

# Manage Fusion 2006 Hands-on-Lab Handout

## Open Manage Client Administrator 3.0

**Instructor:** Jordan Gardner – Dell Technical Strategist

**Description:** The release of OMCA 3.0 included a new Dell specific client solution, which allows you to configure, inventory, monitor you Dell OptiPlex, Dimension, & Latitudes. This lab provides hands-on experience on how you can use OMCA 3.0 to manage your Dell Clients.

**This lab assumes a prerequisite knowledge of basic Microsoft networking skills/experience as well as some experience with Altiris Notification Server.**

**At the end of this presentation you should be able to:**

1. Install the OMCA DCM Agent
2. Gather Hardware inventory of your Dell Clients
3. Gather BIOS inventory of your Dell machines
4. Monitor your Dell Client Hardware
5. Tie the OMCA solutions together to leverage each's functionality.

**Notes:**

- A brief presentation will introduce this lab session and discuss key concepts.
- Feel free to begin this self-paced lab using the instructions on the next page.
- Be sure to ask your instructor any questions you may have.
- You can check off individual steps as they are completed. The boxes to the left of the steps are for this purpose.
- Thank you for coming to our lab session.

## Section 1: Install the Altiris Agent on the Dell OptiPlex Host

This lab will be different than other labs because we'll be interacting with not just another Virtual Machine, but the physical host that our Notification Server VM is running on. We need to install the Altiris agent on the host machine in order to gather Dell specific HW and BIOS information.

- 1. In this exercise you will install the Altiris Agent on the host Dell OptiPlex.
  - a. Load the Altiris web console on Server ATRSNS6 by going to Start->All Programs->Altiris->Altiris Console.
  - b. Once it's loaded proceed to Configuration->Altiris Agent -> Altiris Agent Rollout ->Altiris Agent Installation.
  - c. On the Install Altiris Agent



The integration is not enabled by default. Also, if Recovery Solution is not installed on the NS the integration checkbox will be grayed out.

- d. Press Apply button to finish these steps.

## Section 2: Enable the Install the DCM Agent on the Dell OptiPlex Host

This section we will enable the appropriate policies to install the Dell Client Manager Agent.

- 1. In this exercise you will install Discover Dell Hardware and Install the Dell Client Manager Agent.
  - a. Drill to Configuration-> Solution Settings -> Platform Administrator -> Dell Client Manager -> Dell Client Discovery Policy Rollout -> Dell Client Discovery Policy.
  - b. In the Right Pane, Click the Enable checkbox and click Apply.
  - c. Drill to Configuration-> Solution Settings -> Platform Administrator -> Dell Client Manager -> Dell Client Manager Agent Rollout -> Dell Client Manger Agent Install.
  - d. In the Right Pane, Click the Enable checkbox and click Apply.



Notice the collections to which this policies apply. You may change these collections to target a specific group of Dell Clients (for lab or testing purposes).

Once the Dell Client Manager Agent Install completes on the OptiPlex host machine then we can start taking inventory and monitoring our Dell Client Machines.

### Section 3: Enable the Hardware and BIOS inventory policies

Two separate inventory policies allow you to collect Dell Hardware and Dell BIOS information. Administrators can define when these scans should occur, and can even “wake up” powered off machines to perform the scan. In this section, you will explore and enable the BIOS and Hardware Inventory Policies to collect inventory.

- 1. Explore the Dell Client Manager Inventory Packages.
  - a. On the Tasks tab, drill to Platform Management->Dell Client Manager -> Dell Inventory Policies.
  - b. Click on the Dell BIOS **or** Dell Hardware Inventory Package and in the right pane click the Programs tab.

**Dell Client BIOS Inventory Package**

Package Programs Package Servers Advanced

Program  
Dell BIOS Inventory

Name: Dell BIOS Inventory

Description: This program scans and sends Dell client BIOS inventory.

Command line: OmcaClientModule.exe -file:BiosInventory.xml

Working directory:

Success codes: 0, 2

Failure codes:

Estimated disk space: 1024 Kb

Estimated run time: 5 minutes

Terminate after: 10 minutes  
A blank value defaults to 360 (6 hours).

