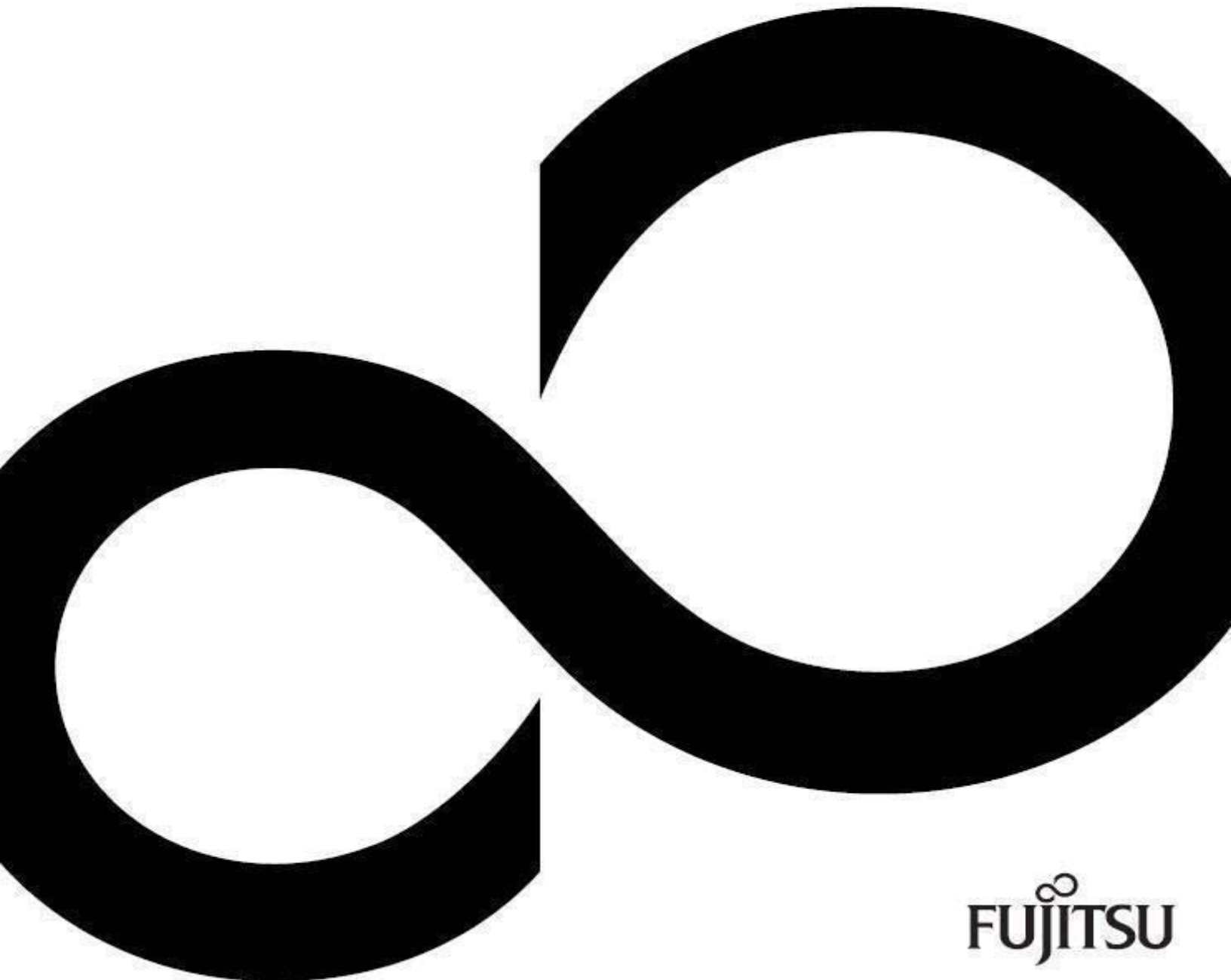


# DeskView Version 10

---



## Notice

Fujitsu Technology Solutions DeskView 10.72

Copyright © 2006-2010 Fujitsu Technology Solutions and its third party licensors. All rights reserved.

Document Date: April 5, 2010

The content of this documentation is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by Fujitsu Technology Solutions or Symantec. Fujitsu Technology Solutions or Symantec Corporation assumes no responsibility or liability for any errors or inaccuracies that may appear in this documentation.

DeskView is a trademark of Fujitsu Technology Solutions.

CELSIUS, FUTRO and SCENIC are registered trademarks of Fujitsu Technology Solutions.

ESPRIMO is a trademark of Fujitsu Technology Solutions.

ServerView® and PRIMERGY® are trademarks of Fujitsu Technology Solutions.

Altiris™, and the Altiris logo are trademarks of Symantec Corporation in the United States and other countries.

Microsoft, Windows, and the Windows logo are trademarks, or registered trademarks of Microsoft Corporation in the United States and/or other countries.

All other brand names are trademarks or registered trademarks of their respective companies.

All other trademarks referenced are trademarks or registered trademarks of their respective owners, whose protected rights are acknowledged.

All rights, including rights of translation, reproduction by printing, copying or similar methods, in part or in whole, are reserved.

Offenders will be liable for damages.

All rights, including rights created by patent grant or registration of a utility model or design, are reserved.

---

# Contents

---

<b>Chapter 1: Introducing DeskView</b> . . . . .	<b>6</b>
About DeskView . . . . .	6
What's new in DeskView . . . . .	7
Products installed with DeskView . . . . .	7
How DeskView works . . . . .	7
What you can do with DeskView . . . . .	7
Where to get more information . . . . .	8
<b>Chapter 2: Installing DeskView</b> . . . . .	<b>10</b>
System requirements . . . . .	10
About DeskView requirements . . . . .	10
About client computer requirements . . . . .	10
Installing the DeskView product . . . . .	11
Post-installation tasks . . . . .	11
Uninstalling DeskView . . . . .	11
Uninstalling the DeskView agents from client computers . . . . .	12
Uninstalling DeskView from the Notification Server computer . . . . .	12
<b>Chapter 3: Getting started with DeskView</b> . . . . .	<b>13</b>
About the Symantec Management Console . . . . .	13
About the DeskView "Home" . . . . .	13
<b>Chapter 4: Preparing target systems from Fujitsu Technology Solutions for systems management</b> . . . . .	<b>14</b>
Preparing target systems for management . . . . .	14
Discovering computers . . . . .	15
Installing the Altiris Agent . . . . .	15
Configuring the Altiris Agent settings for evaluation use . . . . .	16
Discovering systems from Fujitsu Technology Solutions . . . . .	16
Installing DeskView agents . . . . .	17
About upgrading existing DeskView Client 5.x/6.x software . . . . .	18
Installing the DeskView Agent . . . . .	18
Installing the DeskView Diagnostics Agent . . . . .	19
Installing the Altiris Power Scheme Agent . . . . .	20
Viewing DeskView agents installation reports . . . . .	20
<b>Chapter 5: Configuring DeskView</b> . . . . .	<b>21</b>
Importing the Best Fit file . . . . .	21
Configuring the Inventory Cache purging . . . . .	21
<b>Chapter 6: Using DeskView</b> . . . . .	<b>23</b>
About running tasks and policies . . . . .	23
Viewing tasks and policies . . . . .	23
Using DeskView Client Tools . . . . .	24
Archiving and updating BIOS and BIOS settings . . . . .	24
Using DeskFlash to harmonize BIOS settings in your environment . . . . .	25
Managing the power state of the client computer . . . . .	26
Turning off client computers at a specific time . . . . .	27

Updating drivers on the client systems . . . . .	28
Configuring BIOS settings and enabling/disabling interfaces . . . . .	29
Booting a computer from the network . . . . .	30
Diagnosing client computers' hardware . . . . .	31
Changing power scheme settings . . . . .	32
Disabling mass storage devices . . . . .	33
Managing serial numbers . . . . .	34
Running DeskView Client Tools using a command line . . . . .	36
Using DeskView Notifications . . . . .	36
Configuring the Notification Server computer . . . . .	37
Selecting notifications . . . . .	38
Forwarding notifications by email . . . . .	38
Enabling DeskView notifications . . . . .	39
Configuring the notification settings . . . . .	39
Viewing DeskView notifications . . . . .	40
Viewing the system data of a DeskView managed system . . . . .	40
Accessing the Resource Manager . . . . .	41
Viewing DeskView inventory . . . . .	41
Viewing DeskView events . . . . .	41
Viewing DeskView System Data . . . . .	42

**Chapter 7: Context-sensitive topics . . . . . 43**

DeskFlash tool . . . . .	43
Archive BIOS task . . . . .	43
Update BIOS task . . . . .	45
Update BIOS settings task . . . . .	46
Update processor microcodes task . . . . .	48
DeskView Energy Management tool: Change Power State task . . . . .	49
DeskView Energy Management tool: Change power scheme settings task . . . . .	50
DeskUpdate tool: Update drivers task . . . . .	50
DeskView BIOS Settings tool . . . . .	51
Set BIOS-Default values task . . . . .	52
Update BIOS boot order task . . . . .	52
Update BIOS password task . . . . .	52
Update bluetooth options task . . . . .	53
Update diskette controller options task . . . . .	53
Update flash write protection options task . . . . .	54
Update infrared options task . . . . .	54
Update LAN remote boot options task . . . . .	55
Update parallel port options task . . . . .	55
Update USB host controller options task . . . . .	56
Update Wake on LAN options task . . . . .	56
Update WLAN options task . . . . .	57
Update 0-Watt PC options task . . . . .	57
Update Audio Controller options task . . . . .	58
Update Hyper Threading options task . . . . .	58
Update Memory Protection options task . . . . .	59
Update Virtualization options task . . . . .	59
Update POST Diagnostic Screen options task . . . . .	60
Update Show Boot Menu Prompt (F12) options task . . . . .	60
Update USB Port Compatibility options task . . . . .	61
Update Front USB ports options task . . . . .	61
Update Rear USB ports ptions task . . . . .	62
Update Core multi-processing options task . . . . .	62

Update Enhanced Intel Speedstep Technology options task . . . . .	63
Update Enhanced Idle Power State options task . . . . .	63
Update Turbo Boost Technology options task . . . . .	64
Update Internal camera options task . . . . .	64
Update Show setup prompt (F2) options task . . . . .	64
Update USB legacy support options task . . . . .	65
Update Boot from removable media options task . . . . .	65
Update Low Power Soft Off options task . . . . .	66
Update DASH technology support options task. . . . .	66
Update Keyboard check options task. . . . .	67
Update PS/2 Mouse configuration options task . . . . .	67
Update USB ports options task . . . . .	68
DeskView Diagnostics tool: Hardware diagnostics task . . . . .	68
DeskView Security tool: Configure Mass Storage Access task. . . . .	69
. . . . .	69
DeskView Notifications . . . . .	70
DeskView Enable/Disable Notifications policy . . . . .	70
DeskView Configure Data Disk free space policy . . . . .	71
DeskView Configure System disk free space policy . . . . .	71
DeskView Configure Lease expiration policy . . . . .	71
Configure General Notification Email Forwarding page. . . . .	72
Configure General Notification Selection page . . . . .	73
DeskView Serial Numbers tool . . . . .	75
Apply imported serial numbers task . . . . .	75
Assign single serial number task . . . . .	75
Generate serial number task . . . . .	75
Manage serial numbers page . . . . .	76
DeskView System Data page . . . . .	77
DeskView Notifications page . . . . .	78
Cleanup Inventory Cache task . . . . .	79
<b>Appendix A: Glossary . . . . .</b>	<b>80</b>
<b>Index. . . . .</b>	<b>83</b>

---

# Chapter 1

## Introducing DeskView

---

This chapter includes the following topics:

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

## About DeskView

DeskView is a client management software developed by Fujitsu Technology Solutions. Optimized for Fujitsu hardware, it helps to minimize the total cost of ownership of managing your client hardware infrastructure. Based on industry standards, DeskView manages STYLISTIC tablet PCs, ESPRIMO Mobile and LIFEBOOK Professional Notebooks, FUTRO Thin Clients, SCENIC and ESPRIMO Professional PCs, CELSIUS Workstations, and PRIMERGY servers. DeskView makes use of the features that are offered by the system for inventory management, system health monitoring, remote BIOS configuration and updates, and more. DeskView lets you manage your client infrastructure completely from your desk.

DeskView is comprised of the following components, which are installed as separate solutions. You can install and use only the selected solutions or all of them, depending on the needs specific for your organization.

Component	Description
DeskView for Business Clients	DeskView for Business Clients supports Fujitsu Technology Solutions systems running Microsoft Windows XP Professional and Windows 7. In addition to comprehensive hardware and software inventory, DeskView for Business Clients provides access to an extensive number of DeskView Client Tools.
DeskView for Displays	DeskView for Displays lets you inventory and manage Fujitsu Technology Solutions display devices remotely from your administrator's desk. This solution effectively manages Fujitsu displays of Premium and Business Line equipped with a VESA-DDC/CI-compatible interface. DeskView for Displays supports inventory management and remote setting of display adjusts.

# What's new in DeskView

The following new features are introduced in the 10.72 release of DeskView:

- Support for the new 0-Watt PC option on the DeskView Client
- Enhance support for client computers under the different versions of the operating System Windows 7
- Enhanced BIOS options through the new DeskView Client software

# Products installed with DeskView

The Altiris management products that are installed and used with DeskView are shown in the following table:

<b>Product</b>	<b>Description</b>
Symantec Management Platform	The base management platform.
Altiris™ Real-Time Console Infrastructure	Provides out-of-band management tasks for computers with DASH, ASF, or Intel AMT.
Altiris™ Power Scheme Task	This add-on lets you configure the client computer's power-saving options remotely.
Altiris™ Event Console	This add-on lets you collect SNMP and solution specific alerts to quickly respond to problems using automated actions.
Altiris™ Network Discovery	This add-on lets you discover devices in your network.
Altiris™ Pluggable Protocol Architecture	This add-on lets you communicate with and manage network devices using different protocols required for your environment.

# How DeskView works

DeskView is a software that runs under the Symantec Management Platform software. DeskView lets you discover supported systems that are manufactured by Fujitsu Technology Solutions and install the DeskView Agent on these computers. The DeskView Agent communicates with the Symantec Management Platform and lets you perform management tasks from the Symantec Management Console.

# What you can do with DeskView

With DeskView you can collect inventory data about client computers and view this inventory in the Symantec Management Console. DeskView lets you configure and update BIOS, run computer diagnostics, update drivers, and configure security settings remotely from the Symantec Management Console.

