Eaton® Intelligent Power Manager® (IPM)

User's Guide

Powering Business Worldwide

Class A EMC Statements

FCC Information

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

ICES-003

This Class A Interference Causing Equipment meets all requirements of the Canadian Interference Causing Equipment Regulations ICES-003.

Cet appareil numérique de la classe A respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

Eaton is not responsible for damage to this product resulting from accident, disaster, misuse, abuse, non-Eaton modification of the product, or other events outside the reasonable control of Eaton or not arising under normal operating conditions.

CE C TÜVRheinland US 1F61 I.T.E.

Special Symbols

The following are examples of symbols used on the UPS or accessories to alert you to important information:

RISK OF ELECTRIC SHOCK - Observe the warning associated with the risk of electric shock symbol.

CAUTION: REFER TO OPERATOR'S MANUAL - Refer to your operator's manual for additional information, such as important operating and maintenance instructions.

This symbol indicates that you should not discard waste electrical or electronic equipment (WEEE) in the trash. For proper disposal, contact your local recycling/reuse or hazardous waste center.

Table of Contents

Chapter 1 Introduction

The Eaton® Intelligent Power Manager® (IPM) is a power environmental device supervision tool for IT environments. The Eaton IPM delivers a global view across the network from any PC with an Internet browser. Exceptionally versatile, the software is compatible with any device that supports a network interface, such as environmental sensors, other manufacturer's Power Distribution Unit (PDU) or the Eaton Enclosure Power Distribution Unit (ePDU®), other manufacturer's uninterruptible power systems (UPSs), and applications. The Eaton IPM can also organize a management table by groups, centralize alarms, and maintain events logs for preventive maintenance of the entire installed equipment base.

The Eaton IPM provides the following:

- Discovery and supervision of power devices connected to the network including UPSs, ePDUs, automatic transfer switches (ATSs) (for a complete list, click on one of the following links: Eaton Operating System Compatibility List or Eaton UPS and Connectivity Compatibility List)
- Supervision of the remote servers hosting the Eaton Intelligent Power Protector® (IPP) or Network Shutdown Module V3 application
- Advanced management feature (mass configuration and mass upload) with the Network Management Cards [Network-MS (example, 66102/103006826), Modbus-MS (example, 66103), and eNMC for ePDU G3]
- Local computer graceful shutdown through Network or local connectivity, such as USB or RS-232 port
- An agentless method for directly managing and controlling most virtualized infrastructure hypervisors currently available including VMware® vCenter®, Microsoft® Hyper-V®, and Citrix® Xen® (for a complete list, click on one of the following links: Eaton Operating System Compatibility List or Eaton UPS and Connectivity Compatibility List)
- A powerful event manager able to launch alerts and/or corrective actions with customizable conditions
- A growing set of sophisticated actions to improve business continuity in industrial and IT environments

Figure 1 shows an example of the Eaton IPM Node Map page.

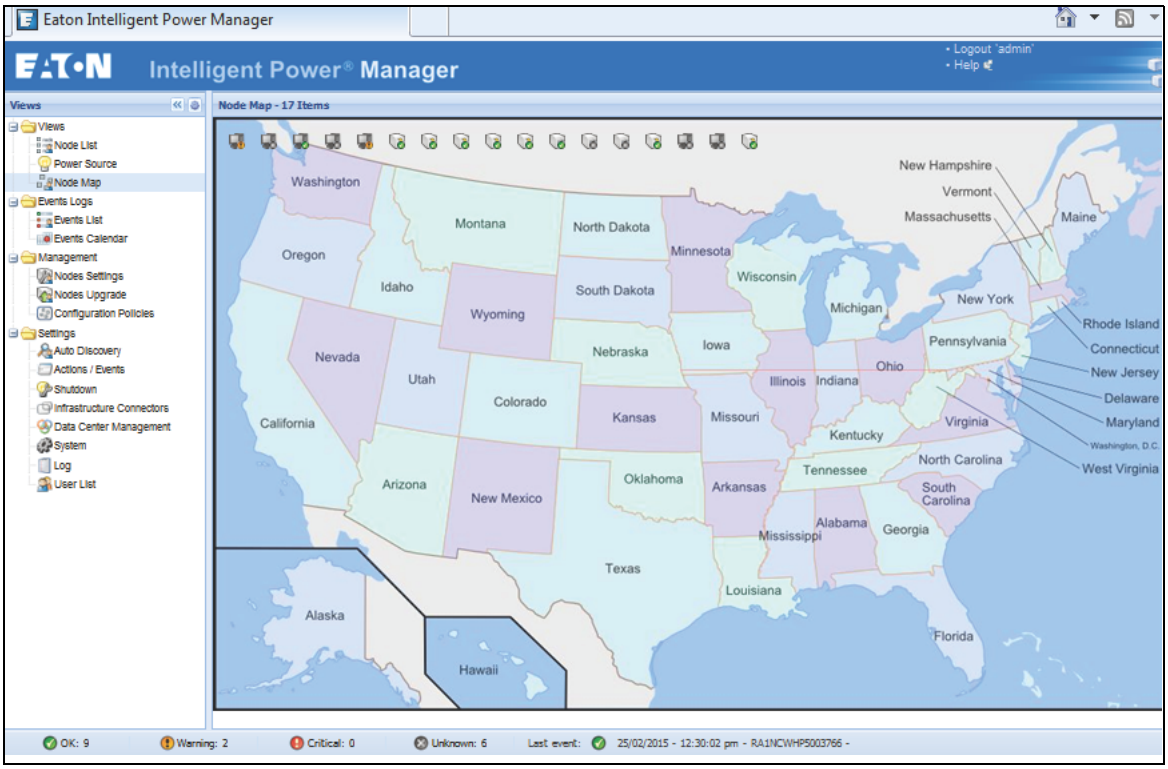

Figure 1. Eaton IPM Node Map Page

Compatibility

Eaton has tested the compatibility of the Eaton IPM with a comprehensive list of devices and applications (for a complete list, click on one of the following links: Eaton Operating System Compatibility List or Eaton UPS and Connectivity Compatibility List).

NOTE If a device doesn't support the Quick Scan feature, it can be supervised if Address Scan or Range Scan operations are performed. See "Discover Nodes Connected on the Network" on page 17 for more information.

Eaton IPP Management

The Eaton IPP can be remotely managed, configured, and updated using Eaton IPM supervisory software. Using the Eaton IPM, you can perform mass configurations and mass updates of Eaton IPP applications. The Eaton IPM can also remotely perform the following:

- Display an Eaton IPP configuration
- Configure a single Eaton IPP
- Synchronize multiple Eaton IPP configurations
- Trigger an Eaton IPP upgrade

Performance Evaluations

To provide a performance evaluation, Eaton has tested the following configurations:

Test with a typical hardware

- CPU: Intel Core® 2 Duo 6600 @2.4GHz
- Memory: 2Go DDR2
- HDD: 1 HDD 220 GB 7200 rpm
- OS: Microsoft® Windows Vista® Enterprise 32 bits

Test conditions during 40 hours:

- 1000 nodes (including ~50 real), mainly Eaton IPMs, and some NSM and Network Management Card.
- Average CPU load: ~60%
- Memory load: 200 ~300MB

NOTE These tests have been performed on Windows Server Operating System. The Windows 2003 or 2008 Operating Systems do not have the limitation of 10 simultaneous connections.

Network Ports

Table 1 lists the network ports used by the Eaton IPM.

Table 1. Network Ports

Protocol	Mode Port	Eaton Network Card-MS, NMC	Eaton Gigabit Network Card	Other Eaton UPS Management Cards*	Eaton IPP with Shutdown Controller	Eaton IPP and Eaton IPM
SMTP	TCP/25	OUT	OUT	OUT	OUT	OUT
DHCP	UDP/67	OUT	OUT	OUT	X	X
TFTP	UDP/69	IN	X	X	OUT	OUT
HTTP	TCP/80	IN	IN	IN	IN/OUT	IN/OUT
SMTP/StartTLS	TCP/587	OUT	OUT	X	OUT	OUT
MDNS SD	UDP/5353	X	IN/OUT	X	IN/OUT	IN/OUT
MQTT	TCP/8883	X	IN/OUT	X	IN/OUT	IN/OUT
NTP	UDP/123	OUT	OUT	OUT	X	X
SNMP	UDP/161	IN	IN	IN	OUT	OUT
SNMP Traps	UDP/162	OUT	OUT	OUT	X	X
UNMP	UDP/200	X	X	OUT	IN/OUT	IN/OUT
HTTPS	TCP/443	IN	IN	IN	IN/OUT	IN/OUT
Eaton Supervision	TCP/4679	X	X	X	IN/OUT	IN/OUT
Eaton Notification Broadcast	UDP/4679	IN/OUT	X	X	IN/OUT	IN/OUT
Eaton SSL Supervision	TCP/4680	X	X	X	IN/OUT	IN/OUT
Eaton Alarms Broadcast	UDP/4680	OUT	X	X	IN	IN
Eaton Connected Alarms	TCP/5000	IN	X	X	OUT	OUT
Eaton Connected Alarms	TCP/5001	X	X	X	IN	OUT
IPP-Unix (NUT)	TCP/3493	X	X	X	IN/OUT	IN/OUT

***** PXGX2000, PXGXUPS, ConnectUPS-BD, ConnectUPS-X, Network-MS

Terms

This section provides related terms and definitions.

IP Address

When Transmission Control Protocol/Internet Protocol (TCP/IP) is installed on a computer, an Internet Protocol (IP) address is assigned to the system. Each address is unique and is made up of four numbers, each between 0 and 255, such as 168.8.156.210.

Secure Socket Layer

The Secure Socket Layer (SSL) is a solution for securing transactions over the internet. SSL is a communication protocol that authenticates the data exchanged, as well as ensuring its confidentiality and integrity. The protocol uses a recognized encryption method, the RSA algorithm with a public key. SSL is built into Internet Web browsers. The padlock in the bottom of your browser screen automatically displays if the server sending information uses SSL.

Transmission Control Protocol/Internet Protocol

TCP/IP is a family of network and communication protocols for the transport and network layers. Also known as the Internet Protocol suite of network communication protocols.

Acknowledgements

The Eaton software development team is grateful to the following projects:

- Spider Monkey
- Ext JS®
- SQLite®
  - The SQLite Project (http://www.sqlite.org) generously donated source code to the public domain that helped us for this project.
- OpenSSL®
  - This Eaton IPM product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org).
  - This Eaton IPM product includes cryptographic software written by Eric Young (eay@cryptsoft.com).
  - This Eaton IPM product includes software written by Tim Hudson (tjh@cryptsoft.com).
- Lib USB
- Net SNMP

The full license version for each of these projects is available from Eaton IPM using the ***Settings > System > About*** selection path.

Java Licensing

Eaton's advanced software (infra connector) uses the OSGI framework technology. All the constituent modules of the new features (virtualization, storage, Cisco UCS) are based on OpenJDK (Open Java Development Kit, which is a free and open source implementation of the Java Platform).

A Java Runtime Environment (JRE) must be installed on the target machine to use these features. This one can be open source, such as OpenJRE, or business, such as Oracle.

IMPORTANT

Acceptance of licenses, related to Java Runtime Environment, is the responsibility of the end user.

Chapter 2 Installation

This chapter provides Eaton Intelligent Power Manager (IPM) installation prerequisites and quick start installation procedures. Procedures for uninstalling and upgrading the product are also included.

For a complete operating systems compatibility list, click on the following link:
Eaton Operating System Compatibility List

Installation Prerequisites

This section provides installation prerequisites for the following:

- Systems hosting the Eaton IPM
- Systems that display the Web-based graphical user interface (GUI)

On the System Hosting Eaton IPM

The Eaton IPM can be installed on several versions of Microsoft® Windows servers.

For full compatibility, click on the following link:

- Eaton Operating System Compatibility List

- For better performances with multiple nodes, Eaton recommends a Microsoft® Windows Server® OS (that does not have the limitation of 10 simultaneous network connections)
- To avoid network or serial port access conflicts, do not install the Eaton IPM on a machine that also hosts:
  - Network management system, such as HP OpenView® or CA Unicenter®
  - Eaton Intelligent Power Protector (IPP)
  - Eaton Enterprise Power Manager
  - Eaton Network Shutdown Module
  - Network Management Proxy
  - Eaton UPS Management Software

NOTE The Eaton UPS Management Software is a legacy Eaton software product for managing UPSs. If you were using it previously, remove it before installing the new Eaton IPM software.

On the System that Displays the Web-based GUI

The Eaton IPM graphical interface can be accessed remotely using a simple Web browser. Access to this interface can be secured through Secure Socket Layer (SSL) connection and is also secured through login and password.

The Eaton IPM graphical interface has been tested with:

- Google® Chrome™
- Mozilla Firefox®
- Microsoft® Internet Explorer® (IE) version 9 and later

NOTE For optimal performance, Google Chrome or Firefox is recommended. For good performance, IE version 9 and later is recommended.

JRE Prerequisites

For all features correlated to the infrastructure connector (such as VMware, UCS, NetApp), a Java Runtime Environment (JRE) must be installed on the system hosting Eaton IPM (see "JRE Installation" on page 8).

JRE Installation

The installation of the JRE is Operating System platform-dependent. All new Eaton components have been developed and tested for the Java version 1.8 or later. After installing the correct JRE, the IPM must be reloaded, to take account this new environment.

NOTE 1 IPM (since version 1.66) is compatible with OpenJDK 1.8, tested with Microsoft Installer (msi) package (available on Github: https://github.com/ojdkbuild/ojdkbuild).

NOTE 2 OpenJDK already provides JRE.

Quick Start Instructions

This section includes quick start installation and configuration instructions.

Graphical Installation

To install the Eaton IPM:

1. On a computer with a Windows OS, run the Eaton Intelligent Power Manager package under an administrator account. A Web browser displays the Eaton Intelligent Power Manager Installer Welcome screen.
2. Observe the prompt and verify that the communication device is connected. Click **Next** (see Figure 2). The Login screen displays.

Figure 2. Welcome Screen

3. Read the application description on the Login screen. Type the login and password and click **Login** (see Figure 3).

NOTE The default entry for login and password is **admin**.

Figure 3. Login Screen

Configuration

When started, the application automatically performs a discovery using the "Quick Scan" option:

- Using the "Quick Scan" operation, you will discover the following through broadcast: Eaton Gigabit Network Card, Network Management Cards Network-MS and Modbus-MS, PXGXUPS, ConnectUPS-BD, ConnectUPS-X, ConnectUPS-MS, Intelligent Power Protector, Network Shutdown Module V3, Eaton G3 ePDU cards, HPE UPS cards, monitored and managed HPE PDU cards, Dell UPS card, or Lenovo UPS cards, or IBM UPS card.
- Display the discovered nodes using ***Settings > Auto Discovery*** (see Figure 4).

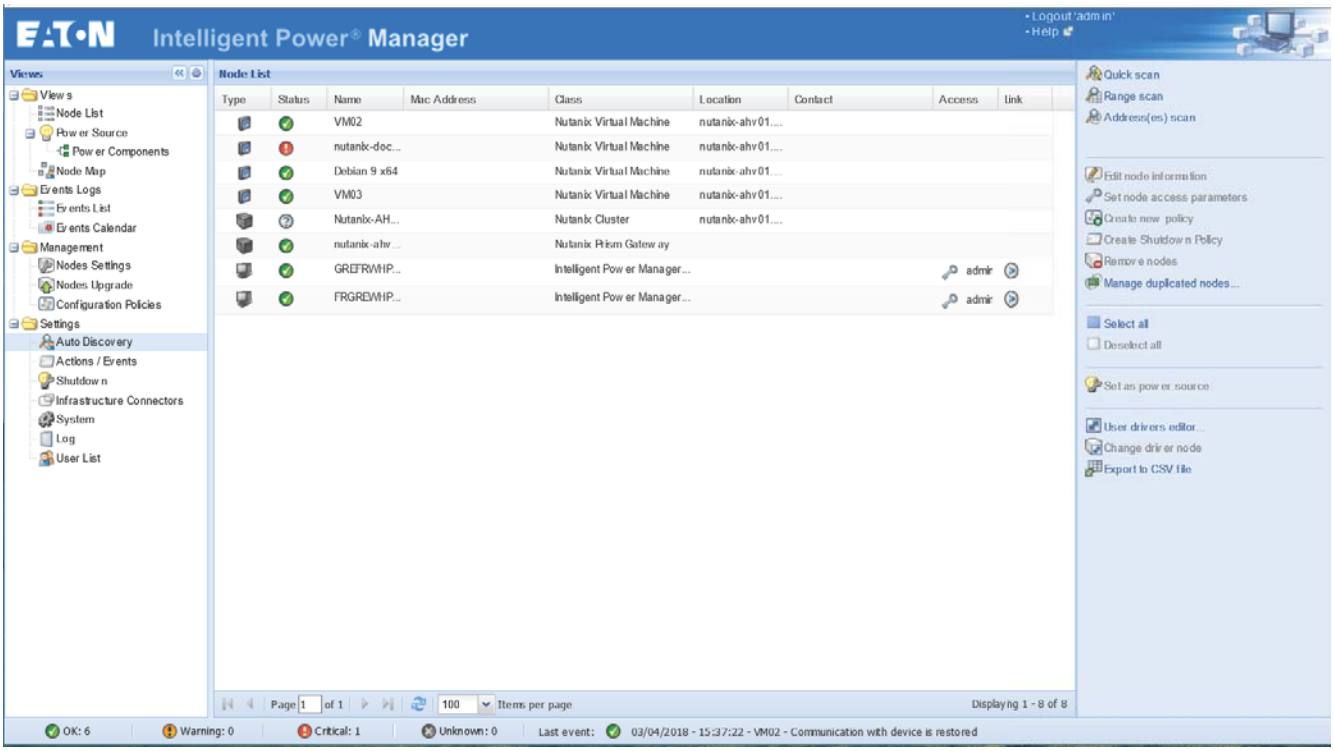

Figure 4. Quick Start - Auto Discovery Page

- For the other nodes, perform the discovery based on IP address ranges using the "Range Scan" option. Using "Range Scan" discovers the nodes that are outside of the network segment and nodes that are not compatible with the "Quick Scan" feature.
- Refer to the Compatibility list to determine if your node supports the "Quick Scan" feature.

(**Optional**) To set the computer running Eaton IPM to shut down in the event of a power failure:

1. Select ***Settings > System***. In the far right panel, select **Edit modules settings**. The Edit modules settings dialog displays.
2. Select the **Shutdown** checkbox on the Edit modules settings dialog (see Figure 5). The Shutdown menu selection displays in the Settings menu hierarchy list (see Figure 6).

