

#####

DELL(TM) MANAGEMENT CONSOLE VERSION 1.1.0 README

#####

Version - 1.1.0  
Release Date - March 2010

NOTE: Dell Management Console and its documentation are available on the Dell Management Console DVD and on the Dell Support web site at support.dell.com.

Dell Management Console provides a central point of access to monitor and manage systems on a local area network (LAN) or the wide area network (WAN). By providing administrators a comprehensive view across the enterprise, Dell Management Console can increase system uptime, reduce repetitive tasks, and prevent interruption in critical business operations.

This readme.txt contains updated information for Dell Management Console User's Guide and any other technical documentation included with Dell Management Console.

#####

CONTENTS

#####

This file contains the following sections:

- \* Criticality
- \* Compatibility/Recommended Requirements
- \* Release Highlights
- \* Installation
- \* User Notes
- \* Known Issues
- \* Disclaimer

#####

CRITICALITY

#####

2 - Recommended

#####

COMPATIBILITY/RECOMMENDED REQUIREMENTS

#####

=====  
Supported Operating System Requirements for Dell Management Console  
=====

Windows Server 2003 R2 or SP2 (32 bit only) Standard or Enterprise Editions

---

---

## Recommended Minimum Hardware Configuration for Dell Management Console

---

---

### \* Physical Server

- 2 Physical Processors
- 4 GB RAM
- DVD Drive
- Microsoft .NET 3.5 (SP1 is supported)
- Windows Internet Information Services (IIS) 6.0
- Microsoft SQL 2005 Express
- SQL Server 2005 32-bit, SQL Server 2005 64-bit (Remote), SP1, SP2, SP3
- SQL Server 2008 32-bit, SQL 2008 Express, SQL Server 2008 x64 (Remote)
- Windows Internet Explorer version 7.0 or 8.0

---

---

## Recommended Hardware for Configurations over 500 Devices

---

---

### \* Physical Server

- 4 or more Processor Cores
- 8 GB RAM
- DVD Drive
- Microsoft .NET 3.5 (SP1 is supported)
- Windows Internet Information Services 6.0
- SQL Server 2005 SP1/SP2/SP3 or SQL Server 2008 (32-bit or 64-bit remote)
- Internet Explorer version 7.0 or 8.0

Note: Dell recommends remote 64-bit database for larger environments.

---

---

## Additional Software Required to Run Some Features of Dell Management Console

---

---

\* For Dell/EMC storage arrays, ensure the array is FLARE(R) version 26 or later.

\* Navisphere(R) Secure CLI (version 26 or above) installed on the management station.

NOTE: This CLI software is included on the Dell Management Console media.

---

---

## Recommended SQL Server Updates

---

---

\* SQL Server 2005 SP1 or SP2 or SP3 is required for using SQL Server 2005 as the default database.

\* Optimize your SQL Server maximum memory settings as indicated in Microsoft(R) knowledge base articles KB321363 and KB319942. This configuration may significantly improve product performance.

\* Altiris KB location <https://kb.altiris.com>

- #34345 "Notification Server performance issues due to SQL index fragmentation"
- #38917 "Links to Notification Server/SQL Server Maintenance and Tuning Articles"

NOTE: Ensure that during installation of the SQL Server 2005, you select a case-insensitive collation setting. If you select a case-sensitive collation setting, then the agent health Web part

for an individual discovered device will not contain any information.

NOTE: The default collation setting in SQL Server 2005 is case-insensitive.  
[281173]

---

---

## Configuring SSL/HTTPS

---

---

\* If you are configuring your installation for SSL/HTTPS, configure SSL before installing the Dell Management Console and the Altiris Server Management Suite. After SSL is configured, the settings cannot be changed.  
[242160] [247707]

#####  
RELEASE HIGHLIGHTS  
#####

\* This release of Dell Management Console 1.1.0 includes Symantec(R) Notification Server (NS) 7 SP3. The details are as follows:

\* Symantec SMP 7 SP3:

- Numerous issues were addressed in Symantec Management Platform 7.0 SP3, for details, see [kb.altiris.com #49356](http://kb.altiris.com/#49356).