You can run these tasks on a collection of computers, immediately, or at a later time, also you can connect to a specific system from Fujitsu Technology Solutions directly,

view live inventory data, and run management tasks in real time from the Symantec Management Console.

## 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.	<a href="http://kb.altiris.com/">http://kb.altiris.com/</a>  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.	<ul style="list-style-type: none"> <li>• The Documentation Library, which is available in the Symantec Management Console on the Help menu.</li> <li>• The Product Support page, which is available at the following URL: <a href="http://www.symantec.com/business/support/all_products.jsp">http://www.symantec.com/business/support/all_products.jsp</a> When you open your product's support page, look for the Documentation link on the right side of the page.</li> </ul>
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.
DeskView Client 6 User Manual	Information about the DeskView Client Tools command-line parameters and output codes.  This information is available in PDF format.	<ul style="list-style-type: none"> <li>• The Documentation Library, which is available in the Symantec Management Console on the Help menu.</li> <li>• The Fujitsu Technology Solutions Web site: <a href="http://ts.fujitsu.com/solutions/it_infrastructure_solutions/manageability/deskview_downloads.html">http://ts.fujitsu.com/solutions/it_infrastructure_solutions/manageability/deskview_downloads.html</a></li> </ul>

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

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

---

## Chapter 2

# Installing DeskView

---

This chapter includes the following topics:

- [System requirements](#)
- [Installing the DeskView product](#)
- [Post-installation tasks](#)
- [Uninstalling DeskView](#)

## System requirements

DeskView has the following system requirements:

- DeskView installation requirements  
See [About DeskView requirements](#) on page 10.
- DeskView Agent installation requirements  
See [About client computer requirements](#) on page 10.

## About DeskView requirements

DeskView requires the following:

- Symantec Management Platform 7.0

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 8.

## About client computer requirements

The DeskView Agent can only be installed and run on the following systems from Fujitsu Technology Solutions:

- Tablet PCs
- Notebooks
- Thin clients
- Professional PCs
- Workstations

The DeskView Agent supports Windows XP Professional, Windows Vista and Windows 7 operating systems.

For a list of supported systems please see also our Manageability & Security Feature Finder at

[http://www.ts.fujitsu.com/solutions/it\\_infrastructure\\_solutions/manageability/featurefinder.html](http://www.ts.fujitsu.com/solutions/it_infrastructure_solutions/manageability/featurefinder.html).

# Installing the DeskView product

Use Symantec Installation Manager to install DeskView.

For more information on installing products, see the *Symantec Management Platform Installation Guide*.

## Post-installation tasks

For DeskView to receive ASF (Alert Standard Format) and Intel® AMT notifications from client computers, you must install the Microsoft Windows SNMP (Simple Network Management Protocol) receiver and the ASF Proxy on the Notification Server computer.

### To install Microsoft Windows SNMP receiver

1. On the Notification Server computer, click the Windows Start button and click **Control Panel > Add or Remove Programs**.
2. In the Add or Remove Programs dialog box, click **Add/Remove Windows Components**.
3. In the Windows Components Wizard, in the Components window, click **Management and Monitoring Tools**, and then click **Details**.
4. In the Management and Monitoring Tools dialog box, check **Simple Network Management Protocol**.
5. Click **OK**.
6. Click **Next**.
7. Click **Finish**.

### To install the ASF Proxy

1. Run the ASFProxy.msi program that is located on the Notification Server computer, in case of a default installation, at C:\Program Files\Altiris\DeskView\Web\ASFProxy.
2. Follow the instructions in the wizard.
3. Restart the Notification Server computer.

## Uninstalling DeskView

To uninstall DeskView, perform the following steps:

Step	Action	Description
Step 1	Uninstall the DeskView agents from client computers.	This step is required if you do not want to reinstall DeskView later.  See <a href="#">Uninstalling the DeskView agents from client computers</a> on page 12.
Step 2	Uninstall DeskView from the Notification Server computer.	This step removes the product from the Notification Server computer.  See <a href="#">Uninstalling DeskView from the Notification Server computer</a> on page 12.

## Uninstalling the DeskView agents from client computers

Agent uninstall policies let you remove the DeskView agents from supported client computers. Remove the agents if you do not want to reinstall DeskView later.

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

See [Configuring the Altiris Agent settings for evaluation use](#) on page 16.

We recommend that you do not uninstall the DeskView software from Notification Server until the agent uninstallation tasks have run on all client computers. When DeskView is uninstalled, there is no automated way to uninstall the agents.

### To uninstall the DeskView Agent

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. In the left pane, click **Agents and Plug-ins > DeskView Agent 6.xx.yyyy \*)- Uninstall**.  
\*) The appropriate DeskView Agent version.
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**.

### To uninstall the DeskView Discovery Agent

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. In the left pane, click **Agents and Plug-ins > DeskView Discovery Agent - Uninstall**.
3. Turn on the policy.
4. Click **Save changes**.

### To uninstall the DeskView Diagnostics Agent

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. In the left pane, click **Agents and Plug-ins > DeskView Diagnostics Agent - Uninstall**.
3. Turn on the policy.
4. Click **Save changes**.

## Uninstalling DeskView from the Notification Server computer

Use Symantec Installation Manager to uninstall DeskView.

For more information on uninstalling products, see the *Symantec Management Platform Installation Guide*.

---

## Chapter 3

# Getting started with DeskView

---

This chapter includes the following topics:

- [About the Symantec Management Console](#)
- [About the DeskView "Home"](#)

## About the Symantec Management Console

You perform all DeskView configuration and administration tasks in the Symantec Management Console.

The Symantec Management Console is the Web-browser-based administration console for working with Altiris Notification Server and Altiris solutions, including DeskView. 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 computer. 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 the reports that have already been run.

For more information on the console, see the Symantec Management Platform documentation, 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 DeskView "Home"

DeskView provides a home page that introduces you to DeskView components and provides links to common tasks.

To open the DeskView home page, in the Symantec Management Console, on the Home menu, click **DeskView**.

---

## Chapter 4

# Preparing target systems from Fujitsu Technology Solutions for systems management

---

This chapter includes the following topics:

- [Preparing target systems for management](#)
- [Discovering computers](#)
- [Installing the Altiris Agent](#)
- [Configuring the Altiris Agent settings for evaluation use](#)
- [Discovering systems from Fujitsu Technology Solutions](#)
- [Installing DeskView agents](#)
- [Viewing DeskView agents installation reports](#)

## Preparing target systems for management

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

Step	Action	Description
Step 1	Discover manageable computers in your environment.	Discovery lets you find computers on which you can install the Altiris Agent.  See <a href="#">Discovering computers</a> on page 15.
Step 2	Install the Altiris Agent to the client computers.	The Altiris Agent lets Notification Server get information from and interact with the client computers.  See <a href="#">Installing the Altiris Agent</a> on page 15.
Step 3	(Optional) Configure the Altiris Agent settings for evaluation use.	For easier configuration and evaluation of DeskView, you can make the Altiris Agent to request configuration from Notification Server more frequently.  See <a href="#">Configuring the Altiris Agent settings for evaluation use</a> on page 16.
Step 4	Discover systems from Fujitsu Technology Solutions.	The DeskView Discovery Agent lets you find systems from Fujitsu Technology Solutions that are supported by DeskView.  See <a href="#">Discovering systems from Fujitsu Technology Solutions</a> on page 16.
Step 5	Install DeskView agents.	Install the DeskView management software to supported systems from Fujitsu Technology Solutions in your environment.  See <a href="#">Installing DeskView agents</a> on page 17.

## 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 systems for management](#) on page 14.

### To discover computers

1. In the Symantec Management Console, on the Actions menu, click **Discover > Import Domain Membership/WINS**.
2. In the Add Domain box, type the domain name, and then click the **Add** symbol.
3. Check **Domain Membership** and click **Discover Now**.
4. As the discovery process finishes, click **View discovery reports**.
5. Open a report to view the list of discovered computers.  
For example, right-click the **Discovered Computers** report, and then click **Open**.

## 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 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 DeskView.

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

See [Preparing target systems for management](#) on page 14.

### To install the Altiris Agent

1. In the Symantec 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 Symantec Management Console).

# Configuring the Altiris Agent settings for evaluation use

(Optional)

By default, the Altiris 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 DeskView Discovery Agent - Install policy) to reach the target 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 systems for management](#) on page 14.

## To configure the Altiris Agent for evaluation use

1. In the Symantec 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 'Package 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 that 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 systems from Fujitsu Technology Solutions

Before you can manage computers using DeskView, you must identify the computers as manageable systems from Fujitsu Technology Solutions. To do this, you must install the DeskView Discovery Agent to computers in your environment.

After you install the DeskView Discovery Agent on systems from Fujitsu Technology Solutions, it will report basic inventory data to Notification Server and identify the computer resources as DeskView manageable systems.

If you have a previous version of the DeskView Discovery Agent already installed on the managed computers, we recommend that you upgrade the DeskView Discovery Agent.

See [Preparing target systems for management](#) on page 14.

## To install the DeskView Discovery Agent

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. In the left pane, click **Agents and Plug-ins > DeskView Discovery 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**.

#### **To upgrade the DeskView Discovery Agent**

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. In the left pane, click **Agents and Plug-ins > DeskView Discovery Agent - Update**.
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**.

#### **To view discovered systems from Fujitsu Technology Solutions**

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. In the left pane, click **Agent and Plug-in Filters**.
3. To view new discovered systems from Fujitsu Technology Solutions, click **DeskView Agent Not Installed**.
4. To view discovered systems from Fujitsu Technology Solutions with DeskView Agent already installed, click **DeskView Agent Installed**.

## **Installing DeskView agents**

DeskView agents let the DeskView solution gather different type of information from and interact with the client systems.

See [Preparing target systems for management](#) on page 14.

Install the agents that are shown in the following table:

<b>Agent</b>	<b>Description</b>
DeskView Agent	<p>This agent installs DeskView Client software on the client systems and is required for the DeskView solution to communicate with the client systems from Fujitsu Technology Solutions.</p> <p>See <a href="#">Installing the DeskView Agent</a> on page 18.</p> <p>Also see <a href="#">About upgrading existing DeskView Client 5.x/6.x software</a> on page 18.</p>

<b>Agent</b>	<b>Description</b>
DeskView Diagnostics Agent	This is an optional agent. Install this agent if you want to run hardware diagnostics on the client systems.  See <a href="#">Installing the DeskView Diagnostics Agent</a> on page 19.
Altiris Power Scheme Agent	This is an optional agent. Install this agent if you want to configure power scheme settings on the client systems.  See <a href="#">Installing the Altiris Power Scheme Agent</a> on page 20.

## About upgrading existing DeskView Client 5.x/6.x software

It is possible to deploy the latest DeskView Agent on a system where a DeskView Client version 5.x/6.x is already installed. When deploying the DeskView Agent with the rollout policy, the complete current DeskView Client 5.x/6.x version is automatically uninstalled and then, without a restart, the DeskView Client 6.x, the DeskView Agent, and (if required) the ASF component are installed on the target computer.

However, the rollout policy cannot automatically uninstall DeskView Client 5.x/6.x if this software was manually installed outside of Notification Server. In this case, you must manually uninstall DeskView Client 5.x/6.x from the computers to which you want to roll out the DeskView Agent.

See [Installing DeskView agents](#) on page 17.

## Installing the DeskView Agent

The DeskView Agent is a client software package that includes a DeskView Agent as well as the DeskView Client tools. You can deploy this package remotely on the manageable systems from Fujitsu Technology Solutions using the Install Recommended DeskView Agent policy. Another option is to use the dedicated DeskView Agent 6.xx.yyyy \*)-Install policy.

\*) The appropriate version of DeskView Agent.

We recommend that you use the Install Recommended DeskView Agent policy and let the DeskView software choose which version of the agent to install onto each of the target computers.

Before you install the DeskView Agent, you must discover systems from Fujitsu Technology Solutions.

See [Discovering systems from Fujitsu Technology Solutions](#) on page 16.

See [Installing DeskView agents](#) on page 17.

### To install the DeskView Agent

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. Do one of the following:
  - In the left pane, click **Agents and Plug-ins > Install Recommended DeskView Agent**.

- In the left pane, click **Agents and Plug-ins > DeskView Agent 6.xx.xxxx - Install**.
- 3. If you want to install ASF components, check **Install ASF components on ASF capable computers**.
- 4. If you want to install DeskView Presentation, check **Install DeskView presentation mode**.  
DeskView Presentation is a button in the taskbar that lets users turn off the screensaver while running a presentation.
- 5. If you want to reinstall the existing DeskView client components, check **Force existing components reinstallation**.  
This is useful when you want to repair the DeskView components that are already installed on the client system.
- 6. Sometimes a restart is required to complete the installation or upgrade of the DeskView Agent. If you want to restart the target system after running the task, under Power Management, check **Restart the computer after task**.
- 7. If you want, under **Applied To**, edit the targets to which the policy is applied.
- 8. Turn on the policy.  
To turn on the policy, at the upper right of the page, click the colored circle, and then click **On**.
- 9. Click **Save changes**.

## Installing the DeskView Diagnostics Agent

The DeskView Diagnostics Agent is a client software package that lets you remotely run hardware diagnostics on the client computers and see the results in the Symantec Management Console.

You can deploy this package remotely on manageable systems from Fujitsu Technology Solutions with Microsoft Windows XP or later and with the DeskView Agent installed.

See [Installing the DeskView Agent](#) on page 18.

After you deploy the DeskView Diagnostics Agent on systems from Fujitsu Technology Solutions, you can run remote hardware diagnostics.

See [Diagnosing client computers' hardware](#) on page 31.

Use the Resource Manager to see the results.

See [Viewing DeskView events](#) on page 41.

See [Installing DeskView agents](#) on page 17.

### To install the DeskView Diagnostics Agent

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. In the left pane, click **Agents and Plug-ins > DeskView Diagnostics 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**.

## 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 computers.

See [Installing DeskView agents](#) on page 17.

### To install the Altiris Power Scheme Agent

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. In the left pane, click **Getting Started > DeskView for Business Clients Getting Started > 1. Getting Started > Step 4. Install Power Scheme Agent**.
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**.

## Viewing DeskView agents installation reports

DeskView includes reports that provide information about the status of the DeskView agents on your client computer. These reports provide installation and execution status of the agents as well as the agents version information.

