
Making My Environment Manageable for Dell OpenManage Essentials

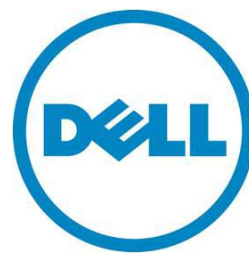
This white paper details how to configure Dell devices so that they may be discovered and managed by Dell OpenManage Essentials

Author(s)

Nitin M. Bhambere &
Ashish Suyal

Updated for OME 1.1 by

Zach Douglas &
Mun Min



This document is for informational purposes only and may contain typographical errors and technical inaccuracies. The content is provided as is, without express or implied warranties of any kind.

© 2013 Dell Inc. All rights reserved. Dell and its affiliates cannot be responsible for errors or omissions in typography or photography. Dell, the Dell logo, and PowerEdge are trademarks of Dell Inc. Intel and Xeon are registered trademarks of Intel Corporation in the U.S. and other countries. Microsoft, Windows, and Windows Server are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. 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 disclaims proprietary interest in the marks and names of others.

January 2013 | Rev 1.0

Contents

Executive summary	4
Managing Servers Agent Free	4
Managing Servers with agent (OMSA) Installed	5
Configuring Multiple Dell 12G iDRAC7s for Agent Free Management using RACADM command with OME's Remote Tasks Wizard.	6
Configuring Dell 12G iDRAC7 for Agent Free Management using the iDRAC7 console.	13
Configuring Multiple Dell 11G iDRAC6 for Agent Free Management using RACADM Commands with OME's Remote Tasks Wizard.	16
Configuring Dell 11G iDRAC6 for Agent Free Management using iDRAC6 Console.....	20
Managing Servers with agent (OMSA) Installed.....	22
Configuring Dell PowerEdge Server with Windows Server Operating System (including Hyper-V) with Dell OpenManage Server Administrator (OMSA)	22
Configuring Dell PowerEdge Linux Servers With Dell OpenManage Server Administrator (OMSA).....	26
Configure Dell PowerEdge ESXi 4 and ESXi 5 Servers With Dell OpenManage Server Administrator (OMSA)	31
Configure Dell 12G and 11G PowerEdge Servers for Agent Free Software Updates	32
Configure Dell Client Systems using OpenManage Client Instrumentation (OMCI)	32
Configuring Dell PowerEdge Servers (9G/10G) with Windows Server or Windows Hyper-V using WMI ...	32
Configuring Dell PowerEdge Linux Servers (9G/10G) to use SSH.....	33
Configure Dell EqualLogic Storage Devices	36
Configure Dell Force10 Network Switch	37
Configure Dell PowerConnect Network Switch.....	38
Configure Dell Chassis Management Controller (CMC)	40
Configure Dell PowerVault Modular Disk Storage (MD Array)	41
Configure Dell Power Distribution Unit (PDU)	43
Configure Dell Universal Power Supply (UPS)	45

Executive summary

This document contains information to help you configure various Dell devices in order to manage them using Dell OpenManage Essentials (OME). Once devices are properly configured, they can be discovered and classified in OME's device tree. In the device tree you can find health status, as well as discovery and inventory (asset data) information about the devices. You will also be able to receive alerts (SNMP traps or Platform Event Traps) from properly configured devices when their health status changes.

For Dell hardware devices such as switches, storage arrays, or PDUs, device settings are typically configured using a console with a graphical interface or alternately by using a command line interface (CLI).

When configuring Dell PowerEdge Servers for management, you may choose to use the Dell Agent (OpenManage Server Administrator or "OMSA") or to go Agent free if you have 12G or 11G servers.

Using OMSA requires SNMP settings on the operating system to be configured and for OMSA to be installed on the operating system. OMSA is supported in Windows, Linux (Red Hat, SUSE), and ESXi or XEN operating systems. Details for configuring SNMP and OMSA for each are found in this document.

Dell's 11G and 12G servers allow for Agent free Management. By communicating directly with the server's integrated remote access controllers (iDRAC), a software agent is not needed. Management can take place if the operating system is down or even if an operating system is not present. Configuration for Agent Free management can be done in a web console or via RACADM commands. The processes to configure the managed servers are also detailed in this document.

The following tables show the features that are supported for various generations of Dell PowerEdge Servers with Agent Free Management as well as management via Dell OMSA Agent.

Managing Servers Agent Free

Functionality	Discovery and Inventory	Monitoring	System Updates	Remote Tasks
Server Generation				
12G	A. Classification as Server B. Deep hardware Inventory from iDRAC7 See: Configuring Dell 12G iDRAC7 for Agent free management	A. Complete Server Health (including attached storage) B. Full SNMP Alerts and PETs (including storage) See: Configuring Dell 12G iDRAC7 for Agent free management	A. Deploy BIOS and Firmware updates via iDRAC. See: Configure Dell 12G and 11G PowerEdge Servers for Agent Free Software Updates	A. RACADM, IPMI Command line Tasks

Functionality	Discovery and Inventory	Monitoring	System Updates	Remote Tasks
11G	<p>A. Classification as Server</p> <p>B. Deep hardware Inventory from iDRAC6</p> <p>See: Configuring Dell 11G iDRAC6 for Agent free management</p>	<p>A. Partial Server Health (no storage health)</p> <p>B. Limited SNMP Alerts and PETS (No storage alerts)</p> <p>See: Configuring Dell 11G iDRAC6 for Agent free management</p>	<p>A. Deploy BIOS and Firmware updates via iDRAC.</p> <p>See: Configure Dell 12G and 11G PowerEdge Servers for Agent Free Software Updates</p>	<p>A. RACADM, IPMI Command line Tasks</p>
10G/9G	<p>A. Classification as Server</p> <p>B. Basic Inventory.</p> <p>See: Configuring Linux servers using SSH or Configuring Windows using WMI protocol.</p>	Not supported	Not supported	<p>A. RACADM, IPMI Command line Tasks</p>

Managing Servers with agent (OMSA) Installed

The supported operating systems supported are Windows, Linux, ESXi, ESX, and Xen (refer to the OpenManage 7.1 support matrix).

Functionality	Discovery and Inventory	Monitoring	System Updates	Remote Tasks
Server Generation				
12G	<p>A. Classification as Server</p> <p>B. Deep hardware Inventory</p> <p>See: Configuring OMSA for Windows, Linux, or ESXi</p>	<p>A. Complete Server Health.</p> <p>B. SNMP Alerts from OMSA</p> <p>See: Configuring OMSA for Windows, Linux, or ESXi</p>	<p>A. Deploy Driver, BIOS and Firmware updates via OMSA</p> <p>See: Configuring OMSA for Windows, Linux, or ESXi</p>	<p>A. OMSA Command Line Task</p>

Functionality	Discovery and Inventory	Monitoring	System Updates	Remote Tasks
11G	A. Classification as Server B. Deep hardware Inventory See: Configuring OMSA for Windows , Linux , or ESXi	A. Complete Server Health. B. SNMP Alerts from OMSA See: Configuring OMSA for Windows , Linux , or ESXi	A. Deploy Driver, BIOS and Firmware updates via OMSA See: Configuring OMSA for Windows , Linux , or ESXi	A. OMSA Command Line Task
10G/9G	A. Classification as Server B. Deep hardware Inventory See: Configuring OMSA for Windows , Linux , or ESXi	A. Overall Server Health. B. SNMP Alerts from OMSA. See: Configuring OMSA for Windows , Linux , or ESXi	A. Deploy Driver, BIOS and Firmware updates via OMSA. See: Configuring OMSA for Windows , Linux , or ESXi	A. OMSA Command Line Task

Configuring Multiple Dell 12G iDRAC7s for Agent Free Management using RACADM command with OME's Remote Tasks Wizard.

1. Configure SNMP Settings and enable alerts using RACADM commands with OME tasks

If iDRAC7s are discovered in OME, you can run RACADM command line tasks to configure the SNMP settings on the iDRAC7s. This method allows you to avoid configuring the iDRACs individually.

You will create these 5 command line tasks in OME to enable Platform Event Alerts, set the destination IP address (OME Server IP), set the community name, and enable all possible alerts. Detailed steps follow this list. For more information on RACADM commands and configuring the iDRAC7, go to:

<http://support.dell.com/support/edocs/software/smdrac3/idrac7/1.20.20/en/index.htm>

Note: This example covers IPV4 settings. If you need to use IPV6 also, refer to the link above for the appropriate commands.

Making My Environment Manageable for Dell OpenManage Essentials

List of RACADM commands needed to remotely configure iDRAC7 to enable all alerts, set the community string, and set the OME server as the destination:

```
config -g cfgipmilan -o cfgipmilanalertenable 1  
config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i 1 1  
config -g cfgIpmiPet -o cfgIpmiPetAlertDestIpAddr -i 1 {OME Server IP}  
config -g cfgIpmiLan -o cfgIpmiPetCommunityName {community string}  
eventfilters set -c idrac.alert.all -a none -n snmp
```

To configure iDRAC7 using the OME Remote Task Wizard, perform the following steps:

1. After launching the OME console, navigate to **Manage > Remote Tasks**.
2. Click **Create Command Line Task**.
3. Name the task.
4. Select **RACADM Command Line** as the type of task.
5. Enter the following command in the command box to enable Platform Event Traps (IPMI traps):

```
config -g cfgipmilan -o cfgipmilanalertenable 1
```
6. **Ping Device** is optional. This will ping the device first and if it fails, no command is run.
7. **Output to file** is recommended. This will create a log file for each command run.

Create a Command Line Task

General | Task Target | Schedule and Credentials

Task Name

Remote Server Administrator Command
 Generic Command
 IPMI Command
 RACADM Command Line

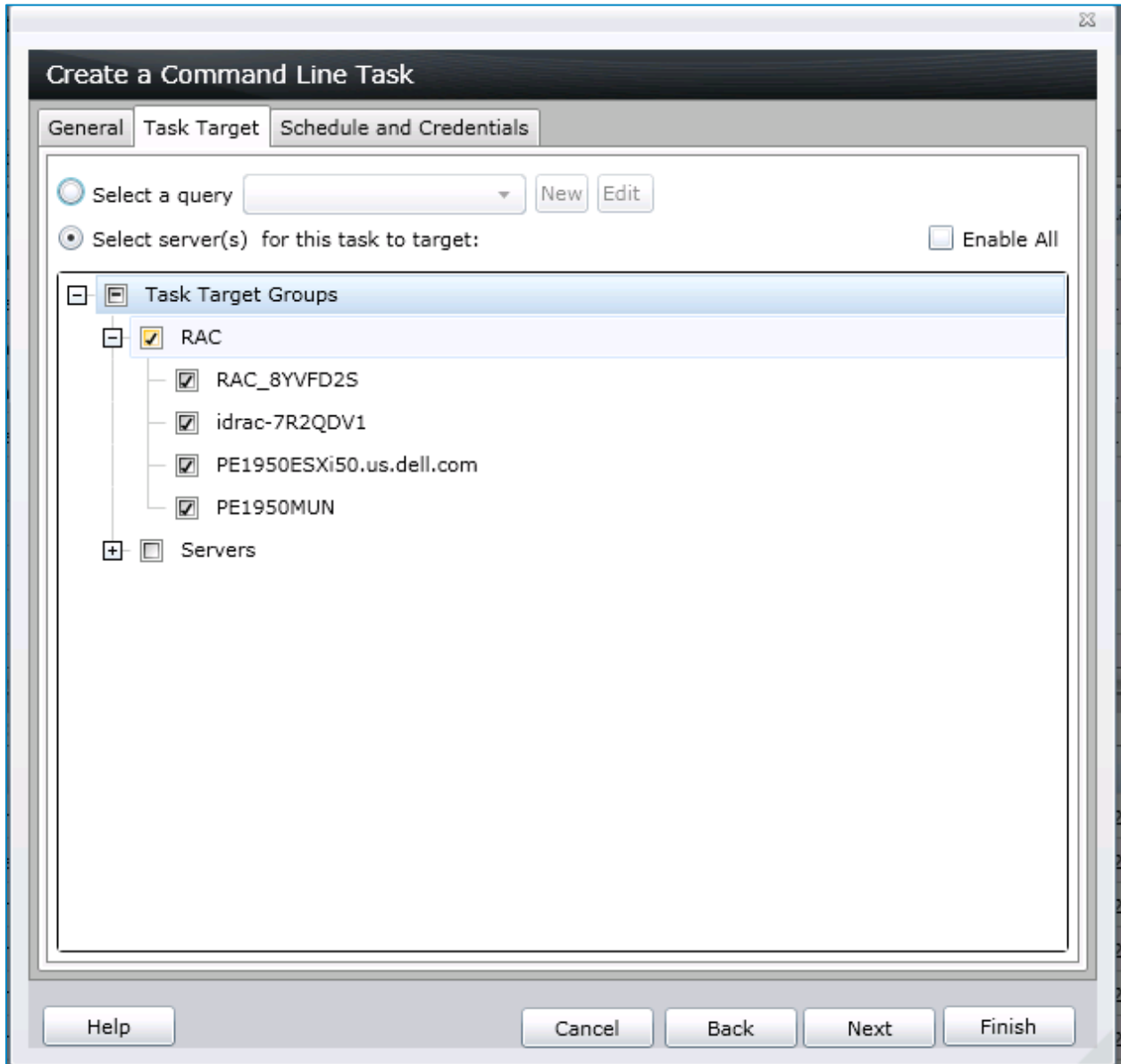
Command:

Ping Device
 Output to file
 Append Include errors

Help Cancel Next Finish

8. Click the **Task Target** tab. Click on any or all RAC devices in the target selection tree that you wish to run the task against.