\* Symantec NS 7 SP3:

- Numerous issues were addressed in Symantec Notification Server 7.0 SP3. For details, see [kb.altiris.com #46976](http://kb.altiris.com/#46976).

\* Power Monitoring feature for Dell Servers.

\* Lifecycle Controller enabled updates for Dell Servers.

\* Virtual Machines (VM) - DMC can be installed in a virtual machine (ESX 3.5 U4).

\* Use the Troubleshoot tool present in the DVD\Tools directory to diagnose discovery related issues with respect to specific protocol. Refer its readme.txt, in that same folder, for more details.

---

---

## New Features

---

---

\* Power Monitoring support for all Dell servers with supporting hardware and instrumentation. Refer to DELL MANAGEMENT CONSOLE Hardware Support Matrix. <http://support.dell.com/support/edocs/software/smdmc/>

\* Updates for Lifecycle Controller enabled servers that enable you to perform updates for servers with Lifecycle Controller version 1.3 and Integrated Dell Remote Access Controller (iDRAC) version 6.

\* Support for Inventory of EqualLogic devices.

\* New devices support. Refer to DELL MANAGEMENT CONSOLE Hardware Support Matrix.

---

---

## Fixes and Enhancements

---

---

- \* The Dell OpenManage(TM) Server Administrator Agent Deploy Solution is updated to allow deployment of OpenManage(TM) Server Administrator V 6.2.

#####  
INSTALLATION – POINTS TO NOTE  
#####

- \* Installing Dell Management Console version 1.1.0

The Dell Management Console Install Guide is available on the Dell Tech Center website at [www.delltechcenter.com](http://www.delltechcenter.com).

See the Dell Management Console page in the OpenManage Systems Management section.

Also see the Dell Management Console User's Guide on the Dell Support website at [support.dell.com/manuals](http://support.dell.com/manuals) for more information on installing the Dell Management Console.

- \* Symantec Installation Manager (SIM) is the installer for Dell Management Console. It may take several minutes to launch SIM if your server is not connected to the Internet.

If you do not have access to the Internet, you can only install products locally available on the Dell Management Console DVD.

- \* During install, take note of the following:

- Do not disable or disconnect any network port while the installation is in progress.
- Dell Management Console may require more available ports for agentless monitoring support. This change requires a system restart. <http://technet.microsoft.com/en-us/library/cc758002%28WS.10%29.aspx>
- If you are using a remote SQL database on a system that has its firewall enabled, ensure that the firewall ports are open for the SQL Server instance to which the Symantec Platform will connect; otherwise you will encounter errors during installation. Alternatively, disable the firewall completely.
- Refer to this article on How to configure SQL Server 2005 to allow remote connections: <http://support.microsoft.com/kb/914277>
- Refer to this article for an overview and network port requirements for the Windows Server system: <http://support.microsoft.com/kb/832017>
- To prevent Microsoft Windows Installer conflicts, do not run another install while Dell Management Console installation is in progress.
- Register at <http://www.dell.com/openmanage/register> to receive a free Dell Management Console license. When installing the free Dell Management Console license, the license Web part is removed from the Dell Management Console portal page and you can customize the portal page.

\* After installing Dell Management Console 1.1.0, do the following:  
-- Enable the Altiris(R) Agent upgrade policy so that the Agent-based functionality is not interrupted.

-- For Windows Altiris Agent:  
Go to Settings > All Settings > Agents/Plug-ins > Altiris Agent > Windows > Altiris Agent for Windows - Upgrade.  
Change this policy to On and save changes.

-- For Linux Altiris Agent:  
Go to Settings > All Settings > Agents/Plug-ins > Altiris Agent UNIX/Linux/Mac > Altiris Agent for UNIX/Linux/Mac - Upgrade  
Change this policy to On and save changes.

- After a successful upgrade of the Altiris Agent on the Dell Management Console system, if the Monitor Agent service has stopped, ensure that you restart the service manually.

- Be aware the proper operation of the Altiris agent on the managed systems may require opening ports on any firewall that may be in operation. See the Dell Management Console Ports document in the Dell Management Console section of the [www.delltechcenter.com](http://www.delltechcenter.com) website.