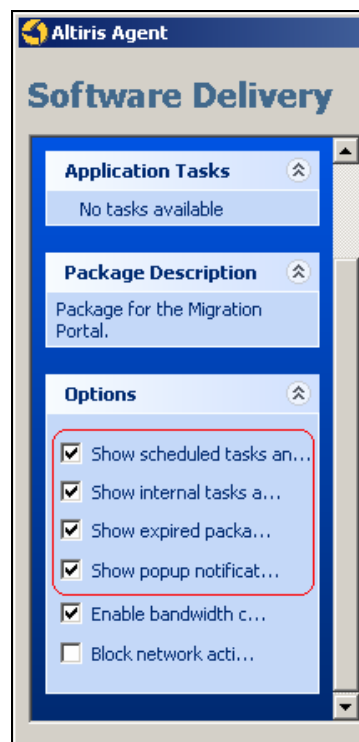
After running: No action required

Apply Cancel Update Distribution Points



The Dell Client Manager sub-agent exposes Dell specific BIOS and Hardware inventory properties via WMI. The OmcaClientModule.exe & answer files (BiosInventory.xml & HardwareInventory.xml) execute the WMI queries and format the output to one .NSE which is forwarded back to the Notification Server. The OmcaClientModule.exe query takes only a few seconds to complete.

- 2. Enable the BIOS Inventory Policy.
  - a. On the Tasks tab, drill to Platform Management->Dell Client Manager -> Dell Inventory Policies.
  - b. Click on the Dell BIOS Inventory Policy
  - c. In the Right Pane, change the Inventory frequency to every 1 minute.
  - d. Click the Enable checkbox and click Apply.
- 3. Enable the Hardware Inventory Policy.
  - a. On the Tasks tab, drill to Platform Management->Dell Client Manager -> Dell Inventory Policies.
  - b. Click on the Dell Hardware Inventory Policy
  - c. In the Right Pane, Click the Enable checkbox and click Apply.
- 4. View the Inventory Status on the target computer.
  - a. On the Host machine (the Dell OptiPlex) – double click on the Altiris Agent in the SysTray.
  - b. Ensure the appropriate “Options” (shown below) are checked



- c. The HW and BIOS Inventory Tasks will be listed and should be complete.

## Section 4: Explore the BIOS and HW Inventory Reported

The Dell specific inventory can be view in each Dell Clients Resource manager as well as from the pre-canned reports. In this exercise we will explore the Resource Manager and pre-canned reports.

- 1. View available Data Classes that Dell Client Manager creates.
  - a. Click on the Reports Tab.
  - b. Click the Dashboards → Dell Client Discovery and Installation Summary
  - c. Double-click the OptiPlex column in the dashboard graph (to drill into more details). Another report will open.
  - d. Double-click the OptiPlex count graph.
  - e. In the list of OptiPlex computers, locate the HOST Computer. Right-click and select “Resource Manager” from the context menu.



The Resource Manager of Dell Client computers running the DCM agent will contain a Dell Client Manager Summary.

The screenshot shows the GXCLIENT interface with the following details:

- System Summary Status:**
  - Model: OptiPlex GX620
  - BIOS Version: A01
- Dell Client Hardware Status:**
  - System Global Status: 3 = OK
  - Operating System Status: OK
  - System Summary Status: OK
  - Hard Disk Drive: PHYSICALDRIVED
    - Status: OK
    - Model: ST340014AS
    - Size: 37.25 GB
  - SMART Hard Disk Drive Serial Numbers: ST340014AS → 5MQ26ZQ4
  - Fan Status:
    - Fan 0: 0 = OK
    - Fan 1: 0 = OK

- f. Now click on the Inventory Tab of the Resource Manager.
- g. Expand the Data Classes -> Dell Client Manager Inventory -> Dell Client BIOS Settings Folder **and** Dell Client Hardware Inventory Folder. Note the Chassis Intrusion Status, in the SMBIOS Settings data class.



You can now see the available Data Classes that the Dell Client Manager inventory scans populate. These are the actual table names within the Altiris Database and can be used to create custom reports.

The screenshot shows the GXCLIENT interface with the 'SMBIOS Settings' data class selected. The left pane shows a tree view of data classes, with 'SMBIOS Settings' highlighted. The right pane displays a table of properties and their values.

