Dell® Client Manager 3.0

User's Guide

Notice

Dell® Client Manager 3.0

Document Date: January 21, 2009

Special thanks to the following individuals and groups that contributed significantly to Dell Client Manager:

James Lathan and the Dell Client Technologists; The Dell Systems Engineers; Joe Kozlowski, Dell Customer Support; Kevin Winert, Dell OpenManage Product Marketing; Steven Breed, Dell Software Engineering.

Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014
http://www.symantec.com

Contents

Chapter 1
Introducing Dell Client Manager

This chapter includes the following topics:

About Dell Client Manager

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

Dell Client Manager is a suite of integrated tools that are developed by Dell and Symantec. These combined technologies work under the Symantec Management Platform infrastructure. You manage Dell resources across your network using a single, integrated, and secure Dell Management Console.

What's new in Dell Client Manager

The following new features are introduced in the 3.0 SP1 release of Dell Client Manager:

- It is now possible to upload the BIOS update file using the Symantec Management Console that is opened on a computer, other than the Notification Server computer.
- A Power Scheme Settings report has been added. This report lets you view the list of computers whose power scheme settings do not follow your company's energy policies.

Products installed with Dell Client Manager

The following table shows the Altiris management products that are installed and used with Dell Client Manager:

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

How Dell Client Manager works

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

Dell Client Manager can also connect to a target Dell computer directly through WMI and query OMCI for inventory and configuration information and display this information in the Symantec Management Console's Resource Manager, in the Real-Time view.

What you can do with Dell Client Manager

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

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

Where to get more information

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

Document	Description	Location
Release Notes	Information about new features and important issues. This information is available as an article in the Altiris Knowledge Base.	http://kb.altiris.com/ You can search for the product name under Release Notes.
User's Guide	Information about how to use this product, including detailed technical information and instructions for performing common tasks. This information is available in PDF format.	• 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 • The Context command, which is available in the Symantec Management Console on the Help menu.

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

Resource	Description	Location
Altiris Knowledgebase	Articles, incidents, and issues about Altiris products.	http://kb.altiris.com/
Altiris Juice	An online magazine that contains best practices, tips, tricks, and articles for users of Altiris products.	http://www.altiris.com/juice/dell/
Online Forums	Forums for users of Altiris products.	http://forums.altiris.com/

Chapter 2
Installing Dell Client Manager

This chapter includes the following topics:

System requirements

Dell Client Manager has the following system requirements:

- Dell Client Manager installation requirements.
  See *About Dell Client Manager requirements* on page 9.
- Dell Client Manager Agent installation requirements.
  See *About Dell client computer requirements* on page 9.

About Dell Client Manager requirements

Dell Client Manager requires the following:

- Symantec Management Platform 7.0 SP1

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 7.

Dell Client Manager installs Out of Band Management Component on the 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*.

About Dell client computer requirements

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

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

The Dell Client Manager Agent requires the following:

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

Supported languages are English, French, German, Japanese, Simplified Chinese, Spanish, and Portuguese.

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.

Uninstalling Dell Client Manager

To uninstall Dell Client Manager perform the following steps:

Step	Action	Description
Step 1	Uninstall the Dell Client Manager Agent from the client computers.	This step is required if you do not want to reinstall Dell Client Manager later. See *Uninstalling the Dell Client Manager Agent from client computers* on page 10.
Step 2	Uninstall Dell Client Manager from the Notification Server.	This step removes the product from the Notification Server. See *Uninstalling Dell Client Manager from the Notification Server computer* on page 11.

Uninstalling the Dell Client Manager Agent from client computers

The Dell Client Manager Agent, Dell OMCI, and EnTech SoftOSD Software Uninstall task lets you remove all Dell Client Manager components from supported client computers. Because the Dell Client Manager Agent communicates with the Altiris Agent and Notification Server, and the Dell OMCI software is used to communicate with the Dell Client Manager Agent, you cannot run any Dell Client Manager tasks after uninstallation.

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

See *(Optional) Configuring the Altiris Agent settings for evaluation use* on page 16.

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

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

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

Uninstalling Dell Client Manager from the Notification Server computer

Use Symantec Installation Manager to uninstall Dell Client Manager.

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

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 on licensing, see the Symantec Installation Manager documentation.

Chapter 3
Getting started with Dell Client Manager

This chapter includes the following topics:

About the Dell Management Console

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

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

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

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

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

About the Dell Client Manager home page

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

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

See *About the Dell Management Console* on page 12.