See [Preparing target systems for management](#) on page 14.

### To view the DeskView agents installation status reports

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. In the left pane, click **Reports > Business Clients > Installation**.
3. Click a report.  
For example, click the **Installation Status DeskView Agents** report.

---

## Chapter 5

# Configuring DeskView

---

This chapter includes the following topics:

- [Importing the Best Fit file](#)
- [Configuring the Inventory Cache purging](#)

## Importing the Best Fit file

DeskView uses the information about various models of Fujitsu Technology Solutions available in your organization to assign the most appropriate DeskView Agent package version to each managed system. Each new released DeskView Client Pack contains and installs an updated assignment list (Best Fit File).

Fujitsu Technology Solutions can also produce an updated assignment list without releasing a new DeskView Client Package. For example, an updated assignment list can be released together with the release of a new Fujitsu Technology Solutions system that uses one of the existing client packages.

### To import the Best Fit File

1. If available, you can download the Best Fit File to a temporary location on your computer.  
You can download the Best Fit File from the following location: [http://ts.fujitsu.com/solutions/it\\_infrastructure\\_solutions/manageability/deskview\\_downloads.html](http://ts.fujitsu.com/solutions/it_infrastructure_solutions/manageability/deskview_downloads.html)
2. In the Symantec Management Console, on the Home menu, click **DeskView**.
3. In the left pane, click **Configuration > Import Best Fit File**.
4. In the right pane, type the path to the file that you downloaded, or click **Browse** to browse for the file.
5. Click **Import**.

## Configuring the Inventory Cache purging

DeskView uses an inventory cache folder (by default, C:\Program Files\DeskView\InventoryCache) to store inventory information events that are received from managed systems before the events get processed by DeskView. After DeskView processes the inventory from a managed system, the corresponding event file is deleted. However, if DeskView cannot process inventory events, the events can be accumulated infinitely. To prevent an out-of-space situation on the disk, the Cleanup Inventory Cache task monitors the size of the inventory cache folder and maintains its size according to parameters that you specify.

By default, the task is configured to run daily. When the conditions you specified are met, the cached data is purged.

### **To configure the Inventory Cache purging**

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. In the left pane, click **Configuration > Cleanup Inventory Cache task**.
3. In the right pane, configure the settings.  
For help, in the Symantec Management Console, press **F1** or click **Help > Context**.

---

## Chapter 6

# Using DeskView

---

This chapter includes the following topics:

- [About running tasks and policies](#)
- [Using DeskView Client Tools](#)
- [Running DeskView Client Tools using a command line](#)
- [Using DeskView Notifications](#)
- [Viewing the system data of a DeskView managed system](#)

## About running tasks and policies

You can run DeskView tools using tasks or task-based policies.

If you want a tool to run immediately or on a specific schedule, use tasks to run the tool.

However, the peculiarity of the task is the following: If a client computer happens to be offline or turned off at the time the task is scheduled to run, the task will fail to run on that computer.

If you want to make sure that, sooner or later, all computers run the tool, use task-based policies. When task-based policies are turned on, they are active at all times. When a computer that is turned off comes back online, it receives and executes the policy.

See [Viewing tasks and policies](#) on page 23.

## Viewing tasks and policies

You can run DeskView tools using tasks or task-based policies.

See [About running tasks and policies](#) on page 23.

### To view tasks

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. In the left pane, click **Tasks**.

### To view task-based policies

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. In the left pane, click **Policies**.

# Using DeskView Client Tools

When you install the DeskView Agent on client computers, the DeskFlash, DeskUpdate, DeskView BIOS Settings, DeskView Diagnostics, DeskView Energy Management, DeskOff, DeskView Security, and DeskView Serial Numbers client tools are installed as part of that installation.

DeskView solution includes the following tools:

<b>DeskView Tool</b>	<b>Description</b>
DeskFlash	Lets you archive and update the BIOS of the target system.  See <a href="#">Archiving and updating BIOS and BIOS settings</a> on page 24.
DeskView Energy Management - DeskOff	Lets you manage the power state of the target system.  See <a href="#">Managing the power state of the client computer</a> on page 26.
DeskUpdate	Lets you update the drivers on the target system.  See <a href="#">Updating drivers on the client systems</a> on page 28.
DeskView BIOS Settings	Lets you change BIOS settings on the target system.  See <a href="#">Configuring BIOS settings and enabling/disabling interfaces</a> on page 29.
DeskView Diagnostics	Lets you diagnose the hardware of the target system.  See <a href="#">Diagnosing client computers' hardware</a> on page 31.
DeskView Energy Management	Lets you manage power-saving schemes on the target systems.  See <a href="#">Changing power scheme settings</a> on page 32.
DeskView Security	Lets you disallow connecting mass storage devices to the target systems.  See <a href="#">Disabling mass storage devices</a> on page 33.
DeskView Serial Number	Lets you manage serial numbers of the target systems.  See <a href="#">Managing serial numbers</a> on page 34.

## Archiving and updating BIOS and BIOS settings

The DeskFlash tool lets you perform the following tasks remotely on client computers:

- Archive the BIOS
- Update the BIOS
- Update the BIOS settings
- Update processor microcodes

DeskFlash supports the .omf, .ocf, and .bup file formats for BIOS files.

The DeskFlash tool lets you make BIOS settings the same on all computers in your environment.

See [Using DeskFlash to harmonize BIOS settings in your environment](#) on page 25.

---

**Note**

You must run DeskFlash tools under an administrative user account.

---

---

**Warning**

When a DeskFlash tool runs on a mobile system, the tool checks if the system is plugged into the power source and if the system's battery charge level is more than 33%. If these conditions are not met, DeskFlash aborts the action and reports an error.

---

**To run a DeskFlash task**

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. In the left pane, click **Tasks > DeskFlash**.
3. Click the task you want to run.
4. In the right pane, configure the task.  
For help, in the Symantec Management Console, press **F1** or click **Help > Context**.
5. Run the task one time or on a schedule.  
For information on running tasks, see the *Symantec Management Platform Help*.

**To run a DeskFlash task-based policy**

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. In the left pane, click **Policies > DeskFlash**.
3. Select the policy you want to run.
4. In the right pane, configure the settings.  
For help, in the Symantec Management Console, press **F1** or click **Help > Context**
5. Configure the scheduling options.
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**.

## Using DeskFlash to harmonize BIOS settings in your environment

You can use the DeskFlash tools to harmonize BIOS settings in your environment by creating a reference BIOS and distributing it throughout your systems.

**To harmonize BIOS settings**

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. Do one of the following:

- If you want to use a task, in the left pane, click **Tasks > DeskFlash > Archive BIOS**.
  - If you want to use a task-based policy, in the left pane, click **Policies > DeskFlash > DeskView Archive BIOS policy**.

See [About running tasks and policies](#) on page 23.
- 3. Under BIOS Archive File, choose a path where you want to save the BIOS archive file.  
If you choose to save the archive file to a custom directory, we recommend that you use a network share that client computers can access.  
Example: `\\server\share`
- 4. Click **Specify name or pattern** and type a name for the BIOS archive file.  
Remember the name.  
For more information on the name formats, see [Archive BIOS task](#) on page 43.
- 5. Run the task or the policy on the computer that you want to use as a reference.
- 6. After the task or the policy has run, do one of the following:
  - If you want to use a task, in the left pane, click **Tasks > DeskFlash > Update BIOS settings**.
  - If you want to use a task-based policy, in the left pane, click **Policies > DeskFlash > DeskView Update BIOS settings policy**.  
See [About running tasks and policies](#) on page 23.
- 7. On the Update BIOS settings page, do one of the following:
  - If you want to upload the BIOS archive file to the client systems, click **Copy Selected BIOS Update Files to the systems** and browse for the BIOS Archive file you created in step 4.
  - If you want the client systems to download the BIOS archive file from a network share, click **Get BIOS Update Files from** and type the network share where you saved the file in step 4.  
Example: `\\server\share`  
DeskView can detect BIOS archive files automatically; however, if you want, you can click **Specify filename** and type the BIOS archive file name manually.
- 8. (Optional) Configure other settings.  
See [Update BIOS settings task](#) on page 46.
- 9. Click **Save changes**.
- 10. Run the task or the policy on the computers with the same hardware as on the reference computer.

## Managing the power state of the client computer

The DeskView Energy Management - DeskOff tool lets you perform the following tasks remotely on client computers:

- Restart the computer
- Turn off the computer
- Switch the computer into hibernate mode (works only if the hibernate mode is enabled)
- Switch the computer into standby mode

For example, you can use DeskOff to reduce energy usage in your enterprise by turning off the computers at a specific time.

See [Turning off client computers at a specific time](#) on page 27.

If you turn off or restart a client computer that has an application open, the user will be notified about the shutdown and prompted to save his work. You also have an option to force closing all applications without saving.

### To run a DeskView Energy Management - DeskOff task

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. In the left pane, click **Tasks > DeskView Energy Management > Change Power State**.
3. In the right pane, configure the task.  
For help, in the Symantec Management Console, press **F1** or click **Help > Context**
4. Run the task one time or on a schedule.  
For information on running tasks, see the *Symantec Management Platform Help*.

### To run a DeskView Energy Management - DeskOff task-based policy

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. In the left pane, click **Policies > DeskView Energy Management > DeskView Change Power State policy**.
3. In the right pane, configure the settings.  
For help, in the Symantec Management Console, press **F1** or click **Help > Context**
4. Configure the scheduling options.
5. Turn on the policy.  
To turn on the policy, at the upper right of the page, click the colored circle, and then click **On**.
6. Click **Save changes**.

## Turning off client computers at a specific time

You can use DeskOff to reduce energy usage in your enterprise by turning off the computers at a specific time.

### To turn off client computers at a specific time

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. In the left pane, click **Tasks > DeskView Energy Management > Change Power State**.
3. On the Change power state page, under DeskOff Command, click **Shutdown computer**.
4. If you want to close all open applications, losing all unsaved data, check **Terminate all applications currently running without query**.
5. By default, the tool will run under the Altiris Agent credentials. If you want to run the tool under a different user, click **Advanced** and configure a different user.
6. Under Task Status, on the toolbar, click **New Schedule**.
7. On the New Schedule page, under Schedule, click **Schedule**.

8. Click **At date/time**.
9. (Optional) Modify the date.
10. Specify the time when you want to turn off the computers, for example, 21:00.
11. If you want to repeat this task every day, check **Repeat every** and then select **1** and select **Days**.
12. Under Input, on the toolbar, on the Add menu, click **Target**.
13. Under Filtering rules, click **Add rule**, click **exclude computers not in**, click **Filter**, and select the computer filter you want the task to run on.  
To search for a filter, start typing the first characters of the filter's name. For example, to search for the Professional PCs filter in the list, type `prof` and then select Professional PCs from the drop-down list.  
Computers currently matching the filtering rules you created appear in the list. The task will run on these computers.
14. Click **OK**.
15. Click **Schedule**.
16. Under Task Status, monitor the task's execution.  
For information on running tasks, see the *Symantec Management Platform Help*.

## Updating drivers on the client systems

For a stable network, it is indispensable that the system drivers of the client computers are always kept up to date.

With DeskView you can easily update the drivers in two ways:

- Using the Fujitsu Technology Solutions Web site where the drivers are always kept actual
- Using the Fujitsu Technology Solutions Driver and Utility DVD or CD, which contain the driver versions you need for your clients

The DeskUpdate tool lets you update system drivers on client computers remotely from the Symantec Management Console.

### To run a DeskUpdate task

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. In the left pane, click **Tasks > DeskUpdate > Update drivers**.
3. In the right pane, configure the task.  
For help, in the Symantec Management Console, press **F1** or click **Help > Context**
4. Run the task one time or on a schedule.  
For information on running tasks, see the *Symantec Management Platform Help*.

### To run a DeskUpdate task-based policy

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. In the left pane, click **Policies > DeskUpdate > DeskView Update drivers policy**.
3. In the right pane, configure the settings.  
For help, in the Symantec Management Console, press **F1** or click **Help > Context**

4. Configure the scheduling options.
5. Turn on the policy.  
To turn on the policy, at the upper right of the page, click the colored circle, and then click **On**.
6. Click **Save changes**.

## Configuring BIOS settings and enabling/disabling interfaces

The DeskView BIOS Settings tool lets you perform the following tasks remotely on client computers:

- Set BIOS settings to default values.
- Change boot order.
- Update the BIOS setup password.
- Enable/disable the bluetooth controller.
- Enable/disable the floppy disk controller.
- Allow/disallow flashing BIOS.
- Enable/disable the infrared controller.
- Allow/disallow network boot using BOOTP or PXE.
- Enable/disable the parallel port controller.
- Enable/disable the USB host controller.
- Allow/disallow starting the computer with Wake on LAN.
- Enable/disable the wireless interface.
- Enable (Green PC) or disable the 0-Watt PC option or set an interval for remote management.
- Activate or deactivate the Audio Controller.
- Enable or disable Hyper-Threading.
- Enable or disable the boot menu (F12).
- Show/hide BIOS boot process diagnostic display
- Configure USB 1.1 / 2.0 support.
- Enable or disable the USB ports on the front of the computer.
- Enable or disable the USB ports on the rear of the computer.
- Determine how the unused USB ports should be processed based on device categories.
- Configure USB Legacy support.
- Enable or disable core multiprocessor functionality.
- Enable or disable Enhanced Intel SpeedStep Technology.
- Enable or disable Enhanced Idle Power State (additional power settings).
- Enable or disable Turbo Boost Technology.
- Enable or disable internal camera.

- Enable or disable the BIOS information message that the F2 key can be used during boot-up to jump into BIOS.
- Enable or disable the ability to boot from removable media.
- Enable or disable the Low Power Soft Off support.
- Enable or disable DASH support.
- Enable or disable hardware virtualisation.
- Enable or disable Non-Execution memory protection.
- Configure the PS/2 mouse configuration options.
- Enabled or disable the keyboard check during Boot.

For example, you can use the DeskView BIOS Settings tools to boot a computer from the network.

See [Booting a computer from the network](#) on page 30.

### To run a DeskView BIOS Settings task

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. In the left pane, click **Tasks > DeskView BIOS Settings**.
3. Select the appropriate category of BIOS settings.
4. Click the task you want to run.
5. In the right pane, configure the task.  
For help, in the Symantec Management Console, press **F1** or click **Help > Context**
6. Run the task one time or on a schedule.  
For information on running tasks, see the *Symantec Management Platform Help*.