Property	Value
AutoOn	3 = Disabled
AutoOnHour	0
AutoOnMinute	0
ChassisIntrusion	5 = Silent Enabled
ChassisIntrusionStatus	4 = Not Detected
Hyperthreading	3 = Enabled
BootSequence	2 = Unsupported
BuiltinFloppy	3 = Disabled
BuiltinNIC	5 = Enabled
BuiltinPointingDevice	3 = Enabled
Onboard1394	2 = Unsupported
WakeupOnLAN	7 = Enabled with boot to NIC
PowerManagementSettings	2 = Unsupported
IDEController	2 = Unsupported
PCISlots	4 = Enabled
USBEmulation	4 = Enabled
AGPSlot	2 = Unsupported
Numlock	0 = Unsupported
WirelessControl	0 = Unsupported

- 2. Run pre-canned BIOS version report to create a dynamic collection.
  - a. From the Reports Tab, drill to Reports -> Platform Administration -> Dell OpenManage -> Dell Client Manager -> BIOS Settings -> Systems with Specified BIOS Version report
  - b. In the Right Pane, click “Run this report in a new window”
  - c. This report allows you to specify criteria to generate a very specific subset of Dell Machines. Specify the following and click Refresh

Product Line: **OptiPlex Desktops**  
 Model: **GX620**  
 Operator: **Older Than**  
 BIOS Version: **A03**



This report now lists only those OptiPlex GX620 machines that are running BIOS versions older than A03. Creating a collection to use for a BIOS upgrade from this report can be done in a single mouse click.

### Systems with Specified BIOS Version

Product line:

Model:

Operator:

BIOS Version:

BIOS Version	Product Line	Computer Name	Model
A01	OptiPlex Desktops	GXCLIENT	GX620

- 3. Create a dynamic collection from the BIOS version report to be used later in a BIOS upgrade policy.
  - a. From the report click the dynamic collection from report button

⌵
🏠
✎
{ }
🔗
⚠
📄
🔍
🔄
📅
🗨

### Systems with Specified BIOS Version

- b. A new dynamic collection is created.
- c. Rename the Collection to “GX620’s running older than BIOS A03”

## Section 5: Remotely upgrade the BIOS on you Dell Clients

The Dell Client Manger Solution allows you to remotely upgrade the BIOS on you Dell Machines. To do this, you must first obtain the BIOS file from support.dell.com and extract the .hdr file from it by using the “-writehdrfile” command. In this exercise we will configure the BIOS Upgrade Policy.

- 1. Configure the BIOS Upgrade Policy
  - a. On the Tasks tab, drill to Platform Management->Dell Client Manager -> Dell BIOS Policies.
  - b. Right-click → Clone the “Dell Upgrade Policy”



Cloning policies allows you to schedule separate policies and apply them to multiple collections. For example you could have 1 BIOS upgrade policy apply to your OptiPlex GX620s and another to your Latitude D600s

- c. Right-click → Rename the cloned policy to “**GX620 BIOS A03 Upgrade**”
- d. Highlight the renamed policy. In the right pane, click the Collection link. (The collection browser will open).
- e. In the collection selector dialog, select the collection we created in the earlier exercise. Located in Collections -> Computer Collections -> My Collections -> GX620's running older than BIOS A03



Using the Collection which we created from the BIOS version report ensures that the correct BIOS upgrade is applied to the correct machines. Since our collection is dynamic, any GX620 machine running BIOS Version older than A03 will automatically receive a BIOS upgrade.

- f. You can explore the scheduling options available when rolling out an upgrade.



The BIOS .hdr files can be obtained from the Dell support website. <http://support.dell.com>. This lab will not upgrade the BIOS on the OptiPlex host as a BIOS upgrade requires a reboot and will force the Notification Server VM to close ending the Lab.

- g. This is the end of this exercise.

## Section 6: Remotely configuring BIOS Settings across your network

A 'Dell BIOS Profile' is a template of BIOS settings that you can assign to a collection of computers. Machines included in the assigned collection will then assume those BIOS settings defined in profile. In this section we will remotely configure BIOS settings with BIOS profiles.