The Dell Client Manager home page displays the following summaries:

- Dell Client Discovery and Installation Summary
- BIOS Update Task Summary
- BIOS Settings Task Summary

Dell Client Discovery and Installation Summary displays the following summary information:

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 17.
Dell Client Manager Agent Installed	The total number of supported computers that successfully installed the Dell Client Manager Agent. See *Installing the Dell Client Manager Agent* on page 17.
Supported Dell Client Computers Awaiting Reboot to Finish Installation	The total number of supported computers that require reboot after the Dell Client Manager Agent installation or upgrade. See *(Optional) Restarting Dell client computers awaiting reboot* on page 19.
Computers 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 23.
Computers 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 23.
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 39.

Chapter 4
Preparing target Dell computers for management

This chapter includes the following topics:

Preparing target Dell computers for management

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

See *How Dell Client Manager works* on page 6.

The following is the recommended way of preparing target computers for management:

Step	Action	Description
Step 1	Discover manageable computers in your environment.	Discovery helps you find the hostnames of the computers where you can install the Altiris Agent to. See *Discovering computers* on page 15.
Step 2	Install the Altiris Agent to the client computers.	The Altiris Agent lets the Notification Server get information from and interact with the client computers. See *Installing the Altiris Agent* on page 16.
Step 3	(Optional) Configure the Altiris Agent settings for evaluation use.	For easier configuration and evaluation of Dell Client Manager, make the Altiris Agent request configuration from the Notification Server more frequently. See *(Optional) Configuring the Altiris Agent settings for evaluation use* on page 16.

Step	Action	Description
Step 4	Discover Dell computers.	The Dell Client Discovery policy lets you find Dell computers that are supported by Dell Client Manager. See *Discovering Dell computers* on page 17.
Step 5	Install the Dell Client Manager Agent.	You must install this agent to supported Dell computers in your environment. See *Installing the Dell Client Manager Agent* on page 17.
Step 6	Install the Altiris Power Scheme Agent.	This agent lets you inventory and change power scheme settings. See *Installing the Altiris Power Scheme Agent* on page 18.
Step 7	(Optional) Restart the computers awaiting reboot.	Some computers need to be restarted in order for the Dell management software to work. See which computers need to be restarted and run the restart task. See *(Optional) Restarting Dell client computers awaiting reboot* on page 19.
Step 8	(Optional) Configure the Dell Client Manager Agent.	You can configure alerts, logging, and inventory refresh intervals. See *(Optional) Configuring the Dell Client Manager Agent* on page 20.

Discovering computers

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

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

See *Preparing target Dell computers for management* on page 14.

To discover computers

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

Installing the Altiris Agent

The Altiris Agent is a program that you install on the computers you want to manage, allowing the Symantec Management Platform and solutions to get information from and interact with your computers. The agent enables computers to receive configuration information from and send data to the Notification Server and helps download packages as well as tasks and jobs. The agent lets you change settings on the managed computer and install and manage various solution-specific plug-ins.

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

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

See *Preparing target Dell computers for management* on page 14.

To install the Altiris Agent

1. In the Dell Management Console, on the Actions menu, click **Agents/Plug-ins > Push Altiris Agent**.
2. On the Altiris Agent Installation page, install the Altiris Agent to computers in your environment.
   For more information on how to install the Altiris Agent, see the *Symantec Management Platform Help* (Press **F1** or click **Help > Context** in the Dell Management Console).

(Optional) Configuring the Altiris Agent settings for evaluation use

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

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

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

See *Preparing target Dell computers for management* on page 14.

To configure the Altiris Agent for evaluation use

1. In the Dell Management Console, on the Settings menu, click **Agents/Plug-ins > Targeted Agent Settings**.
2. In the Policy Name field, select the policy that applies to the computers you want to configure, for example: All Desktop computers (excluding 'Package servers').
3. Click the **General** tab if it is not already selected.
4. Change the value in the **Download new configuration every** field to 5 minutes. This forces the agent to check more frequently for changes so you can see the results of the changes you make more quickly.
5. Change the value in the **Upload basic inventory every** field to 15 minutes. This forces inventory data to be sent more frequently.

6. Click **Save changes**.

Discovering Dell computers

You can determine if the computer is manufactured by Dell by using the Dell Client Discovery policy. This policy collects hardware inventory information and reports it to the 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
- <Model> Computers

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

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

See *(Optional) Configuring the Altiris Agent settings for evaluation use* on page 16.

See *Preparing target Dell computers for management* on page 14.

To enable the Dell Client Discovery Policy

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

Installing the Dell Client Manager Agent

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

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

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

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

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

See *(Optional) Configuring the Altiris Agent settings for evaluation use* on page 16.