### To run a DeskView BIOS Settings task-based policy

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. In the left pane, click **Policies > DeskView BIOS Settings**.
3. Select the appropriate category of BIOS settings.
4. Click the policy you want to run.
5. In the right pane, configure the settings.  
For help, in the Symantec Management Console, press **F1** or click **Help > Context**
6. Configure the scheduling options.
7. Turn on the policy.  
To turn on the policy, at the upper right of the page, click the colored circle.
8. Click **Save changes**.

## Booting a computer from the network

You can use DeskView BIOS Settings tasks to boot computers from a PXE server. To do this, first you run the Update LAN remote boot task to enable PXE boot, then you run the Update BIOS boot order task to change the boot order, and then you restart the computer. You can run all these tasks remotely from the Symantec Management Console, without touching the client system.

### To boot a computer from the network

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. In the left pane, click **Tasks > DeskView BIOS Settings > Boot > Update LAN remote boot options**.
3. If required, type the BIOS password.
4. Under LAN remote boot, click **Enable**.
5. Click **Save changes**.
6. Run the task.  
For information on running tasks, see the *Symantec Management Platform Help*.
7. After the task has run successfully, in the left pane, click **Tasks > DeskView BIOS Settings > Boot > Update BIOS boot order**.
8. If required, type the BIOS password.
9. Under Boot sequence, in the Applied Devices box, click **Network (e.g. PXE/BOOTP)**, and then click the **Move up** button until the selected device is at the top of the list.
10. Click **Save changes**.
11. Run the task on the same computer.  
For information on running tasks, see the *Symantec Management Platform Help*.
12. After the task has run successfully, in the left pane, click **Tasks > DeskView Energy Management > Change Power State**.
13. Under DeskOff Command, click **Restart computer**.
14. If you want to close all open applications, losing all unsaved data, check **Terminate all applications currently running without query**.
15. Click **Save changes**.
16. Run the task on the same computer.  
For information on running tasks, see the *Symantec Management Platform Help*.

## Diagnosing client computers' hardware

The DeskView Diagnostics tool lets you remotely diagnose the following hardware on client computers:

- Memory
- CPU
- HDD
- LAN

Before you can use the DeskView Diagnostics tool, you must install the DeskView Diagnostics Agent to client computers.

See [Installing the DeskView Diagnostics Agent](#) on page 19.

### To run DeskView Diagnostics

1. In the Symantec Management Console, on the Home menu, click **DeskView**.

2. In the left pane, click **Filters > DeskView Diagnostics > All DeskView Diagnostics enabled systems**.
3. In the right page, right-click the computer you want to diagnose, and then click **DeskView > Diagnostics > DeskView Diagnostics**.  
The hardware diagnostics task appears.
4. On the hardware diagnostics task page, configure the settings.  
For help, in the Symantec Management Console, press **F1** or click **Help > Context**.
5. Run the task one time or on a schedule.  
For information on running tasks, see the *Symantec Management Platform Help*.

### To view DeskView Diagnostics results

1. Open the Resource Manager for a computer.  
See [Accessing the Resource Manager](#) on page 41.
2. In the Resource Manager, on the View menu, click **Events**.
3. In the treeview pane, click **DeskView Events > DeskView Diagnostics Status**.
4. In the right pane, view the information.  
DeskView Diagnostics can skip some of the tests, for example, if no valid LAN adapter was found, or there is not enough disk space to perform an HDD test. This is not an error.  
If DeskView Diagnostics recognizes an error, a Diagnostics Code is displayed in the results.  
For more information on Diagnostics codes, see the *DeskView Client 6 User Manual* (click **Help > Documentation Library**).

## Changing power scheme settings

The DeskView Energy Management tool lets you activate the custom power scheme remotely on client computers. You can also run the task on schedule (for example, at system startup) to ensure the power options are always set according to your company's energy policy.

We recommend that you use the default power-saving settings provided by the DeskView Change power scheme settings task/policy for optimum power saving and performance.

Before you can use the DeskView Energy Management tool, you must install the Power Scheme Agent to client computers.

See [Installing the Altiris Power Scheme Agent](#) on page 20.

### To run a DeskView Energy Management task

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. In the left pane, click **Tasks > DeskView Energy Management > Change power scheme settings**.
3. In the right pane, configure the task.  
For help, in the Symantec Management Console, press **F1** or click **Help > Context**.
4. Run the task one time or on a schedule.  
For information on running tasks, see the *Symantec Management Platform Help*.

### To run a DeskView Energy Management task-based policy

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. In the left pane, click **Policies > DeskView Energy Management > DeskView Change power scheme settings policy**.
3. In the right pane, configure the settings.  
For help, in the Symantec Management Console, press **F1** or click **Help > Context**
4. Configure the scheduling options.
5. Turn on the policy.  
To turn on the policy, at the upper right of the page, click the colored circle, and then click **On**.
6. Click **Save changes**.

## Disabling mass storage devices

The DeskView Security tool lets you restrict usage of USB mass storage devices (Windows XP) and removable disks (Windows 7). You can use this task to prevent data larceny and unintentional bringing in of extraneous software, like viruses or games, from removable storage devices. You can lock the devices completely or set to read-only.

### To run a DeskView Security task

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. In the left pane, click **Tasks > DeskView Security**.
3. Click the task you want to run.
4. In the right pane, configure the task.  
For help, in the Symantec Management Console, press **F1** or click **Help > Context**
5. Run the task one time or on a schedule.  
For information on running tasks, see the *Symantec Management Platform Help*.

### To run a DeskView Security task-based policy

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. In the left pane, click **Policies > DeskView Security**.
3. Click the policy you want to run.
4. In the right pane, configure the settings.  
For help, in the Symantec Management Console, press **F1** or click **Help > Context**
5. Configure the scheduling options.
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**.

## Managing serial numbers

The DeskView Serial Numbers tool lets you write your own serial numbers remotely into the BIOS of the client computers. You can let DeskView generate the serial numbers or you can import your own list of numbers.

With the DeskView Serial Numbers tool you can perform the following tasks:

- View serial numbers you assigned to systems.
- Assign a serial number to a single system.
- Assign serial numbers using a pattern to multiple systems.
- Import the list of serial numbers from a .csv file, and assign the numbers to multiple systems.

### To view assigned serial numbers

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. In the left pane, click **Configuration > Manage Serial Numbers**.
3. Click **View serial numbers**.
4. Click **Next**.

### To assign a serial number to a single system

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. Do one of the following:
  - If you want to use a task, in the left pane, click **Tasks > DeskView Serial Number > Assign single serial number**.
  - If you want to use a task-based policy, in the left pane, click **Policies > DeskView Serial Number > DeskView Assign single serial number policy**.

See [About running tasks and policies](#) on page 23.
3. In the right pane, configure the settings.  
For help, in the Symantec Management Console, press **F1** or click **Help > Context**
4. Do one of the following:
  - If you are using the task, run the task one time or on a schedule.  
For information on running tasks, see the *Symantec Management Platform Help*.
  - If you are using the task-based policy, configure the scheduling options, turn on the policy, and click **Save changes**.

### To assign serial numbers using a pattern to multiple systems

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. Do one of the following:
  - If you want to use a task, in the left pane, click **Tasks > DeskView Serial Number > Generate serial number**.
  - If you want to use a task-based policy, in the left pane, click **Policies > DeskView Serial Number > DeskView Generate serial number policy**.

See [About running tasks and policies](#) on page 23.

3. In the right pane, configure the settings.  
For help, in the Symantec Management Console, press **F1** or click **Help > Context**
4. Do one of the following:
  - If you are using the task, run the task one time or on a schedule.  
For information on running tasks, see the *Symantec Management Platform Help*.
  - If you are using the task-based policy, configure the scheduling options, turn on the policy, and click **Save changes**.

### **To import the list of serial numbers from a .csv file and assign the numbers to multiple systems**

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. In the left pane, click **Configuration > Manage Serial Numbers**.
3. On the Manage Serial Numbers page, click **Export serial numbers**.
4. Click **Next**.
5. Select a filter that contains the computers you want to export.  
For example, select the "All DeskView managed systems" filter.
6. Click **Next**.
7. Click the **here** link to download the list of computers.
8. Click **Finish**.
9. Open the .csv file you downloaded in a text editor and populate the file with serial numbers.  
Serial numbers are located in the second column of the .csv file. The serial numbers must contain only alphanumeric characters.
10. On the Manage Serial Numbers page, click **Import serial numbers**.
11. Click **Next**.
12. Browse to the .csv file you edited in step 9.
13. Click **Next**.
14. Do one of the following:
  - If you want to use a task, in the left pane, click **Tasks > DeskView Serial Number > Apply imported serial numbers**.
  - If you want to use a task-based policy, in the left pane, click **Policies > DeskView Serial Number > DeskView Apply imported serial numbers policy**.

See [About running tasks and policies](#) on page 23.
15. Do one of the following:
  - If you are using the task, run the task one time or on a schedule.  
For information on running tasks, see the *Symantec Management Platform Help*.
  - If you are using the task-based policy, configure the scheduling options, turn on the policy, and click **Save changes**.

# Running DeskView Client Tools using a command line

The DeskView software contains a set of predefined tasks and task-based policies that let you run DeskView Client Tools from the Symantec Management Console. However, if you want to customize the way a DeskView Client Tool runs, you can run the tool using a customized command line. You can use the script task to run DeskView Client tools using a command line.

The command-line syntax and parameters are listed in the *DeskView Client 6 User Manual*, under the DeskView Client Components chapter. For your convenience, this document is included into the DeskView installation. You can find the *DeskView Client 6 User Manual* in the Symantec Management Console (click **Help > Documentation Library**). You can also download the document from the following Web site: [http://ts.fujitsu.com/solutions/it\\_infrastructure\\_solutions/manageability/deskview\\_downloads.html](http://ts.fujitsu.com/solutions/it_infrastructure_solutions/manageability/deskview_downloads.html)

DeskView includes a sample script task. The task's location is **Home > DeskView > Tasks > DeskView Sample Tasks and Jobs > Set BIOS Settings to predefined (local use) values**.

## To run a DeskView Client Tool using a command line

1. In the Symantec Management Console, on the Manage menu, click **Jobs and Tasks**.
2. In the left pane, click **Client Tasks > DeskView**.
3. Right-click the **DeskView** folder.
4. In the right-click menu, click **New > Job or Task**.
5. In the Create New Task dialog box, in the left pane, click **Run Script**.
6. In the right pane, type a new name for the script.
7. Click **OK**.  
This creates a new script task.
8. On the script task page, in the Script type drop-down list, click **Command Script**.
9. Under Script Details, type the commands you want to execute on the target client system.  
For more information, see the *DeskView Client 6 User Manual*.
10. (Optional) Configure the other settings.  
For help, in the Symantec Management Console, press **F1** or click **Help > Context**
11. Click **Save changes**.
12. Run the task one time or on a schedule.  
For information on running tasks, see the *Symantec Management Platform Help*.

## Using DeskView Notifications

DeskView Notifications let you monitor the hardware and software status of the client systems and receive alerts in the Symantec Management Console when the status changes.

For example, you can configure the client systems to report changes in the S.M.A.R.T. status of their hard drives. S.M.A.R.T. (Self-Monitoring, Analysis, and Reporting Technology) is a diagnostic system integrated into the hard disk, which monitors important parameters, such as temperature, running performance, and data throughput at all times. Receiving early S.M.A.R.T. alerts will help you identify failing hard drives before they become unreadable and important data is lost.

You can also configure DeskView to send you an email when a DeskView Notification is received.

For details about available notifications, see [Configure General Notification Selection](#) page on page 73.

To configure and start using DeskView Notifications, perform the following steps:

Step	Action	Description
Step 1	Configure the Notification Server computer.	You must configure the DCOM protocol on the computer where you installed the Symantec Management Platform.  See <a href="#">Configuring the Notification Server computer</a> on page 37.
Step 2	Select the notification you want to receive.	Various hardware and software notifications are available.  See <a href="#">Selecting notifications</a> on page 38.
Step 3	(Optional) Configure notifications email forwarding.	When a notification is received, DeskView will forward it to your email.  See <a href="#">Forwarding notifications by email</a> on page 38.
Step 4	Enable notifications.	You can enable sending notifications to Notification Server, displaying and logging them on the client computer.  See <a href="#">Enabling DeskView notifications</a> on page 39.
Step 5	(Optional) Change the notifications' settings.	For example, you can change the threshold values for free disk space notifications.  See <a href="#">Configuring the notification settings</a> on page 39.
Step 6	View DeskView notifications.	You can view notifications, sent by the client systems in the Symantec Management Console.  See <a href="#">Viewing DeskView notifications</a> on page 40.

## Configuring the Notification Server computer

DeskView clients use the Distributed Component Object Model (DCOM) wire protocol to transmit asynchronous notifications to Notification Server. Microsoft Windows Server 2003 Service Pack 1 introduced enhanced default security settings for the DCOM protocol, which can block DeskView Notifications functionality. To enable the reception of

DeskView notification on Microsoft Windows Server 2003 SP1, configure the DCOM settings using the Component Services snap-in Microsoft Management Console (MMC).

### To configure DCOM

1. On the Notification Server computer, click the Windows **Start** button, and then click **Run**.
2. Type `dcomcnfg` and click **OK**.
3. In the Component Services dialog box, in the tree pane, click **Component Services > Computers**.
4. In the results pane, right-click **My Computer**, and then click **Properties**.
5. On the COM Security tab, under Launch and Activation Permissions, click **Edit Limits**.
6. In the Launch Permission dialog box, click **Everyone**.
7. Set the following permissions for the Everyone group to "Allow":
  - Local Launch
  - Remote Launch
  - Local Activation
  - Remote Activation
8. Click **OK**.
9. On the COM Security tab, under Launch and Activation Permissions, click **Edit Default**.
10. Repeat steps 6 to 8 to configure the default security for launch permission.
11. Click **OK**.
12. Click **OK**.

## Selecting notifications

You can select the notifications you want to be informed about.

### To select notifications

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. In the left pane, click **Configuration > DeskView Notifications > Notifications Settings > Configure General Notification Selection**.
3. In the right pane, check the notifications you want to be informed about. For example, if you want to be notified of the hard drive failures, check the Hard disks (S.M.A.R.T.) notification. For help, in the Symantec Management Console, press **F1** or click **Help > Context**.
4. Click **Save**.

## Forwarding notifications by email

(Optional)

You can configure DeskView to send an email whenever a notification occurs.