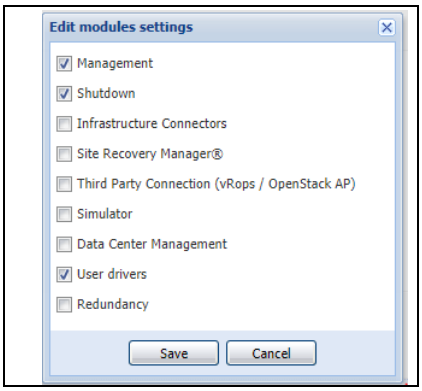

Figure 5. Edit Modules Settings Dialog

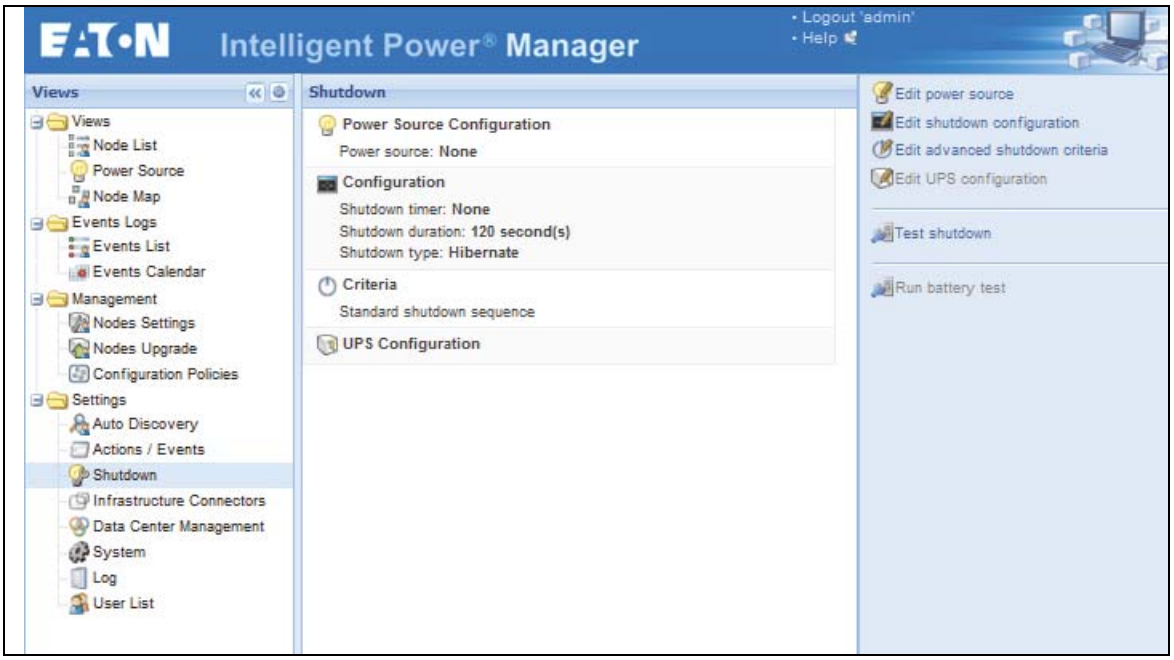

Figure 6. Shutdown Displays in the Settings Menu Hierarchy

3. From the ***Settings > Shutdown*** page, assign the following:
   - IP address of the UPS that powers the local computer (power source)
   - Shutdown configuration parameters (timer, duration, type of shutdown, and (if needed) shutdown script
   - Select or deselect (check or uncheck) the checkbox for standard shutdown sequence

License Code

The Eaton IPM manages up to 10 power devices (including UPS Web Card, ePDU, or Eaton IPP Shutdown Controller) without a license. For more features or more nodes, a license key is required.

Table 2 provides the differences between Basic mode (requires no license code) and Silver and Gold modes.

Table 2. Features for IPM Versions 1.50 and Later

Features	Basic Up to 10 Power Devices	Silver Up to 100 Power Devices	Gold Unlimited** Power Devices
Protected Servers (IPP) and Virtual Servers	•	•	•
Storage Shutdown Module	•	•	•
Generic Drivers and Third Party Devices	•	•	•
Configuration Policy	•	•	•
Advanced Event Action with Standard Events	•	•	•
Plugin for VMware VCenter	•	•	•
Advanced Event Action with Custom Events	—	•	•
Virtualization (Basic Power Actions): • Shutdown Virtual Hosts • Shutdown Virtual Machines • Enter/Exit Maintenance Mode	•*	•*	•
Virtualization (Advanced Power Actions): • Load Shedding • Shutdown Targeted Virtual Machines • Migrate Virtual Machines to Targeted Hosts • Shutdown VMware vAPP • Automate VMware SRM Recovery Plan	—	•*	•

***** Not included for Eaton-Essential UPS Models (9E and 93E) or any non-Eaton UPS Models. Customers need to purchase the Gold License to enable Basic and Advanced virtualization features.

**Tested to 500 NMC and 200 ePDUs

NOTE In some countries, the license key will be distributed electronically, please contact your sales representative.

NOTE Nodes that are not managed due to license limitation appear with this icon: 

Operation

1. Use the ***Views > Node List*** menu item to supervise the current state of the compatible power devices and applications.
2. Select a line in the list and the panels are updated with selected device information (see Figure 7).

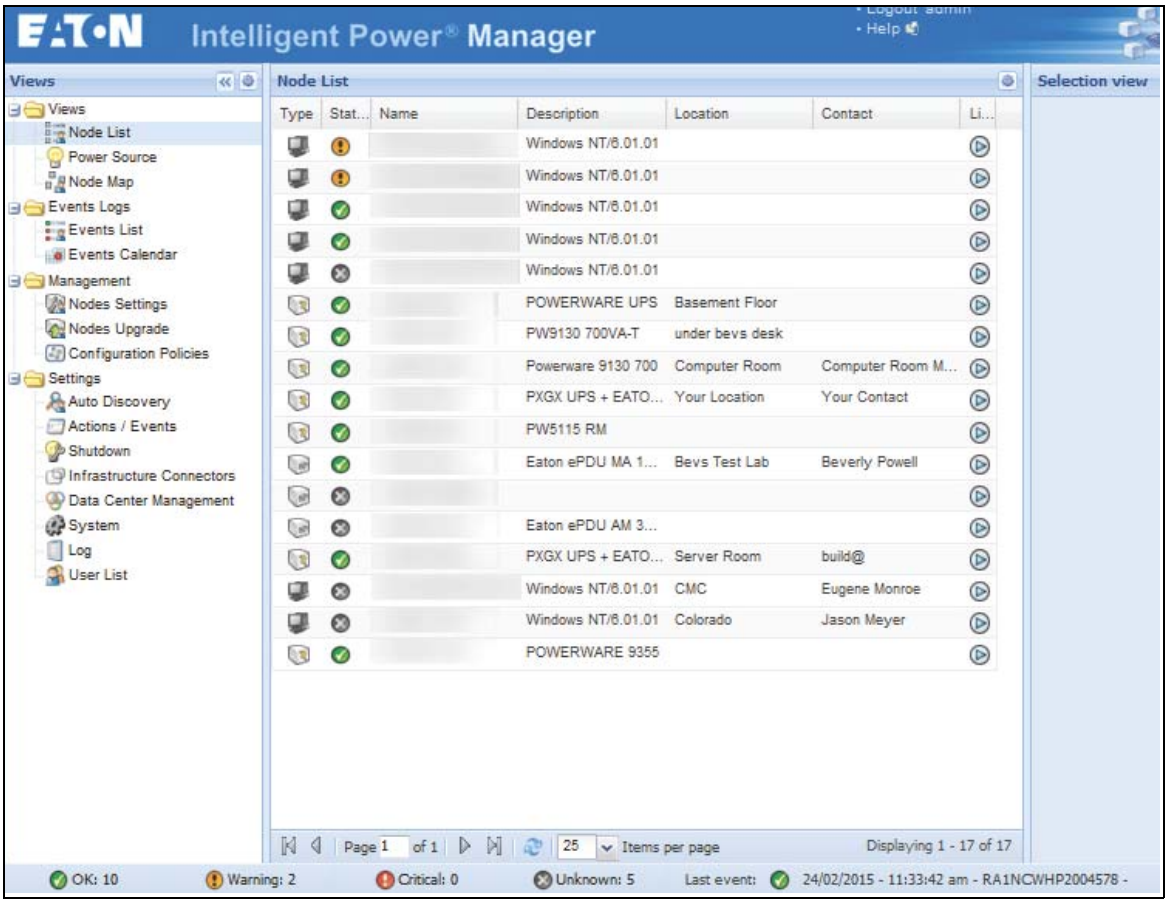

Figure 7. Node List Main Page

- [Optional] If you have enabled the Shutdown module, the ***Views > Power Source*** menu item allows you to supervise the current state of the UPS that powers the server running Eaton IPM. This menu is available when you have enabled the Shutdown module in ***System > Settings > Edit Modules Settings***.
- The ***Events > Event List*** view allows you to view the device events.
- The Management menu provides functions that allow you to mass configure and mass upgrade cards.

Installation Result

IMPORTANT

If you install a new Eaton IPM release without uninstalling the old one, you will keep your database and your product settings.

- At the end of the installation, the following shortcuts are created in the group ***Start > Programs > Eaton > Intelligent Power Manager***:
  - **Open Eaton Intelligent Power Manager**: Starts the main Eaton IPM graphical interface
  - **Start Eaton Intelligent Power Manager**: Starts the service
  - **Stop Eaton Intelligent Power Manager:** Stops the service
  - **Uninstall Eaton Intelligent Power Manager**: Uninstalls the program
- A service called "Eaton Intelligent Power Manager" is also created for the Database Acquisition Engine.
  - This program continuously polls the status of Eaton devices and Applications connected on the network.
  - This service automatically starts on machine boot-up.
  - This service provides the Web Interface.
- A system tray icon displays the alarms on the local computer. Right-click this icon to display the same shortcuts as in the Windows Start menu.

Uninstalling the Eaton IPM

The following methods for uninstalling the Eaton IPM are available:

- Access the control panel selection for your operating system to uninstall programs and remove the **Eaton Intelligent Power Manager Vx.xx** package per your system instructions.
- You can also uninstall from the shortcuts to remove the product and custom files (if you confirm the action): ***Start > Programs > Eaton > Intelligent Power Manager> Uninstall Intelligent Power Manager***.

Upgrading the Eaton IPM Product

If you install a new Eaton IPM Release without uninstalling the old release, you will keep your database and your product settings. See "Nodes Upgrade" on page 94 for upgrade information. Also see "System Settings" on page 28 for information on configuring automatic upgrade.

Installing/Uninstalling the Eaton IPM (Command Line)

You can install or uninstall the Eaton IPM product from a command line in order to deploy the software in a group, with or without using the graphical interface. You can also configure protection settings from the command line.

Detail of available command options can be obtained using the following command:

```
<packageName> -help
<packageName> [COMMAND] [OPTION]...
```

The available commands are:

- -install Launches the installation/upgrade process (default)
- -uninstall Launches the process to uninstall the application

The available options are:

- -debug Displays debugging information on the console
- -silent Installs the application silently

Access the installation folder:

```
-dir <installPath>
```

Example

The command `<packageName> -install -silent -dir "C:\Program Files\MyFolder"` will install the Eaton IPM silently in C:\Program Files\MyFolder.

After the installation is completed, open a Web browser with the following URL:

- http://<host>:4679/, where <host> is the host name or IP address of the machine hosting the Eaton IPM.

Chapter 3 Configuration

This chapter describes how to configure the Eaton Intelligent Power Manager (IPM).

Configure Nodes

Each node (Eaton Gigabit Network Card, Network Management Card, proxy, or application) must have a valid IP address (or a DNS name) in the range that you have entered for auto-discovery (see "Compatibility" on page 2).

Eaton IPM automatically receives the alarms (through notification or polling) without specific configuration on the network card, proxies, or applications.

For SNMP communication, configure the SNMP parameters using the ***System > Scan Settings*** selection.

Discover Nodes Connected on the Network

To discover nodes connected on the network:

1. From the left-side **Views** panel of the Eaton IPM main interface window, select the ***Settings > Auto Discovery*** menu item.
2. From the right panel, select a discovery method (see Figure 8):
   - **Quick Scan**: Automatically performed when application starts
   - **Range Scan**: Click the **Range scan** button
   - **Address Scan**: Click the **Address(es) scan** button

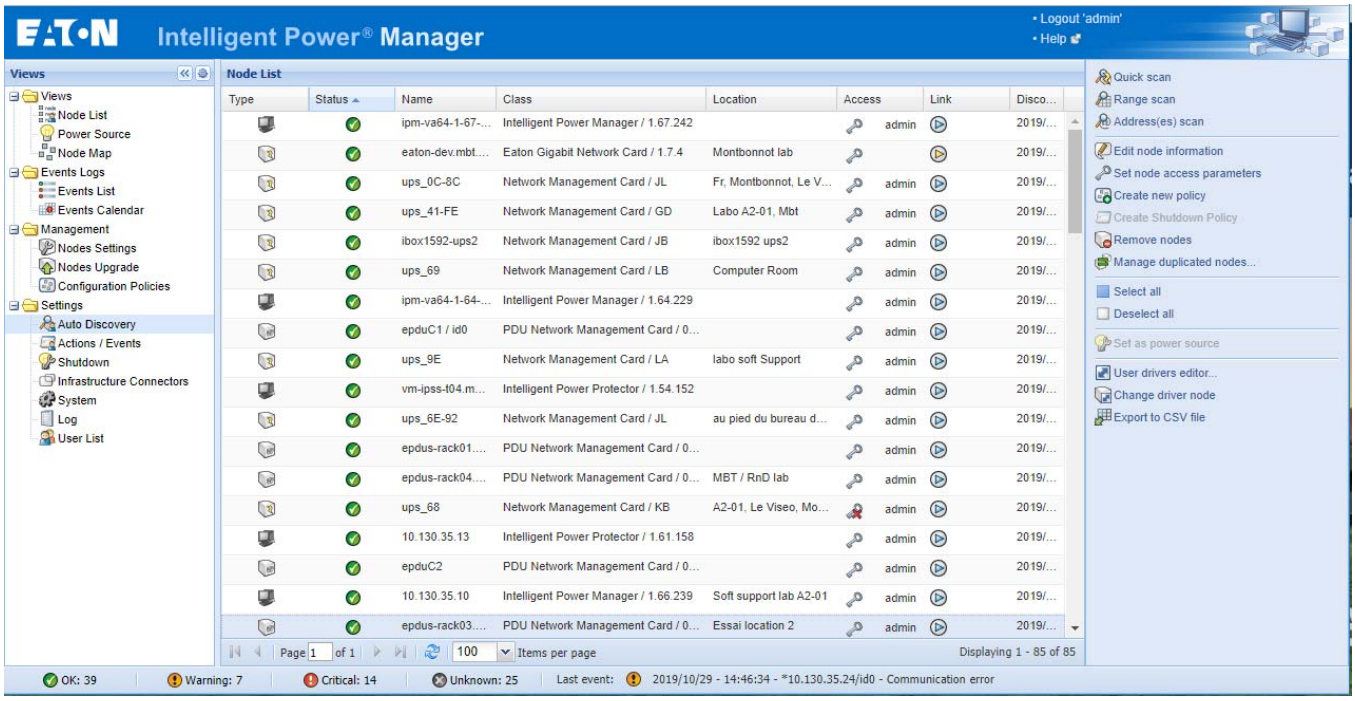

Figure 8. Node List Page from Auto Discovery

Quick Scan

The Quick Scan request is a broadcast frame on 4679 IANA reserved port and 69 standard TFTP port. Using the Quick Scan operation, you will discover any of the following within a few seconds:

- Eaton Gigabit Network Card
- Network Management Cards Network-MS and Modbus-MS (example, 66103)
- PXGXUPS, ConnectUPS-BD, ConnectUPS-X, or ConnectUPS-MS
- ePDUs and sensors EMPDT1H1C2
- Eaton Intelligent Power Protector (IPP) or Network Shutdown Module V3

Range Scan

Using the Range Scan operation, you will discover the nodes that are outside of the Network segment and nodes that are not compatible with the Quick scan feature. See "Compatibility" on page 2 to determine if your node supports Quick scan feature.

In the Range scan dialog box, you can edit IP address ranges. You can also select (check) the **Override global authentication settings** checkbox to specify authentication parameters that are different from global scan settings (see Figure 9).

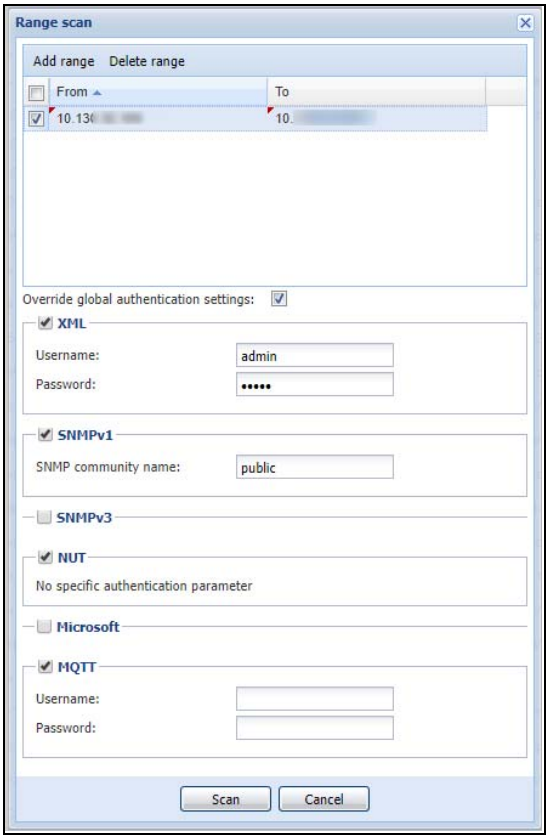

Figure 9. Range Scan Dialog Box

Address Scan

This type of node discovery performs a single address scan (or for several IP addresses separated by the ";" character).

In the Address(es) Scan dialog box, edit IP addresses to scan.

- You can select (check) the **Force node(s) creation** checkbox to create a node with an IP address even if the scan operation did not identify the device.
- You can also select (check) the **Override global authentication settings** checkbox to specify authentication parameters that are different from global scan settings (see Figure 10).

NOTE The option **Force node(s) creation** will create empty nodes if the scan operation did not identify the devices. Then it is possible to assign a different driver to the nodes created (see "Change Driver Node" on page 25).