- 1. Create a BIOS profile by Importing Inventoried settings
  - a. Drill to Tasks → Platform Administration → Dell Client Manger → Dell BIOS Profile
  - b. On the Dell Bios Profile folder Right click → New Dell Bios Profile



Dell BIOS Profiles can be created from scratch, by configuring any desired options one at a time, or you can import existing settings from those Dell Clients which have run the BIOS inventory scan.

- c. From the Dell Bios Profile dialog, Click on Import, Click Find, Select an inventoried Dell Client from the list. The inventoried BIOS settings are imported into the BIOS Profile



You can modify any of the BIOS settings imported, such as the BIOS Password, or Boot Order, or Force PXE on next Boot.

- d. Save the BIOS Profile & Click Close
- 2. Create a BIOS profile by Importing Inventoried settings
    - a. On the Dell Bios Profile folder Right click → New Dell Bios Profile
    - b. In the Dell Bios Profile dialog, check the “Chassis Intrusion Status” checkbox and set the drop down list value to “Clear”
    - c. Save the BIOS Profile as “Clear Chassis Intrusion Profile” & Click Close

□ 3. Rolling out your BIOS Settings Profile

- a. Drill to Tasks → Platform Administration → Dell Client Manger → Dell BIOS Policies → BIOS Settings Policy



The BIOS Setting Policy allows you to select a BIOS profile and define a collection to apply it to. One nice feature of using these Profiles is that they're model independent. You can capture the bios profile settings from a Latitude D610 laptop and apply that profile to all your OptiPlex GX620 Desktops. Option not available on the machine BIOS will be ignored.

- b. Select the Dell profile link, and choose the “Clear Chassis Intrusion Profile” from the list of available BIOS profiles.
- c. Ensure the collection is set to “All Supported Dell Client Computers”



The BIOS Setting Policy allows you to select a BIOS profile and define a collection to apply it to. One nice feature of using these Profiles is that they're model independent. You can capture the bios profile settings from a Latitude D610 laptop and apply that profile to all your OptiPlex GX620 Desktops. Option not available on the machine BIOS will be ignored.

- d. Ensure the scheduling options are set to run ASAP and Click Apply.
- e. Open the Agent Dialog on the HOST machine to watch the Dell BIOS profile apply.

## Section 7: Monitoring your Dell Client Machines with Dell Client Manager

The Dell Client Manager allows you to monitor various items on your Dell Machines, such as Chassis intrusion status, memory or disk changes, Operating System Status, etc. In this exercise we will configure and enable the Dell Client Manager's monitoring policy and configure an Automated Action.

- 4. Configure your Dell Client Monitoring Policy.
  - a. Drill to Tasks → Platform Administration → Dell Client Manager → Dell Client Monitoring Policies.
  - b. Select the Dell Client Monitoring Policy



Notice all the available values and metrics that you can monitor.

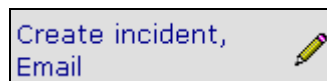
- c. In the Right Pane, Check the Chassis Intrusion Status checkbox and set the values to:


<input checked="" type="checkbox"/> Chassis intrusion status	Any	To	3-Detected
--	-----	----	------------



For Monitor Agents, you have the ability to configure automatic actions if any of these areas being monitored raise an alert. You can define a default action for all triggered alerts, and you can override that default action for specific monitored items

- d. Next to the Chassis Intrusion status dropdown boxes, click the Automated Action link:



- e. Ensure the “Create Incident” checkbox is checked and click on the  to edit the incident.
- f. Edit ONLY the following properties of the incident (as shown below):

Assigned: **Administrator**

Status: **Open**

Category: **Authorize Approve... Desktop**

**Automated Action -- Web Page Dialog**

Name: Create incident

Description: Creates a new incident for the received Chassis Intrusion Alert

Enabled

**Type:** New Incident Automated Action

Resource Guid: %DS:ResourceGuid%

External ID: Source:

Assigned: Administrator Owner:--[auto]--

Priority: ASAP Status: Open


Urgency: High Impact: High

Category: ...Desktop Type: Other

Notify rules:

Acknowledge contact

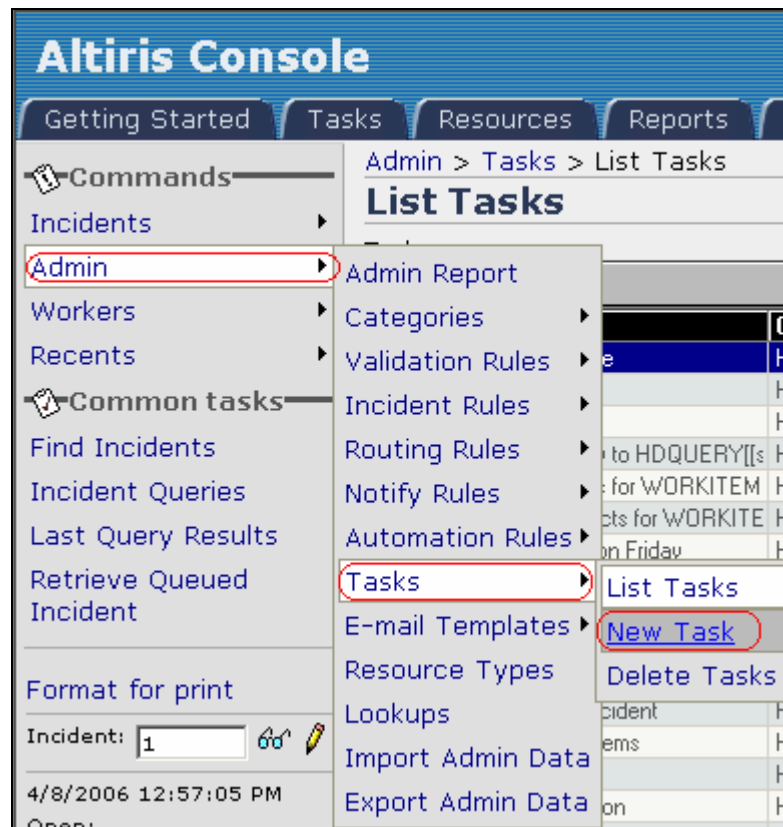
OK Cancel

- g. Click OK to close the “Create Incident” dialog.
- h. (OPTIONAL): You may click the  next to the “Email” automated action to view the details of the email that will be sent when a chassis is opened.
- i. Click Apply to close the “Automated Actions” dialog.
- j. Click Apply to set the changes to the Monitoring Policy.

## Section 8: Integrate Alert Manager (or Helpdesk) with Dell Client Manager

DCM's Monitoring Policy or any Notification Server Policy can create incidents in the Altiris Alert Manager console. (Alert Manager is the free helpdesk console which is apart of Notification Server which allows solutions to create incidents. The full Helpdesk Solution provides the ability of end users and IT administrators to create incidents). In this incident we will integrate Dell Client Manager with Alert Manager by creating a custom "Smart Task" which will link you to the actual Dell machines warranty and support webpage.

- 5. Configure the Alert Manager Smart Task
  - a. Click on the Incidents Tab in the NS Console
  - b. In the left pane, create a new Smart Task by drill to: Admin → Tasks → New Task (as shown below)




- c. For Name enter: View Dell Support & Warranty Information
- d. For Description (Optional) provide: This smart task, when clicked, sends you to the appropriate support and warranty information page for the Dell computer which created the incident.
- e. For Consumer ID provide: Dell Client Manager