See *Preparing target Dell computers for management* on page 14.

To install the Dell Client Manager Agent

1. In the Dell Management Console, on the Home menu, click **Dell Client Manager**.
2. In the left pane, click **Dell Client Manager Agent Install > Dell Client Manager Agent - Install (32-bit)**.
3. Under Power Management, specify if you want to restart the Dell client computer after the Dell Client Manager Agent installation. Restart may be required for the OMCI software to work. If you do not want to restart the computer right after the task, you may do it later on a schedule.
   See *(Optional) Restarting Dell client computers awaiting reboot* on page 19.
4. Turn on the policy (To turn on the policy, at the upper right of the page, click the colored circle, and then click **On**).
5. Click **Save changes**.

To upgrade the Dell Client Manager Agent

1. In the Dell Management Console, on the Home menu, click **Dell Client Manager**.
2. In the left pane, click **Dell Client Manager Agent Install > Dell Client Manager Agent - Upgrade (32-bit)**.
3. Under Power Management, specify if you want to restart the Dell client computer after the Dell Client Manager Agent installation. Restart may be required for the OMCI software to work. If you do not want to restart the computer right after the task, you may do it later on a schedule.
   See *(Optional) Restarting Dell client computers awaiting reboot* on page 19.
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 Altiris Power Scheme Agent

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

See *Configuring power scheme settings* on page 32.

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

See *(Optional) Configuring the Altiris Agent settings for evaluation use* on page 16.

See *Preparing target Dell computers for management* on page 14.

To install the Altiris Power Scheme Agent

1. In the Dell Management Console, on the Home menu, click **Dell Client Manager**.
2. In the left pane, click **Quick Start > Section 2. Enable Hardware Management > Step 4. Configure Agents for Power Schemes Management**.
3. Turn on the policy (To turn on the policy, at the upper right of the page, click the colored circle, and then click **On**).
4. Click **Save changes**.

(Optional) Restarting Dell client computers awaiting reboot

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

See *About the Dell Client Manager home page* on page 12.

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

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

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

See *Preparing target Dell computers for management* on page 14.

To run the sample restart task included in Dell Client Manager

1. In the Dell Management Console, on the Home menu, click **Dell Client Manager**.
2. In the left pane, click **Tasks > Job Samples > Job Tasks > Restart by Power Control**.
3. In the right pane, click the **New Schedule** symbol.
4. In the New Schedule dialog box, configure the scheduling options, and then click **Add > Target**.
5. In the Add Target dialog box, under Filtering Rules, click **Add rule**.
6. To create a new rule, select **exclude computers not in**, then **Filter** and then select the **Supported Dell Client Computers Awaiting Reboot to Finish Installation** filter.
   To easily find the filter you want, type the first letters of the filter's name. This will reduce the number of entries in the drop-down list.
   In this example, type `Supp`.
7. (Optional) To save the target you created, on the toolbar, click the **Save as** symbol.
8. In the Add Target dialog box, click **OK**.
9. In the New Schedule dialog box, click **Schedule**.
10. Under Task Status, on the toolbar, click the **Refresh** symbol to monitor the status of the task.

(Optional) Configuring the Dell Client Manager Agent

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

See *Preparing target Dell computers for management* on page 14.

To configure the Dell Client Manager Agent

1. In the Dell Management Console, on the Home menu, click **Dell Client Manager**.
2. In the left pane, click **Policies > Configuration Policies > Agent Settings Policy**.
3. Check **Notifications** if you want the OMCI to generate alert notifications. OMCI alert notifications duplicate the notifications that are produced by Dell Client Manager, and this option is unchecked by default.
4. Check **Logging** to log alerts into the Windows Application Log on the Dell client computer.
5. Under Basic Inventory Schedule, configure when to send Dell Client Manager discovery and installed components information to the 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**.

Chapter 5
Using Dell Client Manager

This chapter includes the following topics:

About using Dell Client Manager

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

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 23.
  See *Updating BIOS versions* on page 26.
  See *Configuring BIOS settings* on page 29.

See *Configuring Dell display settings* on page 31.
See *Configuring power scheme settings* on page 32.
See *Monitoring computers health* on page 33.

- 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 *Managing individual Dell computers* on page 34.

About actions that require a client restart

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

- Dell OMCI software install and upgrade as part of the Dell Client Manager Agent installation
  See *Installing the Dell Client Manager Agent* on page 17.
- BIOS update
  See *Updating BIOS versions* on page 26.
- BIOS settings change
  See *Configuring BIOS settings* on page 29.

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, and Windows Server 2008 operating systems. This feature is designed to protect data by providing encryption for entire volumes.