Refer to this whitepaper for information on network ports used DMC:  
[http://en.community.dell.com/groups/dell\\_management\\_console/media/p/19527831.aspx](http://en.community.dell.com/groups/dell_management_console/media/p/19527831.aspx)

#####  
UPGRADES – POINTS TO NOTE  
#####

\* When upgrading to Dell Management Console 1.1.0, take note of the following:

\* Insert the Dell Management Console DVD and click Install Dell Management Console on the start-up screen. You may have to update the Symantec Installation Manager (SIM) for the SIM to install first.

\* When SIM launches, click Install New Products and select Dell Management Console.

NOTE: If you have other components besides Dell Management Console, some critical updates will automatically start before you can install the latest Dell Management Console. If you do not see Dell Management Console listed, then you may be pointing the product listing to a different repository. You can change this to point to the DVD product listing:

- 1) On the startup screen of SIM, click Settings.
- 2) Click Change product listing...
- 3) Click Add...
- 4) Browse to the dell.pl.xml in your Dell Management Console DVD.
- 5) Click OK until the startup screen is displayed.  
You should now see Dell Management Console listed in Install new products.

#####  
USER NOTES  
#####

See the Dell Management Console FAQs on the Dell TechCenter website.

=====  
Resource Links  
=====

- 1) The Dell TechCenter  
<http://www.delltechcenter.com/page/Dell+Management+Console>
- 2) Altiris Knowledge Base Articles  
<https://kb.altiris.com/>
- 3) Juice User Community: A Community for Symantec Customers and End Users  
<http://www.symantec.com/community/>

#####  
KNOWN ISSUES  
#####

=====  
General  
=====

\* You must restart the Altiris Agent after the network card is disabled in a dual-homed environment

The Altiris Agent does not bind to a particular network card, but it attempts to connect to the fully-qualified domain name. So, if you are using a connection-specific DNS name and disable the connection, you may experience an issue.

Workaround: Reset the Altiris Agent.

To reset the Altiris Agent, do the following:

1. Right-click the round yellow icon in the lower right-hand corner of the screen and select Altiris Agent.
2. Select the Task Status tab and click Reset Agent.
3. Wait until this message is displayed: Registered with <your\_NS\_server\_name>.

The agent is now reset.

[275039, 282313]

\* Dell Management Console may experience multiple longevity issues when opened for extended periods. It is recommended to close the console (browser) when not in use.

[406]

\* After an upgrade, it is recommended that you restart the system.

[677]

\* If you see an E11: Object expected error message in the console, to resolve the issue restart the IIS Service.

[824]

\* When creating a WS-MAN connection profile using remote browser, the certificate file cannot be uploaded to the Dell Management Console server.

The connection profile for WS-MAN protocol must be created on the server where Dell Management Console is installed.

[767]

---

---

## Install & Upgrades

---

---

\* In the Install New Products screen of Symantec Installation Manager, there is a check-box for Show all available versions. When you install Dell Management Console from the DVD, the previous versions are not available. To get older versions, you must install Dell Management Console online through the global product listing.

\* To point to the online global product (GPL) listing to get the latest Symantec solutions and updates:

1. You need a connection to Internet to reach the GPL online.
2. After verifying that you can access the Internet, launch the Symantec Installation Manager through Program Files > Altiris > Symantec Installation Manager.
3. Click Settings in the start-up page of SIM.
4. Click Change product listing and type <http://www.solutionsam.com/solutions/pl/symantec.pl.xml>.
5. Click OK.

You can access the latest solutions and updates in the Install New Products page.

\* To completely remove DMC from your system, use add/remove program instead Of the SIM installer.

[923]

\* Upgrade of Dell Management Console, Dell Client Manager and SMS to the latest version fails. During the initial installation or upgrade of products/solutions, Symantec Installation Manager (SIM) fails during the stop or restart of services. If you try to restart the service (in this case the service failing was the Altiris Service) manually, the following message is displayed: Failed while starting service: AeXSvc Configuration failed while attempting: Restarting services...