Note: If the server and iDRAC are discovered together in OME 1.1, they will be represented as one device and will be shown with the server name and not the iDRAC name. Devices appearing in RAC group are all iDRACs.



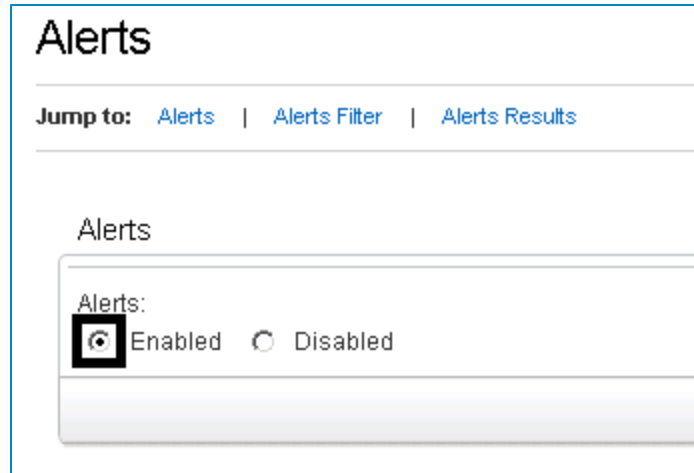
9. Click the **Schedule and Credentials** tab. Run the task now if desired or schedule it for later. Enter the User Name and Password for the RAC devices.

The screenshot shows a dialog box titled "Create a Command Line Task" with three tabs: "General", "Task Target", and "Schedule and Credentials". The "Schedule and Credentials" tab is active. Under "Set schedule:", there are four radio buttons: "Run now" (selected), "Set schedule" (with a date/time picker showing "11/14/2012 1:08 PM" and "(UTC+12:00)"), "Run Once", and "Periodic". An "Activate Schedule" checkbox is unchecked. Below this is a section titled "Enter Remote Access Controller credentials for target(s)" with "User Name:" (text box containing "linux-user") and "Password:" (password box with seven dots). At the bottom are "Help", "Cancel", "Back", and "Finish" buttons.

10. Repeat steps 2-9 with the following command line tasks. You will need to create a RACADM command line task for EACH command. You can right-click on a task you created and use the CLONE feature to make a copy of the command and then edit the command line for each command. With each command shown here, the affected settings in the iDRAC console is also shown for reference.

1. `config -g cfigipmilan -o cfigipmilanalertenable 1`

This command was already created. This command enables alerts.



```
2. config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i 1 1
```

This command enables alerts for 1 out of 4 possible destinations. "-i 1" designates the index (IPv4 Destination1). The second "1" turns alerts ON for that destination.

IP Destination List

Destination Number	State	Destination Address
IPv4 Destination1	<input checked="" type="checkbox"/>	10.36.0.215
IPv4 Destination2	<input type="checkbox"/>	0.0.0.0
IPv4 Destination3	<input type="checkbox"/>	0.0.0.0
IPv4 Destination4	<input type="checkbox"/>	0.0.0.0

```
3. config -g cfgIpmiPet -o cfgIpmiPetAlertDestIpAddr -i 1 10.36.0.215
```


This command sets the destination IP address (OME Server IP address) for 1 out of 4 possible destinations. The "-i 1" designates the index (IPv4 Destination1). Use your OME server IP instead of the example 10.36.0.215.

IP Destination List

Destination Number	State	Destination Address
IPv4 Destination1	<input type="checkbox"/>	10.36.0.215
IPv4 Destination2	<input type="checkbox"/>	0.0.0.0
IPv4 Destination3	<input type="checkbox"/>	0.0.0.0
IPv4 Destination4	<input type="checkbox"/>	0.0.0.0

```
4. config -g cfgIpmiLan -o cfgIpmiPetCommunityName public
```

This command configures the Community String to public. Change community string name as desired.

SNMP Traps and E-mail Settings		
IP Destination List		
Destination Number	State	Destination Address
IPv4 Destination1	<input type="checkbox"/>	10.36.0.215
IPv4 Destination2	<input type="checkbox"/>	0.0.0.0
IPv4 Destination3	<input type="checkbox"/>	0.0.0.0
IPv4 Destination4	<input type="checkbox"/>	0.0.0.0
IPv6 Destination1	<input type="checkbox"/>	::
IPv6 Destination2	<input type="checkbox"/>	::
IPv6 Destination3	<input type="checkbox"/>	::
IPv6 Destination4	<input type="checkbox"/>	::
Community String	<input type="text" value="public"/>	

```
5. eventfilters set -c idrac.alert.all -a none -n snmp
```

This command enables ALL possible alerts by enabling all filters. “-a none” designates that no action is taken on the server. “-n snmp” designates SNMP alert to be turned on for all possible alerts. If you wish to only activate certain filters/alerts, or modify other settings such as email alerts, view the RACADM documentation for specific commands.

To access the RACADM Command Line Reference, go to:

<http://support.dell.com/support/edocs/software/smdrac3/idrac7/1.20.20/en/index.htm>

Alerts Filter

Category:		Severity:	
<input checked="" type="checkbox"/> System Health	<input checked="" type="checkbox"/> Audit	<input checked="" type="checkbox"/> Informational	
<input checked="" type="checkbox"/> Storage	<input checked="" type="checkbox"/> Updates	<input checked="" type="checkbox"/> Warning	
<input checked="" type="checkbox"/> Configuration	<input checked="" type="checkbox"/> Work Notes	<input checked="" type="checkbox"/> Critical	

Alerts Results

Category	Alert	Severity	Email <input type="checkbox"/>	SNMP Trap <input type="checkbox"/>	IPMI Alert <input type="checkbox"/>
System Health	Amperage	Warning	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
System Health	Amperage	Critical	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
System Health	Amperage	Informational	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
System Health	Auto Sys Reset	Critical	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
System Health	Battery Event	Warning	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
System Health	Battery Event	Informational	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
System Health	Battery Event	Critical	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Storage	Battery Event	Warning	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

11. Optional: Send a test trap

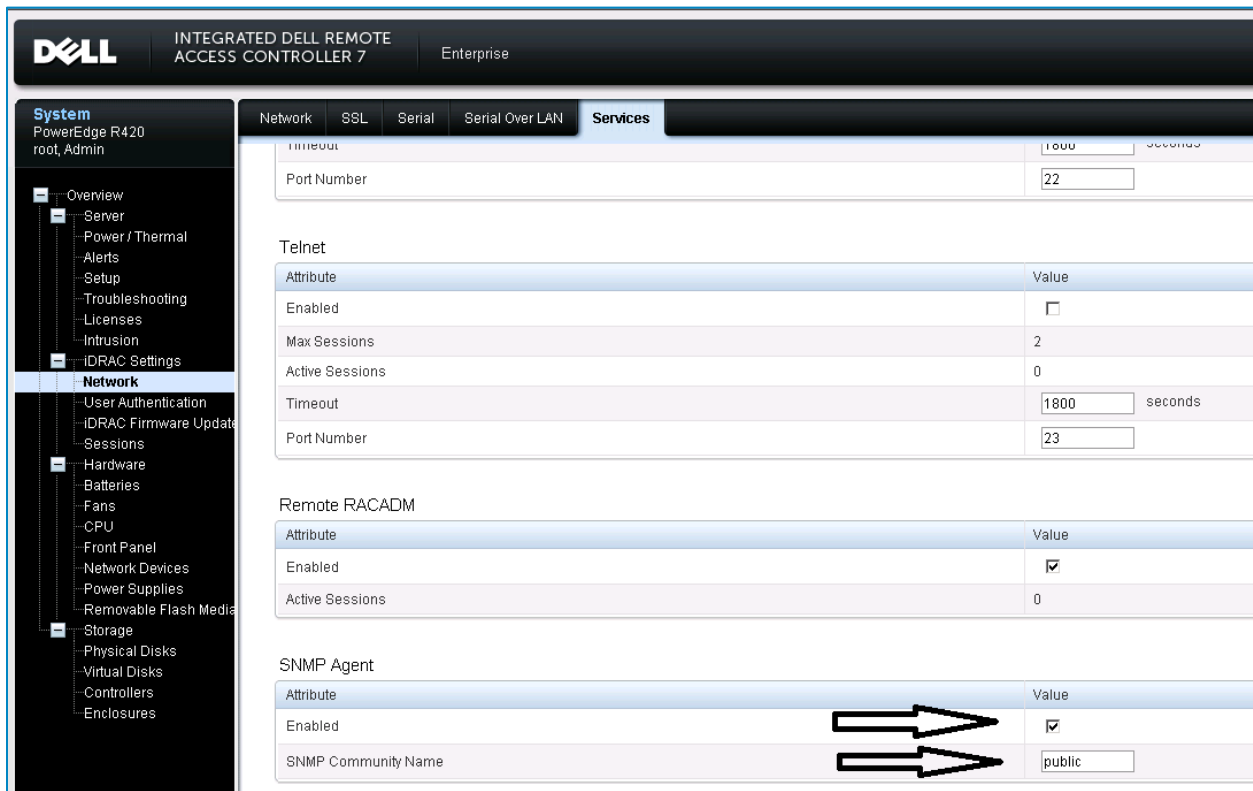
Create a remote task with this command which will send a test trap to the OME IP designated in Index1 (Destination1). You should see this alert in OME console if everything is configured correctly and firewall is open to receive alerts.

```
testtrap -i 1
```

Configuring Dell 12G iDRAC7 for Agent Free Management using the iDRAC7 console.

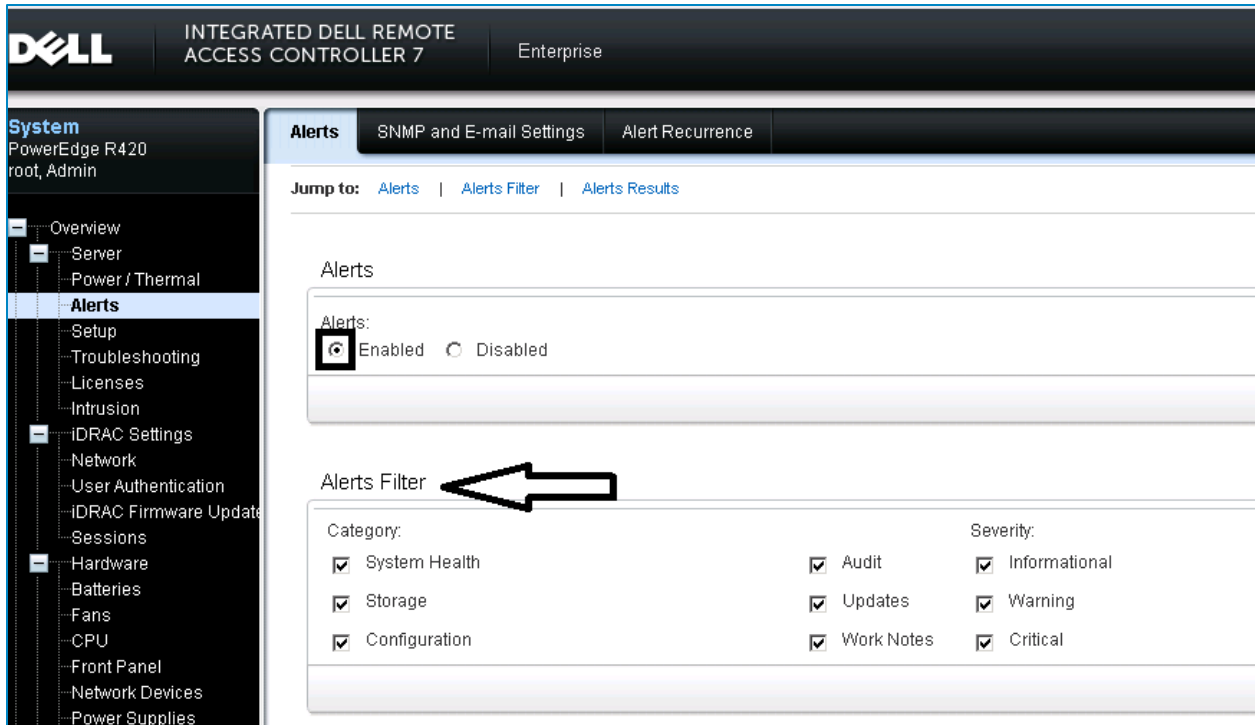
To enable SNMP Agent and alert destinations in the iDRAC7 console, perform the following steps.

1. **Enable SNMP Agent**
 - a. Log in to the Integrated Dell Remote Access Controller 7 console.
 - b. Navigate to **iDRAC Settings > Network > Services**.
 - c. Go to the **SNMP Agent** section.
 - d. Select the check box to enable the SNMP Agent.
 - e. Enter the SNMP Community Name.
 - f. Scroll to bottom of page if needed and click **Apply**.