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

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

See *Updating BIOS versions* on page 26.

See *Configuring BIOS settings* on page 29.

About BIOS password restrictions

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

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

These restrictions apply to both setting passwords and password verification.

See *Updating BIOS versions* on page 26.

See *Configuring BIOS settings* on page 29.

Prerequisites for using Dell Client Manager

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

See *Preparing target Dell computers for management* on page 14.

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

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

- BIOS settings inventory
  See *Collecting BIOS inventory data* on page 23.
- Hardware and BIOS version inventory
  See *Collecting hardware and BIOS version inventory data* on page 24.
- Display settings inventory
  See *Collecting display inventory data* on page 24.
- Power scheme settings inventory
  See *Collecting power scheme inventory data* on page 24.

Collecting BIOS inventory data

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

See *Viewing BIOS, hardware, display, and power scheme settings inventory* on page 25.

To collect BIOS inventory data

1. In the Dell Management Console, on the Home menu, click **Dell Client Manager**.
2. In the left pane, click **Quick Start > Section 3. Hardware Management Tasks > Scan for Current BIOS Settings**.

3. If you want to report only the inventory that has changed since the last inventory scan, check **Only report inventory if changed**, and click **Save changes**.
4. Run the task one time or on a schedule.
   For more information on running tasks, see the *Symantec Management Platform Help.*

Collecting hardware and BIOS version inventory data

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

See *Viewing BIOS, hardware, display, and power scheme settings inventory* on page 25.

To collect hardware inventory data

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

Collecting display inventory data

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

See *Viewing BIOS, hardware, display, and power scheme settings inventory* on page 25.

To collect display inventory data

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

Collecting power scheme inventory data

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

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

See *Installing the Altiris Power Scheme Agent* on page 18.

See *Viewing BIOS, hardware, display, and power scheme settings inventory* on page 25.

To collect power saving inventory data

1. In the Dell Management Console, on the Home menu, click **Dell Client Manager**.
2. In the left pane, click **Quick Start > Section 4. Power Scheme Tasks > Power Scheme Inventory**.
3. Run the task one time or on a schedule.
   For more information on running tasks, see the *Symantec Management Platform Help.*

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

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

See *Collecting BIOS, hardware, display, and power scheme settings inventory* on page 23.

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

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

To view collected power scheme inventory in reports

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

To view collected inventory from the resource manager

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

Updating BIOS versions

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

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

Warning
Do not run the BIOS Update Task on computers with BitLocker. Instead, use the BIOS Update Job.
See *About Windows BitLocker Drive Encryption* on page 22.

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

See *Performing one-to-one BIOS update* on page 37.

The recommended steps for updating BIOS versions with Dell Client Manager are as follows:

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 1	Discover current BIOS versions.	The Hardware Inventory Task lets you collect current BIOS versions inventory. See *Discovering current Dell BIOS versions* on page 27.
Step 2	Save the computers you want to update as a static filter.	From the Systems with Specified BIOS Version report you can find the computers of the specific model that need a BIOS update. Then you can save this list of computers as a static filter. See *Saving computers with older BIOS versions as a filter* on page 27.
Step 3	Update the BIOS	Now you must run the BIOS Update Job on the computers that are listed in the static filter that you saved. See *Running the BIOS Update Job* on page 27.
Step 4	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 29.

Discovering current Dell BIOS versions

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

See *Collecting hardware and BIOS version inventory data* on page 24.

See *Updating BIOS versions* on page 26.

Saving computers with older BIOS versions as a filter

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

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

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

See *Updating BIOS versions* on page 26.

To save computers with older BIOS versions as a filter

1. In the Dell Management Console, on the Home menu, click **Dell Client Manager**.
2. In the left pane, click **Reports > BIOS > Systems with Specified BIOS Version**.
3. In the report, under Parameters, select the product line and the model you want to update the BIOS for.
   In this example, select **OptiPlex Desktops** and **745C** accordingly.
4. In the report, under Parameters, in the Operator drop-down list, click **Older Than**.
5. In the BIOS Version box, type the BIOS version you want to update to.
   In this example, type `1.2.2`
6. On the toolbar, click **Refresh**.
   Computers that need a BIOS update appear in the list.
7. In the list, click the computers you want to update the BIOS version on.
8. On the toolbar, click **Save As**, and click **Static Filter**.
9. In the Save as static filter dialog box, type the name of the new filter that you are creating.
   In this example, type `My OptiPlex 745C Computers with BIOS older than 1.2.2`
10. Click **Save**.