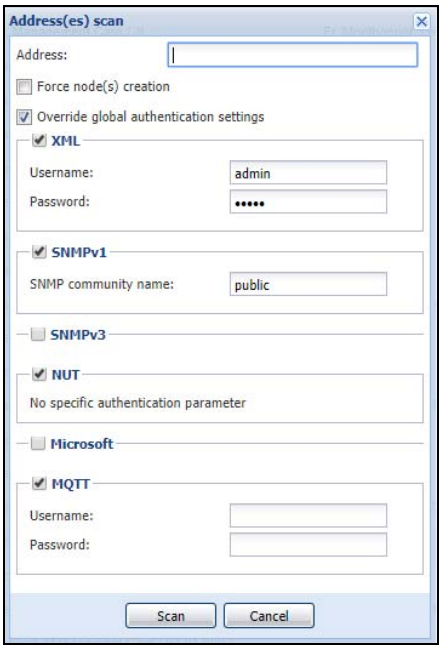

Figure 10. Address(es) Scan Dialog Box (Example 1)

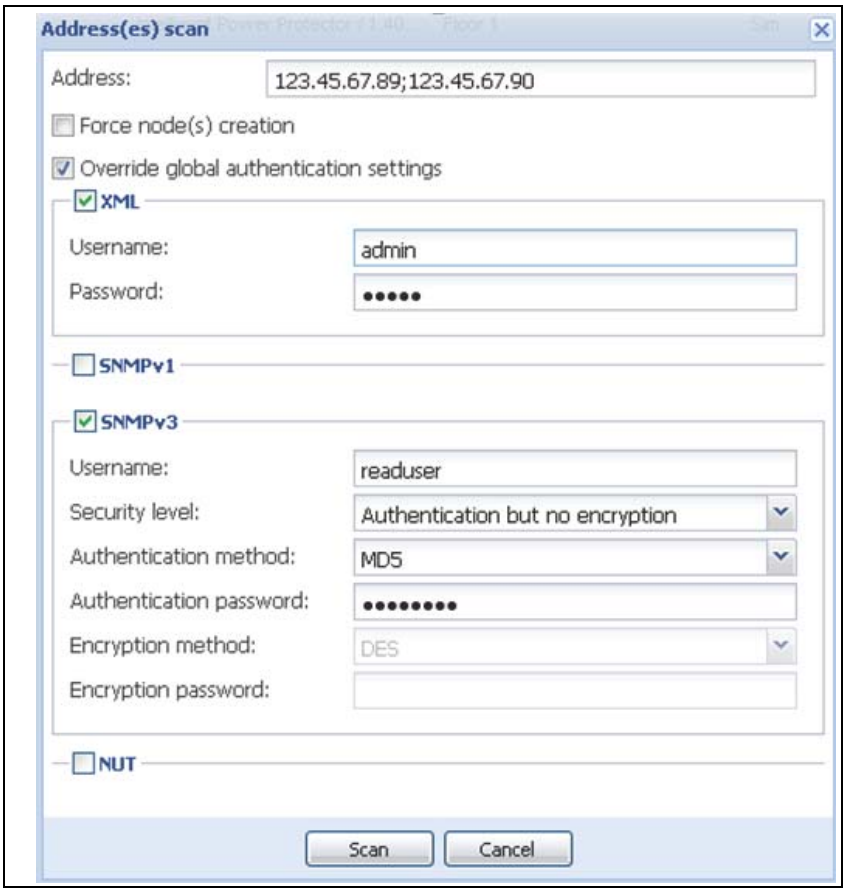

Figure 11. Address(es) Scan Dialog Box (Example 2)

Configure Duplicated Nodes Discovery

Settings

Possibility to deactivate the duplicated nodes automatically. By default the option is activated: When a new discovered node is detected as a duplication of an existing one, it is automatically removed to maintain the existing one.

To remove this option: select ***System > Scan settings*** menu and un-check **Remove duplicated nodes automatically**. Once the option is un-checked, the user can manage manually duplicated nodes

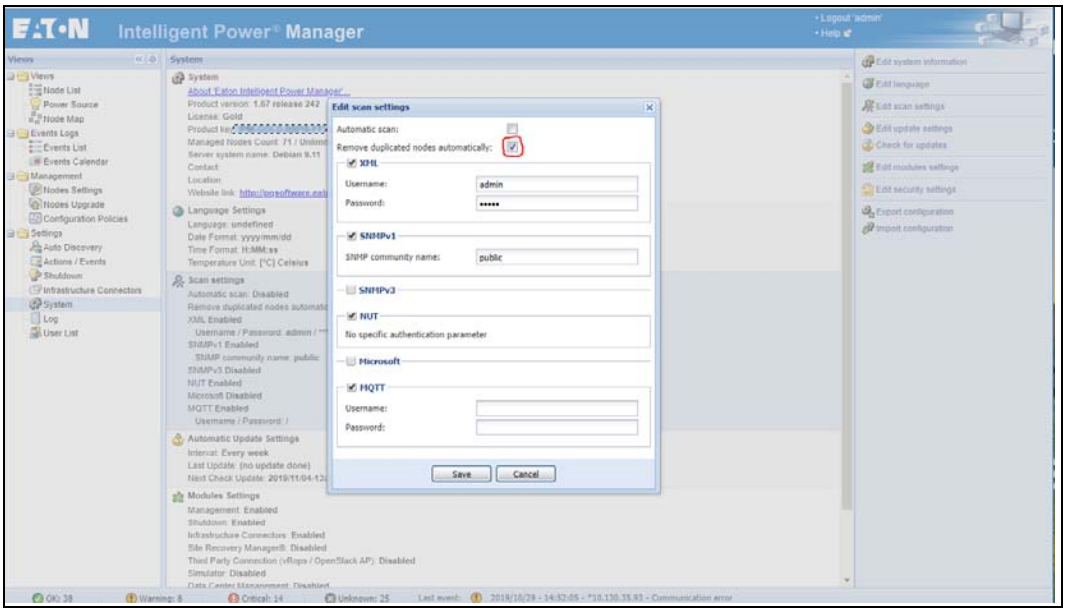

Figure 12. Remove Duplicated Nodes Automatically

Once the option is deactivated, after a discovery nodes action (Quick Scan, Range Scan, Address Scan), users have the possibility to select the nodes that they want to keep or remove: on the right menu, click on the **Manage duplicated nodes** button (see Figure 13)

- Even when the automatic mode is disabled, the correlation algorithm is executed on all newly discovered node (no automatic merge is done at this step).
- Internally, if a new node is detected as identical as an already existing one, they are both marked with a specific marker: "OLD" for the previously discovered and "NEW" for the new one.
- If another scan creates a third duplicated node, the previously "NEW" tag is replaced by "OLD" and the new node is tagged "NEW" (and so on for other duplications).
- When duplicated nodes are detected, the menu entry is activated. It is automatically disabled when no more duplicated nodes are detected.

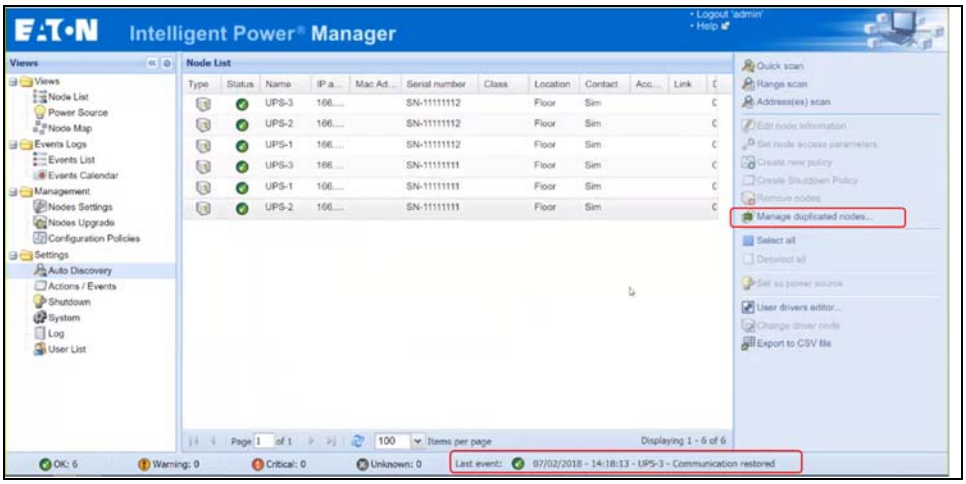

Figure 13. Manage Duplicated Nodes Button

A new modal dialog display all duplicated nodes discovered by IPM:

- When selecting **Select OLD duplicated nodes** button, all nodes from the current view marked as "OLD" are automatically selected.
- At this step the user can manually select or unselect nodes from the list by combining selection action with the CTRL key as he can do it today for multiple selection.
- The button **Remove selected nodes** will allow removing all selected nodes. It is enabled when at least one node from the list is selected.
- When a removing action of a node detected to be marked as "OLD" or "NEW" is executed, the removed node settings are merged in order to re-link removed node configurations to the kept one.

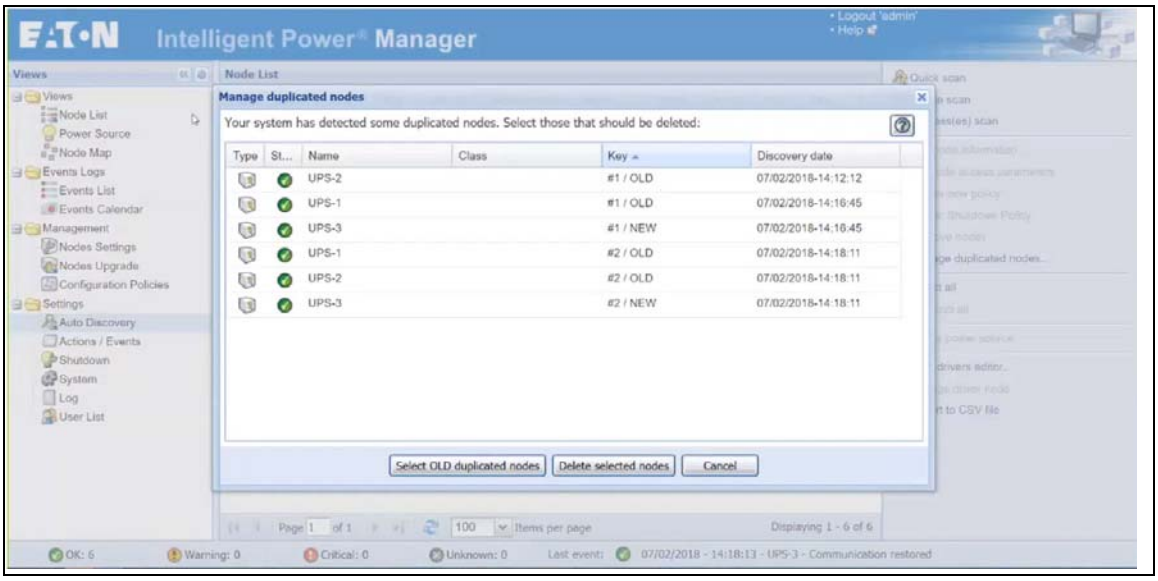

Figure 14. Manage Duplicated Nodes Window

A specific column is available allowing to show duplication markers and to sort from this field. Markers will provide a key allowing to sort nodes while maintaining matching peers together. It is also possible to select the columns to display

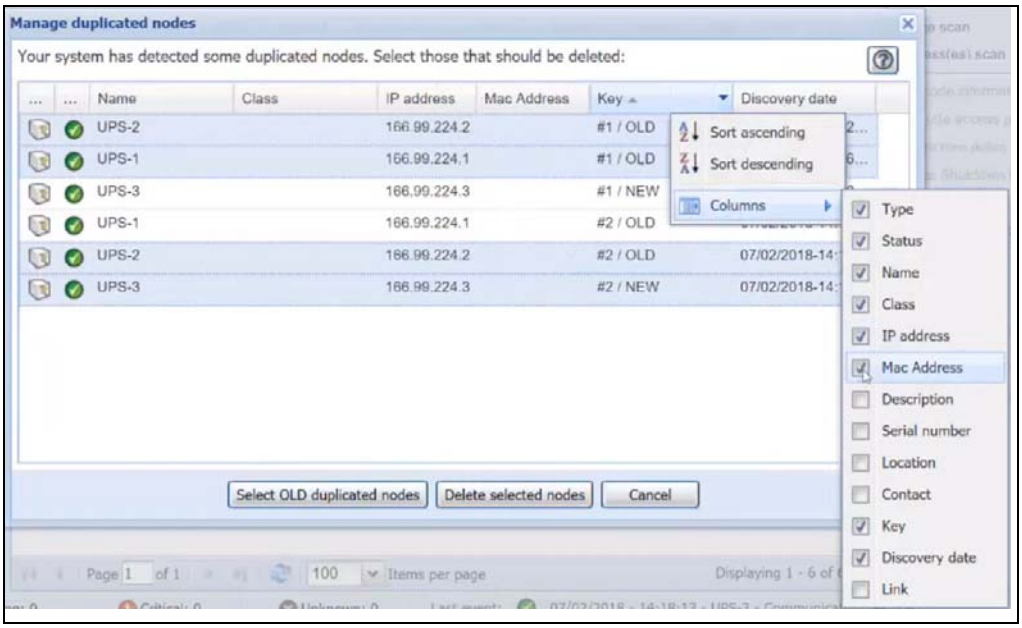

Figure 15. Manage Duplicated Nodes Help Section

The **Help** Button explains how to select nodes to be removed. Configurations related to the deleted nodes will be transferred to the nodes kept by the user.

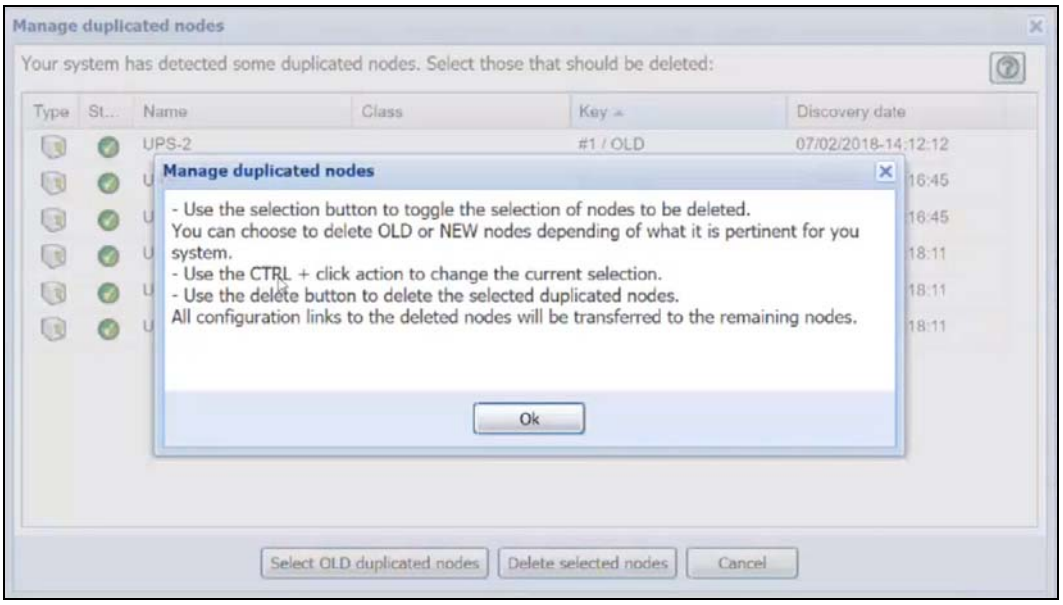

Figure 16. Manage Duplicated Nodes Help Section

Notifications

When at least one duplicated node is detected, an information system event is generated. This will trigger a notification and event log as well as any other actions linked to standard "Information Alarms". When there is no more duplicated nodes, the roll back event is also triggered with the same severity. For large configuration (Gold license), the system event can be individually linked to any action (i.e. email). A system log is also generated for each detection of duplication. User actions on de-duplication are also logged.

Scan Settings for Discovery

Administrators can set scanner authentication parameters that will be used as the default when discovering new devices. These authentication settings can be set for the XML, SNMPv1, SNMPv3, and NUT protocols.

When discovered, manually or automatically, newly discovered devices will use these authentication parameters. Depending on the device-supported protocols, IPM will choose the needed parameters. See "Compatibility" on page 2 to determine which protocols are supported.

The administrator can also activate the automatic scanner to add any automatically discovered devices without a direct scan action of the administrator. For example, with automatic scan enabled, the presence of a new card on the network would be auto-discovered and added.

To change scan settings:

1. From the left-side **Views** panel of the Eaton IPM main interface window, select the ***Settings > System*** menu item. The System page displays.
2. Click the Edit scan settings button on the right-side page. The Edit scan settings dialog box displays (see Figure 17).
3. Set the scan settings by selecting or deselecting checkboxes, typing data, or make selections from the drop-down list.

Figure 17. Edit Scan Settings Dialog Box

Change Driver Node

After discovering a node, it is possible to assign a different driver to this node.

To change driver mode:

1. Select the ***Settings > Auto Discovery*** menu item.
2. From the right-side panel, select **Change driver node** (see Figure 18).
3. By default, the driver of the node is selected. Choose another driver and click **Ok**. The node will use this new driver.

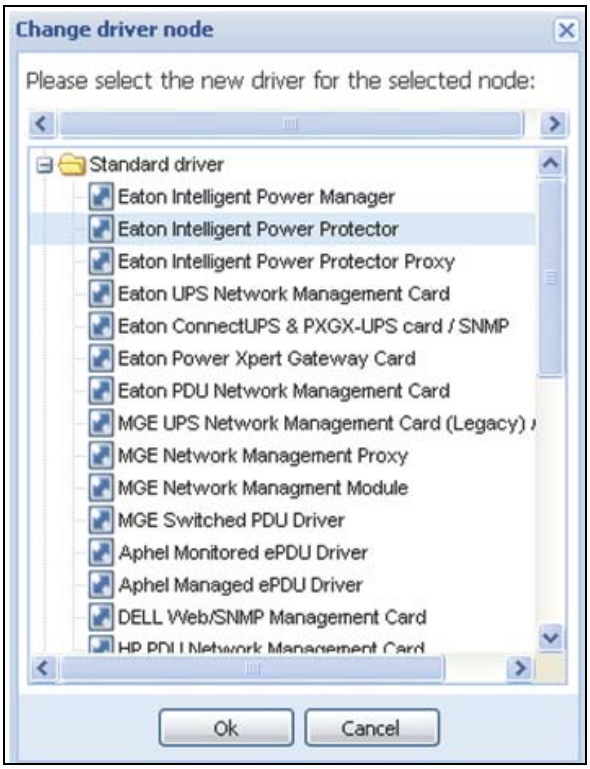

Figure 18. Change Driver Mode Dialog Box

Configure Node Settings

To configure node information and access parameters (administrators only):

1. From the left-side **Views** panel of the Eaton IPM main interface window, select the ***Settings > Auto Discovery*** menu item.The Nodes List page displays.
2. Select a node from the Nodes List page.
3. Click the **Edit node information** button or click the **Set node access parameters** button in the right panel.
4. The Edit Node Information dialog or the Access parameters dialog displays (see Figure 19 and Figure 20):
   - **Edit node information dialog.** The Edit node information dialog box allows editing the node name, the user type, the node description and the associated load alarm threshold.
   - **Access parameters dialog.** You can define the access settings for all selected devices. Only relevant settings are set, depending on the capabilities of the selected device.