### To configure notifications forwarding

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. In the left pane, click **Configuration > DeskView Notifications > Notification Forwarding > Configure General Notification Email Forwarding**.
3. In the right pane, check **Active**, and fill in the fields.  
For help, in the Symantec Management Console, press **F1** or click **Help > Context**
4. Click **Save**.

## Enabling DeskView notifications

You can enable DeskView notifications using the Enable/Disable Notifications policy.

### To enable DeskView notifications

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. In the left pane, click **Configuration > DeskView Notifications > Notifications Settings > DeskView Enable/Disable Notifications policy**.
3. In the right pane, check **Notifications enabled**.
4. (Optional) Configure other settings.  
For help, in the Symantec Management Console, press **F1** or click **Help > Context**
5. Turn on the policy.  
To turn on the policy, at the upper right of the page, click the colored circle, and then click **On**.
6. Click **Save changes**.

## Configuring the notification settings

(Optional)

After you enable notifications, you can change the settings for the following notifications:

- For the "Disk free space" and "System disk space" notifications you can change the error and warning threshold values.
- For the "Lease expiration" notification, you can change the lease expiration date and when to display the lease expiration warning.

### To configure notification settings using a task-based policy

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. In the left pane, click **Configuration > DeskView Notifications > Notifications Settings**.
3. Click the notification you want to configure.
4. In the right pane, configure the settings.  
For help, in the Symantec Management Console, press **F1** or click **Help > Context**
5. Configure the scheduling options.

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**.

## Viewing DeskView notifications

You can view notifications that the client systems sent to Notification Server from the reports or from the Resource Manager.

### To view a summary of DeskView notifications

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. In the left pane, click **Reports > Dashboards > DeskView Notifications**.

### To view new incoming DeskView notifications

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. In the left pane, click **Reports > Dashboards > DeskView New Notifications**.

### To view DeskView notifications for a single computer

1. Open the Resource Manager for a computer.  
See [Accessing the Resource Manager](#) on page 41.
2. In the Resource Manager, on the View menu, click **DeskView Notifications**.

## Viewing the system data of a DeskView managed system

When a computer has the DeskView Agent installed and sends inventory data to the database, it becomes a DeskView managed system.

You can view the system data of a specific DeskView managed system in the Resource Manager.

See [Accessing the Resource Manager](#) on page 41.

You can view the following information on DeskView managed systems:

- Inventory  
See [Viewing DeskView inventory](#) on page 41.
- Events  
See [Viewing DeskView events](#) on page 41.
- Notifications  
See [Viewing DeskView notifications](#) on page 40.
- System data  
See [Viewing DeskView System Data](#) on page 42.

## Accessing the Resource Manager

In the Resource Manager, DeskView displays information about the target computer.

### To open the Resource Manager from computer filters or reports

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. Click **Filters**.
3. Click a filter.  
For example, click **DeskView managed systems > Professional PCs**.
4. In the right pane, double-click the computer for which you want to open the Resource Manager.  
The Resource Manager opens in a new window.

### To open the Resource Manager directly

1. In the Symantec Management Console, on the Actions menu, click **Remote Management > Real-Time Management**.
2. On the Manage page, enter the host name or the IP of the computer for which you want to open the Resource Manager, and then click **Connect**.

## Viewing DeskView inventory

You can view the inventory collected by the DeskView agents in the Resource Manager.

### To view DeskView inventory

1. Open the Resource Manager window for the computer.  
See [Accessing the Resource Manager](#) on page 41.
2. On the View menu, click **Inventory**.
3. In the tree view pane, expand one of the following folders:
  - DeskView System Data  
This folder shows system data that is reported by the DeskView Agent.
  - DeskView System Settings  
This folder shows system settings that are reported by the DeskView Agent.
4. Click the item you want to view.

## Viewing DeskView events

You can use the Resource Manager to track DeskView events, such as Client Tools events, DeskView setup events, and DeskView Diagnostics events.

### To view DeskView events

1. Open the Resource Manager window for the computer.  
See [Accessing the Resource Manager](#) on page 41.
2. On the View menu, click **Events**.
3. In the tree view pane, expand the DeskView Events folder.
4. Click the item you want to view.

## Viewing DeskView System Data

The DeskView System Data page displays the following system data:

- Summary
- Details
- Mainboard
- Graphics
- Network
- Drives
- Software
- Characteristics

### To view DeskView System Data

1. Open the Resource Manager window for the computer.  
See [Accessing the Resource Manager](#) on page 41.
2. On the View menu, click **DeskView System Data**.  
For help, on the DeskView System Data page press **F1** or click **Help > Context**.

---

## Chapter 7

# Context-sensitive topics

---

This chapter includes the following topics:

- [DeskFlash tool](#)
- [DeskView Energy Management tool: Change Power State task](#)
- [DeskView Energy Management tool: Change power scheme settings task](#)
- [DeskUpdate tool: Update drivers task](#)
- [DeskView BIOS Settings tool](#)
- [DeskView Diagnostics tool: Hardware diagnostics task](#)
- [DeskView Security tool: Configure Mass Storage Access task](#)
- [DeskView Security tool: Configure Mass Storage Access task](#)
- [DeskView Notifications](#)
- [DeskView Serial Numbers tool](#)
- [DeskView System Data page](#)
- [DeskView Notifications page](#)
- [Cleanup Inventory Cache task](#)

## DeskFlash tool

This section includes the following topics:

- [Archive BIOS task](#)
- [Update BIOS task](#)
- [Update BIOS settings task](#)
- [Update processor microcodes task](#)

## Archive BIOS task

This task archives the BIOS together with the BIOS setup settings and microcode patches.

See [Archiving and updating BIOS and BIOS settings](#) on page 24.

You can use the BIOS archive files that you create with this task to deploy the identical BIOS settings to other systems.

See [Using DeskFlash to harmonize BIOS settings in your environment](#) on page 25.

---

### Note

You must run DeskFlash tools under an administrative user or system account.

---

The following options are available on this page:

<b>Option</b>	<b>Description</b>
<b>Path</b>	
Directory	<p>Click if you want to store BIOS archive files in a custom working directory. Type the path for the custom working directory.</p> <p>We recommend that you type a network share. Example: <code>\\server\share</code></p> <p>You can also specify a directory on the client system. Example: <code>C:\BIOS_update_files\</code></p>
Store on the Notification Server computer	<p>Click if you want to store BIOS archive files at the default storage that is located on the Notification Server computer.</p> <p>This option lets you store BIOS archive files on the Notification Server computer by using the system account.</p>
<b>File name</b>	
Automatic	<p>Click to create the file with the name based on the internal name syntax (systemname_mainboardname_date_time.bup).</p> <p>Example: <code>MYPC_D1837_12-12-2008_110000.BUP</code></p>
Specify name or pattern	<p>Click to create the file with a custom name. Specify the name of the BIOS archive file.</p> <p>You can create the file with a name according to the pattern specified.</p> <p>You can use the following variables:</p> <ul style="list-style-type: none"><li>• #domain# = System domain</li><li>• #name# = Computer name</li><li>• #system# = System board (mainboard)</li><li>• #date# = Current date</li><li>• #time# = Current time in the format HHMMSS</li><li>• #no# = Automatically generated serial number</li></ul> <p>You can mix fixed name components and variables.</p> <p>Example: <code>MyArch_#name#_#date#.bup</code></p>
Overwrite existing archive	<p>Check to overwrite the archive if a file with the same name already exists in the directory you specified.</p>

Option	Description
<b>User interaction</b>	
Show warning during archive	Check to show a warning message on the system whose BIOS is being archived.
<b>Execution environment</b>	
Run with rights	Select a user with administrative privileges.

## Update BIOS task

This task lets you update the system BIOS.

See [Archiving and updating BIOS and BIOS settings](#) on page 24.

If you use the BIOS archive file that was previously created using the Archive BIOS task, then the Update BIOS task modifies both the BIOS setup settings and microcode patches.

If you use the BIOS update file provided by Fujitsu Technology Solutions, the BIOS setup settings are not modified.

### Note

You must run DeskFlash tools under an administrative user or system account.

The following options are available on this page:

Option	Description
<b>BIOS update file</b>	
Copy Selected BIOS Update Files to the system	<p>Click if you want to upload the BIOS update file to the client system. With this option you can copy BIOS update files to the client system by using the system account.</p> <p>Click <b>Browse</b> and navigate to the BIOS update file that you want the client systems to use.</p> <p>When you click <b>Save changes</b>, this file is uploaded to a share that is located on the Notification Server computer. Then, when the task runs, client systems download the file and store it locally.</p> <p>You can specify more than one file.</p>

<b>Option</b>	<b>Description</b>
Get BIOS Update Files from	<p>Click if you want the client systems to use the BIOS update file located at a specific location.</p> <p>For example, you can specify a network share.</p> <p>Example: <code>\\server\share</code></p> <p>Make sure this share is accessible by all client computers and available until the last computer has run the task.</p> <p>You can also specify a directory on the client system.</p> <p>Example: <code>C:\BIOS_update_files\</code></p>
Automatically select matching file	<p>Click to detect the BIOS update file automatically. DeskFlash can select the appropriate BIOS update file if there is more than one BIOS update file in a directory.</p> <p>This option can slightly increase network traffic.</p>
Specify filename	<p>Click if you want to specify the BIOS update file manually.</p> <p>Example: <code>D1837*.bup</code></p>
Allow to overwrite BIOS by older or equal version	<p>Check if you want to overwrite the BIOS on the client system, even if the update file does not contain a newer BIOS.</p>
<b>User interaction</b>	
Wait for user OK	<p>Click to prompt the local user to accept the task run request. The user will be warned that he should not bring the system to standby or hibernate states before the next restart.</p>
Show warning during flash	<p>Click to run the task immediately. The user will be warned that the task is in progress.</p>
No user interaction	<p>Click to run the task immediately. No message will appear on the client system. Use this option if you run this tool on computers with no users logged on, for example, if you schedule this tool to run at night.</p>
<b>Execution environment</b>	
Run with rights	<p>Select a user with administrative privileges.</p>

## Update BIOS settings task

This task lets you update the BIOS settings.

See [Archiving and updating BIOS and BIOS settings](#) on page 24.

### Note

You must run DeskFlash tools under an administrative user or system account.

The following options are available on this page:

Option	Description
<b>BIOS update file</b>	
Copy Selected BIOS Update Files to the system	<p>Click if you want to upload the BIOS update file to the client system. With this option you can copy BIOS update files to the client by using the system account.</p> <p>Click <b>Browse</b> and navigate to the BIOS update file that you want the client systems to use.</p> <p>When you click <b>Save changes</b>, this file is uploaded to a share that is located on the Notification Server computer. Then, when the task runs, client systems download the file and store it locally.</p> <p>You can specify more than one file.</p>
Get BIOS Update Files from	<p>Click if you want the client systems to use the BIOS update file located at a specific location.</p> <p>For example, you can specify a network share.</p> <p>Example: <code>\\server\share</code></p> <p>Make sure this share is accessible by all client computers and available until the last computer has run the task.</p> <p>You can also specify a directory on the client system.</p> <p>Example: <code>C:\BIOS_update_files\</code></p>
Automatically select matching file	<p>Click to detect the BIOS update file automatically. DeskFlash can select the appropriate BIOS update file if there is more than one BIOS update file in a directory.</p> <p>This option can slightly increase network traffic.</p>
Specify filename	<p>Click if you want to specify the BIOS update file manually.</p> <p>Example: <code>D1837*.bup</code></p>
If BIOS versions differ, perform complete BIOS update	<p>Check if you want to update the BIOS on the client system in addition to changing BIOS settings, if the BIOS versions differ.</p> <p>When unchecked, and the BIOS versions differ, the BIOS settings will not be changed.</p>
<b>User interaction</b>	
Wait for user OK	<p>Click to prompt the local user to accept the task run request. The user will be warned that he should not bring the system to standby or hibernate states before the next restart.</p>

<b>Option</b>	<b>Description</b>
Show warning during flash	Click to run the task immediately. The user will be warned that the task is in progress.
No user interaction	Click to run the task immediately. No message will appear on the client system. Use this option if you run this tool on computers with no users logged on, for example, if you schedule this tool to run at night.
<b>Execution environment</b>	
Run with rights	Select a user with administrative privileges.

## Update processor microcodes task

This task lets you update the processor microcodes.

See [Archiving and updating BIOS and BIOS settings](#) on page 24.

### Note

You must run DeskFlash tools under an administrative user or system account.

The following options are available on this page:

<b>Option</b>	<b>Description</b>
<b>BIOS update file</b>	
Copy Selected BIOS Update Files to the system	<p>Click if you want to upload the BIOS update file to the client system. With this option you can copy BIOS update files to the client by using the system account.</p> <p>Click <b>Browse</b> and navigate to the BIOS update file that you want the client systems to use.</p> <p>When you click <b>Save changes</b>, this file is uploaded to a share that is located on the Notification Server computer. Then, when the task runs, client systems download the file and store it locally.</p> <p>You can specify more than one file.</p>
Get BIOS Update Files from	<p>Click if you want the client systems to use the BIOS update file located at a specific location.</p> <p>For example, you can specify a network share.</p> <p>Example: <code>\\server\share</code></p> <p>Make sure this share is accessible by all client computers and available until the last computer has run the task.</p> <p>You can also specify a directory on the client system.</p> <p>Example: <code>C:\BIOS_update_files\</code></p>

<b>Option</b>	<b>Description</b>
Automatically select matching file	Click to detect the BIOS update file automatically. DeskFlash can select the appropriate BIOS update file if there is more than one BIOS update file in a directory.  This option can slightly increase network traffic.
Specify filename	Click if you want to specify the BIOS update file manually.  Example: D1837*.bup
<b>User interaction</b>	
Wait for user OK	Click to prompt the local user to accept the task run request. The user will be warned that he should not bring the system to standby or hibernate states before the next restart.
Show warning during flash	Click to run the task immediately. The user will be warned that the task is in progress.
No user interaction	Click to run the task immediately. No message will appear on the client system. Use this option if you run this tool on computers with no users logged on, for example, if you schedule this tool to run at night.
<b>Execution environment</b>	
Run with rights	Select a user with administrative privileges.

## DeskView Energy Management tool: Change Power State task

This task lets you turn off or restart a computer.

See [Managing the power state of the client computer](#) on page 26.