Running the BIOS Update Job

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

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

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

Warning
Never run the BIOS Update Task alone on computers with BitLocker. Instead, use the sample BIOS Update Job, included with Dell Client Manager.
See *About Windows BitLocker Drive Encryption* on page 22.

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

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

See *Updating BIOS versions* on page 26.

To update the BIOS

1. In the Dell Management Console, on the Home menu, click **Dell Client Manager**.
2. In the left pane, click **Quick Start > Section 3. Hardware Management Tasks > Update BIOS Version**.
3. On the BIOS Update Job page, click **Run "BIOS Update Task"**.
4. On the toolbar, click the **Edit the selected item** symbol.
5. On the BIOS Update Task page, click **Browse** and navigate to the location of the BIOS upgrade .exe (or extracted .hdr) file.
   In this example, browse to the `O745C-010202.EXE` file - a BIOS update package for Dell OptiPlex 745C computers.
6. If you want to rewrite the BIOS even if the Dell client computer's BIOS version is higher than the one that you uploaded, check **Allow version downgrades**.
7. Type the BIOS setup password if needed.
8. Click **Save changes**.
9. Click **Close**.
10. On the BIOS Update Job page, click **Save changes**.
11. Under Task Status, on the toolbar, click **New Schedule**.
12. On the New Schedule page, select a schedule to run this job on and, if you want, configure Run Options.
13. Under Input, click **Add > Target**.
14. In the Add Target dialog box, under Filtering Rules, click **Add rule**.
15. To create a new rule, select **exclude computers not in**, then **Filter** and then select the filter on which you want to run the BIOS Update Job.
    In this example, select the **My OptiPlex 745C Computers with BIOS older than**

1.2.2 filter you previously created.
To easily find the filter you want, type the first letters of the filter's name. This will reduce the number of entries in the drop-down list.
In this example, type `My Opti`.

16. (Optional) To save the target you created, on the toolbar, click the **Save as** symbol.
17. In the Add Target dialog box, click **OK**.
18. In the New Schedule dialog box, click **Schedule**.
19. Under Task Status, on the toolbar, click the **Refresh** symbol to monitor the status of the job.
    The Job will be executed according to the schedule that you specified. You can double-click the job instance in the Task Status section to see run details of the job. On the Run Details page, you can double-click each computer in the grid and see the details of each task included into the job, their execution status, output, and error codes.

Viewing the BIOS Update Job execution reports

You can view the status of the BIOS update jobs 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 12.

See *Updating BIOS versions* on page 26.

To view the job execution progress reports

1. In the Dell Management Console, on the Home menu, click **Dell Client Manager**.
2. In the left pane, click **Reports > BIOS**.
3. Click **BIOS Update Task Execution Report**. 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 policy, and those that failed.

Configuring BIOS settings

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

You can change BIOS settings on the Dell client computers using the BIOS Settings Task or the BIOS Settings Job.

Warning
Never run the BIOS Settings Task alone on computers with BitLocker. Instead, use the sample BIOS Settings Job, included with Dell Client Manager.
See *About Windows BitLocker Drive Encryption* on page 22.

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

See *Collecting BIOS inventory data* on page 23.

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

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

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

See *Performing one-to-one BIOS configuration* on page 36.

To configure BIOS settings

1. In the Dell Management Console, on the Home menu, click **Dell Client Manager**.
2. In the left pane, click **Tasks > Job Samples > BIOS Settings Job**.
3. On the BIOS Settings Job page, under Jobs/Tasks, click **Run "BIOS Settings Job: BIOS Settings Task"**.
4. On the toolbar, click the **Edit the selected item** symbol.
5. On the BIOS Settings Job: BIOS Settings Task page, under Software Settings, click the check box next to the BIOS settings that you want to change on the target Dell computers, and select a value.
   Also see *About using macros for BIOS settings* on page 30.
6. 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 select the Dell computer from which to import the settings from.
   This is useful when you want to use a Dell computer's BIOS settings as a sample and have other Dell computers configured similarly.
   See *Collecting BIOS inventory data* on page 23.
7. Type the BIOS setup password if needed.
   See *About BIOS password restrictions* on page 22.
8. If you want to send the BIOS inventory after the task has run, check **Refresh inventory on settings change**.
9. Click **Save changes**.
10. Click **Close**.
11. Run the job one time or on a schedule.
    For more information on running tasks, see the *Symantec Management Platform Help.*

About using macros for BIOS settings

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

See *Configuring BIOS settings* on page 29.

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 then is supported for that BIOS setting, the task will fail.

Dell Client Manager also supports the following macros:

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

Configuring Dell display settings

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

See *Collecting display inventory data* on page 24.