If you try to restart the Altiris Service manually, the following message is displayed:  
Error 1053: The service did not respond to the start or control request in a timely fashion.  
Then the Altiris Service stays in 'starting' mode and does not starts (until you reboot the machine or run NET STOP 'service name')  
Resolution: In the Properties' tab of the service, change the AppID from Local Admin Account to a Domain Admin/LocalSystem account that allows the services to keep running, starting, and stopping properly.

More information is in the Altiris KB:

<https://kb.altiris.com/article.asp?article=48505&p=1>

---

---

## Application Launch Solution

---

---

\* Launching Server Administrator for a second time on the same browser results in an error. This is expected behavior. As the part of security fix for XSRF (Cross site request forgery), Server Administrator validates

every session against the secret key generated by the server. Close the first instance and re-launch the Server Administrator launch point.

[271966]

\* All Dell Management Console launch points are hard coded to default values. If the application is installed in another location, edit the launch point from Settings > Console > right-click Actions.

This applies to URL launch points as well.

[248633]

\* When creating a right-click action for a particular Resource Type, several unsupported Data Classes are displayed; Choosing an unsupported Data Class results in an error.

To find the Data Classes that are supported for a resource:

1. Go to the Resource Manager for the Resource Type.
2. Go to View> Inventory.

Ensure that you only choose those Data Classes that are listed in the Resource Manager when creating a right-click action for a Resource Type.

[272329]

---

## Dell OpenManage(TM) Server Administrator Agent Deploy Solution

---

\* Server Administrator Agent deploy task wizard displays the status as waiting for Agent to get the status while the agent deploy and remote installation is in progress on the remote target server.

The functionality to update the task status is not enabled by default. This is because the option to have intermediate task status events being reported back to the server results in more bandwidth usage.

To enable this setting:

1. Click Settings > Notification Server > Site Server Settings > Site Management > Settings > Task Service > Settings > Task Service Settings.
2. Select Send detailed task events and click Save Changes.

After saving the changes, the agent nodes require an updated configuration to apply the changes so that they can start sending detailed events.

3. Run the Update Client Configuration task to update the changes.

The tasks now have this information reported.

[245096]

\* Reboot target machine option will not work when the target machine has Windows 2000 or Windows NT installed without the Microsoft Resource Kit tools.

[270933]

---

## Dell Patch Management Solution

---

\* Use update catalogs and package repository from the same source.

It is recommended that you use the update catalogs and package repository from the same source. Although Patch Management Solution for Dell systems allows you to mix online and offline locations for catalogs and update packages, this may cause problems with the availability of packages described by the catalog.

[266854]

\* Identical server names may produce errors in the second-level report results. Drilling down into report results may produce errors if you have two servers with identical names in a production environment.

\* The Applicable Computers by Individual Update report may display duplicate entries in the first tier report results. The duplicate entries are actually different releases of the update that appear with the same name.

\* To update Dell OS Driver pack using Dell Management Console using the Lifecycle Controller on the managed node, download the catalog from ftp.dell.com. Catalog downloaded using the offline option (Server Update Utility catalog) does not contain the windows updates that Dell Management Console requires.  
[542]

\* For Altiris agent based updates, Rollout Jobs fail to complete because the final system reboot does not occur.  
A server receiving updates from the Dell Management Console may fail to reboot automatically if the Altiris Power Control task fails to execute.  
[273064]

\* Internet Explorer Memory usage is high when you work with the Dell Patch Management solution.  
Internet Explorer allocates memory when a new window is opened and does not free the entire memory when that window is closed. Eventually this decreases the system performance.  
Workaround: Close all browser windows and reopen Internet Explorer.  
[272419]

\* SQL memory usage is high when working with Dell Patch Management solution. The Dell Patch Management solution involves high use of SQL memory and affects system performance. Dell recommends a system with minimum 4 GB RAM and the following SQL memory settings:

Total System Memory	Maximum Memory Setting
2 GB	500 MB (minimum SQL Express memory is 256 MB)
4 GB	750 MB (minimum SQL Server memory is 512 MB)
8 GB	3.5 GB
16 GB	8 GB

For more information, see Microsoft KB 321363 and KB 319942.  
[273614]

\* The Compliance report for a server is displayed only if there are updatable components.