2. Enable Alerts

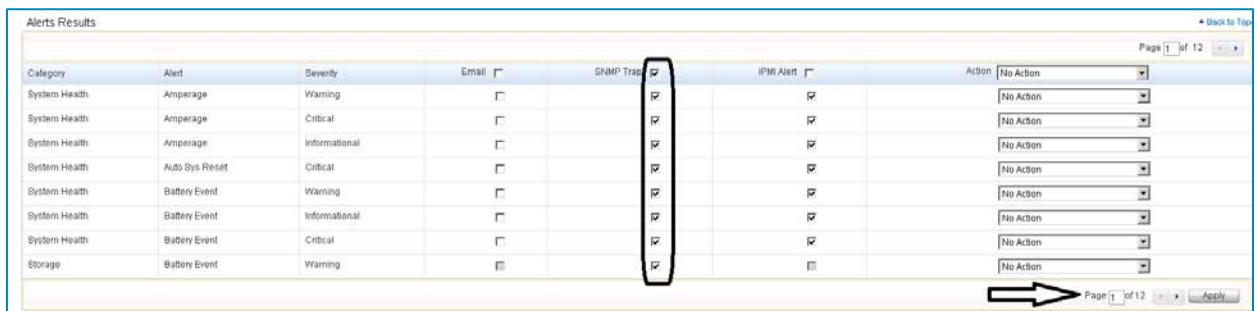
- a. Log in to the Integrated Dell Remote Access Controller 7 console.
- b. Navigate to **Server > Alerts**.
- c. Select the check box to enable alerts.
- d. In the **Alerts Filter** section, select all of the categories that you want to monitor.



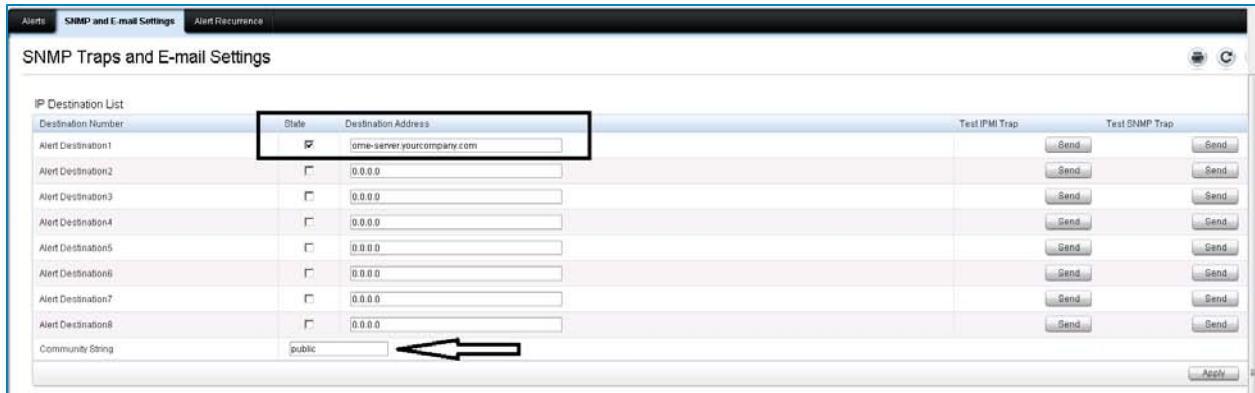
- e. In the **Alerts Results** section, select the SNMP Trap check boxes for all of the specific categories that you want to monitor.

Note: There are multiple pages to scroll through for selections.

- f. Click **Apply** at the bottom right to save the changes



- g. Click on the **SNMP and E-Mail Settings** tab at the top of page.
- h. Enter IP or host name of the OME management station for Destination Address.
- i. Check box for State - enabled with check mark.
- j. Enter the Community String in Community String box at bottom.
- k. You can optionally send a test SNMP trap to OME once you have entered the information.
- l. Click **Apply** at bottom right corner to save changes.



Configuring Multiple Dell 11G iDRAC6 for Agent Free Management using RACADM Commands with OME's Remote Tasks Wizard.

1. Configure SNMP Settings and Enabling Alerts using RACADM commands with OME tasks

If iDRACs are discovered in OME, you can run RACADM command line tasks to configure the SNMP settings on the iDRACs. This method allows you to avoid configuring the iDRACs individually.

You will create these 4 command line tasks in OME to enable Platform Event Alerts, set the destination IP address (OME Server IP), and set the community name. Detailed steps follow this list. For more information on RACADM commands and configuring the iDRAC6, see the "Configuring PET" section of this online manual:

<http://143.166.224.210/support/edocs/software/smdrac3/idrac/idrac20modular/en/ug/html/cha p13.htm#wp50373>

Note: This example covers IPV4 settings. If you need to use IPV6 also, please refer to hyperlink for appropriate commands.

List of RACADM commands needed to remotely configure iDRAC6 to enable alerts with OME server as the destination:

```
config -g cfgipmilan -o cfgipmilanalertenable 1
config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i 1 1
config -g cfgIpmiPet -o cfgIpmiPetAlertDestIpAddr -i 1{OME Server IP}
config -g cfgIpmiLan -o cfgIpmiPetCommunityName {community string}
```

Detailed steps for configuring using OME Remote Task Wizard:

1. After launching OME console, navigate to Manage > Remote Tasks
2. Click on Create Command Line Task
3. Name the task

4. Choose RACADM Command Line as the type of task
5. Enter this command in command box to enable Platform Event Traps (IPMI traps):

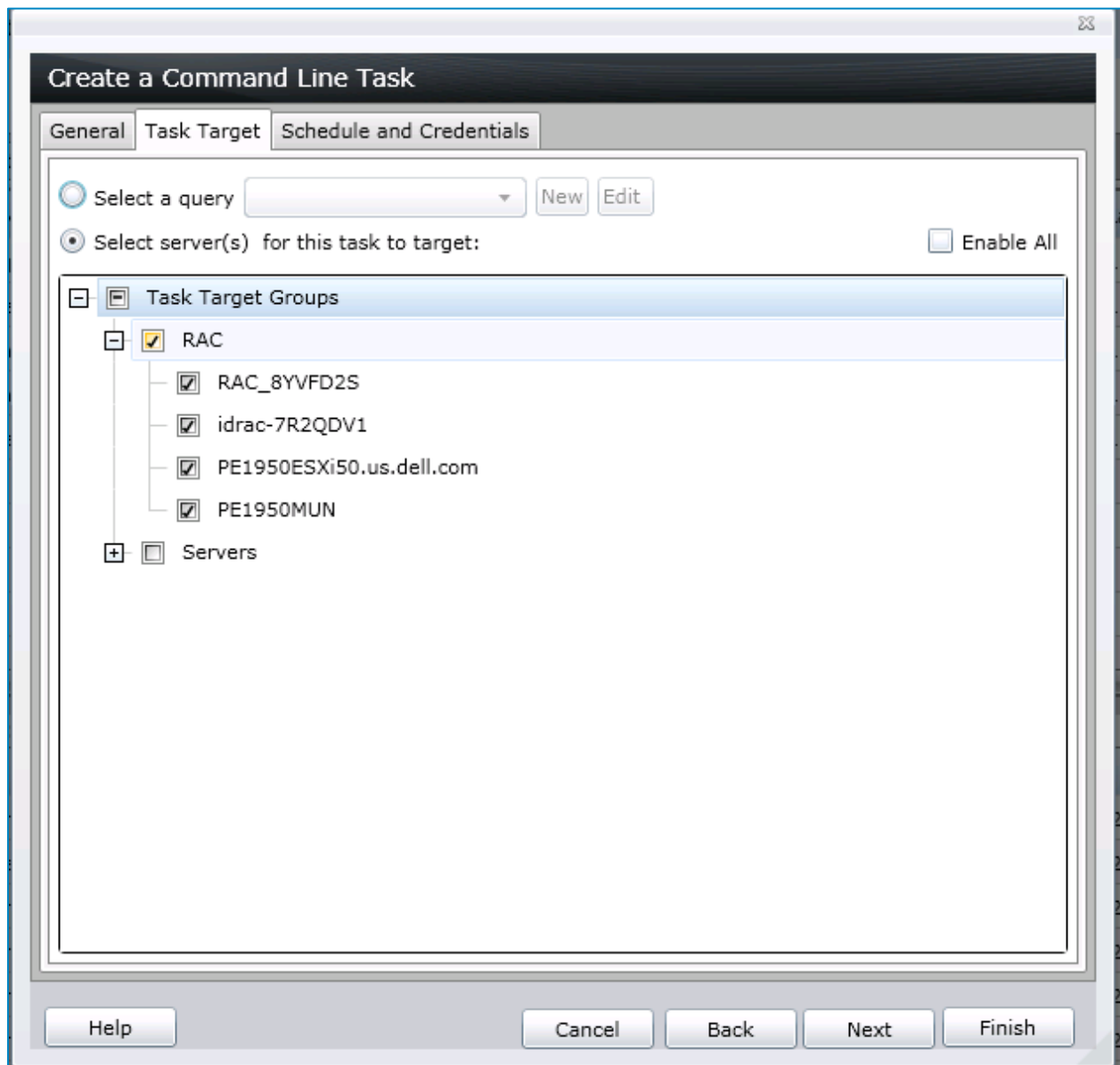
```
config -g cfgipmilan -o cfgipmilanalertenable 1
```

6. Ping device is optional - this will ping the device first and if it fails, no command is run.
7. Output to file is recommended. This will create a log file for each command run.

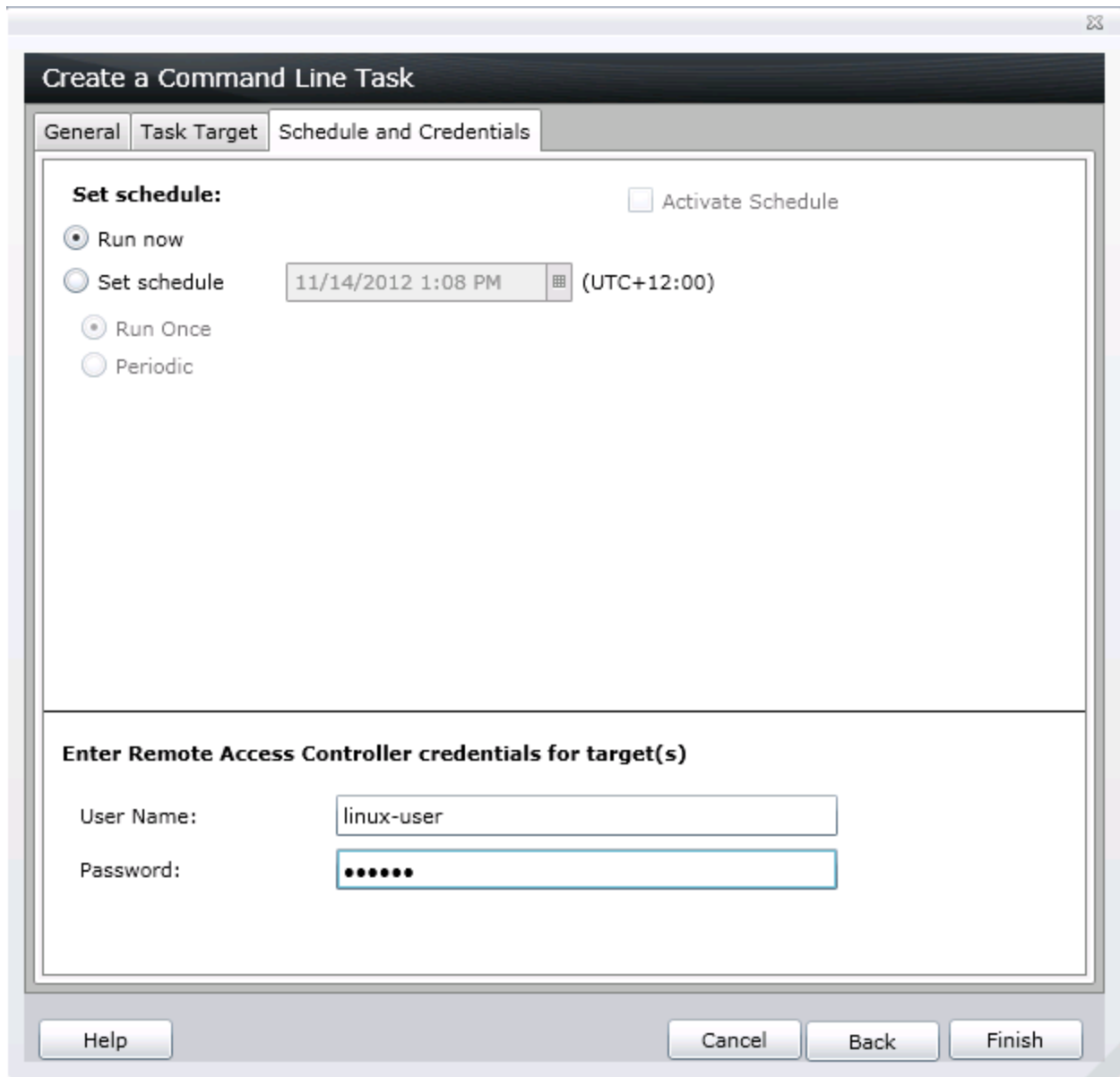
The screenshot shows a wizard window titled "Create a Command Line Task". It has three tabs: "General", "Task Target", and "Schedule and Credentials". The "General" tab is selected. The "Task Name" field contains "Enable PET alerts". Below it are four radio button options: "Remote Server Administrator Command", "Generic Command", "IPMI Command", and "RACADM Command Line" (which is selected). The "Command:" field contains the command "config -g cfgipmilan -o cfgipmilanalertenable 1". There are four checkboxes: "Ping Device" (unchecked), "Output to file" (checked), "Append" (checked), and "Include errors" (checked). The "Output to file" checkbox has a text box next to it containing "c:\pet-alert.txt". At the bottom of the window are four buttons: "Help", "Cancel", "Next", and "Finish".

8. Continue through Wizard to Task Target tab. Click on any or all RAC devices in the target selection tree that you wish to run the task against.