The following options are available on this page:

<b>Option</b>	<b>Description</b>
Restart computer	Click to restart computers.
Shutdown computer	Click to turn off computers.
Terminate all applications currently running without query!	Check to log off the user even if applications are opened on the target computer. All unsaved work will be lost.  When not selected, a logoff will not be performed until the user closes all applications.

## DeskView Energy Management tool: Change power scheme settings task

This task lets you change the power scheme settings on the target computers.

You must install the Altiris Power Scheme Agent before you can run this task.

See [Installing the Altiris Power Scheme Agent](#) on page 20.

---

### Note

Computers that are running the Microsoft Windows 2000, 2003, or XP operating system cannot display custom period values in the Control Panel > Power Options Properties dialog.

---

## DeskUpdate tool: Update drivers task

For a stable network, it is indispensable that the system drivers of the client computers are always kept up to date.

With DeskView you can easily update the drivers in two ways:

- Using the Fujitsu Technology Solutions Web site where the drivers are always kept actual
- Using the Fujitsu Technology Solutions Driver and Utility DVD or CD, which contain the driver versions you need for your client computers

This task lets you update system drivers on client computers.

See [Updating drivers on the client systems](#) on page 28.

The following options are available on this page:

Option	Description
Fujitsu Technology Solutions Web site	Click to download drivers from the Fujitsu Technology Solutions Web site.  This option requires the client computers to be connected to the Internet.
Custom directory	Click to load the drivers from a local network share.  Type a path to the "deskupdate" folder of the Fujitsu Technology Solutions Driver and Utility DVD or CD, which contains the driver versions you need for your client computers is located.  This option does not require an Internet connection.
Drivers	Select this option to update all Fujitsu Drivers.
System Related Applications	Select this option to update all hardware specific Fujitsu applications.
Fujitsu recommended Windows® Software Updates	Select this option to update all Fujitsu recommended Windows Hotfixes.

# DeskView BIOS Settings tool

This section includes the following topics:

- [Set BIOS-Default values task](#)
- [Update BIOS boot order task](#)
- [Update BIOS password task](#)
- [Update bluetooth options task](#)
- [Update diskette controller options task](#)
- [Update flash write protection options task](#)
- [Update infrared options task](#)
- [Update LAN remote boot options task](#)
- [Update parallel port options task](#)
- [Update USB host controller options task](#)
- [Update Wake on LAN options task](#)
- [Update WLAN options task](#)
- [Update 0-Watt PC options task](#)
- [Update Audio Controller options task](#)
- [Update Hyper Threading options task](#)
- [Update Memory Protection options task](#)
- [Update Virtualization options task](#)
- [Update POST Diagnostic Screen options task](#)
- [Update Show Boot Menu Prompt \(F12\) options task](#)
- [Update USB Port Compatibility options task](#)
- [Update Front USB ports options task](#)
- [Update Rear USB ports options task](#)
- [Update Core multi-processing options task](#)
- [Update Enhanced Intel Speedstep Technology options task](#)
- [Update Enhanced Idle Power State options task](#)
- [Update Turbo Boost Technology options task](#)
- [Update Internal camera options task](#)
- [Update Show setup prompt \(F2\) options task](#)
- [Update USB legacy support options task](#)
- [Update Boot from removable media options task](#)
- [Update Low Power Soft Off options task](#)
- [Update DASH technology support options task](#)
- [Update Keyboard check options task](#)
- [Update PS/2 Mouse configuration options task](#)

- [Update USB ports options task](#)

## Set BIOS-Default values task

This task lets you revert all the values in the BIOS of the client computers to their default settings.

See [Configuring BIOS settings and enabling/disabling interfaces](#) on page 29.

The following options are available on this page:

Option	Description
Existing BIOS password	If necessary, enter the BIOS setup password.

## Update BIOS boot order task

This task lets you update the BIOS boot order of the client computers. You can specify the sequence of drives or system components that the BIOS will search for during the boot process.

See [Configuring BIOS settings and enabling/disabling interfaces](#) on page 29.

The following options are available on this page:

Option	Description
Existing BIOS password	If necessary, enter the BIOS setup password.
Boot Sequence	Use the <b>Add</b> , <b>Remove</b> , <b>Move up</b> , and <b>Move down</b> buttons to specify the sequence of drives and system components that the BIOS searches for during the boot process to start the operating system.  Add only the really required devices into the bootorder, because devices which are not present in the client's boot devices list will fail the task.

## Update BIOS password task

This task lets you update the BIOS setup password of the client computers. The supervisor password prevents unauthorized call up of BIOS Setup. Only those who know the supervisor password can call up BIOS Setup.

See [Configuring BIOS settings and enabling/disabling interfaces](#) on page 29.

The following options are available on this page:

Option	Description
Existing password	If necessary, enter the BIOS setup password.
New password	Enter a new password. All alphanumeric characters can be used. No differentiation is made between upper-case and lower-case.  <b>Warning</b> Don't use the numerical keypad to enter digits.
Confirm password	Re-enter the new password.

## Update bluetooth options task

This task lets you enable or disable the bluetooth interface of the client computers.

This item is only available on models featuring onboard Bluetooth.

See [Configuring BIOS settings and enabling/disabling interfaces](#) on page 29.

The following options are available on this page:

Option	Description
Existing BIOS password	If necessary, enter the BIOS setup password.
Bluetooth	Select if you want to enable or disable bluetooth on the client computers.  Disable: Bluetooth is disabled.  Enable: Bluetooth is enabled.

## Update diskette controller options task

This task lets you enable or disable the built-in floppy disk controller on the mainboard of the client computers.

This item is only available on models with an onboard diskette controller.

See [Configuring BIOS settings and enabling/disabling interfaces](#) on page 29.

The following options are available on this page:

Option	Description
Existing BIOS password	If necessary, enter the BIOS setup password.
Diskette controller	Select if you want to enable or disable the floppy disk controller (IRQ 6) on the client computers.  Disable: The onboard diskette controller is disabled.  Enable: The diskette controller is enabled.

## Update flash write protection options task

This task lets you write-protect the system BIOS flash memory of the client computers and prevent the BIOS from being re-programmed.

See [Configuring BIOS settings and enabling/disabling interfaces](#) on page 29.

The following options are available on this page:

Option	Description
Existing BIOS password	If necessary, enter the BIOS setup password.
Flash write	Select if you want to enable or disable the flash write ability.  Enable: The system BIOS can be written to or deleted if the corresponding switch (see manual for the mainboard) is set accordingly. Flash BIOS update is possible.  Disable: The flash write-protection is set. The System BIOS can neither be written to nor deleted. Flash BIOS update is not possible.  See <a href="#">Archiving and updating BIOS and BIOS settings</a> on page 24.

## Update infrared options task

This task lets you enable or disable the onboard infrared controller of the client computers.

See [Configuring BIOS settings and enabling/disabling interfaces](#) on page 29.

The following options are available on this page:

Option	Description
Existing BIOS password	If necessary, enter the BIOS setup password.
Infrared	Select if you want to enable or disable the infrared controller on the client computers.  Enable: The infrared controller is enabled.  Disable: The infrared controller is disabled.

## Update LAN remote boot options task

This task lets you enable or disable booting from a server using either BOOTP (Bootstrap Protocol) or PXE (Preboot Execution Environment) protocol.

This function is used in particular when neither floppy disk nor hard disk drives are installed, or these have been disabled.

See [Configuring BIOS settings and enabling/disabling interfaces](#) on page 29.

The following options are available on this page:

Option	Description
Existing BIOS password	If necessary, enter the BIOS setup password.
LAN remote boot	Select if you want to enable or disable booting from the network on the client computers.  Enable: LAN remote boot is activated and allows the operating system to be loaded from a server via a local network connection. Enabling LAN remote boot does not force a LAN boot.  If a LAN boot is required you also have to update the BIOS boot order.  Disable: LAN Remote Boot is deactivated.

## Update parallel port options task

This task lets you enable or disable the onboard parallel port controller of the client computers.

See [Configuring BIOS settings and enabling/disabling interfaces](#) on page 29.

The following options are available on this page:

Option	Description
Existing BIOS password	If necessary, enter the BIOS setup password.
Parallel port	Select if you want to enable or disable the parallel port controller on the client computers.  Enable: The parallel port is enabled and automatically set to an available combination (address, interrupt).  Disable: The parallel port is disabled.

## Update USB host controller options task

This task lets you specify whether the USB hardware can be switched on the client computers. If this function is disabled, the USB controller will not be recognized by any operating system and no USB device (such as USB mouse, USB keyboard, USB SmartCard reader or USB mass storage devices) can be operated as a result.

See [Configuring BIOS settings and enabling/disabling interfaces](#) on page 29.

The following options are available on this page:

Option	Description
Existing BIOS password	If necessary, enter the BIOS setup password.
USB host controller	Select if you want to enable or disable the USB host controller on the client computers.  Enable: The USB 2.0 Host Controller will be set to 'Enabled', and the USB Legacy Support and the USB BIOS Supported Devices parameters will be set to 'Enabled' and 'Auto' respectively, in the client computer's BIOS. The USB Boot Delay parameter setting will not change.  Disable: The USB 2.0 Host Controller will be set to 'Disabled', and the USB Legacy Support and the USB BIOS Supported Devices parameters will be set to 'Disabled' and 'None' respectively, in the client computer BIOS. In addition, the USB Boot Delay parameter will be set to '0 seconds'.

## Update Wake on LAN options task

This task lets you allow or disallow the client computers to be switched on by means of network signals (Magic Packet) that are received by the LAN controller (Wake on LAN).

See [Configuring BIOS settings and enabling/disabling interfaces](#) on page 29.

### Warning

If you enable the Wake On LAN option, the BIOS Setup password check will be disabled at startup (if the computer BIOS supports this feature). This BIOS setting prevents the computer from prompting the user for a password during the Wake on LAN startup.

The following options are available on this page:

Option	Description
Existing BIOS password	If necessary, enter the BIOS setup password.
Wake on LAN	Select if you want to enable or disable Wake on LAN on the client computers.  Enable: Wake On LAN will be enabled  Disable: Wake On LAN will be disabled.

## Update WLAN options task

This task lets you enable or disable the onboard wireless interface of the client computers.

See [Configuring BIOS settings and enabling/disabling interfaces](#) on page 29.

The following options are available on this page:

Option	Description
Existing BIOS password	If necessary, enter the BIOS setup password.
WLAN	Select if you want to enable or disable the wireless interface on the client computers.  Enable: The onboard WLAN controller is enabled.  Disable: The onboard WLAN controller is disabled.

## Update 0-Watt PC options task

This task lets you enable or disable the 0-Watt PC options or specify a time interval in which the client computers can be remotely managed. Enabling the 0-Watt PC option means that the power consumption in switched-off state is reduced to 0 Watt (Green PC).

See [Configuring BIOS settings and enabling/disabling interfaces](#) on page 29.

The following options are available on this page:

Option	Description
Existing BIOS password	If necessary, enter the BIOS setup password.
Settings for a switched off 0 Watt PC	Select if you want to enable, disable or configure the 0-Watt PC options on the client computers.  Enable 0-Watt Feature: The power consumption is 0-Watt (Green-PC). In this state the computer cannot be remotely woken and administered.  Disable 0-Watt Feature: The computer can be remotely woken and administered.  Enable Remote Management: On this setting a time must be specified at which point the computer must switch from power-saving mode into administrative mode. Also a time must be specified at which point the computer must switch from administered mode into power-saving mode.  Both time formats are hh:mm (hours:minutes)

## Update Audio Controller options task

This task activates or deactivates the Audio Controller of the client computers. If the audio controller is equipped on the mainboard, it can be switched on or off.

See [Configuring BIOS settings and enabling/disabling interfaces](#) on page 29.

The following options are available on this page:

Option	Description
Existing BIOS password	If necessary, enter the BIOS setup password.
Audio Controller	Select if you want to enable or disable the audio controller on the client computers.  Enable: All audio controllers are enabled. The system BIOS determines which system resources (interrupts, addresses, DMAs) are occupied.  Disable: The onboard audio controller is disabled.

## Update Hyper Threading options task

This task lets you enable or disable the hyper threading option of the client computers.

See [Configuring BIOS settings and enabling/disabling interfaces](#) on page 29.

The following options are available on this page:

Option	Description
Existing BIOS password	If necessary, enter the BIOS setup password.
Hyper Threading	Select if you want to enable or disable the hyper threading option on the client computers.  Enable: An ACPI operating system can use all logical processors within a physical processor.  Disable: An ACPI operating system can only use the first logical processor of the physical processor. This setting should only be used if hyper-threading technology has not been correctly implemented in the ACPI operating system.

## Update Memory Protection options task

This task lets you enable or disable the memory protection option of the client computers. This option defines the protection for executable memory areas (anti-virus protection). The function is only effective if it is supported by the operating system, too.

See [Configuring BIOS settings and enabling/disabling interfaces](#) on page 29.

The following options are available on this page:

Option	Description
Existing BIOS password	If necessary, enter the BIOS setup password.
Memory Protection	Select if you want to enable or disable the memory protection option on the client computers.  Enable: Enables the operating system to switch on the function "Execute Disable" or "No Execute".  Disable: Prevents the operating system from being able to switch on the function "Execute Disable" or "No Execute".

## Update Virtualization options task

This task lets you enable or disable the Intel Virtualization Technology for Directed I/O options of the client computers. VT-d is a hardware support for the common use of I/O devices by several virtual machines. VMM systems (Virtual Machine Monitor) can use VT-d to manage several virtual machines which access the same I/O devices.

See [Configuring BIOS settings and enabling/disabling interfaces](#) on page 29.

The following options are available on this page:

Option	Description
Existing BIOS password	If necessary, enter the BIOS setup password.
Virtualization	Select if you want to enable or disable the virtualization option on the client computers.  Disable: VT-d is disabled and is not available for VMMs.  Enable: VT-d is available.

## Update POST Diagnostic Screen options task

This task lets you enable or disable the POST Diagnostics Screen options of the client computers. This option specifies whether the Boot menu can be invoked during the POST process by pressing the F12 key.

See [Configuring BIOS settings and enabling/disabling interfaces](#) on page 29.

The following options are available on this page:

Option	Description
Existing BIOS password	If necessary, enter the BIOS setup password.
POST Diagnostic Screen	Choose, if you want to see the POST Diagnostic Screen or the Boot Logo during system boot on the client computer.  Enable: The POST information will be displayed on the screen.  Disable: The boot logo is displayed. The system will switch to displaying the POST diagnostic screen if the Esc key is pressed or errors occur.