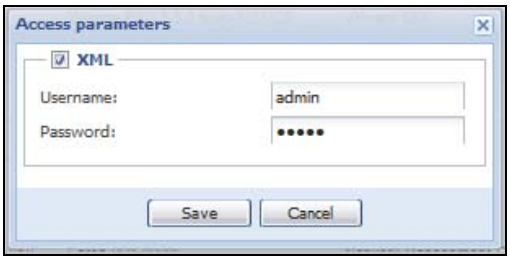

Figure 19. Node Access Parameters Dialog

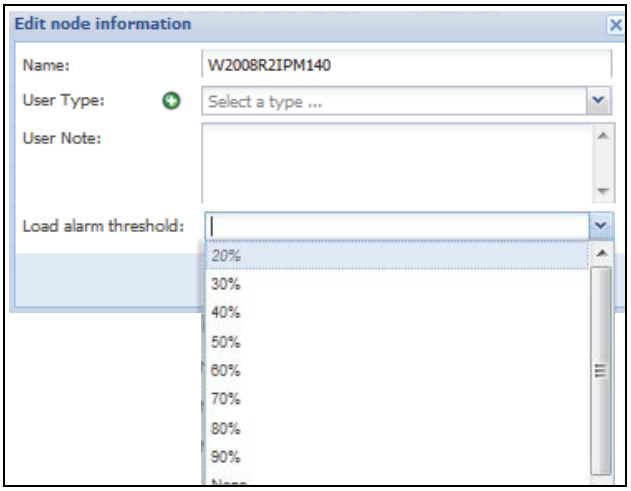

Figure 20. Edit Node Information Dialog

Configure User Accounts

To configure multiple user accounts:

1. From the left-side **Views** panel of the Eaton IPM main interface window, select the ***Settings > User List*** menu item. The User List page displays (see Figure 21).
2. Click **Add user.** The Add user dialog box displays.
3. Type the user's login and the user's password (see Figure 22).
4. Select the user's profile level. The following levels are available:
   - **Admin:** User will be able to access all the features
   - **User:** User will only access the visualization and cannot set changes to the system or nodes
5. Click **Create new user**.

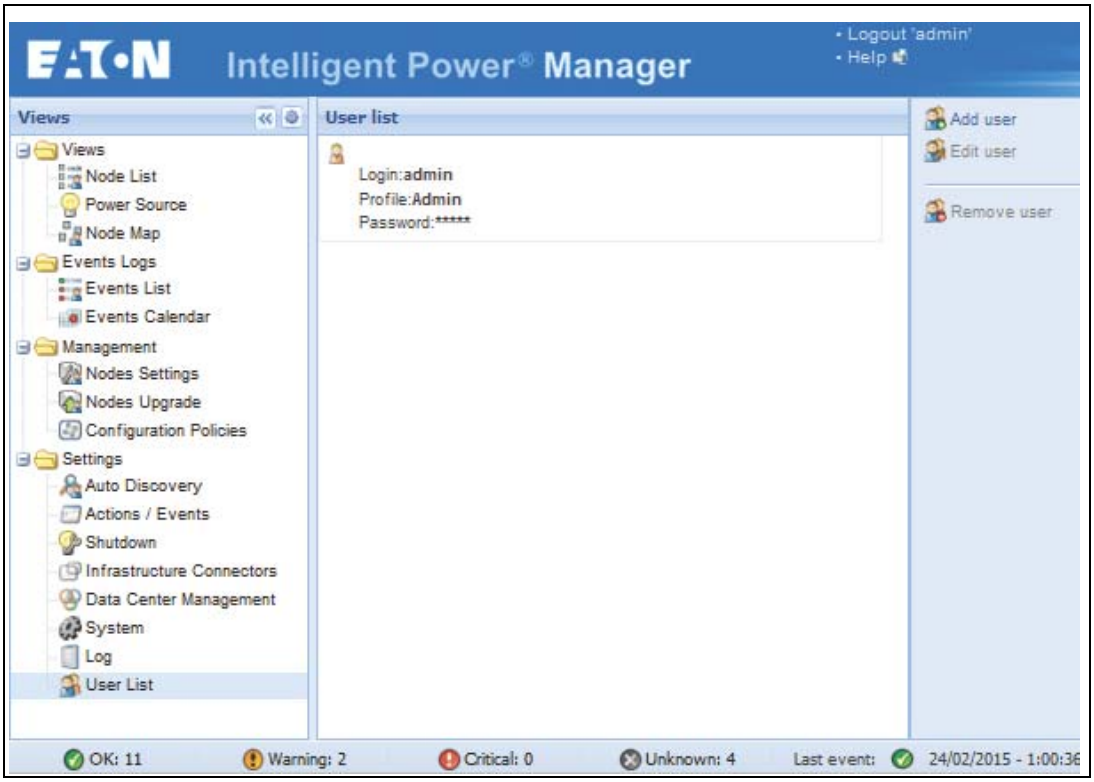

Figure 21. User List Page for User Account

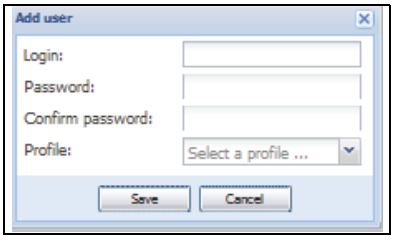

Figure 22. Add User Dialog Box

Note that the Eaton IPM contains a default Administrator profile with:

- "admin" as login
- "admin" as password

WARNING

For security reasons, Eaton recommends that you change the default password immediately after the installation. A pop-up message provides a security warning if the password contains less than eight characters.

System Settings

From the ***Settings > System*** menu item, you can edit system information and settings (see Figure 23).

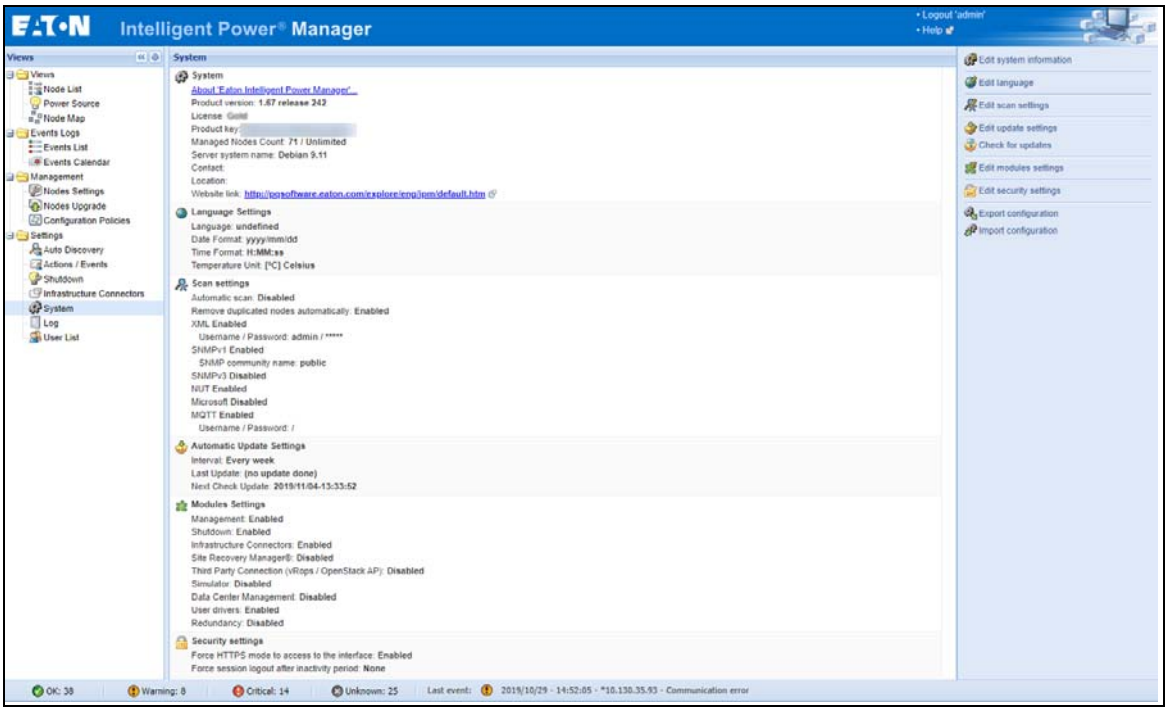

Figure 23. System Settings Page

Select one of the items on the System page, and then double-click the item, or single-click the corresponding button in the right-hand side menu:

- **Edit system information** modifies contact and location information.
- **Edit language** allows you to change the interface language (Czech, English, French, German, Japanese, Korean, Polish, Portuguese, Russian, Simplified Chinese, Spanish, or Traditional Chinese).
- **Edit scan settings** are the default access settings that are automatically set for new discovered nodes.
- **Edit update settings** and **Check for updates** provide features that allow the system to automatically check for Eaton software updates for you. When a new software version is detected on www.eaton.com, a wizard displays and provides upgrade instructions for you. (Database information is retained with this operation.)

- **Edit modules settings** allows you to enable/disable Eaton IPM optional modules:
  - **Management** enables nodes settings mass configuration and nodes upgrade features
  - **Shutdown** enables shutdown of the computer running Eaton IPM in the event of a power failure
  - **Infrastructure Connections** enables management of third party equipment, including storage and virtualized IT systems
  - **Site Recovery Manager** enables the migration for a virtualized cluster
  - **Third Party Connection (vRops / OpenStack AP)** enables the Rest API to connect to third party application
  - **Simulator** enables to create simulated nodes
  - **Data Center Management** connects to the CA Nimsoft (R) infrastructure manager
  - **User Drivers** integrates new devices in the IPM supervision application by using predefined common base objects and user-specific objects
  - **Redundancy** provides support for >1 UPS in N+1 redundant configurations

NOTE The "User Drivers" feature allows IPM to supervise any SNMP- or Network UPS Tools (NUT)-available devices. You can customize and adapt the IPM acquisition engine to any kind of Data Center device, such as HVAC, Rack controller, storage, or DC Power System controller.

Automatic Data Purge

All IPM data (logs, measures and events) are stored in a database. This database automatically purges the accumulated data when necessary according the purge parameter settings for the following parameters:

- **<maxTime>**: Maximum timestamp for the oldest records (in ms)
- **<maxCount>**: Maximum number of records, where the oldest records are removed first

These parameters can be modified in the "config.js" file in the logManager/purge section.

The default settings for purge include:

- Data of type alarm (see events section) **maxTime**: 28 days **maxCount**: 50000
- Data of type measure (see measures section) **maxTime**: 7 days **maxCount**: 200000
- Data of type statistic (see stats section) **maxTime**: 28 days **maxCount**: 20000
- Log system (see system section) **maxTime**: 28 days **maxCount**: 50000

Configuration Export/Import

You can backup the configuration to an external file. The external file can be used to restore the configuration.

This function is accessible through the GUI in the ***Settings > System*** page with the "Export configuration" and "Import configuration" options available in the right column.

On windows systems, the same function can be called from the command line with the following syntax:

- **Export:** C:\Program Files (x86)\Eaton\IntelligentPowerManager>mc2.exe -export configipm.ice
- **Import:** C:\Program Files (x86)\Eaton\IntelligentPowerManager>mc2.exe -import configipm.ice

The limitations of this function include:

- Using the same version of IPM when exporting and importing
- Using the same OS when exporting and importing
- Restoring the complete configuration (the configuration cannot be partially restored)

Chapter 4 Advanced Events and Actionswith

This chapter describes Event Action features for automated control of actions and notifications in the Eaton Intelligent Power Manager (IPM).

IMPORTANT

Because of the potential complexity of final configuration, it is strongly recommended to test the complete chain of events and actions before going into production.

Note that some restrictions could apply regarding your software licence and kind of devices you are managing. Please check the license for more details.

Customized Action on Standard Events

An action is the operation resulting of one or many triggered events. For example, an action could be to send an e-mail when an alarm is generated.

Each action is defined for a specific purpose:

- **E-mail:** Action to send an e-mail.
- **Command:** A command is executed by the supervision application when this action is triggered.
- **Notification:** A Notification produces a one line message displayed in the 'Notifications' window.
- **Event Log:** This action provides an event message to the node event list.
- **Host Power Action**: This action executes a power command on the host target. A power command can be ShutdownHost, ShutdownVMsThenHost, EnterMaintenanceMode, EnterMaintenanceModeThenShutdown, ExitMaintenanceMode, EnterStandByMode or ExitStandByMode.
- **VM Power Action:** This action executes a power command on a virtual machine. A power command can be power on, power off, guest shutdown, or suspend.
- **VM Migrate Action:** This migrates a virtual machine from its host to another host.
- **vApp Power Action:** This action initiates the execution of a power command on a virtual application. The power command can be startup, shutdown, or suspended.
- **Start a Recovery Plan:** This starts a recovery plan in fail-over mode. The SRM module must be active. Choose a recovery plan for a RECOVERY site.
- **SSH Action:** This action will execute a command on a server via a SSH connection.
- **Command PDU Outlets:** This action is used to start or stop one or several outlets of a PDU after a delay.
- **Cluster Shutdown:** Select this action to shutdown a cluster.
- **Storage Action:** To execute an action on a storage node.
- **Volume Migration:** Migrate a storage volume to another storage host.
- **Power Capping:** This action initiates a power capping action on a hardware server.
- **Simulator VMA Action:** To simulate an action on a simulated VMA node.

IMPORTANT

Be careful. VM power, VM migrate, and vApp power actions are not available on Hyper-V. To protect Hyper-V virtualization servers, please perform configuration using selections in the following path ***Management > Nodes Settings > Node configuration*** panel.

When triggered, an event provides the order for the action to occur while providing information to the events' origin (ID, type of the event, and parameters) related to this type of event). That permits to the action to use them and communicate more precisely about the source of this operation.

The application offers six standard events by default:

- Information Alarm
- Warning Alarm
- Critical Alarm
- Unknown State Alarm
- Power Failure
- Runtime Threshold reached

If these standard events are not enough to determine the possible cause of an action, users can define their own custom events (see "Define Custom Events" on page 32).

Configuration Policies

The configuration policies panel allows you to define some policies using parameter sets and apply them either to a single device or to any group of devices or applications monitored by IPM devices and applications monitored by IPM.

In addition, the configuration policies panel is used to attach properties, such as the following:

- Power Source
- Runtime Threshold Settings
- User Settings
- Asset Information

It can be used to group devices by criticality, shutdown settings, power source, or what you think is relevant to your environment.

A device or application that is attached to a configuration policy with a power source and Runtime Threshold settings will be monitored and protected through the standard event called Runtime Threshold Reached.

Define Custom Events

A custom event is used to re-factorize existing triggers in its own customized logic or to listen to other existing objects.

- A trigger is associated with an object and an event is associated with triggers.
- An event could be a combination of multiple sources of information.

Use Custom Events to Launch Custom Actions

There is no restriction on the order of the operations between the action creation or definition, event configuration, and the use of configuration policy settings.

- Actions can be linked to already defined events from their definition dialog.
- Events can be linked to already defined actions from their definition dialog.
- Settings attached to nodes through configuration policies can be used to define both event rules criteria and action parameters.
- Any standard or custom events can be linked to any number of actions.
- Any standard or custom event can be combined together to build a rule of a new custom event.

Example Procedures

For more scenarios about how to use the new advanced features, see "Appendix A" on page 207. Those scenarios will give you some examples of usage, but also a general approach to find out what has to be configured to achieve a specific goal.

The process followed in the examples consists of three simple steps:

1. Do I need a configuration policy setting?
   a. If Yes, select the appropriate classes and the members for each configuration policy needed.
2. Do I need custom events?
   a. If Yes, a Silver or Gold license is required (but standard events in conjunction with configuration policies already address many situations).
3. Create the final action:
   a. Enter the action settings (if any).
   b. Select the appropriate event defining when the action has to be launched.

In your own context, you will able to discover other ways to configure automated actions because the interface is flexible enough for you to configure the settings in the most logical or practical order you choose.

Configuration Policy Settings

Configuration policy settings provide the ability to define a set of information that can be attached to several nodes.

This is a way to create extensions for nodes by providing a new set of data and attaching new features to one node or to a group of nodes.

The configuration policies view is accessible for all users (see Figure 24).

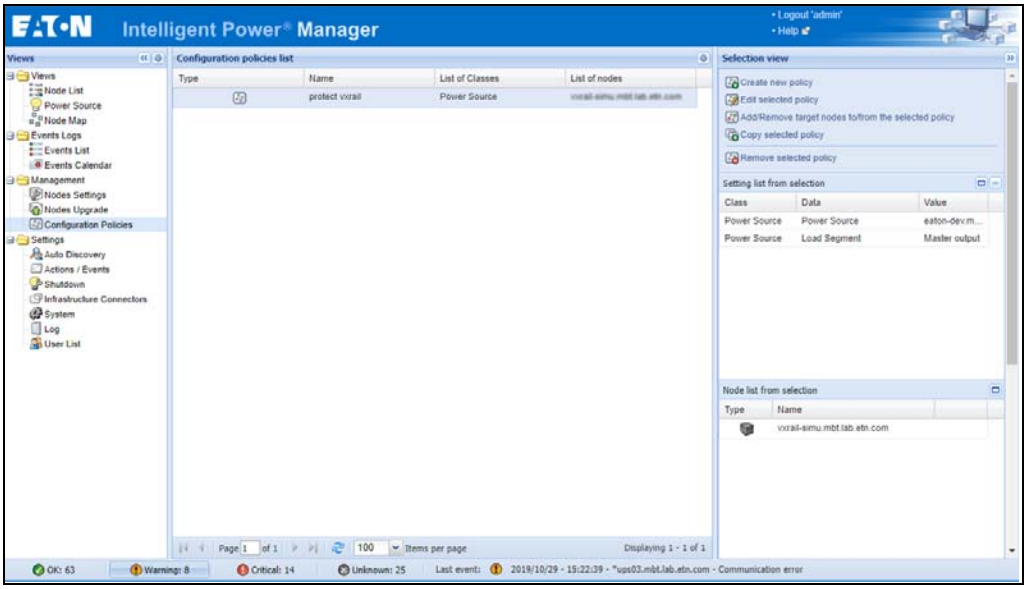

Figure 24. Configuration Policies View

To create a configuration policy, click over a selection of target nodes in any node list (see Figure 25). For example, if you intend to create a configuration policy and apply it to three well identified virtual machines, you can select those three VMs, right click on the selection, and select **Create new policy**. This opens the "Edit selected policy" dialog box with the target node field already initialized with the content of the selection (see Figure 26).

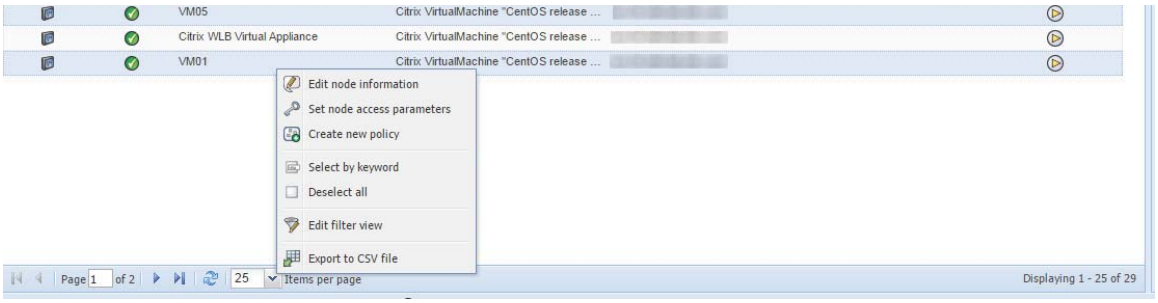

Figure 25. Node List Panel

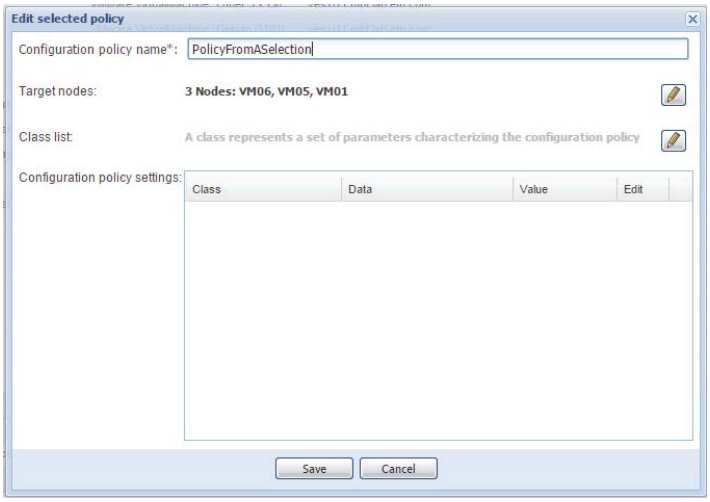

Figure 26. Edit Selected Policy Dialog Box

Configuration Policies Class

A class represents a set of parameters characterizing the configuration policies.