\* Systems that are rebooted after an update still display a Reboot Required message.  
The return code is from the actual update process. You can go to the

job and check the status of the task, including the status of the reboot.

[272827]

\* The Check applicable updates by Computers report may display multiple entries for the same server name even if the report is grouped by computer name.

[261236]

\* Patch Rollout Job fails with message Schedule occurs in the past. Scheduling a stage and distribute task does not schedule the Staging and Preparing For Distribution task. It only schedules the Rollout Job.

If the staging and preparing for distribution task takes a longer time and surpasses the scheduled time for rollout job, the rollout job times out and the update task does not run on schedule. In such cases, Dell recommends using the Run now option to apply the patch.

If scheduling is required, then maintain a time delay between Staging and distribute task and a Rollout job, so that the Rollout Job can start after the staging and distribute task is completed.

[278453]

\* A Server Error message is displayed when you launch the Security Permissions page by clicking Settings> Security> Permissions menu on the Web page that is opened from the Getting Started Web part on Dell Patch Management solution portal page.

Work-around: The security permissions page can be launched without errors from the main console window by clicking Settings> Security> Permissions.

[280961]

\* For a server that supports updates using Altiris Agent and updates using Lifecycle Controller, if an update is applied using one of the methods, that update is still seen as applicable under the Hardware Update Compliance reports.

Work-around: After applying the update to the server using either the Altiris Agent or the Lifecycle Controller, the user needs to run the following tasks for the Hardware Update Compliance reports to display the correct info -

1. Compliance Check task on Windows/Linux Servers
2. Dell Management Console Inventory task
3. Compliance task on Lifecycle Controller Enabled Servers

[845]

\* Dell 32 bit Diagnostics do not appear in the hardware compliance reports when updating Lifecycle Controller enabled servers. As this update does not report component type currently, it cannot be updated using Patch Management Solution.

\* Under hardware compliance reports, Lifecycle Controller based updates will show up when the OS Type is selected as Windows or Linux. The Operating System column in the report will either be blank or is

displayed as NA for Lifecycle Controller based updates.

[776]

\* When a bundle update is run on multiple Lifecycle Controllers Enabled Servers using WS-MAN (Apply updates using Lifecycle Controller), some of the updates may fail with an error message "A WSMAN connection could not be established". Run the job instance again to perform the update.

[939]

\* When a server and its iDRAC is discovered and inventoried using SNMP + WS-MAN protocol, users may see SNMP inventory information only. Re-run discovery and inventory to get WS-MAN inventory. Without WS-MAN inventory, you cannot apply updates using Lifecycle Controllers.

[925]

---

## Event Console

---

\* Alert Initiated Discovery will not work for the PowerVault MD storage devices.

MD Array Traps are forwarded from the server where Dell PowerVault Modular Disk Storage Manager application is installed and the Host IP address in the trap is the server's IP address instead of the MD Storage Device. Alert Initiated discovery is run on the Host IP which in this case is the device that is managing the MD Storage device.

[271840]

\* Traps from some Dell printers such as model number 2330dn and 2145cn may not be categorized properly in the Event Console. These models may not support the standard printer MIB (RFC 3805) for trap classification. Such traps will be received by the Event Console but displayed as Unknown Event Name, Unknown Event Category and Undetermined severity.

Work-around: You can perform all actions, such as Resolve, Acknowledge, and View Details that can be performed on other recognized alerts. The difference between recognized and unrecognized traps is that Name, Category, and Severity do not display the proper values.

[255399]

\* Traps may not be received when both IT Assistant and Dell Management Console are installed on the same management station. To correct this behavior, restart the Altiris Event Engine and Altiris Event Receiver services.