See *Changing brightness and contrast settings* on page 31.

See *Restoring display factory default settings* on page 32.

See *Turning off displays* on page 32.

Changing brightness and contrast settings

You can change brightness and contrast settings for displays, manufactured by Dell.

See *Configuring Dell display settings* on page 31.

To change brightness and contrast settings

1. In the Dell Management Console, on the Home menu, click **Dell Client Manager**.
2. In the left pane, click **Tasks > Display Tasks > Change brightness and contrast settings**.
3. If you want to change the brightness, check **Brightness** and set the desired brightness level.
4. If you want to change the contrast, check **Contrast** and set the desired contrast level.
5. Click **Save changes**.
6. Run the task one time or on a schedule.
   For more information on running tasks, see the *Symantec Management Platform Help.*

Restoring display factory default settings

You can restore factory default settings for displays, manufactured by Dell.

See *Configuring Dell display settings* on page 31.

To restore display factory default settings

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

Turning off displays

You can turn off displays, manufactured by Dell.

See *Configuring Dell display settings* on page 31.

To turn off displays

1. In the Dell Management Console, on the Home menu, click **Dell Client Manager**.
2. In the left pane, click **Tasks > Display Tasks > Turn off display**.
3. Run the task one time or on a schedule.
   For more information on running tasks, see the *Symantec Management Platform Help.*

Configuring power scheme settings

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

See *Collecting power scheme inventory data* on page 24.

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

See *Installing the Altiris Power Scheme Agent* on page 18.

To configure power scheme settings

1. In the Dell Management Console, on the Home menu, click **Dell Client Manager**.
2. In the left pane, click **Quick Start > Section 4. Power Scheme Tasks** and click a power scheme, for example, **Minimal Power Management Scheme**.
3. If you want, under Altiris Power Scheme Task settings, configure the settings 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.*

Monitoring computers health

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

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

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

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

Also see *Viewing the list of computers that are triggering alerts* on page 34.

To enable health monitoring

1. In the Dell Management Console, on the Home menu, click **Dell Client Manager**.
2. In the left pane, click **Policies > Dell Client Monitoring Policies > Dell Client Monitoring Policy**.
3. If required, type the BIOS setup password. Some Dell models require a BIOS setup password to perform some monitoring tasks (such as chassis intrusion alert).
   See *About BIOS password restrictions* on page 22.
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, select the action you want Dell Client Manager to perform. The default action is Email Automated Action for Dell Client Manager Alert.
   For more information on automated action settings, see the topics on automated actions in the *Symantec Management Platform Help*.
6. Click **Edit input parameters** and configure parameters for the action. For example, for the default action, configure where to send the email.
7. (Optional) To write an alert to the Windows application log on the Dell client computer that triggers an alert, under Client actions, check **Log events**.
   For more information, see the tooltip help.
8. (Optional) To display a popup message to the logged in user on the Dell client computer that triggers an alert, under Client actions, check **Display alert notification**.
   For more information, see the tooltip help.
9. Under Applied to, click **Apply to** and select the computers on which you want the policy to run.

Viewing the list of computers that are triggering alerts

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

See *Monitoring computers health* on page 33.

To view the systems triggering alerts

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

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 35.

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 36.
- 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 36.

- Change boot order
  See *Performing one-to-one boot order configuration* on page 36.
- Change BIOS password
  See *Performing one-to-one BIOS password change* on page 38.
- Update BIOS version
  See *Performing one-to-one BIOS update* on page 37.

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.

See *Managing individual Dell computers* on page 34.

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

1. In the Dell Management Console, on the Home menu, click **Dell Client Manager**.
2. Click **Filters**.
3. Click a filter, for example, **Supported Dell Client Computers**.
4. In the right pane, double-click the computer you want to manage.
5. In the Resource Manager, on the View menu, click **Real-Time**.
6. In the treeview pane, click **Real-Time Consoles**.
   See *About the Real-Time Consoles page* on page 35.

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 you want to connect to, and click **Connect**.
3. In the Resource Manager, on the View menu, click **Real-Time**.
4. In the treeview pane, click **Real-Time Consoles**.
   See *About the Real-Time Consoles page* on page 35.

About the Real-Time Consoles page

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

If credentials are displayed as invalid, verify that your connection profile is using the correct credentials. Use the Credentials Manager to add or modify credentials and then Protocol Manager to create or modify a connection profile for a specific technology.

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

Also see *Troubleshooting connection through the Real-Time view* on page 42.