A list of predefined configuration policies classes are associated with a set of features, such as:

- Asset Information
- Runtime Threshold Settings
- Power Source
- User Settings

Dynamic Group For Configuration Policy

It is possible to edit a configuration policy by selecting a group of nodes. Therefore the configuration policy will apply to all nodes defined in this group.

- Groups are defined manually when creating a new policy. Nodes will be populated automatically to the group, by selecting a criteria on node properties.
- Nodes are automatically added or removed from the group regarding this criteria.

Use Cases

- When a discovery is launched, nodes are automatically attached to a group depending of their location, contact information, etc... removing manual operation requirements.
- When a VM is moved from a VMHost to another, its shutdown settings are automatically inherited from the configuration policy attached to its new power source.
- A modification on the device configuration automatically upgrades the configuration policy target list.
- Search string is flexible by using wildcard '*' and combination operator '|'.
- A node can be attached to several groups and therefore inherit from a combination of configuration policies.

Attachment Rules to an Automatic Assignation Group

A list of available node properties on which to check for matching:

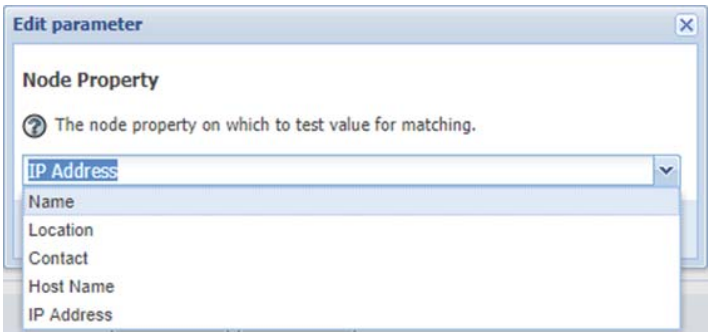

Figure 27. Available Node Properties

Table 3. Node Properties

Property Name	Usage
Name	• The node name can generally handle a large amount of information about the IT organization. • It can refers to infrastructure, services, etc... • Node name can be defined / overridden by the user in IPM. • Populating configuration policies regarding its content should be often used.
Location	Location usually matches with the facility infrastructure that is probably consistent with the power infrastructure.
Contact	Use of contact information can help to populate policies to target actions such as e-mail to specific users.
Host Name / IP Address	Relevant to populate policies regarding Network organization.

Populate the group regarding IP addresses:

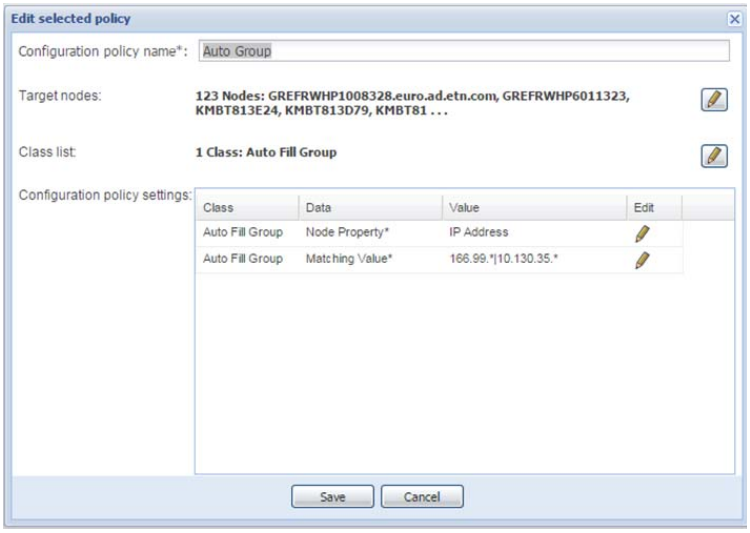

Figure 28. IP addresses

Populate group regarding Location:

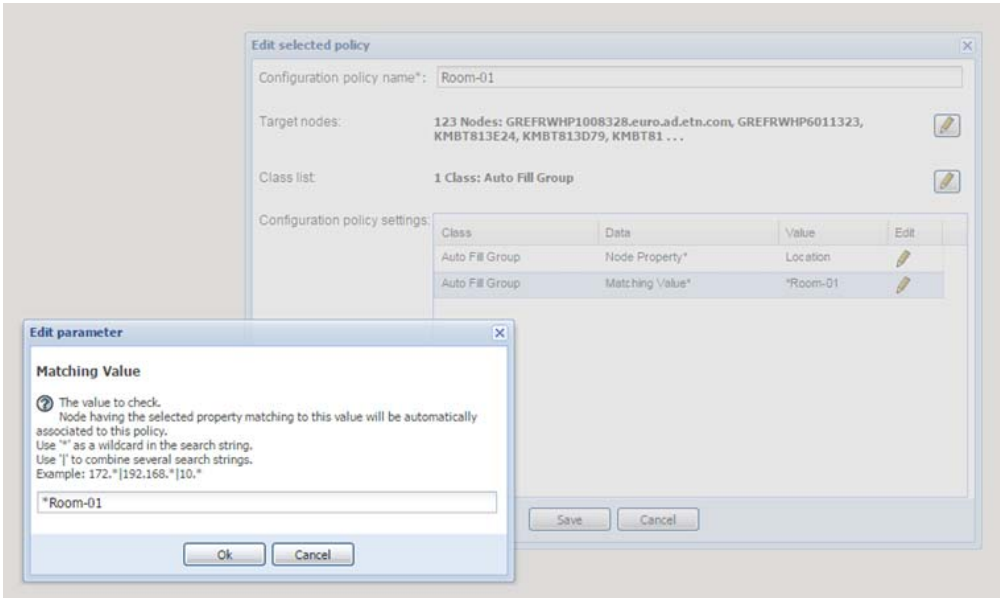

Figure 29. Location Parameter

Automatically attach servers to the UPS regarding their Location property and setup their shutdown settings.

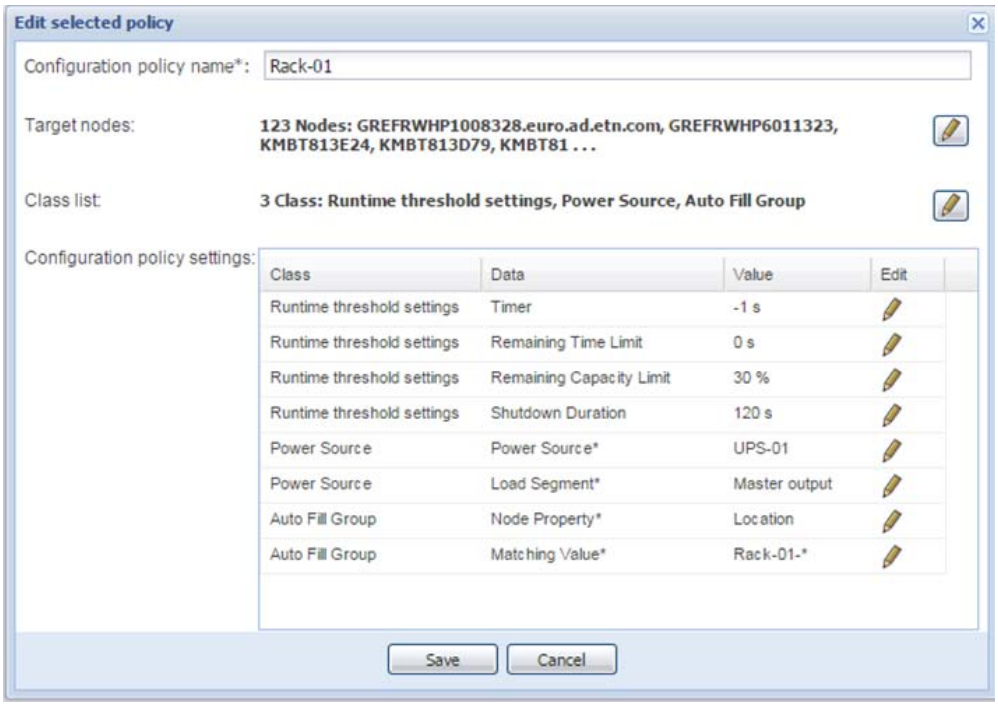

Figure 30. shutdown settings

Action Settings

From the ***Settings > Actions / Events*** menu item, notifications or executable actions can be set to occur as the result of specific Eaton IPM actions (see Figure 31).

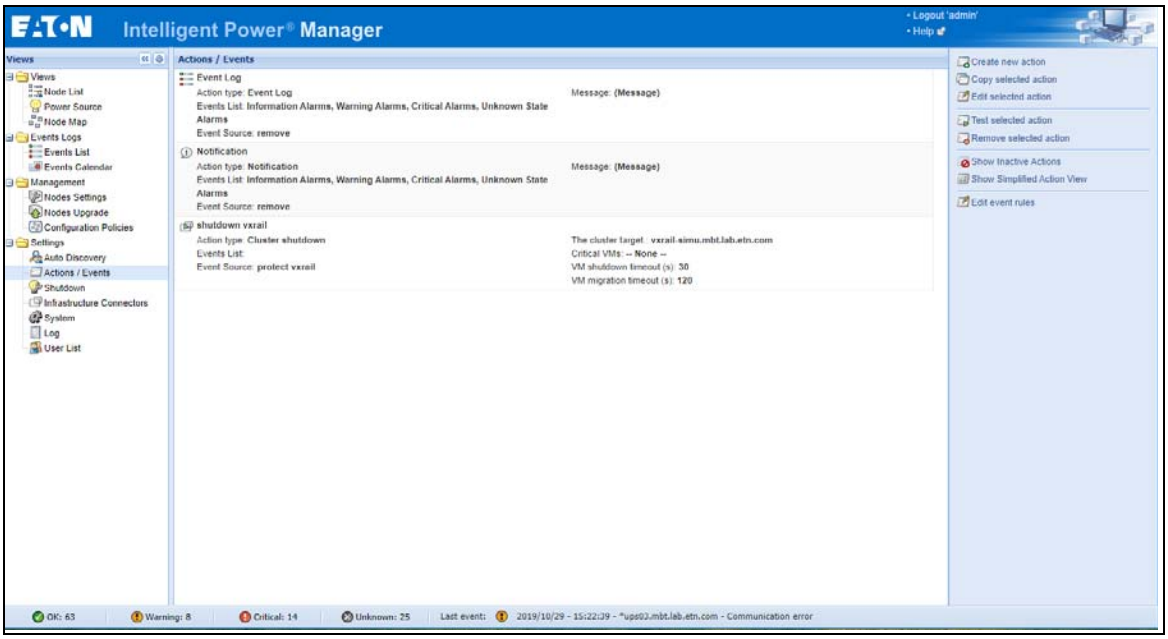

Figure 31. Actions / Events Settings

Create a New Action

A new action can be created by selecting the **Create new action** command. Use the "Create new action" dialog box to define all data for this new action (see Figure 32).

The following rules apply for mandatory fields:

- All red fields marked with the "*" character are mandatory and must be defined.
- An action cannot be saved if all mandatory fields are not defined.

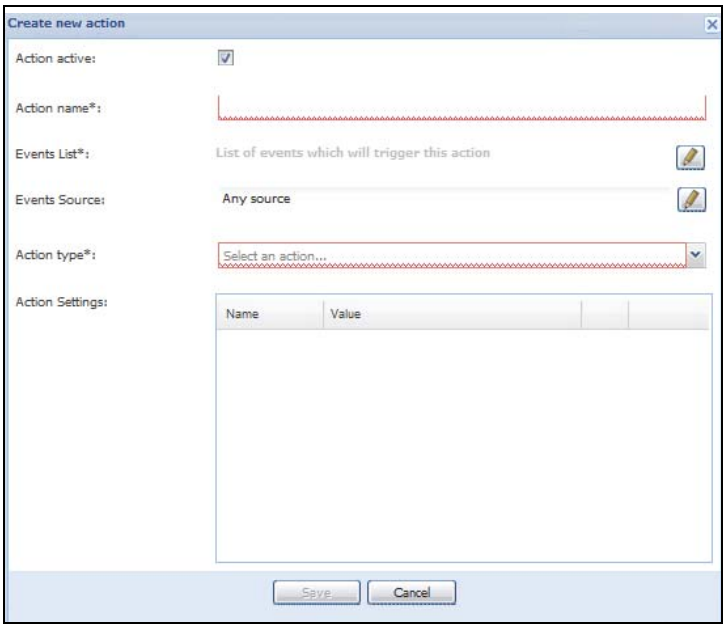

Figure 32. Create a New Action Dialog Box

An action has the following characteristics:

- **Name:** The name of the action. It cannot be unique.
- **Type:** Defines the sort of action that will be executed. (See "Action Type Descriptions" on page 43 for more details)
- **List of Events:** Establishes where this action will be executed. Events can be selected by pressing the pencil icon button next to the field and using the Associated Events dialog (see Figure 33).
- **List of Settings:** Differ in function from the selected action type.

Tool tips with information for each action setting are available on the 'Name' column.

All red fields marked with the "*" character are mandatory and must be defined.

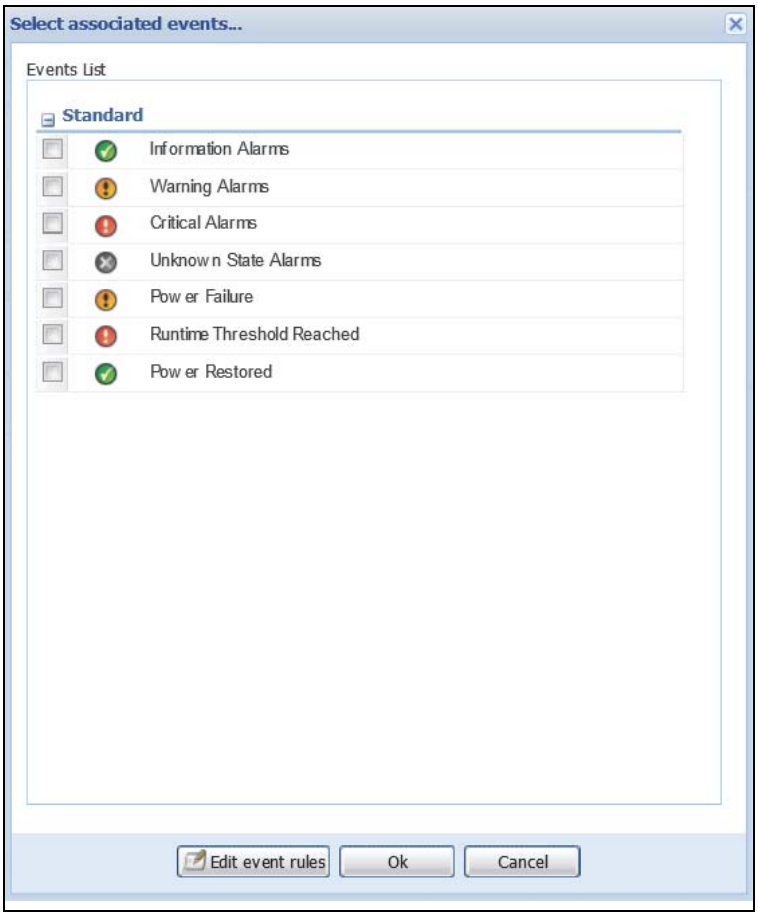

Figure 33. Associated Events

Edit Selected Action

In order to edit action settings from the Action settings grid, you must have already selected an action type. After the action type has been selected, there are two ways to edit an action setting:

- In the list of settings, press the icon button on the row of the setting to edit.
- Double-click the row of the setting in the Action settings list.

Each setting type has its own edit window. You can insert an Object by pressing the icon button on the right of the field displaying an object selector window (see Figure 34).

- Object are represented by a label between "{" and
- "}" characters.
- It is possible to insert an object at the focus place in the field or by replacing an array of highlighted characters.
- Use the button to insert an object. Do not write an object label directly in a field.
- After making all modifications, click **Ok** to save the new action.

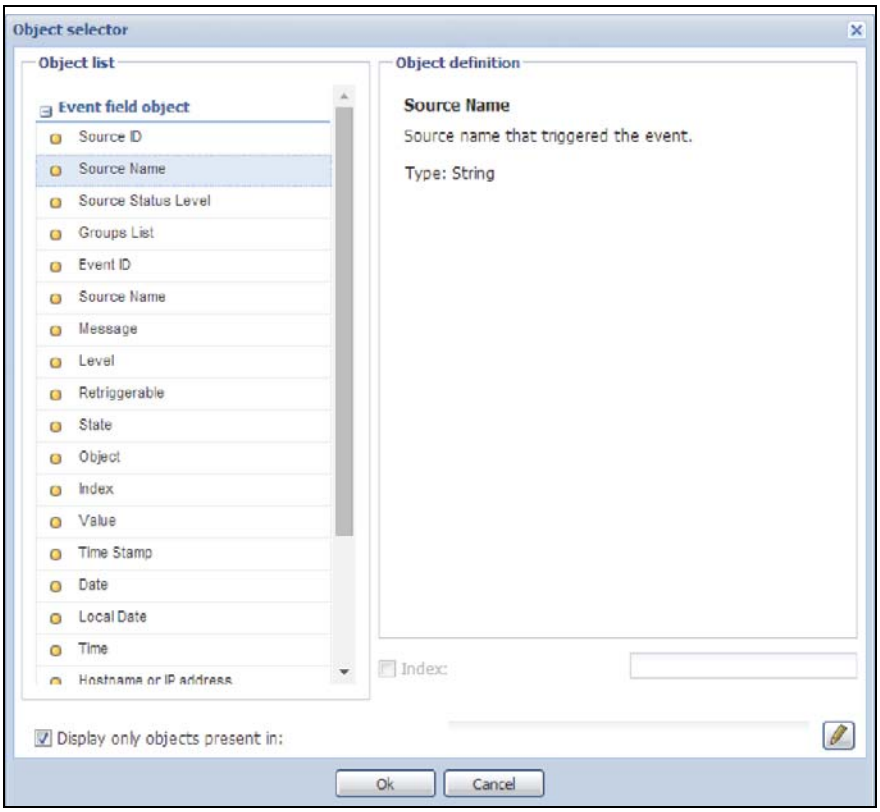

Figure 34. Object selector

Editing

After creating an action, it is possible to modify it later.

