. The firewall does not allow incoming WMI connections. See "Configuring the firewall to allow WMI connection" on page 88. Simple file sharing is enabled. See "Disabling simple file sharing on Windows XP SP2" on page 91. **User Access Control** is turned on. See "Configuring User Access Control on Windows Vista and Windows 7" on page 92. You are connecting to Microsoft Windows XP Home Edition, where WMI remote connection is not available. You are connecting with a user that has an empty password.

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

Technology	Possible reasons
ASF	The connection credentials are incorrect. ASF is turned on in the BIOS but not configured. For more information on configuring computers with ASF, see the *Out of Band Management Component Implementation Guide*. ASF is turned off in the BIOS. The computer is not connected to the network. The target computer is not ASF capable.
Intel AMT	The connection credentials are incorrect. The Intel AMT device is not configured. For more information on configuring computers with Intel AMT, see the *Out of Band Management Component Implementation Guide*. The Intel AMT device is in secure mode, but the connection profile is not configured to use the correct certificates, and vice versa. For more information on configuring connection profiles, see the *Symantec Management Platform Help*. Intel AMT is turned off in the BIOS. The computer is not connected to the network. The computer is not Intel AMT capable.
DASH	The connection credentials are incorrect. DASH is turned on in the BIOS but not configured. For more information on configuring computers with DASH, see the *Out of Band Management Component Implementation Guide*. DASH is turned off in the BIOS. The computer is not connected to the network. The target computer is not DASH capable.

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

Technology	Possible reasons
IPMI	The connection credentials are incorrect. The IPMI device is not configured. The IPMI device is in secure mode, but the connection profile is not configured to use the correct certificates. IPMI is turned off in the BIOS. The computer is not connected to the network. The target computer is not IPMI capable.
SNMP	The SNMP community string is incorrect. SNMP is not installed on the target computer. The SNMP service is not running on the target computer. The Notification Server computer is not in the list of hosts to accept the SNMP packets from. Check SNMP service properties.

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 89.
- 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 89.
- Temporarily disable the firewall.

See "Troubleshooting connection through the Real-Time view" on page 86.

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 88.

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 88.

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 86.

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 86.

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**.

Appendix B

Technical reference

This appendix includes the following topics:

- Dell client computers that support BIOS updates
- Dell Update Package error codes
- About using macros for BIOS settings

Dell client computers that support BIOS updates

You can use the **BIOS Update Job** or the **Real-Time** view to update BIOS on most pre-2008 Dell Precision, OptiPlex, and Latitude client computers.

See "Updating BIOS versions " on page 44.

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 61.

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 Dell Update Packages (DUPs), 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	Possible explanations are as follows: ■ 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	The Update Package is not applicable. Possible explanations are as follows: ■ 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.

About using macros for BIOS settings

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

See “Configuring BIOS settings ” on page 48.

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 B-3 Macros that Dell Client Manager supports

Macro	Description
%username%	The name of the user that is logged on.
%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.

Index

A

alerts
- configuring 56
- resetting the chassis intrusion alert 75

ASF 86

B

BIOS
- changing password 74
- collecting inventory 40
- configuring settings 48, 50, 73
- password restrictions 27
- updating version 44
- upgrading 44

BIOS inventory
- collecting 40

BIOS password
- changing 74

BIOS version inventory
- collecting 41

BitLocker
- about 27

boot order
- configuring 73

C

chassis intrusion alert
- resetting 75

collecting
- BIOS inventory 40
- BIOS version inventory 41
- display inventory 42
- hardware inventory 41
- inventory 40
- power scheme inventory 43

computers
- Dell computer summary 72
- discovering 31
- discovering Dell systems 33
- installing Dell Client Plug-in 34

computers *(continued)*
- installing Power Scheme Agent 35
- installing Symantec Management Agent 31
- managing one-to-many 26
- managing one-to-one 26
- preparing for management 29
- restarting 35

configuring
- alerts 56
- BIOS settings 48, 73
- BIOS settings from reports 50
- boot order 73
- connection profile 71
- Dell Client Plug-in 36
- Dell displays settings 54
- packet privacy 71
- patch management settings 37
- power scheme settings 55

connection profile 71

context-sensitive help 13

D

DASH 86

Dell Client Manager 11–13. *See* Dell Client Manager
- about 11
- how it works 13
- installing 18
- licensing 21
- requirements 17
- uninstalling 19
- upgrading 19

Dell Client Manager Agent. *See* Dell Client Plug-in

Dell Client Manager home page
- about 24

Dell Client Manager web parts 24

Dell Client Plug-in
- configuring 36
- installing 34
- uninstalling 20

Dell Management Console
- about 23

Dell Management Console *(continued)*
viewing 23
Dell OMCI. *See* OMCI
Dell Update Package. *See* DUP
discovering Dell systems 33
discovering manageable computers 31
display inventory
collecting 42
displays
configuring settings 54
documentation 13
DUP 63
error codes 94

E

EnTech SoftOSD software 13
installing 34
Event Console 12

F

filters 33
firewall
configuring 88

H

hardware inventory
collecting 41
health monitoring 56
help
context-sensitive 13

I

installing
Dell Client Manager 18
Dell Client Plug-in 34
Power Scheme Agent 35
Intel AMT 86
inventory
collecting 40
viewing 43
IPMI 86

L

Latitude 18, 33
licensing
Dell Client Manager 21

M

macros 95
managing
multiple computers 26
single computers 26
Microsoft Windows 7
viewing capable computers 58

N

Notification Server 23

O

OMCI 13
installing 34
one-to-many
configuring BIOS settings 48, 50
updating BIOS version 44
one-to-many management 26
one-to-one
changing BIOS password 74
changing system password 74
configuring BIOS settings 73
configuring boot order 73
resetting the chassis intrusion alert 75
one-to-one management 26, 69
OpenManage Client Instrumentation. *See* OMCI
OptiPlex 18, 33
Out of Band Management Component 12, 17

P

packet privacy 71
password
changing BIOS password 74
changing system password 74
password restrictions 27
patch management
configuring settings 37
determining patchable computers 64
downloading update catalog 63
monitoring progress 66
reports 66
staging and distributing updates 65
updating computers 61
viewing applicable updates 65
viewing patchable computers 65
power scheme
collecting inventory 43
configuring settings 55

Power Scheme Agent
installing 35
Power Scheme Task 12
Precision 18, 33
product key 21

R

Real-Time Console Infrastructure 12
Real-Time Home page 72
Real-Time view 13, 69
opening 71
troubleshooting connection via 86
Release Notes 13
requirements
Dell client computer 18
Dell Client Manager 17
restarting
computers awaiting reboot 35
when restart is needed 26

S

SNMP 86
supported Dell computers 59
Supported Models database 59
Symantec Installation Manager 18–21
Symantec Management Agent
about 31
configuring for evaluation 32
installing 31
troubleshooting installation 85
Symantec Management Platform 12, 17
system password
changing 74

T

trial license 21

U

uninstalling
Dell Client Manager 19
Dell Client Plug-in 20
unsupported Dell computers 59
updating
BIOS version 44
upgrading
BIOS 44
Dell Client Manager 19

V

viewing
Dell computer summary 72
inventory results 43

W

Windows 7. *See* Microsoft Windows 7
WMI 13, 86, 88