Note: If the server and iDRAC are discovered together in OME 1.1, they will be represented as one device and will be shown with the server name and not the iDRAC name. Devices appearing in RAC group are all iDRACs.



9. Continue in Wizard to Schedule and Credentials. Run the task now if desired or schedule for later. Enter the User Name and Password for the RAC devices.



10. Repeat steps 2-9 with the following command line tasks. You will need to create a RACADM command line task for EACH command. You can right click on a task you created and use the CLONE feature to make a copy of the command and then edit the command line for each command. With each command shown here, the affected settings in the iDRAC console is also shown for reference.

```
config -g cfigipmilan -o cfigipmilanalertenable 1
```

This command was already created. This command enables alerts.

```
config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i 1 1
```

This command enables alerts for 1 out of 4 possible destinations. "-i 1" designates the index (IPV4 Destination1). The second "1" turns alerts ON for that destination.

```
config -g cfgIpmiPet -o cfgIpmiPetAlertDestIpAddr -i 1 10.36.0.215
```

This command sets the destination IP address (OME Server IP address) for 1 out of 4 possible destinations. The "-i 1" designates the index (IPV4 Destination1). Use your OME server IP instead of the example 10.36.0.215.

```
config -g cfgIpmiLan -o cfgIpmiPetCommunityName public
```

This command configures the Community String to public. Change community string name as desired.

11. Optional: Send a test trap

Create a remote task with this command which will send a test trap to the OME IP designated in Index1 (Destination1). You should see this alert in OME console if everything is configured correctly and firewall is open to receive alerts.

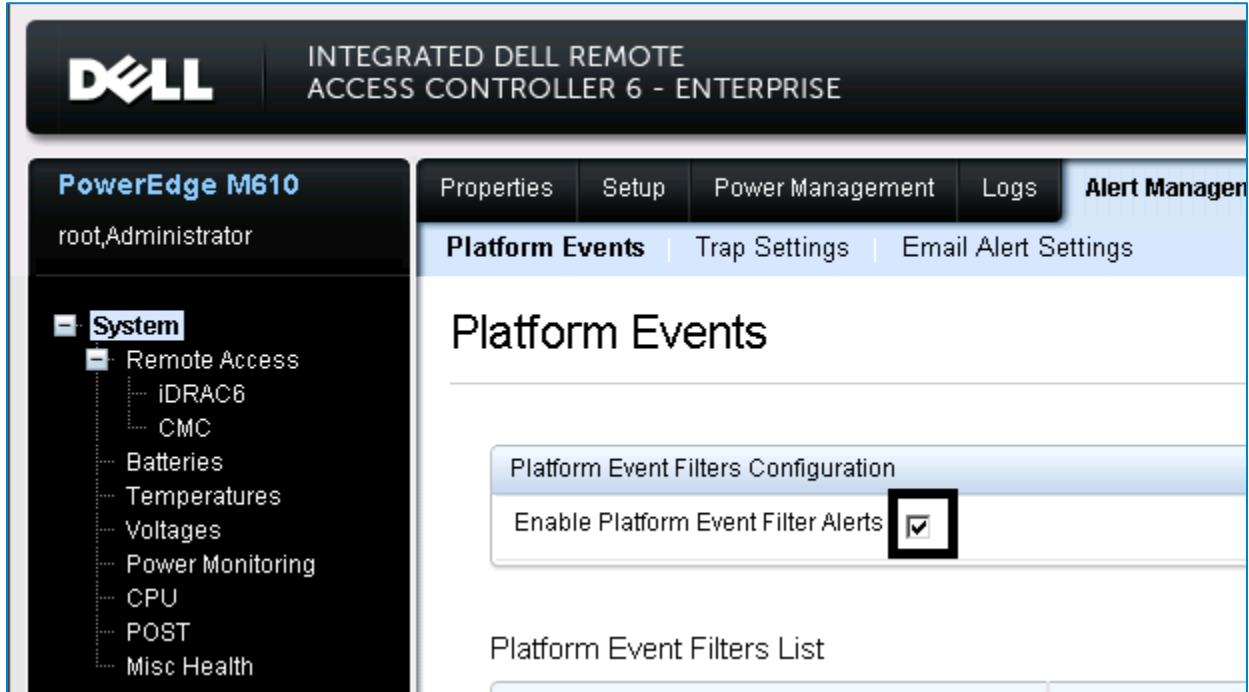
```
testtrap -i 1
```

Configuring Dell 11G iDRAC6 for Agent Free Management using iDRAC6 Console

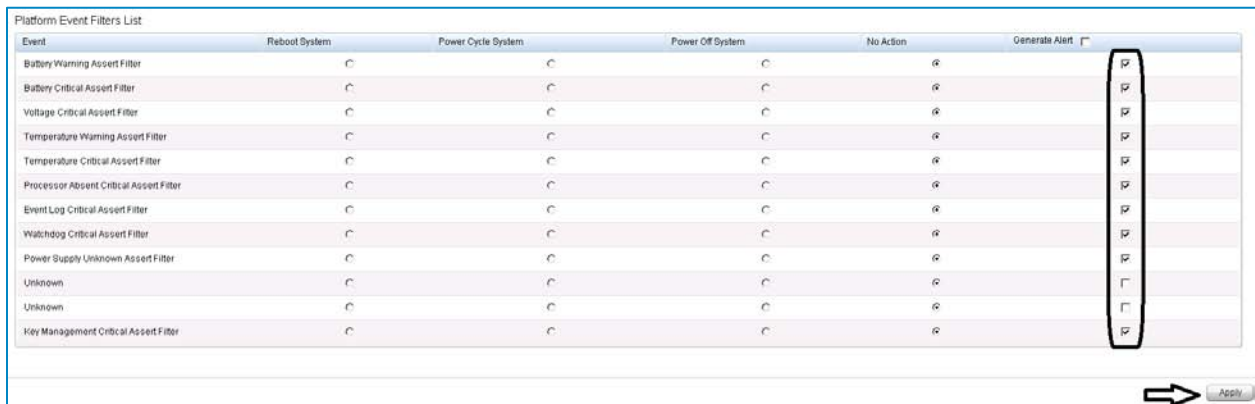
Note: Configure platform event filters before you configure the platform event traps or e-mail alert settings.

Note: Depending on your iDRAC6 firmware version, the console GUI options and look and feel may differ slightly from the pictures shown in this document.

1. Log in to the Integrated Dell Remote Access controller 6 console.
2. Navigate to Alert Management
3. Check box for Enable Platform Event Filter Alerts

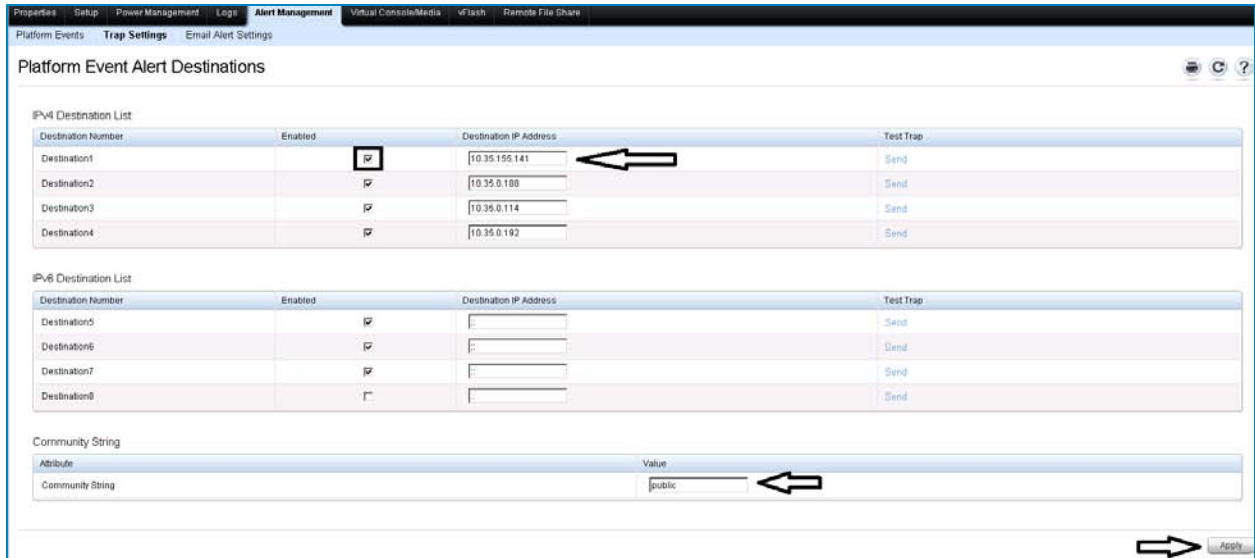


4. Check all boxes for the types of alerts you wish to receive under the Platform Event Filters List
5. Click **Apply** at bottom right to save changes



6. Navigate to **Trap Settings** tab.
7. Check the **Enabled** box for a Destination.
8. Enter OME Management Station IP in the Destination IP Address.
9. Enter SNMP Community Name.
10. Scroll to bottom of page if needed and click **Apply**.

Note: You can optionally send a test trap on this page and receive it in OME.



Managing Servers with agent (OMSA) Installed

All generations of Dell PowerEdge Servers can be managed using a software agent called Dell OpenManage Server Administrator (OMSA). The following sections detail installation of OMSA and SNMP settings needed for supported operating systems including: Windows Server, Linux, ESXi, ESX, and Xen. View the complete and detailed OMSA compatibility matrix at the link here:

<http://support.dell.com/support/edocs/SOFTWARE/smcomp/3.0/PDF/CompatibilityMatrix.pdf>

Configuring Dell PowerEdge Server with Windows Server Operating System (including Hyper-V) with Dell OpenManage Server Administrator (OMSA)

1. Install Open Manage Server Administrator (OMSA) on the Windows server.

- a. Download OMSA package from support.dell.com

At the time of this document, the current version of OMSA for Windows Server is 7.1 which can be found here:

<http://www.dell.com/support/drivers/us/en/04/DriverDetails?driverId=30T1C&fileId=2962652264>

You can always find the most current version of OMSA at www.dell.com/support.

After downloading the .exe, double click to extract files for the setup. Once extracted, run the setup.exe which will be in the default location of

c:\openmanage\windows\setup.exe

Follow the installation wizard to complete setup.

- b. You can also install Server Administrator using the *Dell Systems Management Tools and Documentation* DVD. The DVD provides a setup program to install, upgrade, and uninstall Server Administrator, managed system and management station software components.

For more information and advanced installation options, see the *Dell OpenManage Server Administrator Installation Guide* [here](#):

<http://support.dell.com/support/edocs/software/svradmin/>

2. Configure SNMP service and make sure SNMP service is active and running.

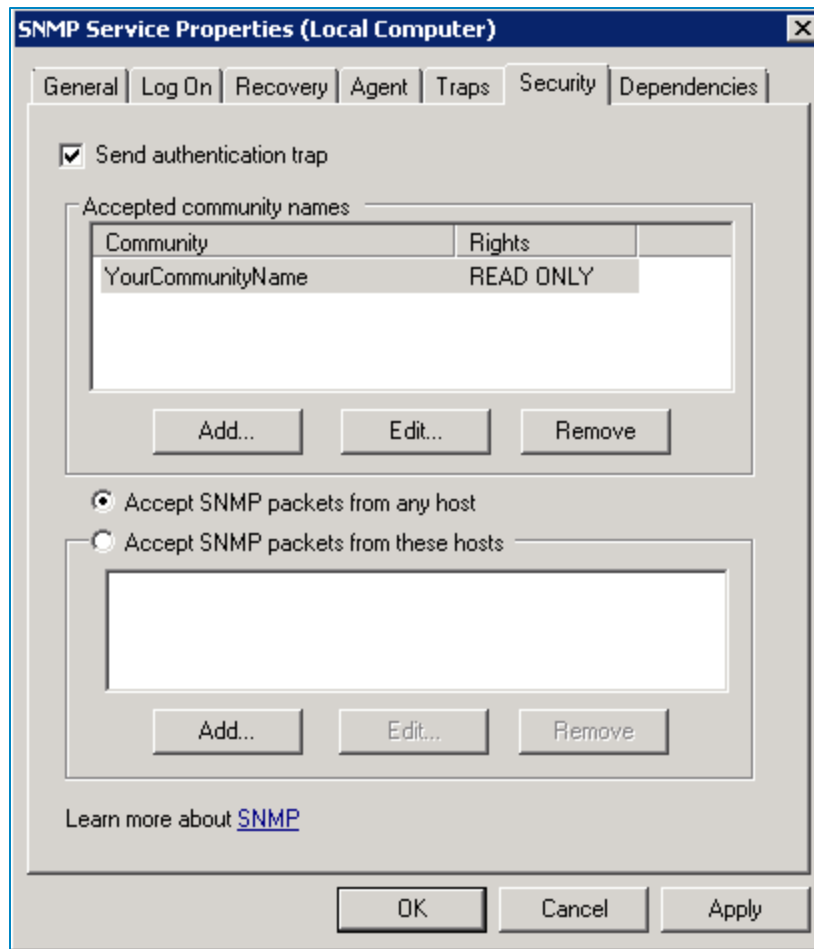
Follow the steps below to open the SNMP Service Properties:

1. To open the services console, click the Windows Start menu and select 'Run'
2. Type 'services.msc' in the 'Open' text box and click 'OK'.
3. Browse the list of services and select 'SNMP Service'.
4. Right click on the 'SNMP Service' and select 'Properties'.

Note: If you do not see SNMP Service, it is not installed. Follow links below for more information on installing SNMP Service if it is not present.