To edit an action:

1. Select the action to edit in the list of actions and selecting the "Edit selected action" command in the right panel (see Figure 35).
2. Double-click the action in the Action Settings panel (see Figure 36).

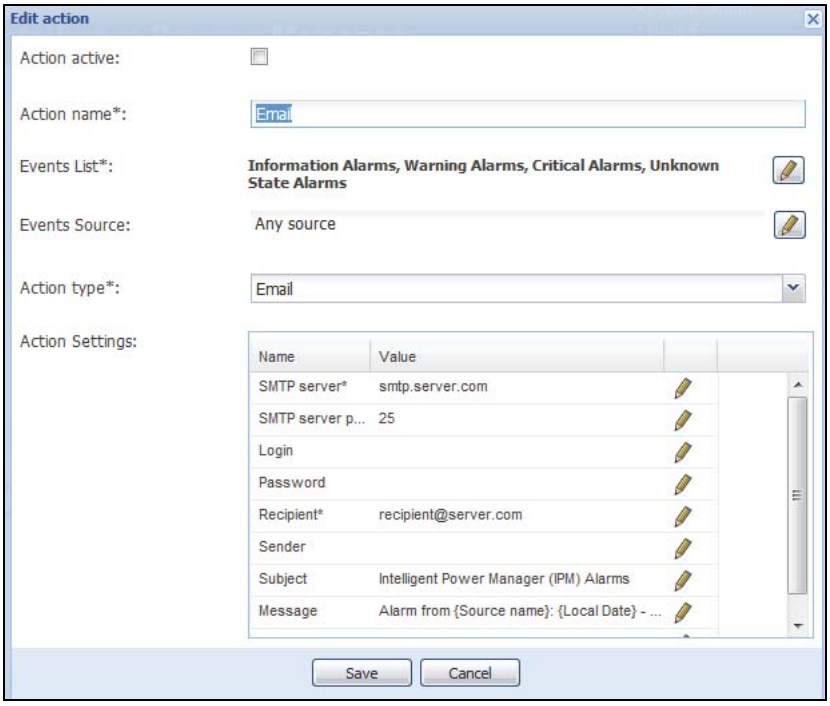

Figure 35. Editing a Selected Action

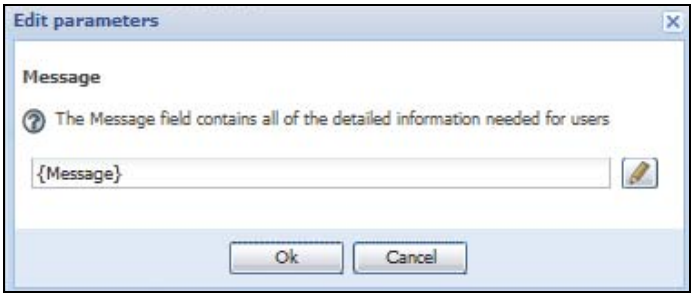

Figure 36. Edit Window for Messages

Then, the same window as shown in the creation process displays with all data from the selected action (see Figure 32 on page 38).

Copy

You can clone an action by selecting one in the list of actions and selecting the Copy selected action command.

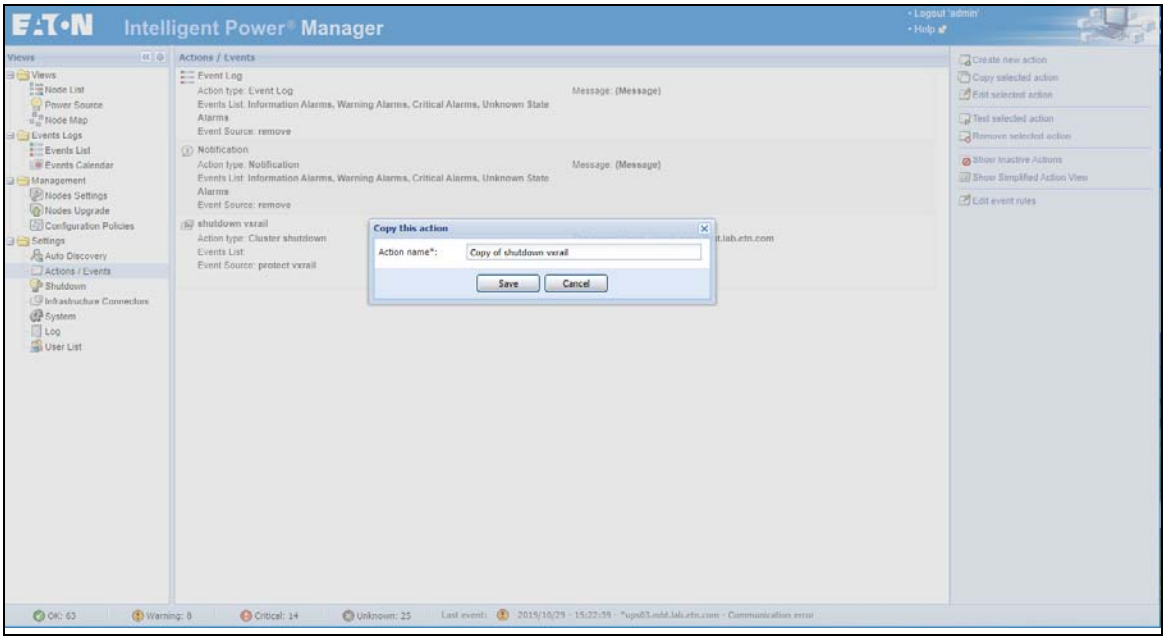

Figure 37. Copy This Action

The Copy this action pop-up dialog displays a default name that is predefined and can be changed to your choice (see Figure 37).

After saving a new action, it is listed on the Actions / Events page containing all the same data as the original action.

Test

An action can be tested by selecting the "Test selected action" command in the right panel.

Select Yes to launch the test on the action (see Figure 38).

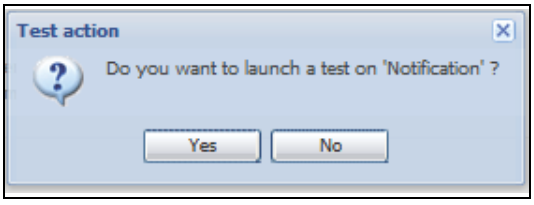

Figure 38. Test Action

Remove

You can delete an action by selecting one in the list of actions and selecting "Remove selected action" command in the right panel.

A pop-up window provides a validation message for the remove process.

Click **Yes** to remove the selected action (see Figure 39).

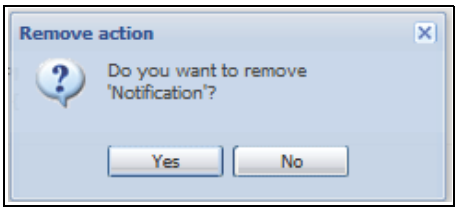

Figure 39. Remove Selected Action

After confirming, the selected action is removed from the list of actions.

Action Type Descriptions

Each action is defined for a definite purpose:

E-mail

E-mail actions need parameters such as the SMTP Server and recipients data provided by e-mail addresses.

You must indicate the SMTP server address and recipient e-mail address. Both logins and passwords are used when the SMTP server requests authentication.

You can select between two modes (SSL or TCP) depending on your SMTP server capabilities and your deployment constraints.

For advanced use:

- Optional: You can customize the Subject, such as when you use a third-party service provider to translate e-mail into SMS.
- Optional: You can specify that you want to receive a consolidation of the alarms that occurred during a delay time duration (Digest period). For example, if you specify none, each alarm generates an e-mail. With this setting, you will receive more e-mail for the same number of events.

Command

The command is executed by the supervision application when an action is triggered.

In order to execute a program on UPS events, the program path is required. The program is executed under the SYSTEM account.

- If an action (script or program) cannot be executed under the SYSTEM account, it is necessary to modify the execution context before it can run.
- To allow a user to run specific tools and programs with permissions that are different from those assigned to the user's account, use the Windows "Run As" command. This allows you to save the password (Windows XP Service Pac 2 and more recent versions).
- Use the following Microsoft command:
- > runas /profile /user:<windows_ login> /savecred <my_program.exe>
- When first executed, a password is required; it is saved for subsequent executions.

SSH Action

To launch a command on an SSH server, type the host name, port, a valid credential, and the command itself. This action is suitable, for example, to remotely shut down any SSH enabled server or storage without an agent.

Notification

Notification produces a one line message displayed in the "Notifications" window. It is not necessary to include the date and the origin object name of the action in the message as they are included in the notification.

Event Log

This action provides an event message to the node event list.

Host Power Action

This action executes a power command on the host target. A power command can be ShutdownHost, ShutdownVMsThenHost, EnterMaintenanceMode, EnterMaintenanceModeThenShutdown, ExitMaintenanceMod, EnterStandByMode or ExitStandByMode.

VM Power Action

This action executes a power command on a VM. A power command can be power on, power off, guest shutdown, or suspend. Note that these actions are only available for VMware virtualization infrastructure.

VM Migrate Action

This migrates a virtual machine from its host to another host.

vApp Action

Allows you to start, shut down, or suspend a whole vApp in one action.

Start a Recovery Plan

This starts a recovery plan in failover mode. The SRM module must be active. Choose a recovery plan of a RECOVERY site.

Power Capping

This action initiates a power capping action on a hardware server. HPE OneView connector must be configured first. This action is applicable on HPE servers retrieved by the connector HPOV.

Storage Action

Currently one storage action is available: shutdown. It allows you to seamlessly shut down a storage or a set of several storages (via policies). This procedure replaces the "Start a Recovery Plan" procedure required in earlier IPM versions.

Cluster Shutdown

Parameters

1. Cluster target: the vCenter that manages the infrastructure to shut down
2. Critical group: select the configuration policy for all critical VMs to subscribe to. Those VMs are shut down last and restarted at start up.
3. VM shutdown timeout: maximum time allowed for non-critical VMs shutdown
4. VM migrated timeout: maximum time allowed for critical VMs migration

Usage Sum-up

1. Create a configuration policy (***Management > Configuration Policies***).
2. Type the name you want (e.g., CriticalLoad).
3. Select the VMs as target nodes to:
   - Stop the latest
   - Restart automatically when power is back

   IPM and vCenter do NOT need to be put in this configuration policy.
4. Create a new action (***Settings > Action / Events***).
5. Type an Action Name (e.g., Shutdown-Infra).
6. Select the Action Type **Cluster shutdown**.
7. Select the vCenter you want to protect as the first parameter.
8. Select the critical workload as the second parameter by choosing the configuration policy you created in Step 1.

   If it doesn't show up in the available choices, check that:
   - It is in the list of configuration policies ***Management > Configuration Policy***
   - It applies to at least one VM
   - You have the appropriate license level to benefit from this advanced feature
9. Check that the two timeout default values are suitable for your needs.
10. If the timeout value is incorrect, type it in seconds in the corresponding field.
11. Click **Save**.

Cluster Shutdown and Restart Workflow

Cluster Shutdown Scenarios Supported by IPM:

- Cluster Shutdown for VMware
- Cluster Shutdown for VMware HA +DRS
- Cluster Shutdown for VMware vSAN
- Cluster Shutdown for Dell/EMC VxRail

Critical VMs definition:

- **Shutdown Management VMs** (vCenter and IPM) shown with Orange icons
  vCSA_6.5
- VMs from a configuration policy that are defined in a Cluster shutdown as Critical. These VMs are chosen by user and will be shut down as late as possible.

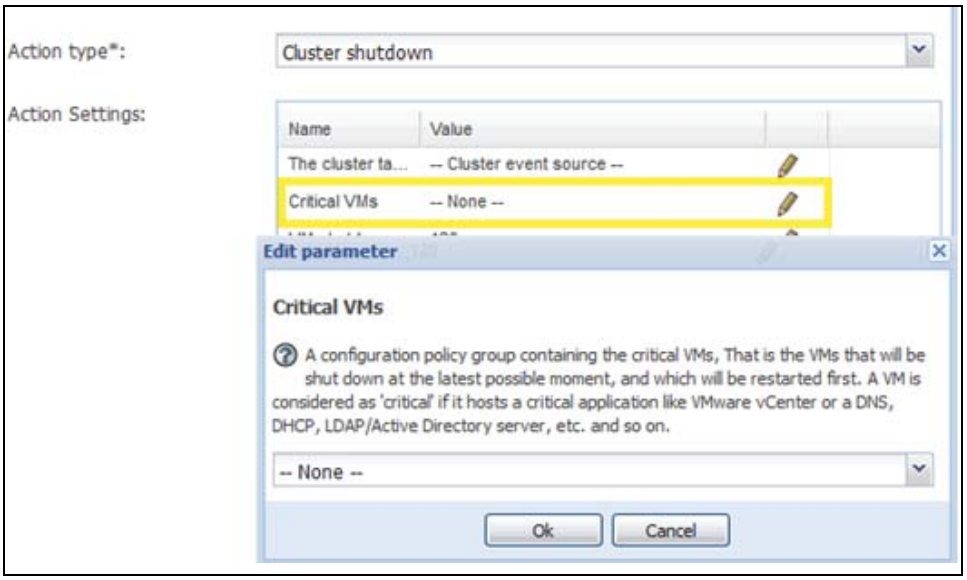

Figure 40. Cluster Shutdown

Cluster Shutdown for VMware

Shutdown Workflow without Critical VMs or Shutdown Management VMs

- Guest shutdown of all VMs
- Shutdown all ESXi once the **VMs shutdown timeout** has been reached
- End of scenario

Startup

- The VMs will restart following the configuration of each ESXi **Auto start/stop VMs**

NOTE You can use the System Startup State object from custom events combined with the Grace Period to power on the remaining VMs as soon as vCenter is up and running.

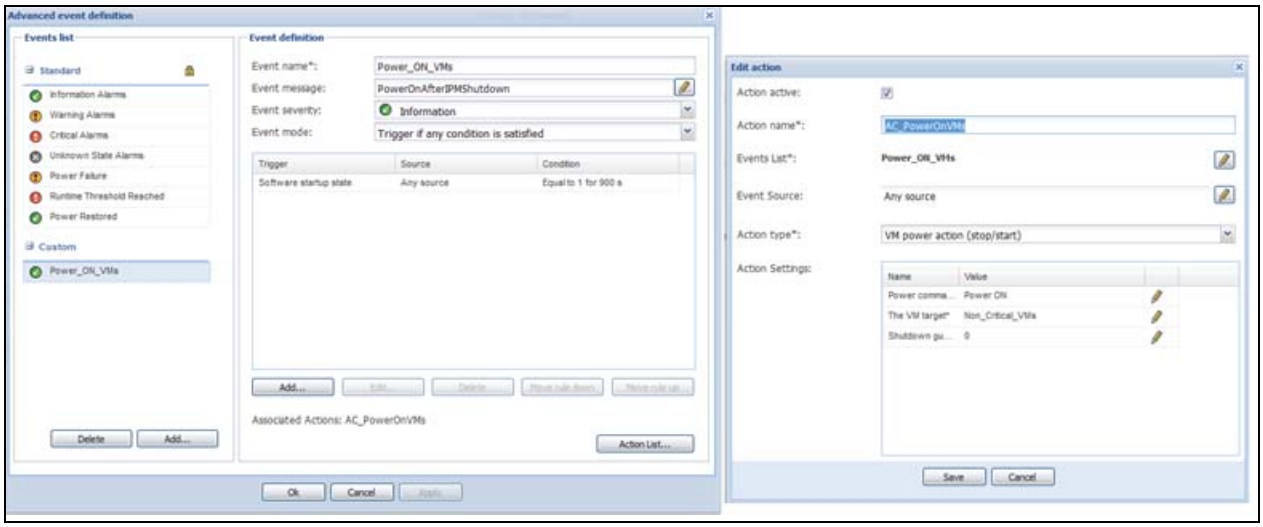

Figure 41. Cluster Shutdown for VMware

Shutdown Workflow with Critical VMs or Shutdown Management VMs

Shutdown Management VMs are detected automatically by IPM, no need to add them to the Critical VMs policy.

- Guest shutdown all non-critical VMs
- Once "**VM shutdown timeout**" has been reached IPM will choose the ESXi that will shut down the latest

Make sure that all the ESXi are able to host all critical and shutdown management VMs.

NOTE vCenter, IPM and critical VMs should run on the same ESXi

1. The ESXi hosting vCenter
2. The ESXi hosting IPM
3. The ESXi hosting the more critical VMs
   - Migrate critical VMs to the chosen ESXi
   - Once the "**VM migration timeout**" has been reached, IPM will reconfigure "**Auto start/stop VMs**" of the chosen ESXi adding the critical VMs
   - Shutdown all ESXi except the chosen one.
   - Shutdown latest ESXi (VMs will be gracefully shut down by VMware)
   - End of scenario

Startup

- Critical VMs will restart automatically as IPM added to ESXi "**Auto start/stop VMs**" configuration.

NOTE You can use the System Startup State object from custom events combined with the Grace Period to power on the remaining VMs as soon as vCenter is up and running.

Cluster Shutdown for VMware HA + DRS

Shutdown Workflow without Critical VMs or Shutdown Management VMs

- Guest shutdown of all VMs
- Shutdown all ESXi once the "**VMs shutdown timeout**" has been reached
- End of scenario

Startup

- The VMs will restart following the configuration of each ESXi "**Auto start/stop VMs**"

NOTE You can use the System Startup State object from custom events combined with the Grace Period to power on the remaining VMs as soon as vCenter is up and running.

Shutdown Workflow with Critical VMs or Shutdown Management VMs

Shutdown Management VMs are detected automatically by IPM, no need to add them to the Critical VMs policy.

- Change DRS mode
- Disable HA
- Guest shutdown of all non-critical VMs
- Once "**VM shutdown timeout**" has been reached IPM will choose the ESXi that will shut down the latest

1. The ESXi hosting vCenter
2. The ESXi hosting IPM
3. The ESXi hosting the more critical VMs
   - Migrate critical VMs to the chosen ESXi
   - Once the **VM migration timeout** has been reached, IPM will reconfigure **Auto start/stop VMs** of the chosen ESXi adding the critical VMs
   - Shutdown all ESXi except the chosen one.
   - Shutdown latest ESXi (VMs will be gracefully shut down by VMware)
   - End of scenario

Startup

- Critical VMs will restart automatically ‘as IPM added to ESXi **Auto start/stop VMs** configuration.
- Once IPM service is restarted, IPM will enable HA + DRS.

NOTE You can use the System Startup State object from custom events combined with the Grace Period to power on the remaining VMs as soon as vCenter is up and running.