## Update Show Boot Menu Prompt (F12) options task

This task lets you enable or disable the Show boot menu prompt (F12) options of the client computers. This option specifies whether the Boot menu can be invoked during the POST process by pressing the F12 key.

See [Configuring BIOS settings and enabling/disabling interfaces](#) on page 29.

The following options are available on this page:

Option	Description
Existing BIOS password	If necessary, enter the BIOS setup password.
Show boot menu prompt (F12)	Select if you want to enable or disable the Show boot menu prompt (F12) options on the client computers.  Enable: The Boot menu can be invoked.  Disable: The Boot menu cannot be invoked.

## Update USB Port Compatibility options task

This task lets you enable or disable the USB Port Compatibility options of the client computers. This option defines which USB host controller speeds are supported.

See [Configuring BIOS settings and enabling/disabling interfaces](#) on page 29.

The following options are available on this page:

Option	Description
Existing BIOS password	If necessary, enter the BIOS setup password.
USB Port Compatibility	Select if you want to enable or disable the USB Port Compatibility options on the client computers.  USB 1.1: Only the USB 1.1 host controller is enabled.  USB 2.0: The USB 1.1 and USB 2.0 controllers are enabled.  Only choose USB 1.1 when absolutely necessary. In some cases certain USB ports will not be available if USB 1.1 has been selected. The setting USB 2.0 ensures that all USB ports are available.

## Update Front USB ports options task

This task lets you enable or disable the Front USB ports options of the client computers.

See [Configuring BIOS settings and enabling/disabling interfaces](#) on page 29.

The following options are available on this page:

Option	Description
Existing BIOS password	If necessary, enter the BIOS setup password.
Front USB ports	Select if you want to enable or disable the Front USB ports options on the client computers.  Enable: The front USB ports will be operational.  Disable: The front USB ports will not be operational.

## Update Rear USB ports options task

This task lets you enable or disable the Rear USB ports options of the client computers.

See [Configuring BIOS settings and enabling/disabling interfaces](#) on page 29.

The following options are available on this page:

Option	Description
Existing BIOS password	If necessary, enter the BIOS setup password.
Rear USB ports	Select if you want to enable or disable the Rear USB ports options on the client computers.  Enable: The rear USB ports will be operational.  Disable: The rear USB ports will not be operational.

## Update Core multi-processing options task

This task lets you enable or disable the core multi-processing options of the client computers.

See [Configuring BIOS settings and enabling/disabling interfaces](#) on page 29.

The following options are available on this page:

Option	Description
Existing BIOS password	If necessary, enter the BIOS setup password.
Core multi-processing	Select if you want to enable or disable the Core multi-processing options on the client computers.  Disable: All but one logical processors are deactivated.  Enable: All available logical processors are active.

## Update Enhanced Intel Speedstep Technology options task

This task lets you enable or disable the Enhanced Intel Speedstep Technology options of the client computers. "Enhanced Intel SpeedStep® Technology" (EIST) is an energy saving function. The processor clock rate is adapted to the respective system requirements. A reduction in the clock frequency causes less power to be required by the system.

See [Configuring BIOS settings and enabling/disabling interfaces](#) on page 29.

The following options are available on this page:

Option	Description
Existing BIOS password	If necessary, enter the BIOS setup password.
Enhanced Intel Speedstep Technology	Select if you want to enable or disable the Enhanced Intel Speedstep Technology options on the client computers.  Disable: Enhanced SpeedStep functionality is not available.  Enable: Enhanced SpeedStep functionality is available.

## Update Enhanced Idle Power State options task

This task lets you enable or disable the Enhanced Idle Power State options of the client computers. If supported by the operating system, the CPU is stopped if possible (C2 state / stop clock) to save energy.

See [Configuring BIOS settings and enabling/disabling interfaces](#) on page 29.

The following options are available on this page:

Option	Description
Existing BIOS password	If necessary, enter the BIOS setup password.
Enhanced Idle Power State	Select if you want to enable or disable the Enhanced Idle Power State options on the client computers.  Disable: Enhanced Idle Power State functionality is not available.  Enable: Enhanced Idle Power State functionality is available.

## Update Turbo Boost Technology options task

This task lets you enable or disable the Turbo Boost Technology options of the client computers. The Turbo Boost Technology permits an acceleration of the processor above the specified frequency when the operating system requests a higher performance state (P0).

See [Configuring BIOS settings and enabling/disabling interfaces](#) on page 29.

The following options are available on this page:

Option	Description
Existing BIOS password	If necessary, enter the BIOS setup password.
Turbo Boost Technology	Select if you want to enable or disable the Turbo Boost Technology options on the client computers.  Disable: Turbo Boost Technology is not available.  Enable: Turbo Boost Technology is available.

## Update Internal camera options task

This task lets you enable or disable the built-in Internal camera options of the client computers.

See [Configuring BIOS settings and enabling/disabling interfaces](#) on page 29.

The following options are available on this page:

Option	Description
Existing BIOS password	If necessary, enter the BIOS setup password.
Internal camera	Select if you want to enable or disable the Internal camera options on the client computers.  Disable: The Internal Camera is Disabled.  Enable: The Internal Camera is enabled.

## Update Show setup prompt (F2) options task

This task lets you enable or disable the Show BIOS setup prompt (F2) options of the client computers.

See [Configuring BIOS settings and enabling/disabling interfaces](#) on page 29.

The following options are available on this page:

<b>Option</b>	<b>Description</b>
Existing BIOS password	If necessary, enter the BIOS setup password.
Show setup prompt (F2)	Select if you want to enable or disable the Show setup prompt (F2) options on the client computers.  Disable: Does not display the BIOS setup prompt (F2).  Enable: Displays the BIOS setup prompt

## Update USB legacy support options task

This task lets you enable or disable the USB legacy support options of the client computers.

See [Configuring BIOS settings and enabling/disabling interfaces](#) on page 29.

The following options are available on this page:

<b>Option</b>	<b>Description</b>
Existing BIOS password	If necessary, enter the BIOS setup password.
USB legacy support	Select if you want to enable or disable the USB legacy support options on the client computers.  Disable: No USB Legacy Support.  Enable: All USB Legacy devices are supported.

## Update Boot from removable media options task

This task lets you enable or disable the Boot from removable media options of the client computers. This options allows supervisors to prevent users from booting from any removable media (the floppy disk, CD-ROM, DVD and CD-R/RW)

See [Configuring BIOS settings and enabling/disabling interfaces](#) on page 29.

The following options are available on this page:

<b>Option</b>	<b>Description</b>
Existing BIOS password	If necessary, enter the BIOS setup password.
Boot from removable media	Select if you want to enable or disable the Boot from removable media options on the client computers.  Disable: Boot from removable media is disabled.  Enable: It's possible to boot from removable media.

## Update Low Power Soft Off options task

This task lets you enable or disable the Low Power Soft Off - sometimes also called "Deep Power-Off" - options of the client computers. This means that the PC is disconnected from the power supply and can only be switched on via the ON/OFF switch.

See [Configuring BIOS settings and enabling/disabling interfaces](#) on page 29.

The following options are available on this page:

Option	Description
Existing BIOS password	If necessary, enter the BIOS setup password.
Low Power Soft Off	Select if you want to enable or disable the Low Power Soft Off options on the client computers.  Enable: Deep Power-Off is available.  Disable: Deep Power-Off is not available.

## Update DASH technology support options task

This task lets you enable or disable the DASH technology support options of the client computers.

See [Configuring BIOS settings and enabling/disabling interfaces](#) on page 29.

Each DASH Profile is described in detail in a corresponding PDF File, which used the profile code as it's name. For example the CPU profile code is DSP 1022 and the corresponding PDF file is call DSP1022.pdf. Additional information can be found at

<http://www.dmtf.org/>

The following options are available on this page:

Option	Description
Existing BIOS password	If necessary, enter the BIOS setup password.
DASH technology support	Select if you want to enable or disable the DASH technology support options on the client computers.  Disable: The DASH technology feature is disabled.  Enable: The DASH technology feature is enabled on the client computer.

## Update Keyboard check options task

This task lets you enable or disable the Keyboard check options of the client computers. This option specifies whether the system performs a keyboard check. This setting is especially convenient for systems which are operated without a keyboard.

See [Configuring BIOS settings and enabling/disabling interfaces](#) on page 29.

The following options are available on this page:

Option	Description
Existing BIOS password	If necessary, enter the BIOS setup password.
Keyboard check	Select if you want to enable or disable the Keyboard check options on the client computers.  Enable: The keyboard test is performed.  Disable: The keyboard test is not performed. Any keyboard faults present will not be detected.

## Update PS/2 Mouse configuration options task

This task lets you configure the PS/2 Mouse configuration options of the client computers.

See [Configuring BIOS settings and enabling/disabling interfaces](#) on page 29.

The following options are available on this page:

Option	Description
Existing BIOS password	If necessary, enter the BIOS setup password.
PS/2 Mouse configuration	Select if you want to enable, disable or configure the PS/2 Mouse configuration options on the client computers.  Enable: Enables PS/2 mouse port.  Disable: Disables PS/2 mouse port.  Automatic: Enables PS/2 mouse port, if devices are detected.  Operating system controlled: Enables PS/2 mouse port and the operating system allocates the resources.

## Update USB ports options task

This task lets you enable or disable the USB ports options of the client computers. This option configures USB ports according to device classes. Any disabled USB ports are neither available under the operating system.

See [Configuring BIOS settings and enabling/disabling interfaces](#) on page 29.

The following options are available on this page:

Option	Description
Existing BIOS password	If necessary, enter the BIOS setup password.
USB ports	Choose the configuration of the USB ports on the client computers.  Disable Unused Ports: All unused USB ports are disabled.  Disable Mass Storage Devices And HUB: All ports with mass storage devices and HUBs will be disabled.  Enable keyboard and mouse: Only ports with keyboard and mouse will be enabled.  Enable all ports: All USB ports are enabled

## DeskView Diagnostics tool: Hardware diagnostics task

This task lets you run hardware diagnostics on the client computers.

You must install the DeskView Diagnostics Agent before you can run this task.

See [Installing the DeskView Diagnostics Agent](#) on page 19.

See [Diagnosing client computers' hardware](#) on page 31.

The following options are available on this page:

Option	Description
Memory	Check to perform a memory test.
CPU	Check to perform a CPU test.
HDD	Check to perform a hard drive test.
LAN	Check to perform a network test.
Quick test	Click to perform a quicker test.
Stress test	Click to run a longer test with a larger number of subtests.

# DeskView Security tool: Configure Mass Storage Access task

This task lets you lock and unlock removable storage devices of the client computers. You can use this task to prevent data abuse and unintentional bringing in of extraneous software, like viruses or games, from removable storage devices.

This task supports USB mass storage devices on Windows XP and removable disks (flash memory or hard drive based removable disks connected, for example, through USB or FireWire) on Windows Vista.

See [Disabling mass storage devices](#) on page 33.

The following options are available on this page:

Option	Description
Lock mass storage devices	Click to lock all removable storage devices.  This action does not lock other USB devices, such as USB keyboard, mouse, or printer. If you want to lock other USB devices, use the Update USB host controller options task.
Unlock mass storage devices	Click to unlock all removable storage devices.  If you have USB host controller disabled in BIOS, this action will not unlock the controller. Use the Update USB host controller options task to unlock the USB host controller.
Set mass storage devices to read only	Click to unlock and set all removable storage devices to read-only mode. This prevents data theft, but does not protect the system against virus attacks.  The read-only mode is supported only by Microsoft Windows XP SP2 or later.

# DeskView Notifications

This section includes the following topics:

- [DeskView Enable/Disable Notifications policy](#)
- [DeskView Configure Data Disk free space policy](#)
- [DeskView Configure System disk free space policy](#)
- [DeskView Configure Lease expiration policy](#)
- [Configure General Notification Email Forwarding page](#)
- [Configure General Notification Selection page](#)

## DeskView Enable/Disable Notifications policy

This policy lets you enable client computers sending hardware and software failure notifications to Notification Server.

Additional to DeskView Client notifications, you can configure client computers to send ASF (Alert Standard Format) and Intel® AMT alerts to Notification Server

See [Using DeskView Notifications](#) on page 36.

The following options are available on this page:

Option	Description
Notifications enabled	Check if you want the client computers to send DeskView Client notifications to the Notification Server computer's IP (shown in the parenthesis).
ASF Enabled	Check to enable ASF (Alert Standard Format) alerts.
Intel® AMT Enabled	<p>Check to enable Intel® AMT alerts.</p> <p>When checked, the DeskView Intel AMT Alerts task will run on the target systems and enable Intel AMT alerts. By default, the task is configured to enable a few critical Intel AMT alerts, such as "BIOS Hang", "CPU Missing", and others. If you want, you can configure other alerts. You can find the DeskView Intel AMT Alerts task at the following location: <b>Home &gt; DeskView &gt; Tasks &gt; Notification Settings &gt; Helper tasks &gt; DeskView Intel AMT Alerts.</b></p> <p>For more information on how to use the DeskView Intel AMT Alerts task, press <b>F1</b> or click <b>Help &gt; Context</b> in the Symantec Management Console.</p>
Local PopUp Window	Check if you want a pop-up window to appear on the client computer when a failure occurs.

Option	Description
Local Log File	Check if you want the notifications to be logged locally on the client computer to a file.  The log file is located at "%DeskView%\Notification\Notificationns.log"
Local System Event Log	Check if you want the notifications to be logged into the client System Event Log.

## DeskView Configure Data Disk free space policy

This task lets you configure when the client computers should send an alert to Notification Server.

See [Using DeskView Notifications](#) on page 36.

The following options are available on this page:

Option	Description
Error occurs when free space less than	Set a limit for the minimum amount of free space on the data partition before the error notification is sent.
Warning occurs when free space less than	Set a limit for the minimum amount of free space on the data partition before the warning notification is sent.
Set defaults	Click to reset the values to its defaults.

## DeskView Configure System disk free space policy

This task lets you configure when the client computers should send an alert to Notification Server.

See [Using DeskView Notifications](#) on page 36.

The following options are available on this page:

Option	Description
Error occurs when free space less than	Set a limit for the minimum amount of free space on the system partition before the error notification is sent.
Warning occurs when free space less than	Set a limit for the minimum amount of free space on the system partition before the warning notification is sent.
Set defaults	Click to reset the values to its defaults.