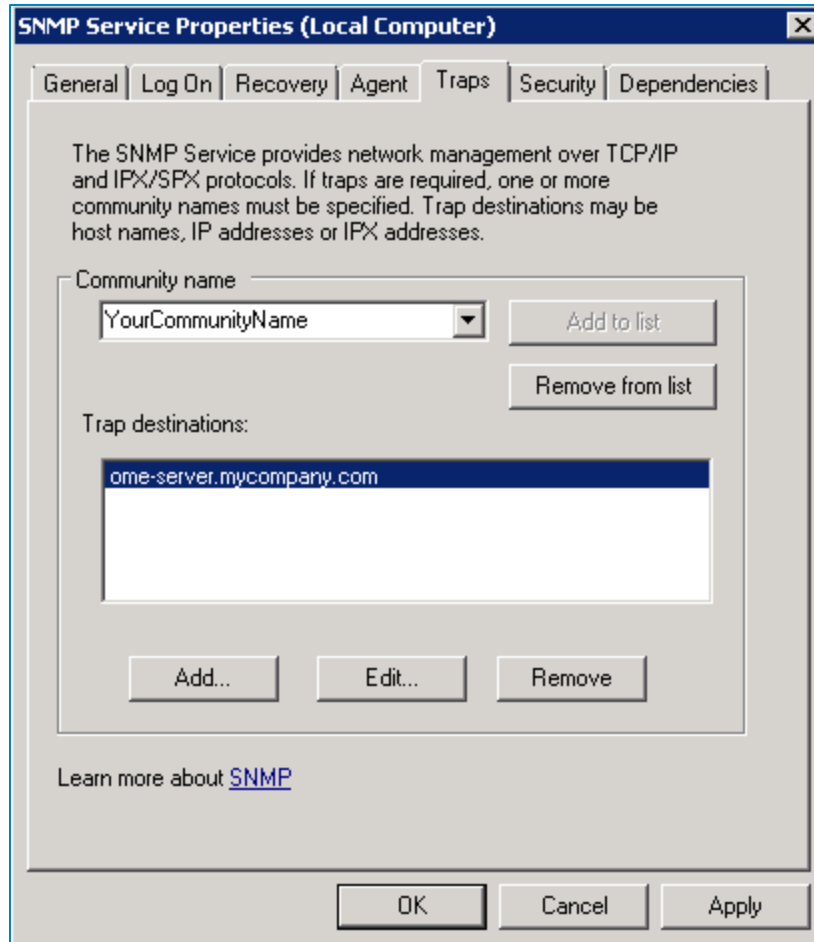
On the SNMP Service Properties Security Tab:

1. Uncheck the **Send authentication trap** option.
2. Add your community name with READ ONLY rights.
3. Select one of the following options:
 - a. 'Accept SNMP packets from any host'
 - b. 'Accept SNMP packets from these hosts' and add the OpenManage Essentials server to the list of accepted hosts.



On the SNMP Service Properties Traps Tab:

1. Add your community name to the community list.
2. Add the OpenManage Essentials server to the trap destinations list.
3. Click **OK** and close out of the properties window.
4. Right-click on the SNMP Service in the list of services and choose **RESTART**.
5. You should receive "linkup" alerts in OME when the SNMP service restarts.



For more information on installing and configuring SNMP service on Microsoft Windows, refer to the link below:

<http://support.microsoft.com/kb/324263>

A Dell video which details how to set up SNMP for OMSA monitoring and alerts can be found here:

<http://en.community.dell.com/techcenter/m/videos/20079605.aspx>

The installation of SNMP starts at 1:00. The configuration of SNMP for OMSA starts at 1:50.

3. Check Firewall Exceptions.

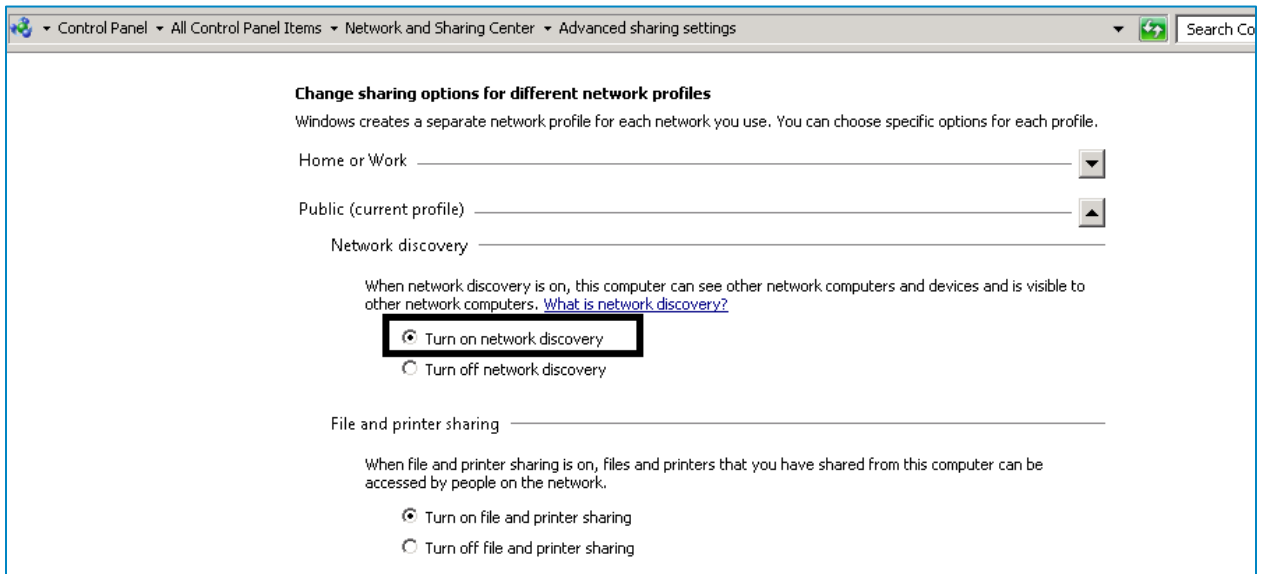
When the Firewall is enabled in your managed system, it will block communications between OpenManage Essentials and managed system. SNMP uses the UDP port 161 for sending and receiving requests, and port 162 for receiving traps from managed system. Configure firewall setting to allow port 161 and 162.

Allow WMI (Windows Management Instrumentation) through Windows Firewall. Enable Remote WMI. Refer link below.

[http://msdn.microsoft.com/en-us/library/windows/desktop/aa822854\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa822854(v=vs.85).aspx)

4. Windows Server 2008 and 2008 R2 Only - Enable Network Discovery

1. Navigate to Control Panel > Network and Internet > Network and Sharing Center > Change Advanced Sharing Settings
2. Select **Turn on network discovery** and save.



Configuring Dell PowerEdge Linux Servers With Dell OpenManage Server Administrator (OMSA)

Background: When Dell OpenManage Server Administrator (OMSA) is installed on a Linux target, deep hardware inventory can be obtained when discovered with OME. Health monitoring, system updates, and remote tasks are also possible via the OMSA agent once installed on the target system.

OMSA is supported only on Red Hat Enterprise Linux and SUSE Linux Enterprise. Please review the latest Dell OpenManage Software Support Matrix for supported Linux operating systems. You can install OMSA on all Linux systems even if the server is not supported, however complete functionality is not guaranteed.

Follow the steps below to install OMSA:

Note: Some steps below such as the pre-requisites for installing OMSA may already be complete on your target system. Run or skip steps as needed.

1. Install Net-SNMP Package (Pre-requisite)

- a. Configure SNMP service and make sure SNMP service is active and running on the Linux server.
- b. You can verify that SNMP service is running, start, or restart the service, with this command:

```
/etc/init.d/snmpd <start | status | restart>
```

If SNMP package is not installed, install the package. You may refer to this link for help installing the package.

http://www.linuxhomenetworking.com/wiki/index.php/Quick_HOWTO_:_Ch22_:_Monitoring_Server_Performance#Installing_SNMP_Utility_on_a_Linux_Server

2. Install OMSA Dependencies (Prerequisite)

OMSA requires several dependency RPMs for remote enablement support. These RPMs are often already installed, so you may wish to skip this step and come back if needed if the OMSA installation reports they are missing.

Required packages:

- libcmplCpplmpl0
- libwsman1
- openwsman-server
- sblim-sfcb
- sblim-sfcc

You can use this command to verify if the packages are installed currently. If they are, this command will return the name of the package. If nothing is returned, there was no matching package found.

- rpm -qa | grep libcmplCpplmpl0*
- rpm -qa | grep libwsman1*
- rpm -qa | grep openwsman*
- rpm -qa | grep sblim-sfcb*
- rpm -qa | grep sblim-sfcc*

If they need to be installed, the RPMs are available in the following directory of the *Dell Systems Management Tools and Documentation DVD* in the following directory:

linux\RPMS\supportRPMS\opensourcecomponents\<OS>\<architecture>

Follow the sequence below to install the required RPMs. Note that libwsman1 and openwsman-clientx should be installed at the same time as they have a cyclic dependency.

- rpm -ivh libcmplCpplmpl0-x.x.x.rpm
- rpm -ivh sblim-sfcb-x.x.x.rpm
- rpm -ivh sblim-sfcc-x.x.x.rpm
- rpm -ivh libwsman1-x.x.x.rpm openwsman-clientx.x.x.rpm
- rpm -ivh openwsman-server-x.x.x.rpm

3. Install Open Manage Server Administrator on the Linux server. There are multiple ways to perform OMSA install:

A. Using the linux.dell.com repository. This is typically the easiest method.

1. Set up the Dell OpenManage Repository at <http://linux.dell.com/repo/hardware>, like this:

```
wget -q -O - http://linux.dell.com/repo/hardware/latest/bootstrap.cgi | bash
```

2. Then, Install OpenManage Server Administrator:

```
yum install srvadmin-all
```

Note: You can install OMSA on all Linux systems even if the server is not supported. However, complete functionality is not guaranteed

Find more detailed information about the Dell linux repository here:

<http://linux.dell.com/wiki/index.php/Repository/OMSA>

B. Using the *Dell Systems Management Tools and Documentation* DVD

<http://support.dell.com/support/edocs/software/smsom/5.4/en/qig/html/index.htm#wp1130494>

C. Downloading the package from support.dell.com.

You can determine your Red Hat version and processor with these commands:

```
uname -a
```

```
cat /etc/issue
```

```
cat /etc/redhat-release
```

You can determine your SUSE version and processor with these commands:

```
uname -a
```

```
cat /etc/issue
```

```
cat /etc/SuSE-release
```

Once the appropriate package is found for your Linux version and processor (i386 or x64) and downloaded to the Linux system. Use these commands to unpackage and install:

```
tar -xzvf OM-SrvAdmin-Dell-Web-LX-7.1.0-5304_A00-00.tar.gz
```

```
./setup.sh
```

Follow the prompts, installing all components.

3. Verify OMSA is installed and services are running

This command will let you see if OMSA services are running:

```
rpm -qa | grep srvadmin
```

To start or restart OMSA services:

```
srvadmin-services.sh start
```

```
srvadmin-services.sh restart
```

4. Verify SNMP Settings for OMSA

1. Open the file for editing:

```
/etc/snmp/snmpd.conf
```

2. Verify the following 3 lines exist or add/modify them to the below if they do not:

```
view all included .1
access notConfigGroup "" any noauth exact all none none
smuxpeer .1.3.6.1.4.1.674.10892.1
```

5. Install Inventory Collector on 64-bit Servers

Inventory Collector is required for using system update on Linux servers. Currently it is available only as a 32-bit version and must be installed separately for 64-bit systems.

For all 64-bit supported Linux operating systems you must complete the following steps:

1. Install the 32-bit version of zlib and compat-libstdc++ libraries.
2. Install the srvadmin-cm package from the following directory of the *Dell Systems Management Tools and Documentation DVD*:

```
/linux/RPMS/supportRPMS/srvadmin
```

6. Configure the SNMP Community String

The community string is a password which must match for the querying server and all devices which it queries.

To modify the community string:

1. Open the file for editing:

```
/etc/snmp/snmpd.conf
```

2. Find the community name in one of these lines and change it as desired if you do not wish to use the default string "public"

1. `com2sec publicsec default public`
or
`com2sec notConfigUser default public`

3. To enable the changes, restart the SNMP agent:

```
/etc/init.d/snmpd restart
```

Note: This step is only needed once after all configuration changes are completed.

7. Configure SNMP Traps to the OME Management Station

1. Open the file for editing:

```
/etc/snmp/snmpd.conf
```

2. Add the following line to the file:

```
Trapsink <OME IP Address> <community name>
```

3. To enable the changes, restart the SNMP agent:

```
/etc/init.d/snmpd restart
```

Note: This step is only needed once after all configuration changes are completed.

Firewall Configuration

If the firewall was enabled during the Linux installation, it will close the SNMP port blocking all external connections by default. Server Administrator will detect this and log a warning message to the system event log.

You must open the SNMP port on the server for OpenManage Essentials to communicate with it or else this will block OME from discovering, inventorying, and receiving alerts for the server.