Cluster Shutdown for VMware vSAN (vSAN Stretched Cluster not supported)

Prerequisite

Shutdown Management VMs (IPM and vCenter) Out of the Cluster

Shutdown Workflow without Critical VMs (HA Disabled)

- Guest shutdown of all VMs
- Once **VM shutdown timeout** has been reached IPM will put host in maintenance mode with **No Action** option for all ESXi in sequential order.
- Shut down all ESXi hosts

Startup

- Customer exit ESXi from maintenance mode
- Customer Power On VMs
- Shutdown workflow with critical VMs (HA disabled)

NOTE This scenario is partially implemented, Critical VMs will not be gracefully shut down.

- Guest shutdown of all non-critical VMs
- Once **VM shutdown timeout** has been reached, the scenario is finished.

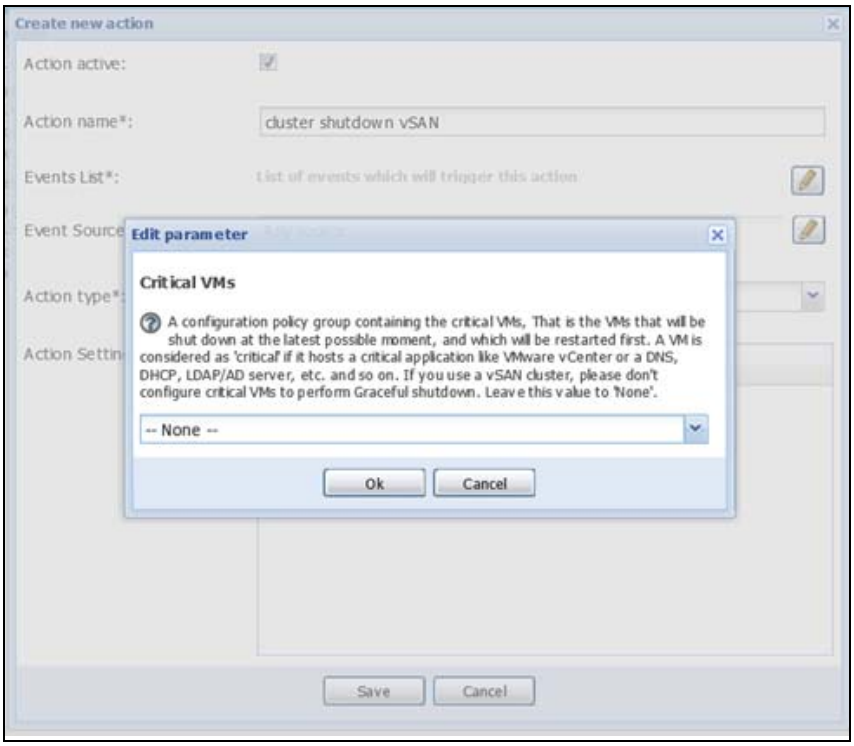

Figure 42. Create Action for vSAN Cluster Shutdown

NOTE vSAN Cluster shutdown with virtual IPM or vCenter within the cluster is not supported.

Cluster Shutdown for Dell/EMC VxRail

Prerequisite

1. IPM version 1.67 and higher.
2. IPM is embedded in the VxRail Cluster: IPM OVA is deployed on the same vCenter as the one managing the VxRail Cluster.
3. VxRail Software Manager version 4.7.000.
4. VxRail Cluster protected by an Eaton UPS managed by an Eaton Gigabit Network Card (FW version 1.7.0 and higher).
5. Dell/EMC VxRail connector configured in IPM (for more details about connector configuration and policy configuration, see "Eaton Solution for Dell/EMC VxRail Cluster" on page 104.
6. No container running on the cluster.

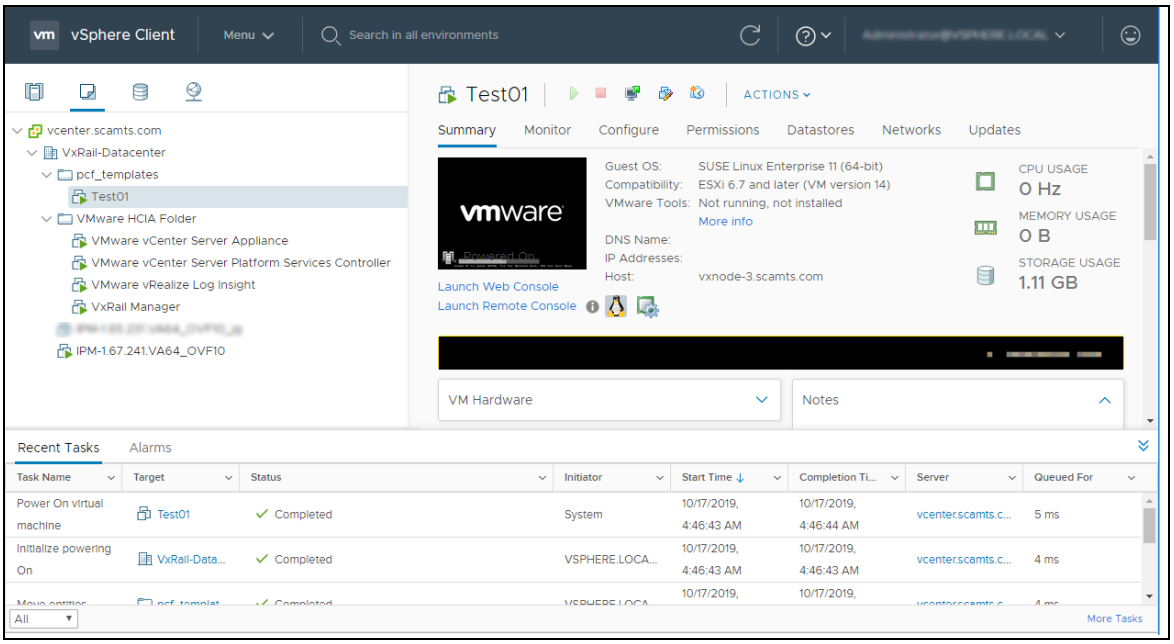

Figure 43. IPM OVA Deployed on VxRail vCenter

Shutdown Workflow with Critical VMs and Management VMs

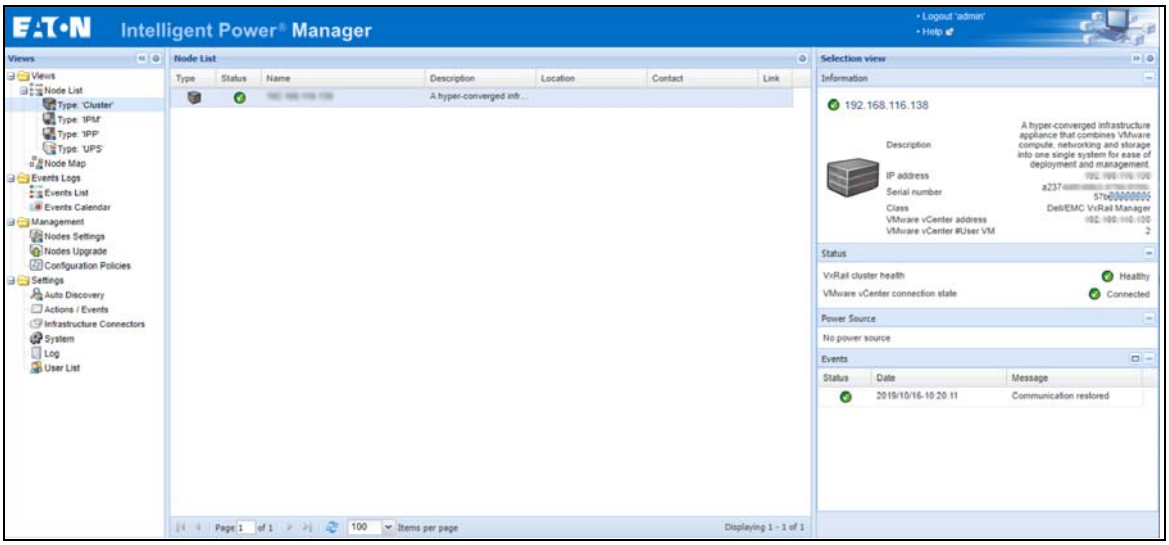

Figure 44. VxRail Cluster Monitoring

System VMs are hidden in IPM UI to prevent users from configuring unsupported actions on them. Only the VxRail Cluster is displayed in IPM.

User VMs and management VMs are detected automatically by IPM, there is no need to add them to the critical VMs in the Configuration Policy.

Shutdown sequence:

1. Guest Shutdown User and Business VMs: Shutdown first (non-critical then critical).
2. IPM orders the Eaton Gigabit Network Card to schedule the Cluster shutdown.
3. Shutdown IPM VM.
4. Eaton Gigabit Network Card requests the VxRail Cluster shutdown API endpoint.
5. Shutdown System/management VMs (managed by the VxRail software manager):
   - VMware vCenter Server Appliance
   - Vmware vCenter Server Platform Services Controller
   - VxRail Manager
   - VMware vRealize Log Insight
   - ESRS_VE.x86_64
6. End of scenario.

NOTE Cluster shutdown cannot start if VMs are still running on the cluster:

- IPM does not support shutdown of the container.
- Execution logs of Cluster shutdown are available from the Eaton Gigabit Network Card (Card Menu/System logs/Download System logs/File name: System)
- IPM does not support the restart of the cluster.

Events

There are two types of events:

- Standard events, which are available to all users
- Custom events, which are available only to users having a Silver or a Gold license.

The following section provides the detailed information about custom events configuration. From the **Settings > Actions / Events** menu item, it is possible to manage advanced events by selecting the "Edit event rules" command on the right panel. The window also displays standard events, but it is just for supervision. They cannot be modified.

An event comprises the following:

- **Event Name:** The name of the event. Events can be grouped together by writing a group name just before the event name and separate from it by a pipeline (|) character. Subgroups are not managed. For example, "NewCustomEvent|event_1" name define the event named'event_1" in a group named "NewCustomEvent."
- **Event Message:** The message to display when the event occurs. An object can be inserted in the message by using the button next to the field displaying an object selector window.
- **Event Severity:** Defines the severity of the event between these gradual choices: "None," "Information," "Warning," "Critical," and "Unknown.
- **Event mode:** Defines the condition for the event to occur in function of its rules. There are two choices:
  - Trigger if all conditions are satisfied: all rules must be satisfied.
  - Trigger if any condition is satisfied: one of the rules is satisfied.

All rules that must be satisfied for the event to occur. (See "Event Rules" on page 53 for more details.)

The order of rules in the grid define the condition order for the event to occur.

To manage and define rules, use the following buttons below the grid:

- **Add...**: Add a new rule
- **Edit...:** Edit the selected rule
- **Delete...** Delete the selected rule(s)
- **Move rule down:** Move the selected rule to a lower position in the table
- **Move rule up:** Move the selected rule to a higher position in the table

A list of associated actions: Actions are launched when the event occurs. The event will appear in the list of events of these selected actions (see "Create a New Action" on page 38). Actions can be selected by using the Action List button displaying an action list configuration window (see Figure 45).

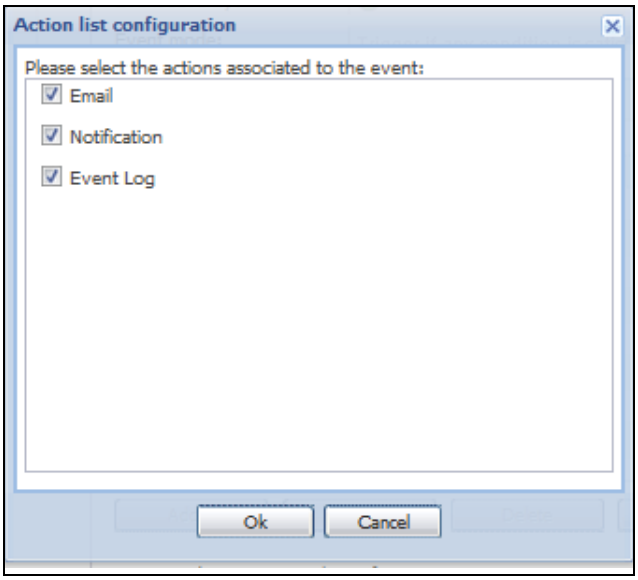

Figure 45. Action List Configuration

Event Rules

The Rule editor dialog allows you to create (add) or edit a rule. As part of defining the relationship between a source object name and a destination object name, condition rules, and parameters are selected and applied in this dialog (see Figure 46).

The Rule editor dialog is obtained by selecting a rule of a custom event, then clicking Edit, (or directly by double-clicking on it). This functionality is not available when the license is basic (no possibility to add custom events).

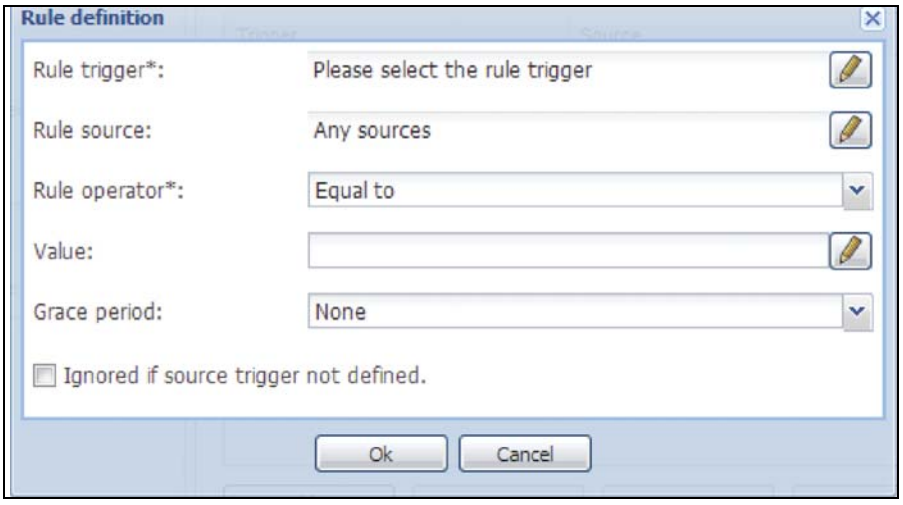

Figure 46. Rule Definition

A rule comprises the following:

A trigger: The destination object that will be triggered by the rule (see "Triggers" on page 54 for more details). An object can be defined using the button next to the field displaying an object selector window.

A source: The source object that will be used to evaluate the rule. It could be a device or a configuration policy. A rule can also have a relationship with any sources. An object can be defined using the button next to the field displaying a source selector window.

An operator: The source object that will be used to evaluate the rule. It could be a device or a configuration policy. A rule can also have a relationship with any sources. An object can be defined using the button next to the field displaying a source selector window. Available operators are:

- **String:** "Equal to," "Different from," "Contains," or "Not contains"
- **Number:** "Equal to," "Different from," "Greater than," "Lower than," "Greater or equal to," or "Lower or equal to"
- **Boolean:** "Equal to" or "Different from"

A value: The comparison value for the operator. This value can also be an object that can be defined using the button next to the field displaying an object selector window.

A grace period: Establishes a predefined period of time before the trigger event. The period must be between 0 to 300 seconds. A rule can be set to be ignored if its source trigger object is not defined on the node.

Triggers

The trigger base contains a list of objects with their trigger characteristics.

- **Types:** This lists objects able to trigger an event. Object can be associated with an item (node or configuration policy) or can be global.
- **Info *(scope: node):*** This lists objects able to trigger an event. Object can be associated with an item (node or configuration policy) or can be global.
- **Alarms *(scope: node):*** Objects used to display information, such as a name, a location, a node ID, a configuration policy, and so forth.
- **Measures *(scope: node):*** Number objects related to a measure of current, voltage, power, time, temperature, humidity, or a percentage rate.
- **Virtualization *(scope: node):*** All objects related to the virtualization, such as VM Host & VApp parameters (name, path, state...), VM Name & Path.
- **User Objects (*scope: node*):** User objects are defined through user driver definition.The trigger type will be defined by the user object definition.
- **Configuration Policy Objects *(scope: configuration policy):*** Triggers issue from configuration policy objects. Can be used as comparison value.
- **Events *(scope: node/configuration policy/system):*** Events can be used as trigger of another event.
- **Date *(scope: system):*** All objects defined a date, a time, a day in the week, or in the month.
- **System *(scope: system):*** Events triggered by the MC2 application.

Object Selector Help

The Object Selector lists all available objects that can be used as a trigger or as a reference value. It contains a hierarchical list of:

- **Nodes Triggers:** The trigger list with the scope "node."
- **Event Triggers:** Predefined events and user defined events.
- **Global Triggers:** The global trigger list.
- **User Defined Objects:** Objects defined through generic driver.
- **Configuration Policy Attributes:** Attributes defined through configuration policy class definition.
- **Action Result Status:** Result status returned by actions having feedback capability.

When the object is indexed, it is possible to select any index value or a specific one. There is no control on the object index capability.The object info help text is provided for all well-known objects. It provides the object description and possible values.

You first make the selection from the Rule Definition value list to display a trigger list or a reference value list. Then you make a selection from the object list. For example, in the figures that follow, the Object selector displays with from either the ***Rule Trigger>Utility present*** selection or the ***Value>{Shutdown timer}*** selection (see Figure 47 or Figure 48).