## DeskView Configure Lease expiration policy

This task lets you configure the lease expiration date value on the client computers.

See [Using DeskView Notifications](#) on page 36.

The following options are available on this page:

<b>Option</b>	<b>Description</b>
Expiration date	Set the lease expiration date.
Display expiration warning	Check to display the lease expiration warning message on the client computer and specify the number of days before the lease expiration date when the warning should be displayed.

## Configure General Notification Email Forwarding page

On this page you can configure email settings for DeskView notifications. An email will be sent using these settings whenever a notification occurs.

See [Using DeskView Notifications](#) on page 36.

The following options are available on this page:

<b>Option</b>	<b>Description</b>
Active	Check to activate forwarding notification to an email.
SMTP Server	Type the IP address or the FQDN of the SMTP server.
From	Type an email address of the sender of the email notification.
To	Type a destination email address. You can separate several addresses by a comma or a semi-colon.
CC	(Optional) Type an email address where you want to send a carbon copy of the email notification.
Subject	Type what you want to be displayed in the subject line of the email.
Message language	Select which language you want to send the notification in.

<b>Option</b>	<b>Description</b>
Additional text	<p>The following notification details are sent by email:</p> <ul style="list-style-type: none"> <li>• computer name</li> <li>• IP address</li> <li>• date</li> <li>• time</li> <li>• event</li> <li>• whether an improvement or a deterioration has taken place</li> <li>• the current status</li> </ul> <p>If you want, type additional text here and it will be attached to the message.</p>
Save	Click to save the settings.
Reset	Click to reset to the last saved settings and ignore the changes.

## Configure General Notification Selection page

On this page you can configure which notifications you want the client systems to send to Notification Server.

See [Using DeskView Notifications](#) on page 36.

The following options are available on this page:

<b>Option</b>	<b>Description</b>
Chassis Intrusion	If the computer is equipped with a sensor for cover opening, the system can check whether the cover was opened or is presently open.
Entity Presence (Heartbeat)	Checks whether the computer can be reached through the LAN connection.
OS Critical Stop	Reacts in case of malfunction of the operating system.
Processor	Checks whether the processor was removed.
System Startup Error	Checks whether an error has occurred during the P.O.S.T. (Power-On Self Test) routine.
Watchdog	Reacts in case of malfunction when starting the system.
Cover opening	If the computer is equipped with a sensor for cover opening, the system can check whether the cover was opened or is presently open.

<b>Option</b>	<b>Description</b>
Cover sensor	Indicates whether a cover opening can be detected.
Device changes	Checks the device changes on the IDE and SCSI interfaces.
Display Change	Checks whether the display has been removed, replaced by another display, or an additional display has been connected to the computer (Does not apply to notebook computers).
Fan deterioration	Checks whether the actual rotational speed of the CPU and power supply fan is within tolerances.
Fan monitoring	Checks whether the controller and its CPU and power supply fan function correctly.
Free hard disk space (data)	Checks the free memory space for data on all existing hard disks except the system drive.
Hard disks (S.M.A.R.T.)	Checks the hard disk drives with Self Monitoring And Reporting Technology.
Free hard disk space (system)	Checks the free memory space on the system drive.
Internal short circuit	Monitors the keyboard, mouse, and USB interface for short circuits.
Lease Expiration	Checks the term of the leasing agreement.
Memory changes	Indicates whether the main memory of the system has changed.
Processor change	Checks whether the processor has been replaced with another one or a processor has been removed or an additional process has been installed.
Temperature	Monitors the inside and outside temperature of the computer.
Voltage	Checks whether the 5V voltage, 12V voltage, and the CMOS battery voltage are within tolerances.
Windows Service Monitoring	Monitors the installed Windows Services.

# DeskView Serial Numbers tool

This section includes the following topics:

- [Apply imported serial numbers task](#)
- [Assign single serial number task](#)
- [Generate serial number task](#)
- [Manage serial numbers page](#)

## Apply imported serial numbers task

This task lets you assign the serial numbers that you imported into DeskView to the client computers.

For more information on importing serial numbers, see [Managing serial numbers](#) on page 34.

## Assign single serial number task

This task lets you assign a single serial number to a specific computer resource.

The serial number must contain only alphanumeric characters.

See [Managing serial numbers](#) on page 34.

## Generate serial number task

This task lets you generate serial numbers using a specified string pattern.

See [Managing serial numbers](#) on page 34.

The following options are available on this page:

Option	Description
Serial number pattern	Enter the string pattern for the serial number to be generated. For example, you can type ABC####, where ABC is the invariable part of the number, and #### is the sequence that increments each time a client computer requests another serial number.
Serial number range	Type initial and final terms of the sequence.
Override currently assigned serial numbers	Check to let the policy to replace the existing serial numbers on the client computers.
Check range availability	(Task-based policy only)  Click to see the number of the DeskView managed resources that need serial numbers and the number of serial numbers that are free.

## Manage serial numbers page

On this page, you can create a serial numbers database that you can later assign to systems from Fujitsu Technology Solutions.

See [Managing serial numbers](#) on page 34.

The following options are available on this page:

Option	Description
View serial numbers	Select to view the list of systems from Fujitsu Technology Solutions, registered with Notification Server, with or without a serial number.
Export serial numbers	Select to export the systems information to a .csv file. You can populate this file with serial numbers using a text editor, and then import the file into the database.  Use the Import serial numbers command on this page to import the .csv file.  See <a href="#">Managing serial numbers</a> on page 34.
Import serial numbers	Select to import the .csv file you created with the Export serial numbers command on this page and populated with serial numbers.  To see the resource information you imported, select the View serial numbers command on this page.  See <a href="#">Managing serial numbers</a> on page 34.
Remove all serial numbers	Select to remove all serial numbers from the serial numbers database.
Remove serial numbers for deleted resources	Select to purge the serial numbers that are not used by existing computer resources.

# DeskView System Data page

The DeskView System Data page in the Resource Manager displays the following system and user data for the client computer:

<b>Option</b>	<b>Description</b>
Summary	Shows the system and user data most frequently used by the administrator for the systems that are selected in the Systems pane.
Mainboard	<p>The General section shows manufacturer-specific information about the mainboard and BIOS version.</p> <p>The Processor section shows the processor type and the maximum clock frequency of the processor.</p> <p>The Memory section shows information about the built-in memory modules.</p>
Graphics	<p>The Display section shows the name and serial number of the connected monitor.</p> <p>The Adapter section shows information about the graphic controller.</p>
Network	<p>The General section shows the name of the system and the system administration structure (workgroup, domain, or Active Directory).</p> <p>The Adapter section shows information about the network cards that are installed in the system.</p>
Drives	<p>The Physical Drives section shows information about the built-in drives. Physical drives belong to the system hardware, but they can also be such devices as memory sticks and so on.</p> <p>The Logical Drives section shows information about the logical drives.</p>
Software	<p>Shows information about the operating system, the DeskView version that is installed on the client, and other applications of the system.</p> <p>Not every application that is installed on the system is displayed. Only the applications that you can add or remove using the Control Panel in Windows are displayed.</p>
Characteristics	Shows what types of notification the selected system can send, the current BIOS settings of the selected system, boot order, and the current access settings of removable disks (Windows Vista) and USB Mass Storage Devices (Windows XP).

# DeskView Notifications page

The DeskView Notifications page displays detailed DeskView Notification data for the selected computer.

See [Using DeskView Notifications](#) on page 36.

The following information is shown for each notification:

<b>Option</b>	<b>Description</b>
Received Time	Shows the date and time when the notification was received by the DeskView Control Center.
Severity	Shows the severity of the event that triggered the notification.  The following degrees of severity are possible: <ul style="list-style-type: none"><li>• Critical or Fatal</li><li>• Warning, Minor, or Major</li><li>• OK</li><li>• Unknown or Other</li></ul>
Category	Shows the category of the event that triggered the notification. For example, "cover open" or "temperature".
System	Shows the name of the system that sent the notification.
Processing Status	Shows the processing status of the notification.  The following processing states are possible: <ul style="list-style-type: none"><li>• New The notification is new and has not yet been processed.</li><li>• Open The notification is still being processed.</li><li>• Closed The notification has been processed; processing is complete.</li></ul>

The following detailed notification information is available on this page:

<b>Option</b>	<b>Description</b>
Time of occurrence	Displays the date and time that the event occurred on the system.
Description of event	Describes the reason for the notification.

<b>Option</b>	<b>Description</b>
Additional information	Displays additional information about the corresponding notification and, if applicable, gives advice on error recovery.
Trending information	Compares the severity of the event that triggered the notification with that of the previous notification that was triggered by the same type of event.  The trending information is relevant only for events that result in two or more notifications.

## Cleanup Inventory Cache task

This task lets you purge the inventory cache that is located on the Notification Server computer. In case of a default DeskView installation, the inventory cache is located at `C:\Program Files\Altiris\DeskView\InventoryCache`.

By default, this task is configured to run daily.

See [Configuring the Inventory Cache purging](#) on page 21.

The following options are available on this page:

<b>Option</b>	<b>Description</b>
HDD Free Space Limit	Check if you want to purge the cache when the free disk space goes below a specific limit.  Type the limit for the minimum amount of free space on the hard disk.  Default: 2048 MB
HDD Usage Limit	Check if you want to purge the cache when its size exceeds a specific limit.  Type the maximum limit for the amount of cached data that is saved.  Default: 10 MB

---

# Appendix A

## Glossary

---

This appendix 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.

### **ASF (Alert Standard Format)**

An industry standard-based technology that lets IT administrators manage computers regardless of the operating system state. ASF provides alerts and power management functionality as long as the computer is plugged in with an Ethernet connection. ASF functions through hardware on the network card or system board, a software agent on the client computer, and management software on the server.

### **CMDB (Configuration Management Database)**

The central database that stores all information about the Symantec Management Platform and its managed computers.

### **DeskView Agent**

The DeskView Agent is software that runs on client computers that can be configured and run remotely using Notification Server task policies. The client software includes a set of the DeskView Client Tools, and an inventory and notification agent (DeskView Agent).

### **DeskView Client Tools**

DeskView Client Tools is a set of tools installed with the DeskView Agent on a client computer. The tools include DeskFlash, DeskOff, DeskView BIOS Settings, DeskView Security, and a tool to change the serial number.

### **DeskView Control Center**

The DeskView Control Center (DVCC) consists of a database and central services. All information of the managed systems are stored in the database. All information from DVCC is also transferred to the Altiris Notification Database.

### **DeskView Discovery Agent**

The DeskView Discovery Agent is software that runs on client computers and identifies DeskView manageable computers.

## **DeskView New Notifications**

A page that shows all new incoming notifications. It is refreshed regularly (the default is once a minute). When you start the DeskView New Notification, all notifications not yet processed are displayed.

## **DeskView Notifications**

Alerts that inform administrators about critical conditions, occurred on the client computers.

## **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.

## **Intel AMT (Intel Active Management Technology)**

A solution that is implemented in hardware and firmware and is connected to the system's auxiliary power plane. Despite the power state or the operating system state of the client computer, Intel AMT provides IT administrators with access to alerts, hardware inventory, power management, circuit breaker, and agent presence functionality. Intel AMT functionality requires the computer to be plugged into the power source and connected to the network. Intel AMT functionality does not require a software agent to be installed on the client computer.

## **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.

## **Manageable Systems**

The computers that have been discovered by the Discovery Agent and have been identified as systems from Fujitsu Technology Solutions.

## **Managed Systems**

Managed systems are systems from Fujitsu Technology Solutions that have the DeskView Agent installed on them and inventory data has been sent to Notification Server.

## **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.

**Symantec Management Console**

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

**task**

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

---

# Index

---

## A

- Agent
  - Altiris Power Scheme 20
  - DeskView 18
  - DeskView Diagnostics 19
- Alert Standard Format
  - see ASF
- Altiris Agent
  - about 15
  - configuring 16
  - discovering resources 15
  - installing 15
- Altiris Power Scheme Agent
  - installing 20
- ASF 11

## B

- Best Fit file 21
- BIOS
  - archiving 24
  - configuring settings 29
  - disabling interfaces 29
  - updating 24
  - updating settings 24

## C

- command line
  - using to run client tools 36
- computer
  - viewing DeskView system data 40

## D

- DeskFlash tool 24
- DeskOff tool 26
- DeskUpdate tool 28
- DeskView
  - about 6
  - components 6
  - installing agents 17
  - Quick Start 13
  - system requirements 10
- DeskView Agent 7, 24
  - installing 18
  - viewing installation events 41
- DeskView BIOS Settings tool 29
- DeskView Diagnostics Agent
  - installing 19
- DeskView Diagnostics events 41
- DeskView Diagnostics tool 31
- DeskView Energy tool 32
- DeskView events

- viewing 41, 41
- DeskView inventory
  - viewing 41
- DeskView Notifications
  - configuring 39
  - enabling 39
  - forwarding by email 38
  - selecting 38
  - using 36
  - viewing 40
- DeskView Security tool 33
- DeskView Serial Numbers tool 34
- DeskView system data
  - viewing 42
- discovering
  - resources 15
- documentation resources 8
- drivers
  - updating 28

## E

- events
  - viewing 41

## H

- hardware
  - diagnosing 31

## I

- installing
  - ASF Proxy 11
  - DeskView 11
  - post-installation tasks 11
  - SNMP receiver 11
- Intel AMT alerts 11
- inventory
  - viewing 41

## M

- manageable computers 16
- mass storage devices
  - disabling and enabling 33

## N

- notifications
  - see DeskView Notifications

## P

- power management 26
- power scheme settings
  - configuring 32
- purging inventory cache 21

## R

- Resource Manager 40, 41, 41
  - viewing 41

## S

- serial numbers
  - managing 34
- SIM 11, 12
- Simple Network Management Protocol
  - see SNMP
- SNMP 11
- Symantec Installation Manager
  - see SIM
- Symantec Management Console 7, 13
- Symantec Management Platform 7, 10

## T

- tools
  - DeskFlash 24
  - DeskOff 26
  - DeskUpdate 28
  - DeskView BIOS Settings 29
  - DeskView Diagnostics 31
  - DeskView Energy 32
  - DeskView Notifications 36
  - DeskView Security 33
  - DeskView Serial Numbers 34
  - viewing events 41

## U

- uninstalling
  - DeskView 11
  - DeskView agents 12
  - DeskView software 12

## V

- VESA-DDC/CI 6
  - viewing events 41
  - viewing inventory 41