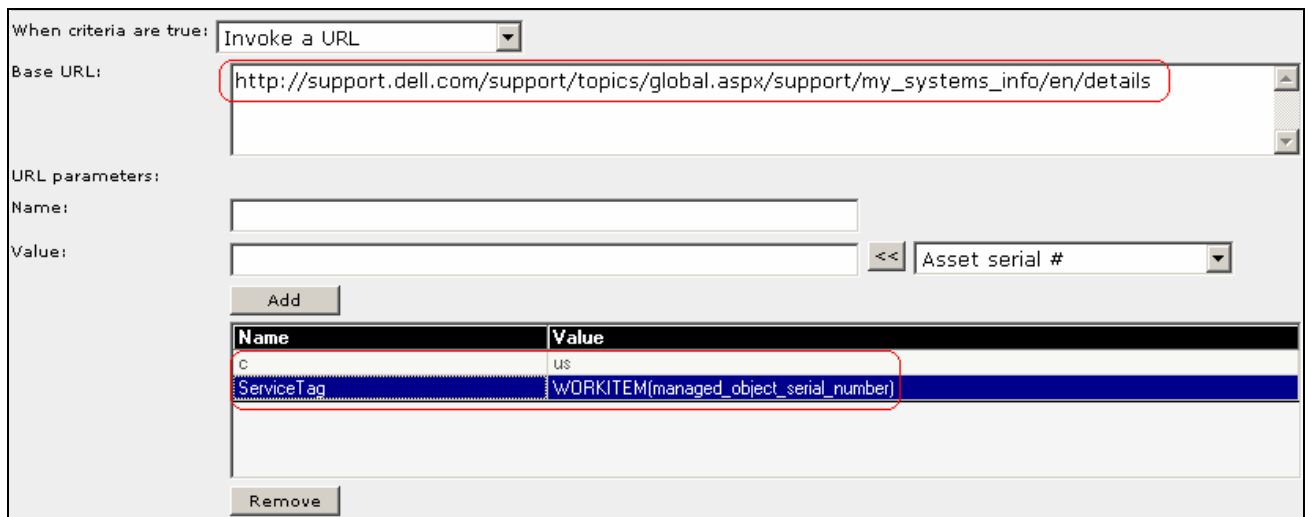
- f. In the “Task is available:” section, select **Created by worker** from the drop down list and click **Add**.

- g. Check the “When the value of ‘Created by worker:’” checkbox.
- h. Set the drop down list value to: **is equal to**
- i. Select **Altiris Dell Client Manager** from the drop down list (see below)

- j. Click OK.
- k. In the “When criteria are true:”, set the drop down list to **Invoke a URL**
- l. For “Base URL:” supply the string:

[http://support.dell.com/support/topics/global.aspx/support/my\\_systems\\_info/en/details](http://support.dell.com/support/topics/global.aspx/support/my_systems_info/en/details)

- m. For URL parameters, we will supply 2 parameters:
- Name: **c** (← The letter “c”)
  - Value: **us**
  - Click **Add**
  - Name: **ServiceTag**
  - For Value, select “**Asset serial #**” from the drop down list, then 
  - Click **Add** (See image below)





When criteria are true: Invoke a URL

Base URL:

URL parameters:

Name:

Value:   Asset serial # 

Name	Value
c	us
ServiceTag	WORKITEM(managed_object_serial_number)

- n. Click **OK** to save the Task.



Now when any incidents are created from the Dell Client Manager Solution, you will have a smart task available that will take you to the Dell support website where you can view original configuration and warranty information about the Dell computer that is associated with the incident.

## Section 9: Test the Dell Client Manager Monitor Policy

In this exercise we will test the Dell Client Manager monitoring policy by popping open the chassis and checking helpdesk and our email for the triggered alert.

- 1. Perform a chassis intrusion
  - a. On the host machine, open the box (special instructions should be given)
  - b. After the chassis has been opened, reattach the chassis.
- 2. Check your Helpdesk console for the triggered Incident
  - a. Click on the **Incidents tab**
  - b. In the left pane, select **Incidents → Worker Report**
  - c. In the right pane, click on the **All Incidents assigned to me:** link
  - d. The incident should be listed (see below)

#	Title	Assigned	Priority	Status
32	Dell Client Manager: Chassis Intrusion Alert	Administrator	ASAP	Open

- e. Double click on the “Dell Client Manager: Cassis Intrusion Alert” incident to view the details. Notice the “Smart Task” which will take you to the Dell Support website.
- f. Read through the incident to see what was sent from the DCM Solution, notice the smart task (displayed below)

Tasks:
• <a href="#">Dell Support and Warranty Information (Altiris Dell Client Manager)</a>



Notice: A smart task is available that will take you to the Dell support website where you can view original configuration and warranty information about the Dell computer that is associated with the incident.

- 3. Check your email for the triggered email
  - a. From the Start menu, or quick launch bar, open Outlook Express
  - b. If no emails appear, click the Send/Receive button
  - c. Open and read the automatically generated email.