[281264]

\* Traps received from a managed node server having Red Hat Enterprise Linux 4 (Update:7) (x86 or 64) installed on it, will show 0 as Trap Description in Event Console. This issue is caused by a net-snmp bug introduced in Red Hat Enterprise Linux 4 (Update:7) operating system and not specific to Dell Management Console. Install the below mentioned rpms on the managed node to fix this issue [307764]:

net-snmp-utils-5.1.2-13.el4\_7.3.x86\_64.rpm  
net-snmp-libs-5.1.2-13.el4\_7.3.x86\_64.rpm and

net-snmp-5.1.2-13.el4\_7.3.x86\_64.rpm

- \* Purge policy will not purge events required for maintaining the device state. If you have large number of alerts it could cause latency in the Console. Work-around: You can clear out the alerts manually in SQL Management Studio by deleting the alert entries in EC\_Alerts table and delete the rulestate file located under [DMC\_INSTALL\_DIR]\Altiris Agent\Monitor Agent. However this will clear all device health until the next device health poll (default: every 1 hour). [866, 860, 861]

---

---

## Monitoring

---

---

- \* Alerts sent from some versions of the PowerVault MD Storage Management Software for the MD3000 family of devices will not be associated with the MD device in Dell Management Console.

As a result, OnDemand polling for the MD Array will not be triggered. An alert will be generated on the next scheduled health polling cycle if the device state has changed. Reduce the polling interval for the primary health metric if you require more timely updates. Changing the interval will also affect other devices. [271243]

- \* If Performance monitoring is not working, it may be due to:

- The performance policies are not enabled by default. See the Dell Management Console User's Guide or the tutorial video for details on how to enable these policies.
- Performance policies for Windows require Windows 2003 or greater.
- The server you are attempting to monitor must be classified as a Dell Computer. This is a licensing restriction of the limited license.
- For WMI support, the credentials defined in the connection profile at the time the device was discovered must be valid credentials for that device. If the credentials are no longer valid for the device, the device must be re-discovered with the proper credentials.
- The last discovery for the device must have included the WMI protocol. When a device is discovered, it will only use the latest connection information to communicate with the device.

[255062]

- \* If any Group Metric target is changed from the default value to a custom target, this custom target must also be added to the policy. Changing this target will also force the group metric report to use this same target. Data from the old target will no longer be visible in the report.

[902]

- \* Under certain circumstances, the custom target may not display properly

in the Monitor Resources by Status Web part.  
[773]

---

---

## Network Discovery

---

---

### \* SNMP Discovery of Windows Server 2008 Devices

An SNMP-only network discovery task will fail to discover a system if that system is running Windows Server 2008 with its Network discovery feature disabled.

Perform the following steps to enable Network discovery on the target server:

- a) Navigate to the target system's Control Panel.
- b) Select Network and Sharing Center.
- c) In the Sharing and Discovery section, set Network discovery to On.

[250493] [253417]

### \* IPMI Discovery

For proper classification of the IPMI device, the Channel Privilege Level Limit on the IPMI device and the IPMI Privilege level of the connection profile must match. If these levels do not match, the device will be classified as a Network Resource.

The following table lists the appropriate level relationships:

IPMI Device	Connection Profile
Channel Privilege Level Limit	IPMI Privilege level
Administrator	admin
Operator	operator
User	user

[270173]

### \* Discovery of Microsoft High Availability (HA) Clusters

HA Clusters can be discovered using SNMP only. The discovery task that is intended to discover HA Clusters must have SNMP enabled in its Connection Profile and the associated credentials must be correct for the target devices.

In order for the members to be discovered, the IP address of each cluster member must be included in the list of addresses to be discovered by the discovery task.

When discovering HA Clusters, the cluster name may replace the name of the active cluster node. To avoid this, do not include the cluster IP address in the discovery range.

If the cluster IP address is the only IP address in the discovery task that is related to the HA Cluster, the currently active cluster node will be discovered and its name will be the same as that of the cluster itself. This results in the cluster name appearing in

several places under the All Devices organizational view.

For example:

- Under HA Clusters as the HA Cluster
  - In the resource pane as the discovered system when the cluster's organizational group is selected
  - In the resource pane as the discovered system when the Servers organizational group is selected
- [250834] [250857] [253557] [266123]

\* Duplicate entries of a server found after running a discovery task

If a server and its associated Dell Remote Access Card (DRAC) are discovered using SNMP (with or without also using IPMI), two entries for that server are displayed under the All Devices organizational view: one entry for the server and one for the DRAC.

[266778]

\* Dell Servers are classified as Computer even if IPMI is enabled in the connection profile.