Refer to your specific Linux distribution for configuring firewall settings. You will need to configure your IPTABLES to allow access to UDP Port 161 and 162 for SNMP communication and TCP Port 1311 for OMSA. There are various options that can be added to the IPTABLES file but here are basic entries for allowing traffic on these ports:

```
-A RH-Firewall-1-INPUT -p udp -m udp --dport 161 -j ACCEPT
```

```
-A RH-Firewall-1-INPUT -p udp -m udp --dport 162 -j ACCEPT
```

```
-A RH-Firewall-1-INPUT -p tcp -m tcp --dport 1311 -j ACCEPT
```

Be sure to save changes to IPTABLES:

```
service iptables save
```

More information on using IPTABLES can be found here

http://www.linuxhomenetworking.com/wiki/index.php/Quick_HOWTO_:_Ch14_:_Linux_Firewalls_Using_iptables#Important_Iptables_Command_Switch_Operations

8. SUSE Only - Enable SNMP Access for Remote Hosts

The default SNMP configuration on SUSE Linux versions does not allow remote access. You must enable remote access for the OpenManage Essentials server to manage the system.

To enable SNMP access for the OpenManage Essentials server:

1. Open the file for editing:

```
/etc/snmp/snmpd.conf
```

2. Edit the line that reads:

```
rocommunity public 127.0.0.1
```

and enter the OME IP address

```
rocommunity public <OME IP Address>
```

4. To enable the changes, restart the SNMP agent:

```
/etc/init.d/snmpd restart
```

Note: This step is only needed once after all configuration changes are completed.

Configure Dell PowerEdge ESXi 4 and ESXi 5 Servers With Dell OpenManage Server Administrator (OMSA)

Detailed instructions for installing OMSA on VMWARE ESXi servers can be found at this location on the Dell TechCenter web site:

http://en.community.dell.com/techcenter/extras/m/white_papers/20071085.aspx

Configure Dell 12G and 11G PowerEdge Servers for Agent Free Software Updates

Agent free system update in OME does not need OMSA on the managed system to gather inventory and deploy firmware and BIOS updates. Agent free updates are applied via Integrated Dell Remote Access Controller (iDRAC6/iDRAC7) on 11th-generation and 12th generation servers.

Prerequisites for Agent free (iDRAC) System Updates.

1. 11th-generation servers

- Modular : Minimum iDRAC6 firmware version 2.20 and higher
- Monolithic : Minimum iDRAC6 firmware version 1.40 and higher

2. 12th-generation servers

- Express or Enterprise license

3. iDRAC is discovered and inventoried using WS-Man protocol

For more information on iDRAC, refer to

<http://content.dell.com/us/en/enterprise/d/solutions/integrated-dell-remote-access-controller-idrac.aspx>

A detailed white paper on using OME to perform software updates can be found on the on the Dell Tech Center site. Since the URL of the document may change over time, search for the document entitled “Update Dell Servers with OpenManage Essentials” at www.delltechcenter.com/ome.

Configure Dell Client Systems using OpenManage Client Instrumentation (OMCI)

Basic management, system health, and inventory can be achieved for Dell Client Systems (Optiplex, Precision, and Latitude systems) with use of OMCI. Instructions for using OMCI and downloads for 32bit and 64-bit client systems can be found here:

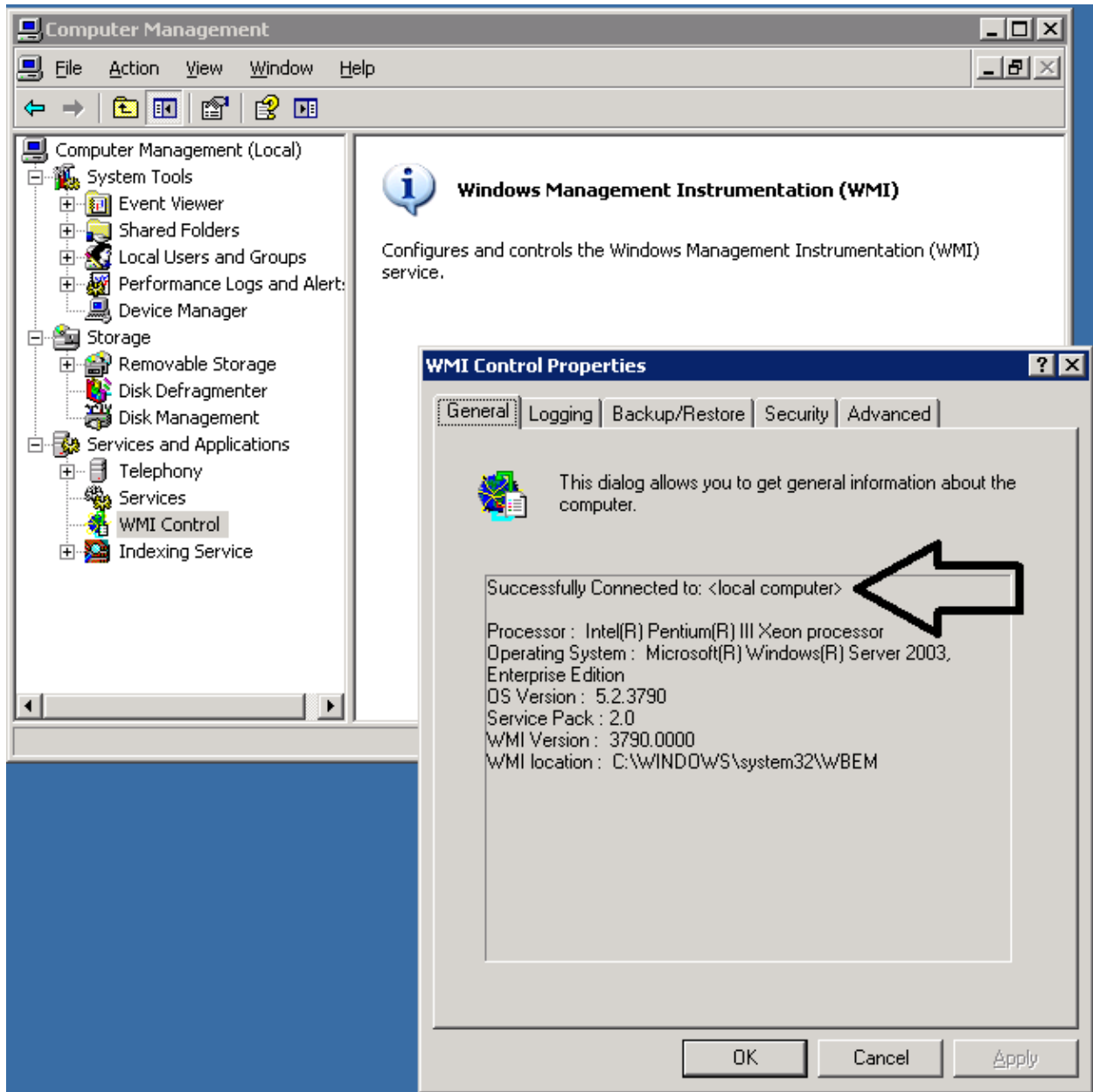
<http://en.community.dell.com/techcenter/systems-management/w/wiki/1773.openmanage-client-instrumentation-omci.aspx>

Configuring Dell PowerEdge Servers (9G/10G) with Windows Server or Windows Hyper-V using WMI

Background: OME 1.1 can now use the WMI protocol to discover and retrieve basic information about a system without OMSA installed. Minimal set up is needed on the target to achieve this.

WMI should be installed by default on Windows Server 2003 and 2008, 2012. To test that it is working, right click on MY COMPUTER, and choose MANAGE. From Computer Management, under Services and

Applications, right click on WMI Control. If the General tab of the WMI Window shows it is connected to the local computer, then WMI should be active. See below screenshot.



Configuring Dell PowerEdge Linux Servers (9G/10G) to use SSH

Background: OME can now use SSH to discover and retrieve basic information from Dell 9G and 10G PowerEdge systems without OMSA installed. The Linux command, `DMIDECODE`, is used to retrieve hardware information from the system. If you are running OME and using a root user to discover your Linux servers, then no configuration is needed. As a best practice you should NOT use the root

account. A non-root user should be used and configured to allow OME to use SSH for discovery. Primarily, giving access to the DMIDECODE by use of SUDO must be given to the user. Follow the steps below:

1. Enable Password Authentication in sshd_config file

Edit the file `sshd_config` in `/etc/ssh`. In this example we use NANO as editor. You must be root user or have root permission to edit this file.

```
nano /etc/ssh/sshd_config
```

Edit the `sshd_config` file and make sure the line

```
PasswordAuthentication yes
```

is present and not commented out with `#`. Add this line to the file if not present already.

2. Disable requiretty option in SUDOERS file

Edit the file, `SUDOERS`, in `/etc`. Using VISUDO is the preferred method for editing the `SUDOERS` file. You must be root user or have root permission to edit this file. Perform these actions:

```
visudo
```

Edit the file and make sure the line “`Defaults requiretty`” is commented out with `#` :

```
#Defaults    requiretty
```

3. Create a user and add to SUDOERS file to run DMIDECODE command

You may already have user accounts in place you wish to use, but if you need help creating groups or users you may refer to this link:

http://www.linuxhomenetworking.com/wiki/index.php/Quick_HOWTO_:_Ch09_:_Linux_Users_and_Sudo#How_To_Add_Users

The following are basic steps for creating a group and user:

- You can create a group using
`groupadd omeusers`
- You can create a user in the group using
`useradd -g omeusers zach`
- Edit the sudoers file to add the user or group and give permission to run DMIDECODE command using VISUDO.
`visudo`

Here are two example lines which would allow access for either the group or an individual user to access DMIDECODE command using sudo. Also, the NOPASSWD option is used so that password entry is not required for the command.

```
%omeusers ALL= NOPASSWD: /usr/sbin/dmidecode
```

```
zach ALL= NOPASSWD: /usr/sbin/dmidecode
```

4. Finally, you need to add to the path for the user to access DMIDECODE and IFCONFIG, which are located in /usr/sbin and /sbin.

You can change or add to the path in the Linux environment using the .bashrc file. As the root user this file will be located in \$home dir. It is recommended to edit this file in the root user's .bashrc file. This file is a hidden file but editable.

```
cd $home
```

```
nano .bashrc
```

add the line

```
PATH=$PATH:/sbin:/usr/sbin; export PATH
```

Log out and log in as the user to update environment with new path additions.

Note: If the file is not present already, you can create the file and add this content:

```
# Source global definitions

if [ -f /etc/bashrc ]; then
    . /etc/bashrc
fi

# User specific aliases and functions

PATH=$PATH: usr/sbin:/sbin; export PATH
```

5. Test that DMIDECODE can be run with sudo user:

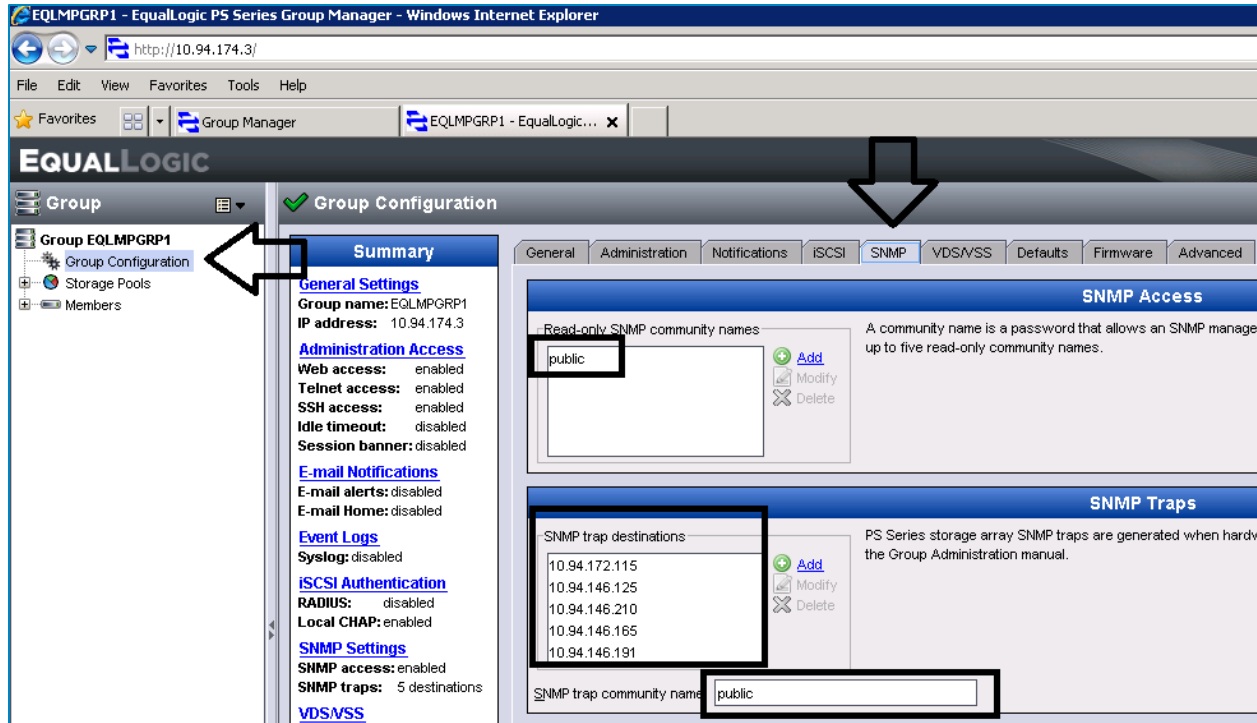
After logging in as the desired user, try command:

```
sudo dmidecode
```

If hardware information is displayed and you are not prompted for any password, your configuration is correct. If you get 'access denied' error, then there may be an issue with the SUDOERS file. If you get an error 'command not found', then there is likely an issue with the path environment being updated correctly. If you are asked for a password, then the SUDOERS file entry for allowing the command to run without password is not correct.