Viewing the Dell client computer summary

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

To open the Dell Client Manager Summary page

1. Open the Resource Manager.
   See *Accessing the Real-Time view* on page 35.
2. In the Resource Manager, on the Summaries menu, click **Dell Client Manager Summary**.

Performing one-to-one BIOS configuration

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

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

Also see *Configuring BIOS settings* on page 29.

Warning
Never run this task on computers with BitLocker enabled.
See *About Windows BitLocker Drive Encryption* on page 22.

See *Managing individual Dell computers* on page 34.

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 35.
2. In the treeview pane, click **Real-Time Consoles > Dell Client Manager** > **General Configuration** > **BIOS Settings**.
3. If the client computer requires a BIOS setup password, type it.
   See *About BIOS password restrictions* on page 22.
4. If you want to restart the target Dell computer after changing the settings, in the Reboot After Change drop-down list, click **True**.
5. Configure the other settings and options.
6. Click **Apply**.

Performing one-to-one boot order configuration

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

Warning
Never run this task on computers with BitLocker enabled.
See *About Windows BitLocker Drive Encryption* on page 22.

See *Managing individual Dell computers* on page 34.

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 35.
2. In the treeview pane, click **Real-Time Consoles > Dell Client Manager** > **General Configuration** > **Boot Order**.
3. If you want to restart the target Dell computer after changing the settings, in the Reboot After Change drop-down list click **True**.
4. Set the boot order for each of the bootable devices.
5. You can also enable or disable the boot status of a device.
6. Click **Apply**.

Performing one-to-one BIOS update

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

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

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

Also see *Updating BIOS versions* on page 26.

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

Warning
Never run this task on computers with BitLocker enabled.
See *About Windows BitLocker Drive Encryption* on page 22.

See *Managing individual Dell computers* on page 34.

To upgrade/downgrade a BIOS one-to-one

1. Open the Real-Time view for the computer that you want to manage.
   See *Accessing the Real-Time view* on page 35.
2. In the treeview pane, click **Real-Time Consoles > Dell Client Manager** > **Management Tasks > BIOS Upgrade**.
3. Click **Browse** and navigate to the location of the BIOS upgrade .exe (or extracted .hdr) file.
4. If required to type a BIOS setup password, type it.
   See *About BIOS password restrictions* on page 22.
5. Click **Accept**.

Performing one-to-one BIOS password change

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

See *About BIOS password restrictions* on page 22.

Warning
Never run this task on computers with BitLocker enabled.
See *About Windows BitLocker Drive Encryption* on page 22.

See *Managing individual Dell computers* on page 34.

To change a BIOS password one-to-one

1. Open the Real-Time view for the computer that you want to manage.
   See *Accessing the Real-Time view* on page 35.
2. In the treeview pane, click **Real-Time Consoles > Dell Client Manager** > **Management Tasks > Change BIOS Password**.
3. Type the current and the new BIOS passwords.
4. Click **Accept**.

Resetting chassis intrusion alert

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

Warning
Never run this task on computers with BitLocker enabled.
See *About Windows BitLocker Drive Encryption* on page 22.

See *Managing individual Dell computers* on page 34.

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 35.
2. In the treeview pane, click **Real-Time Consoles > Dell Client Manager** > **General Configuration > BIOS Settings**.
3. If a chassis intrusion alert has been activated, the Chassis Intrusion Status property value displays “Detected”. Clear the alert by changing it to “Clear”.
4. Click **Apply**.

Assessing Microsoft Windows Vista migration readiness

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

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

Microsoft Windows Vista 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.

Some OS features—like the Aero interface—are only available in premium editions of Window Vista and may require advanced hardware.

For more information, see www.windowsvista.com.

To populate the reports with data, run the BIOS Inventory Task.

See *Collecting hardware and BIOS version inventory data* on page 24.

The following reports are available:

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

To view the Microsoft Windows Vista migration readiness reports

1. In the Dell Management Console, on the Home menu, click **Dell Client Manager**.
2. Click **Reports > Microsoft Windows Vista 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, not listed in the Supported Models Manager. 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. Altiris may release a new supported models XML file and make it available in the predefined location. You can set the Supported Models Manager to automatically download updated supported model files from the Altiris support Web site, or you can manually download the files from the Dell support Web site and save them to a local directory.

To import the supported models list

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

2. In the left pane, click **Policies > Configuration Policies > Supported Models Manager**.
3. On the Supported Models Manager page, modify the URL if needed, and click **Import now**.
4. If you want to update the supported models list on a schedule, select a schedule, turn on the policy and 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**.