When discovering Dell servers using only SNMP or WMI, Server Administrator must be installed and running on the managed system in order for the system to be classified as a Dell Computer.

Consider this situation:

- If IPMI is used in combination with SNMP or WMI,
- You specify both, the server IP address and baseboard management controller (BMC) IP address in the discovery task, and
- Target server is not running Server Administrator

two devices will be discovered: a Computer and a Dell Computer.

In this case, the Dell Computer is associated with the BMC IP address and the Computer is associated with the target server.

[272225]

\* Altiris Agent push fails in certain cases when using SNMP+IPMI or SNMP+WS-MAN to discover a server and its associated iDRAC.

If a server and its DRAC or BMC are discovered using SNMP and IPMI, or SNMP and WS-MAN the IP address of the DRAC/BMC may be associated as the primary IP address of the server.

To avoid this situation, it is recommended you discover the DRAC/BMC in its own discovery task before discovering the server in a separate discovery task.

[285037, 920]

\* When you perform an upgrade from Dell Management Console 1.0 > 1.0.1 > 1.1, the discovery task may fail and a System Format Exception message is displayed. If the devices are visible under Manage > All Devices then you can safely ignore this exception.

[709]

\* With latest firmware version 3.1, Dell PowerConnect switch M6348 will not be discovered as Dell device. As a result, PowerConnect M6348

Switch is not shown in Dell reports.

[630]

- \* On upgrading from DMC 1.0.2 -> 1.1, if the ESXi 4.0 virtual host and its virtual machines are discovered in separate tasks using SNMP protocol, the virtual machines may not be associated to its virtual host. The virtual machine will be shown under Servers organizational group.

Work-around: Discover only the ESXi 4.0 virtual host using SNMP protocol. All the virtual machines running on this virtual host will be discovered and associated as well.

[963]

---

---

## Reports

---

---

- \* PowerConnect M6220, M6348, M8024 and 8024F may not show up in the Ethernet switch report.

At the time of this Dell Management Console release, the shipping version of the firmware for these switches was not providing the information needed to display them in this report. This is being addressed in newer firmware releases for the individual switches.

[630, 736]

- \* Removed Altiris Agent Version report under Dell Reports folder. Use reports located under Notification Server>Agent reports folder.

[822]

---

---

## Tasks

---

---

- \* To run IPMI-related tasks against IPMI-capable devices, such as Dell servers, you must enable the IPMI protocol to discover these devices. The discovery task for IPMI devices should include the IP Addresses that support the IPMI protocol. For Dell servers, these are the IP Addresses by which the DRAC and/or BMC communicate.

[270643]

- \* On managed systems running Windows, if you want to set the front panel LCD text to a multi-word text that contains spaces, use the Command Line Builder task or the BIOS Configuration task. Also, enclose the text in quotes. For example, PowerEdge 2950.

[265432]

- \* On managed systems running Linux, you cannot set the front panel LCD text to a string with embedded spaces using the Command Line Builder or BIOS configuration tasks. PowerEdge 2950 is not a valid setting for LCD text on Linux systems.

Managed systems running Linux have additional restrictions on custom text: some special characters like & and ( cannot be used in the custom text for the above tasks.

[235693]

\* In the Associate Dell Devices task, in Target Selection, (Apply to> Computers,) if you choose the filter (Add Rule): exclude computers not in> Group> Computers, then it only displays (managed) systems that have the Altiris agent installed on them.

To select unmanaged computers, choose the following filter:  
exclude computers not in> Computer list> Computers.  
[267443]

\* Some Server Administrator commands displayed in the Command Line Builder and Hardware Configuration tasks may not be backward compatible. For example, Server Administrator 5.x has nic1 and nic2 attributes but no nic attribute, whereas Server Administrator 4.3 has only the nic attribute.

See the respective versions of Dell OpenManage Server Administrator User's Guide for the complete list of commands and options supported.  
[270384]

\* Exporting a task or policy to an external USB device does not release the device handle.