Configure Dell EqualLogic Storage Devices

1. Log in to the management console of the Dell EqualLogic device.
 2. Click **Group Configuration** and select **SNMP** tab
 3. Click **Add** and provide the SNMP community name
 4. Add IPs or Hostnames for SNMP traps as desired
-
1. Click **Add** and provide the SNMP community name
 2. Add IPs or Hostnames for SNMP traps as desired



Configure Dell Force10 Network Switch

1. Configure SNMP Community Name

1. Log in to the switch using the management IP address with serial connection or a telnet session.
2. Use the following command to set up SNMP community name. Note you can use `ro` or `rw` to specify read/write or read only.

```
snmp-server community rw public  
or
```

```
snmp-server community ro public
```

2. Configure SNMP Traps

From the command line management interface, use these commands to turn on SNMP traps and add a destination IP or hostname for the OME console

```
snmp-server host {ip-address}
```

This command will enable ALL available traps from the Force10 Switch

```
snmp-server enable traps
```

```
snmp-server enable traps snmp
```

You can find more information on configuring Force10 Switches here:

<http://www.force10networks.com/CSPortal20/KnowledgeBase/Documentation.aspx>

Configure Dell PowerConnect Network Switch

1. Configure SNMP Community Name

1. Log in to the switch using the management IP address with serial connection or a telnet session.
2. Use the following command to set up SNMP community name. Note you can use ro or rw to specify read/write or read only. Su can be used to specify SNMP administrator access. The IP of the OME console (management station) is placed at the end.

Examples

```
snmp-server community public rw 192.168.7.10
```

or

```
snmp-server community private ro 192.168.7.10
```

2. Configure SNMP Traps

From the command line management interface, use these commands to turn on SNMP traps and add enter community name.

```
snmp-server host host {IP} community{community name string} [1 | 2]
```

1—SNMPv1 traps is used.

2—SNMPv2 traps is used (Default)

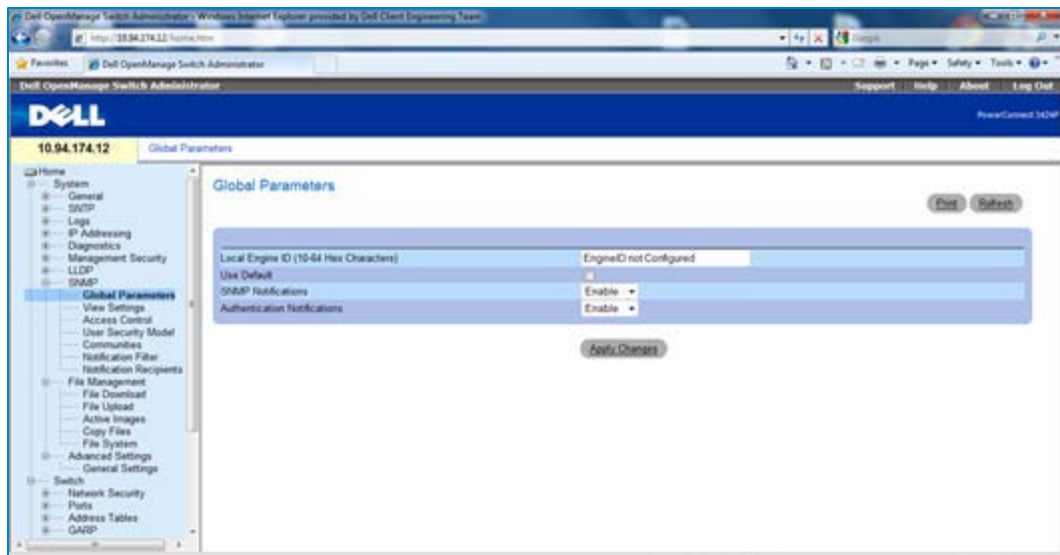
Example:

```
snmp-server host 192.168.1.10 public 2
```

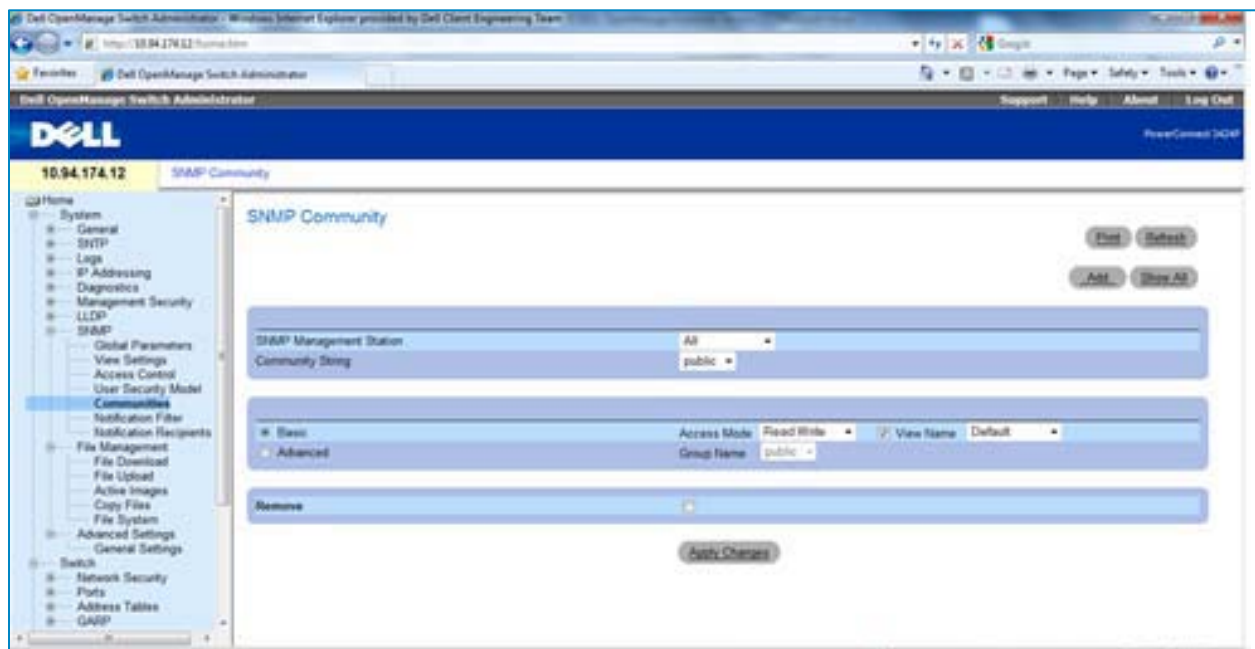
3. Configure Settings using console

1. Log in to the remote Web client of the Dell PowerConnect switch.
2. Navigate to Home > **SNMP** > **Global Parameters**.
3. Enable SNMP Notifications and Authentication Notifications: click **Apply Changes**.

Making My Environment Manageable for Dell OpenManage Essentials



4. Navigate to Home > SNMP > Communities.
5. Set SNMP community String > Click **Apply Changes**.
6. Navigate to Home > SNMP > Notification Recipients.
7. Add Recipient IP [OpenManage Essentials system IP].



Configure Dell Chassis Management Controller (CMC)

1. Configure Chassis Event Filters using Web Console

Note: To add or configure SNMP alerts, you must have Chassis Configuration Administrator privilege.

Note: For added security, Dell strongly recommends that you change the default password of the root (User 1) account. The root account is the default administrative account that ships with the CMC. To change the default password for the root account, click User ID 1 to open the User Configuration page. Help for that page is available through the Help link at the top right corner of the page.

1. Log in to the CMC Web interface
2. Select Chassis in the system tree.
3. Click the Alert Management tab. The Chassis Events page appears.
4. Enable alerting:
 - a. Select the check boxes of the events for which you want to enable alerting. To enable all events for alerting, select the Select All check box.
 - b. Click **Apply** to save your settings.

The screenshot shows the Dell Chassis Management Controller (CMC) web interface. The browser address bar shows <https://10.35.0.169/cgi-bin/webcgi/main>. The interface includes a navigation menu with tabs: Properties, Setup, Power Management, Logs, Network/Security, Alert Management, Troubleshooting, and Update. The 'Alert Management' tab is selected, and the 'Chassis Events' sub-tab is active. The left sidebar shows a system tree with 'Chassis' selected, containing 'CMC' and 'Servers' (listing users 1-16) and 'I/O Modules' (listing Gigabit Ethernet and Slot Empty). The main content area is titled 'Chassis Events' and includes a breadcrumb: 'Chassis Event Filters Configuration > Chassis Events List'. Below this is the 'Chassis Event Filters Configuration' section, which has a checkbox for 'Enable Chassis Event Alerts' that is checked. A note below states: 'Note: This check box must be selected to transmit alerts to a valid destination.' Below the note is a '[Back to top]' link. The 'Chassis Events List' section contains a table with the following data:

Event	Generate Alert
Fan Probe Failure	<input checked="" type="checkbox"/>
Battery Probe Warning	<input checked="" type="checkbox"/>
Temperature Probe Warning	<input checked="" type="checkbox"/>
Temperature Probe Failure	<input checked="" type="checkbox"/>
Redundancy Degraded	<input checked="" type="checkbox"/>
Redundancy Lost	<input checked="" type="checkbox"/>
Power Supply Warning	<input checked="" type="checkbox"/>
Power Supply Failure	<input checked="" type="checkbox"/>
Power Supply Absent	<input checked="" type="checkbox"/>

At the top right of the table, there is a 'Generate Alert' section with a 'Select/Deselect All' checkbox.

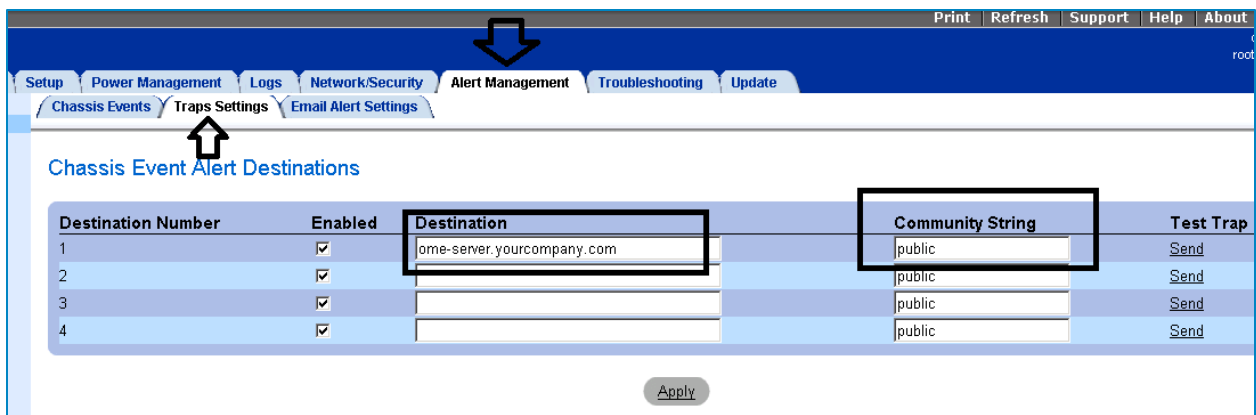
5. Click the Traps Settings sub-tab. The Chassis Event Alert Destinations page displays.
6. Type a valid IP address in an empty Destination IP Address field.

Note: A valid address is an address that receives the trap alerts. Use the "quad-dot" IPv4 format, standard IPv6 address notation, or FQDN. For example:

123.123.123.123 or 2001:db8:85a3::8a2e:370:7334 or dell.com

7. Type the SNMP Community String to which the destination management station belongs.

Note: The community string on the Chassis Event Alert Destinations page differs from the community string on the Chassis | Network | Services page. The SNMP traps community string is the community that CMC uses for outbound traps destined to management stations. The community string on the Chassis | Network | Services page is the community string that management stations use to query the SNMP daemon on CMC.



8. Click **Apply** to save your changes.

To test an event trap for an alert destination:

1. Log in to the CMC Web interface.
2. Select **Chassis** in the system tree.
3. Click the **Alert Management** tab. The Chassis Events page appears.