Appendix A
Troubleshooting Dell Client Manager

This appendix includes the following topics:

Troubleshooting the Altiris Agent push installation

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

- Windows firewall
  See *Configuring the firewall to allow push installation* on page 41.
- Simple file sharing enabled (Windows XP SP2)
  See *Disabling simple file sharing on Windows XP* on page 41.
- User Account Control is enabled (Windows Vista)
  See *Configuring User Access Control on Windows Vista* on page 42.

Configuring the firewall to allow push installation

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

See *Troubleshooting the Altiris Agent push installation* on page 41.

To configure the firewall for the Altiris Agent push installation

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

Disabling simple file sharing on Windows XP

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 are logging onto such computers over the network are forced to use the Guest account.

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

- Uncheck "Use simple file sharing" under 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 KB articles:

http://support.microsoft.com/default.aspx?scid=KB;EN-US;180548
http://support.microsoft.com/default.aspx?scid=kb;en-us;290403

See *Troubleshooting the Altiris Agent push installation* on page 41.

Configuring User Access Control on Windows Vista

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

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

See *Troubleshooting the Altiris Agent push installation* on page 41.

Troubleshooting connection through the Real-Time view

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

Technology	Possible reasons
WMI	The connection credentials are incorrect.
	The computer is powered 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 43.
	Simple file sharing is enabled. See *Disabling simple file sharing on Windows XP* on page 41.
	User Access Control is turned on. See *Configuring User Access Control on Windows Vista* on page 42.
	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.
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.

Technology	Possible reasons
Intel AMT	The connection credentials are incorrect.
	The Intel AMT device is not configured. For more information on configuring computers with ASF, see the *Out of Band Management Component Implementation Guide*.
	The Intel AMT device is in secure mode, but the connection profiles is not configured to use the correct certificates. 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.
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 is not in the list of hosts to accept the SNMP packets from. Check SNMP service properties.

Configuring the firewall to allow WMI connection

The WMI credentials can be displayed as "Invalid" on the Real-Time Consoles page when you try to perform one-to-one management of a computer with Windows XP Service Pack 2 or Windows Vista operating system.

This issue can occur when the default configuration of the Windows Firewall program in Windows XP SP2 and Vista 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 44.
- Configure the firewall on all computers in the domain using group policy.
  See *Configuring the firewall on multiple domain computers using group policy* on page 44.
- Temporarily disable the firewall.

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 43.

To configure the firewall on Windows XP SP2

1. Log on to the target computer as administrator.
2. Click **Start > Run**, type `gpedit.msc` in the **Open** 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 click **OK**.

To configure the firewall on Windows Vista

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

Configuring the firewall on multiple domain computers using 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 on how to use 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 43.

To configure the firewall on multiple domain computers using 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** field, and then click **OK**.
   - Expand your domain, right-click the organizational unit that you want to create the Group Policy in, 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 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** field, 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, 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 field.
    For example, to permit remote administration from a particular IP address, type that IP address in the Allow unsolicited incoming messages from field. 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 about 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.

Appendix B
Glossary

This section introduces important terms used in this document.

Altiris Agent

The software that is installed on the computers that you want to manage. It facilitates interactions between Notification Server and a managed computer. The agent receives requests for information from Notification Server, sends data to Notification Server, and downloads files. The Altiris Agent also lets you install and manage solution plug-ins that add functionality to the agent.

Dell Management Console

The Web-based user interface for managing the Symantec Management Platform and any other installed solutions.

discovery

The process of searching for computers or other resources on your network that meet specific requirements.

filter

A query that identifies a dynamic group of resources that share common criteria.

job

A group of one or more tasks that are run in a particular sequence. Jobs can include conditions that specify when the task runs.

Notification Server

The Symantec Management Platform service that communicates with the Altiris Agent and the CMDB to provide management, security, and administrative functionality. It processes events, facilitates communications with managed computers, and coordinates the work of the other Symantec Management Platform services.

policy

A set of rules that control the execution of automated actions. Policies can be scheduled or based on incoming data that triggers an immediate action. Policies determine when an action should start and who or what should be notified of the results.

resource

Any item that Notification Server can track or manage, such as a user, site, installed application, computer, switch, router, or handheld device.

Resource Manager

A feature that displays information about a resource, such as its properties and current state. It also lets you troubleshoot and perform actions on managed resources.

solution

A product that is installed as a plug-in and adds functionality to Notification Server.

Symantec Management Platform

The platform that provides a set of services for IT-related solutions. These services include security, scheduling, client communications and management, task execution, file deployment, reporting, centralized management, and CMDB services.

task

An action that is performed on a computer. Server tasks are run on Notification Server. Client tasks are run on managed computers.

Index

S

T

U

V

W