To work around this issue, export the task or policy to a local drive and copy the exported files to the external USB device.  
[236272]

\* When two or more tasks are added to a Server job, the job may stop responding if any of the tasks in the job is unable to find an applicable target device. If the job stops responding, any remaining tasks in the job may not run.  
[284549]

\* Dell Web Server (DWS) Configuration is not supported for Linux targets in OMSA 6.1. As a consequence configuring DWS using either the DWS Configuration Task or the OpenManage Command Line Interface (OMCLI) task on Linux targets will cause the task to fail. Due to an issue in the task framework with Linux targets, these tasks when executed against Linux targets take a long time (~1 hour) to show the failure.  
[322877]

\* If you click on the "Warranty Report" link from the "Warranty Extractor Task" UI on an SSL enabled DMC, you are required to enter Administrator credentials to access the page. This is due to an issue in the framework API used to retrieve the URL prefix. If you provide the correct credentials, you can view the report from the Task UI page. Alternately, you can choose to view the report from the "Reports"-> "Dell Reports" page, where you are not required to supply credentials.  
[330609]

\* Remote Server Administrator command line task may fail for Server Administrator running on Microsoft Windows 2008 and Microsoft Windows 2008 R2. To enable the successful functioning of remote Server Administrator CLI, the managed system and the management station must be on the same domain or there should be a trust relationship between the two domains.

If you have a Windows firewall configured on either the management station or the managed system, change these settings:

On the management station:

1. Open TCP port 135.
2. Add the "omremote.exe" application (located in \dmc\DMCTasksSolution\ToolsBin) to the firewall exception list.

On the managed system:

On the command prompt, type:

```
"netsh firewall set service RemoteAdmin"
```

For more information on connecting through the Windows firewall, see Microsoft's MSDN website for Platform SDK: Windows Management Instrumentation (Connecting through Windows Firewall) at:

- <http://support.microsoft.com/kb/875605>
- [http://msdn.microsoft.com/en-us/library/aa822854\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/aa822854(VS.85).aspx)

Ensure the following settings are applied for users with non-administrator privileges:

1. Grant DCOM remote launch and activation permissions for a user or group.
2. Grant DCOM remote access permissions.
3. Allow users access to a specific WMI namespace.

For more information see [http://msdn.microsoft.com/en-us/library/aa393266\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/aa393266(VS.85).aspx)

\* When 10G or 11G servers are discovered using multiple protocols (SNMP+IPMI or WMI+IPMI), the task substitution tokens %DELL\_DEVICE\_IPADDRESS% and "%DELL\_RAC\_IPADDRESS%" may not work properly.  
[275724]

\* When a task is running, the task status may be incorrectly shown as Pending. Double click on the task run instance to view the correct status.  
[413]

---

## ESX Support

---

\* The Altiris Agent is not supported on ESX 4.0 (classic). As a result, Dell Patch Management and Performance metrics are not supported.

---

## Installing Dell Management Console into a Virtual Machine (VM)

---

\* Dell Management Console is tested to install in the following VM environment:  
--ESX 3.5 U4

Other notes for VM installs:

- Minimum 4GB Virtual RAM
- Minimum 4 Virtual Processors
- Physical server should have VT enabled processors
- Use a remote SQL database
- Variations on this configuration may work, but have not been tested.
- See kb.altiris.com - 45258 and 45257 for additional details.

#####  
DISCLAIMER  
#####

Information in this document is subject to change without notice.  
Copyright(C) 2010 Dell Inc. All rights reserved.

Reproduction in any manner whatsoever without the written permission  
of Dell Inc. is strictly forbidden.

Trademarks used in this text: Dell, OpenManage, PowerConnect,  
and PowerEdge are trademarks of Dell Inc.; Microsoft, Windows,  
Windows Server, and Excel, are registered trademarks of Microsoft  
Corporation; Novell, NetWare, and SUSE are registered trademarks  
of Novell Inc.; Red Hat and Red Hat Enterprise Linux are registered  
trademarks of Red Hat, Inc.; EMC, Flare, and Navisphere are  
registered trademarks of EMC Corporation; Java and JRE are  
trademarks of Sun Microsystems.

Other trademarks and trade names may be used in this document to refer  
to either the entities claiming the marks and names or their products.

Dell Inc. disclaims any proprietary interest in trademarks and trade  
names other than its own.

March 2010