Configure Dell PowerVault Modular Disk Storage (MD Array)

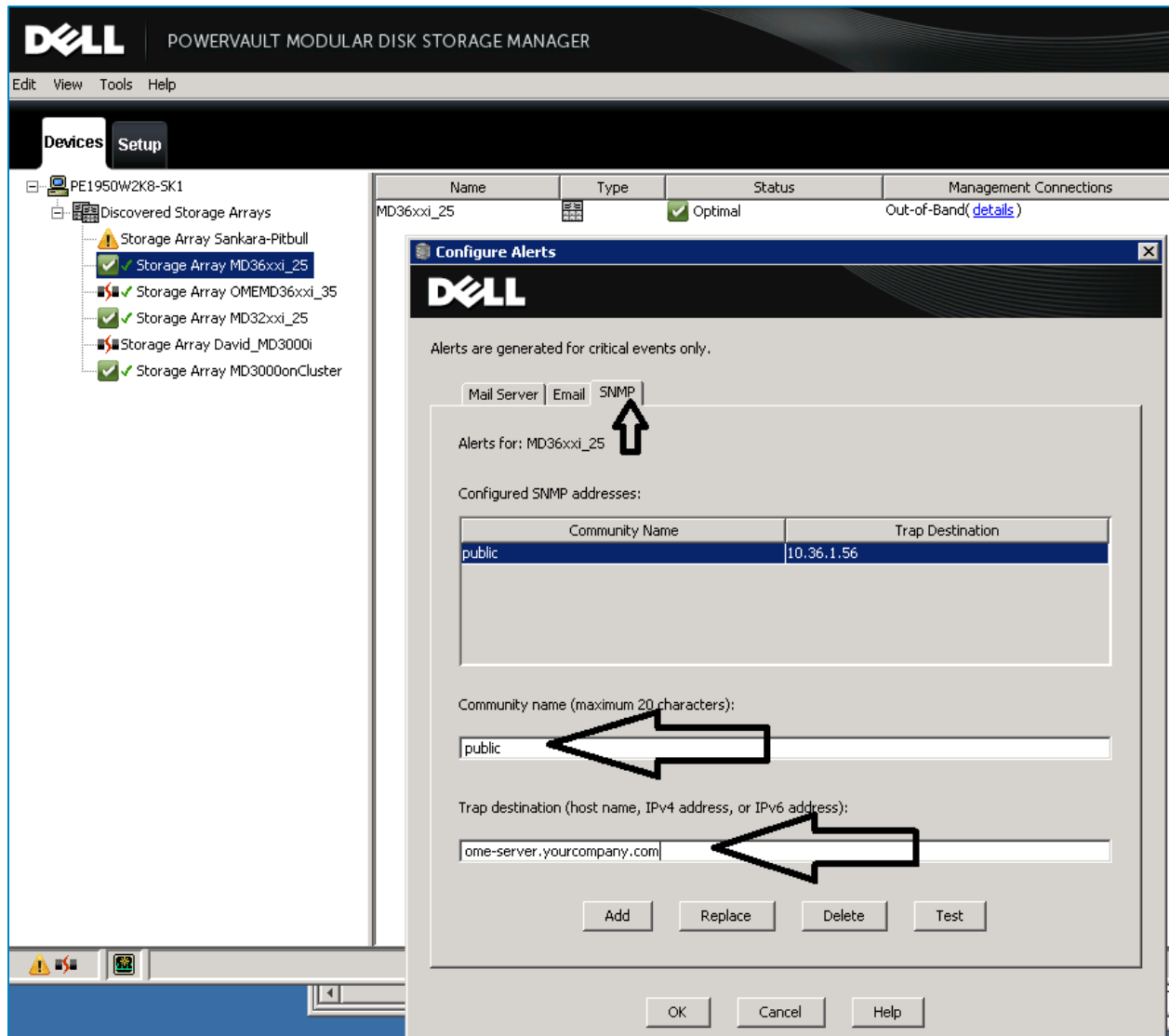
1. Configuring SNMP Alerts

Receiving SNMP alerts from Dell PowerVault Modular Disk Storage requires the PowerVault Modular Disk Storage Manager application. This application can be found on the Dell resource disc that ships with the storage device or from support.dell.com.

Once installed, you can add the OME console IP to the list of destinations to send alerts to on the MD array.

To add an OME console to the list of addresses configured to receive SNMP alerts:

1. Click the **Edit** file menu or right click on an Array and choose **Configure Alerts**.
2. In the **Configure Alerts** window, click on **SNMP**.
3. Enter the Community Name.
4. Enter the IP address for the OME server to receive the alerts.
5. Click **Add**.
6. Repeat steps 3-5 to add additional management stations to the list to receive the alerts if desired.
7. Click **OK** when done.



Configure Dell Power Distribution Unit (PDU)

1. Configuring SNMP Alerts

1. Log in to the management console of the PDU using IP of PDU in browser.
2. Navigate to **Administration > trap receivers**.
3. Click on **Add Trap Receiver**.

The screenshot shows the Dell OpenManage Essentials interface for a Metered Rack PDU. The main navigation tabs are Home, Device Manager, Environment, Logs, and Administration. Under Administration, the sub-tabs are Security, Network, Notification, and General. The Notification tab is active, and a 'No Alarms' status is shown in the top right corner.

On the left side, there is a sidebar menu with the following sections:

- Event Actions
 - by event
 - by group
- E-mail
 - server
 - recipients
 - test
- SNMP Traps
 - trap receivers (highlighted)
 - test

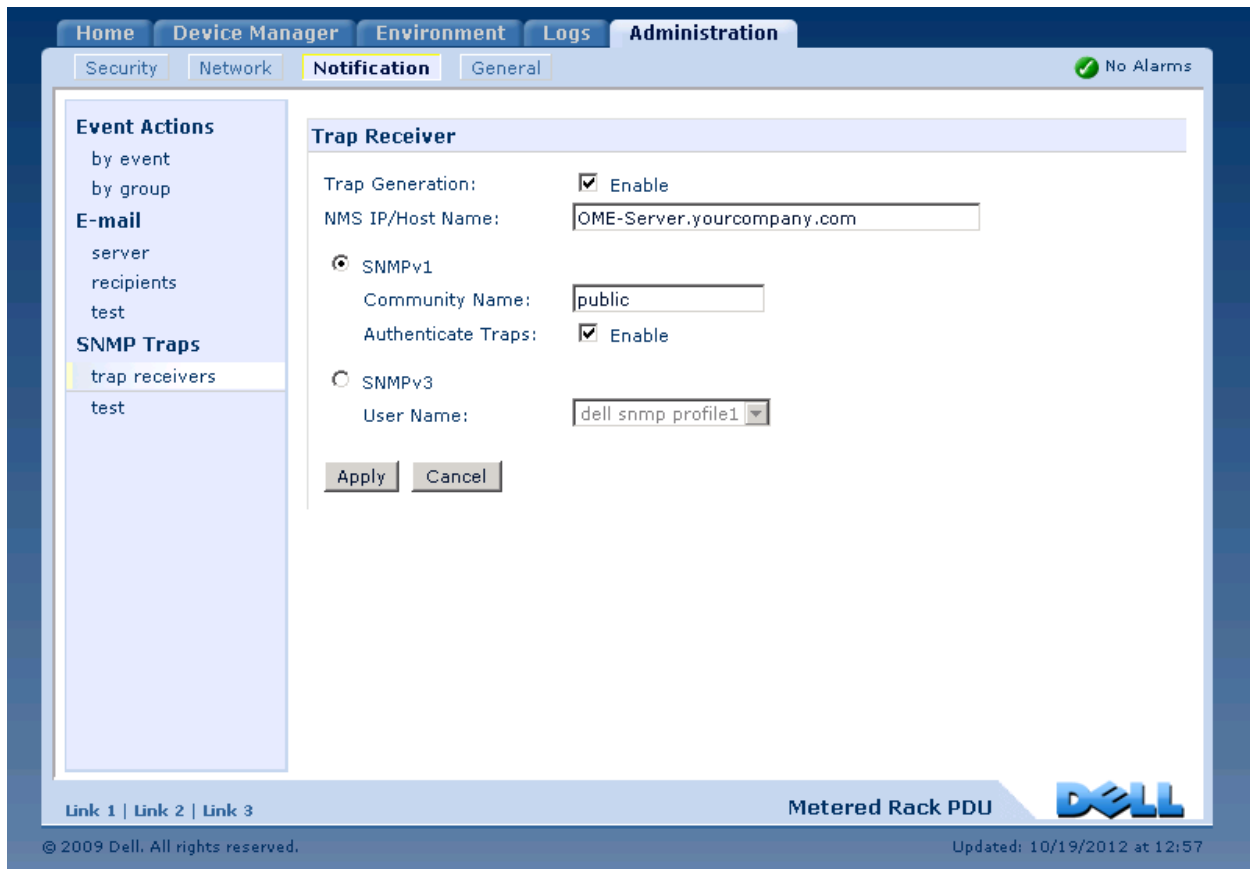
The main content area displays the 'Trap Receivers' configuration page. It features a table with the following data:

NMS IP/Host Name	Trap Type	Generation
10.94.168.65	SNMPv1	Enabled
10.94.168.111	SNMPv1	Enabled
10.94.174.194	SNMPv1	Enabled
10.94.151.227	SNMPv1	Enabled
10.36.0.107	SNMPv1	Enabled

Below the table is an 'Add Trap Receiver' button, which is highlighted with a large black arrow pointing to it from the right.

At the bottom of the page, there are links for 'Link 1 | Link 2 | Link 3', the text 'Metered Rack PDU', the Dell logo, and the footer information: '© 2009 Dell. All rights reserved.' and 'Updated: 10/19/2012 at 12:54'.

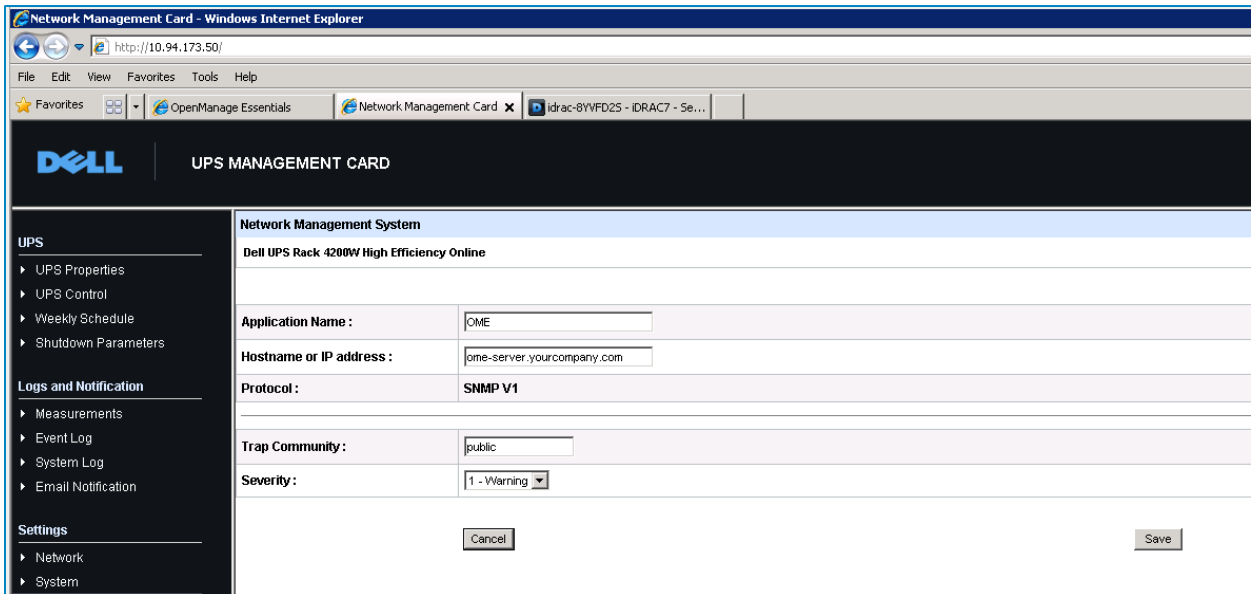
4. On the next window, check the box for **Trap Generation**.
5. Enter the hostname or IP of the OME management console.
6. Enter the community name.
7. Click **Apply**.



Configure Dell Universal Power Supply (UPS)

1. Configuring SNMP Alerts and Community String

1. Log in to the Dell UPS Console.
2. Navigate to Notified Applications.
3. Click on Add NMS.
4. Enter Application Name (OME).
5. Enter the OME management station IP address or hostname.
6. Enter the SNMP Community Name.



The screenshot shows a web browser window titled "Network Management Card - Windows Internet Explorer" with the address bar displaying "http://10.94.173.50/". The browser tabs include "OpenManage Essentials", "Network Management Card", and "Idrac-8YVFD25 - IDrac7 - Se...". The main content area is titled "UPS MANAGEMENT CARD" and features a navigation menu on the left with sections for "UPS", "Logs and Notification", and "Settings". The main panel is titled "Network Management System" and displays the configuration for a "Dell UPS Rack 4200W High Efficiency Online". The configuration fields are as follows:

Field	Value
Application Name :	OME
Hostname or IP address :	ome-server.yourcompany.com
Protocol :	SNMP V1
Trap Community :	public
Severity :	1 - Warning

At the bottom of the configuration area, there are "Cancel" and "Save" buttons.

7. Navigate to **Settings > Access Control**.
8. Enable SNMP.
9. Enter the SNMP community string.

The screenshot shows the 'UPS MANAGEMENT CARD' interface. The top header includes the Dell logo and the title 'UPS MANAGEMENT CARD'. Below this is a navigation sidebar on the left with sections for 'UPS', 'Logs and Notification', 'Settings', and 'Time'. The 'Settings' section is expanded to show 'Access Control' as the selected option. The main content area is titled 'Access Control' and displays configuration options for a 'Dell UPS Rack 4200W High Efficiency Online'. The configuration includes fields for 'Enter New Manager Login' (set to 'admin'), 'Enter New Password', and 'Confirm New Password'. The 'SNMP' status is set to 'Enabled'. The 'Current Community Read-Only' is 'public', and the 'Change Community Read-Only' field is also set to 'public'. Under 'Security mode', three radio buttons are present: 'Authentication for configuration' (selected), 'Full authentication', and 'SSL and full authentication'. At the bottom, there is a 'Save modified settings' label and a 'Save' button.

Access Control	
Dell UPS Rack 4200W High Efficiency Online	
Enter New Manager Login :	<input type="text" value="admin"/>
Enter New Password :	<input type="password" value="....."/>
Confirm New Password :	<input type="password" value="....."/>
SNMP :	Enabled <input type="button" value="v"/>
Current Community Read-Only is :	public
Change Community Read-Only :	<input type="text" value="public"/>
Security mode :	<input checked="" type="radio"/> Authentication for configuration
	<input type="radio"/> Full authentication
	<input type="radio"/> SSL and full authentication
Save modified settings :	<input type="button" value="Save"/>