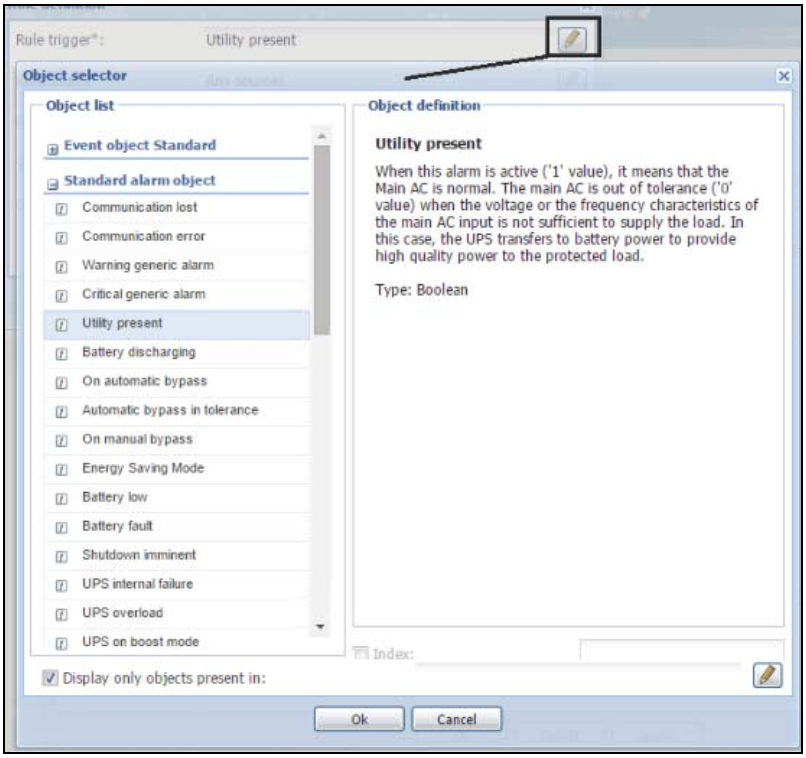

Figure 47. Object Selector (Rule Trigger)

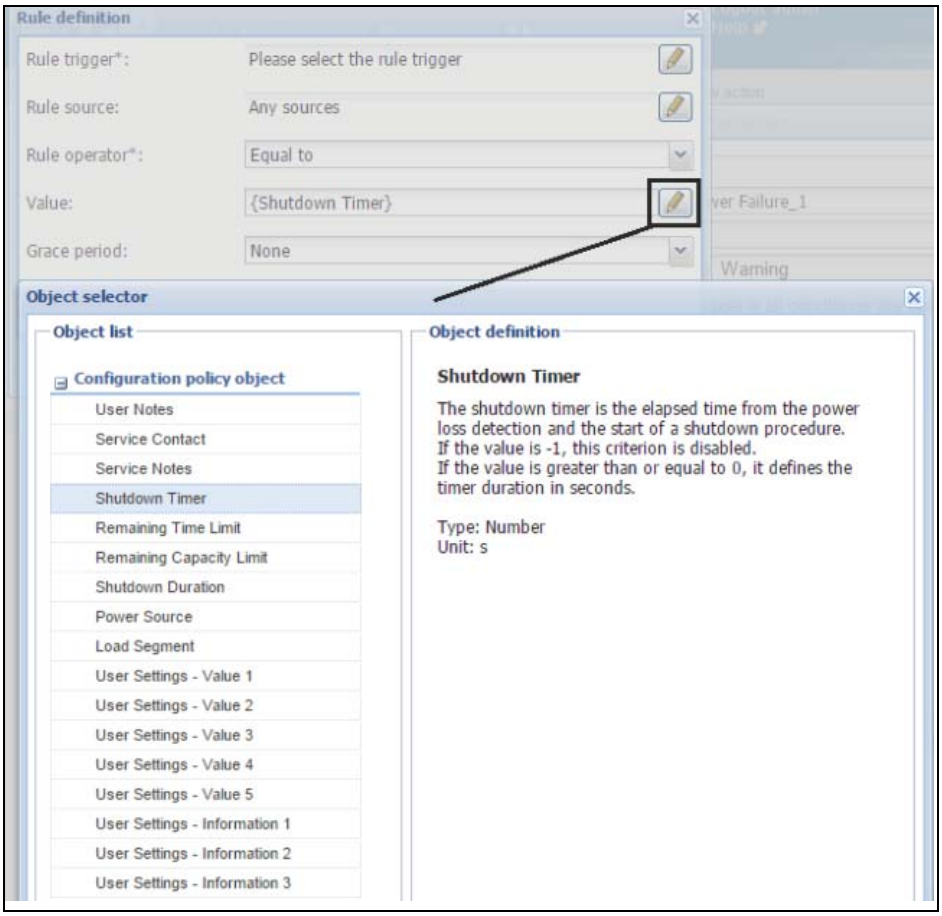

Figure 48. Object Selector (Value)

It contains a hierarchical list of:

- **Nodes Triggers:** The trigger list with the scope "node" listed above.
- **Event Triggers:** Predefined events and user defined events.
- **Global Triggers:** The global trigger list listed above.
- **User Defined Objects:** Objects defined through generic driver.
- **Configuration Policy Attributes:** Attributes defined through configuration policy class definition.
- **Action Result Status:** Result status returned by actions having feedback capability.

When the object is indexed, it is possible to select any index value or a specific one. There is no control on the object index capability.

The object info help text is provided for all well-known objects. It provides the object description and possible values.

Alarm Box Notification Actions

The alarms are displayed on the local computer in an alarm box (see Figure 49). The status portion of the alarm box is optional. It only appears if a power source has been declared in the Runtime configuration settings.

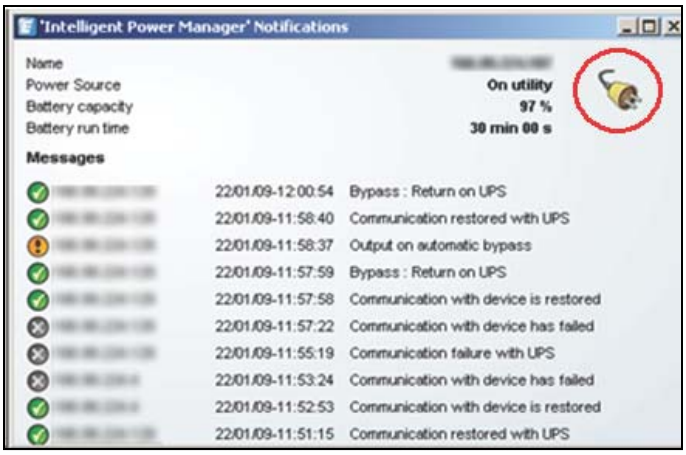

Figure 49. Alarm Notification Box with System Tray Icon

The Alarm notification box is accessible from the System Tray icon (see Table 4 and Table 5). Click the icon to open the window that displays the alarms on the local computer.

System Tray Icons

If no Power Source has been declared, the System Tray Icon will have the states described in Table 4.

Table 4. System Tray State Icons (Power Source not Declared; Shutdown module disabled)

Icon	State Description
	(BLUE) The System Tray Icon correctly receives alarms from Eaton IPM.
	(GRAY) Communication is lost between the System Tray and the Eaton IPM.

If a Power Source has been declared, the System Tray Icon will have the states described in Table 5.

Table 5. System Tray State Icons (Power Source Declared)

Icon	State Description
	The System Tray Icon correctly receives alarms from the Eaton IPM. AC is present on the power source.
	The System Tray Icon correctly receives alarms from the Eaton IPM. The power source runs in battery mode.
	The System Tray Icon correctly receives alarms from the Eaton IPM. A Warning event occurred on the power source.
	The System Tray Icon correctly receives alarms from the Eaton IPM. A critical event occurred on the power source.
	Communication with the power source has failed.

NOTE Right-click the System Tray icon for fast access to the start and stop operations.

Typical Use Cases Configuration

See Appendix A for example procedures that typify use cases configuration steps.

Advanced Use Cases Configuration

Advanced Events and Actions Customization

In the IPM installation folder, you can see a configs/scripts folder containing a sample user-defined action script (`sample_user_script.js`).

You can modify this script or create new scripts that define very specific events and actions. The sample script in this folder provides details about the expected structure and syntax for defining new actions and triggers.

Advanced Sound Alarm Customization

To configure sound alarms on events:

1. In the file {`INSTALL DIRECTORY}\Eaton\IntgelligentPowerManager\configs\config.js`, change the configuration as follows:

```
'systray':
{
    'soundAlarm': false,
    'notificationIcon': true,
    'notificationBox': true
}
```

2. Change 'soundAlarm': false, to 'soundAlarm': true, as shown below:

```
'systray':
{
  'soundAlarm': true,
  'notificationIcon': true,
  'notificationBox': true
}
```

3. Close and restart the Windows session so that this configuration is taken into account.

NOTE 1 You can change the alarm sound by setting the Windows sound preferences from the Control Panel.

NOTE 2 The Eaton IPM alarms are linked to the audible "Low Battery Alarm" alarm sound that you can change by selecting another wav. file.

Chapter 5 Supervision

This chapter describes supervision features in the Eaton Intelligent Power Manager (IPM).

Access to the Monitoring Interface

You can access the interface locally or remotely.

Local Access

From the system where Eaton IPM is installed, you can use the following shortcut:

Start > Programs File > Eaton > Intelligent Power Protector > Open Eaton Intelligent Power Manager

Remote Access

1. From a remote computer, you can type either of the following URLs in a Web browser:

   https://<name or IP address of computer hosting Eaton IPM>:4680/

   -or-

   http://<name or IP address of computer hosting Eaton IPM >:4679/
2. In SSL mode, accept the certificate using the procedure provided by your Browser.
3. Enter the login and password.

Node List View

The Node List view results from the ***Settings > Auto Discovery*** menu item selection. The following default columns are displayed on this page (see Figure 50):

- **Type:** Graphical icon to differentiate UPS/ePDU and applications
- **Status:** Status icon represents the severity of the most critical event active on the monitored device
- **Name:** IP address, the DNS name or user-defined name
- **MAC Address:** MAC address
- **Class:** Type of management software
- **Location:** Node location
- **Contact:** Node contact
- **Access:** Graphical icons located on the left of the login indicating "Access denied" or "Access OK,"
- **Link:** Link to the device Web site (if available)
- **Creation Date:** The date the node was created in the node list. This is used by default to sort the list (the most recent items created appear first in the list)

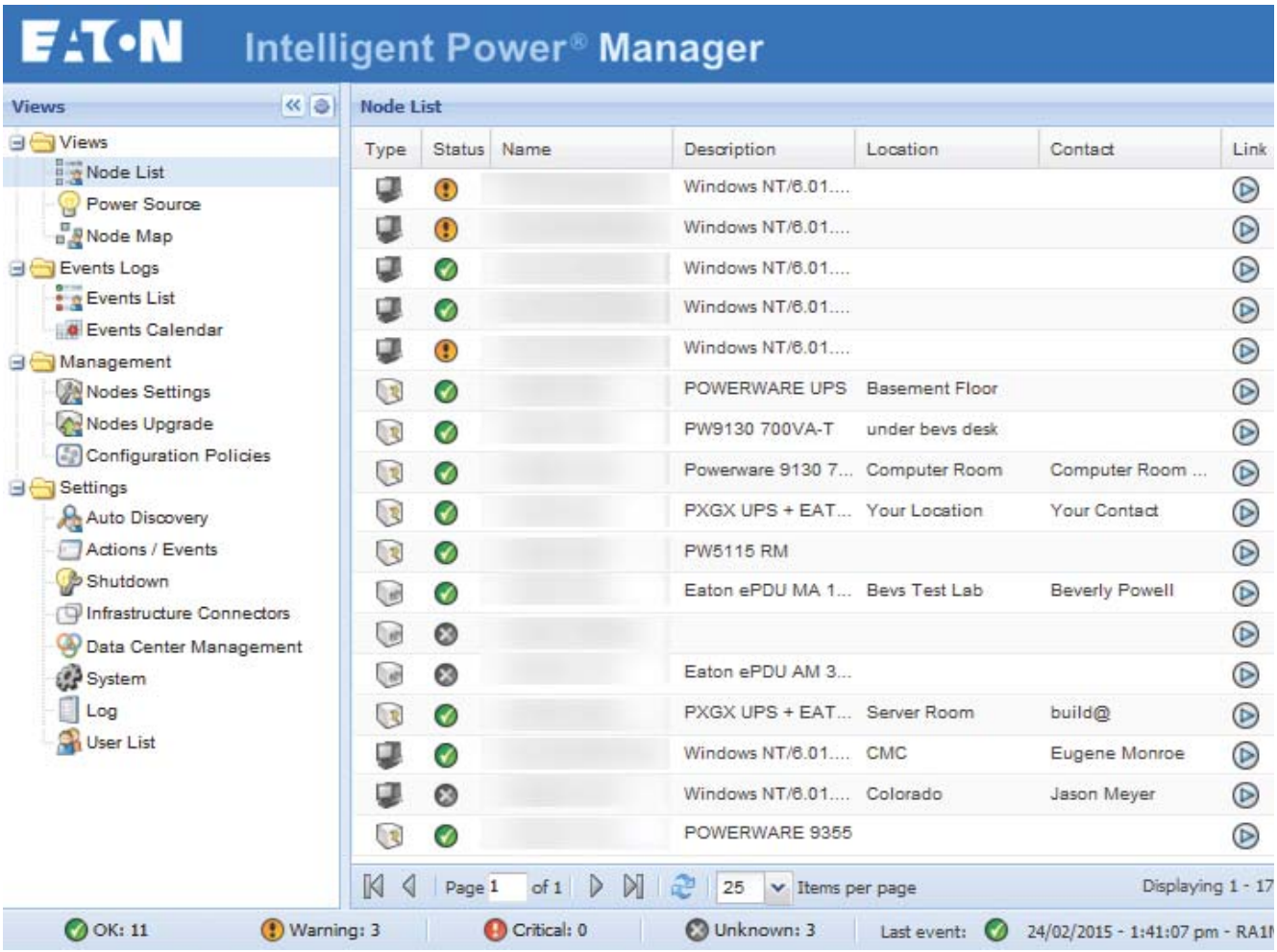

Figure 50. Node List View

You can sort (ascending or descending) your device list by clicking the column titles (Status, Name, Description, Location, Load Level, etc.). You can also add columns, as illustrated in Figure 51.

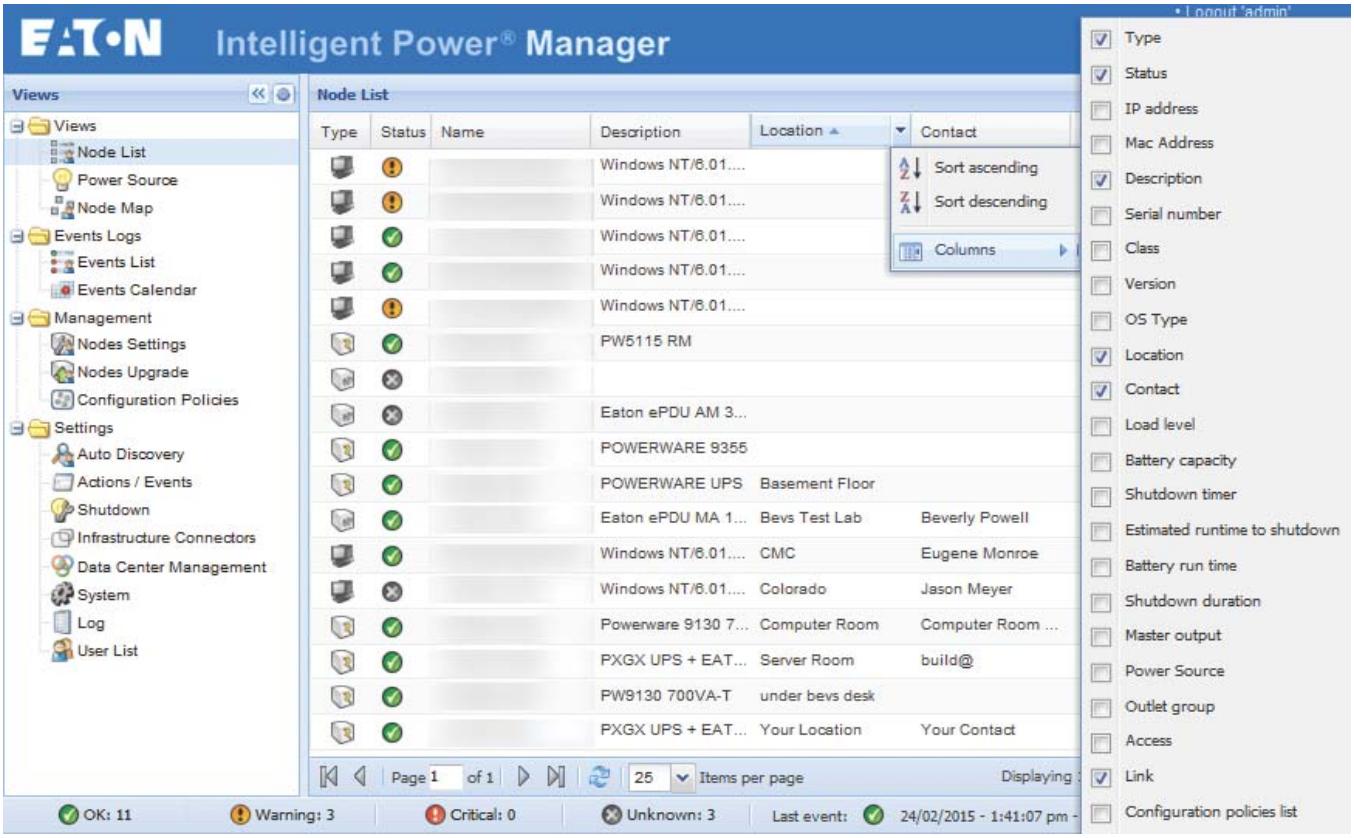

Figure 51. Adding Columns in Node List View

Flexible Panels View

To select which panels display in the view:

1. Select a device/applications in the list and Select panels displays in the right side of the window.
2. Click the bar title to collapse/extend the panel.
3. You can also show or hide all the views menu or selection view menu.
4. Select or deselect (check or uncheck) to select which panels you want to add in the selection view (see Figure 52).

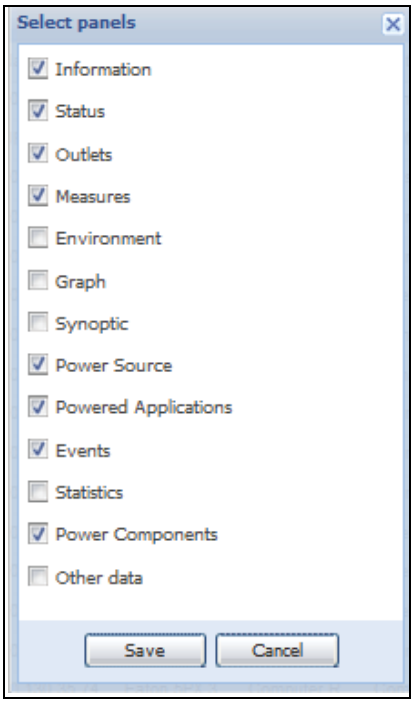

Figure 52. Panel Selection Dialog Box

NOTE Some of the panels are only available for specific node types.

Information Panel

The following node information displays in this panel (see Figure 53):

- **166.99.xx.yy:** DNS name (or IP address) displayed near the "status icon"
- **Description:** Commercial product name
- **Nominal Apparent Power:** Device load capacity in VA
- **IP address:** Device IP address
- **Mac address:** Device MAC address
- **Serial Number:** Device serial number (if available)
- **Class:.** Type of card
- **Location:** Device location (value of syslocation object can also be configured in the Device page)
- **Contact:** Device contact (value of syscontact object can also be configured in the Device page)
- **Link:** Link to device Web site (if available)

NOTE The information displayed in this panel depends on the node types you are viewing.

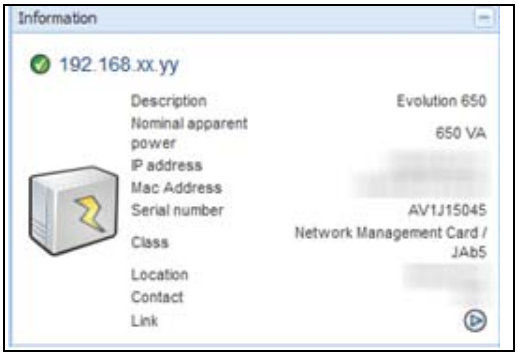

Figure 53. Information Panel

Status Panel

The following node status displays in this panel (see Figure 54):

- **Battery state:** Charging, Discharging, Default, Floating, Resting
- **Power Source:** AC Power, Battery, On utility
- **Load level:** Output load level of the device
- **Battery capacity:** Battery capacity of the device
- **Battery run time:** Device remaining backup time
- **Master output:** Main output status (On, Off, Internal Failure, On Automatic Bypass, Manual ByPass, Overload)
- **Output outlet status:** Output outlet status (On, Off) for outlet or load segment

NOTE The information displayed in this panel depends on the node capabilities.

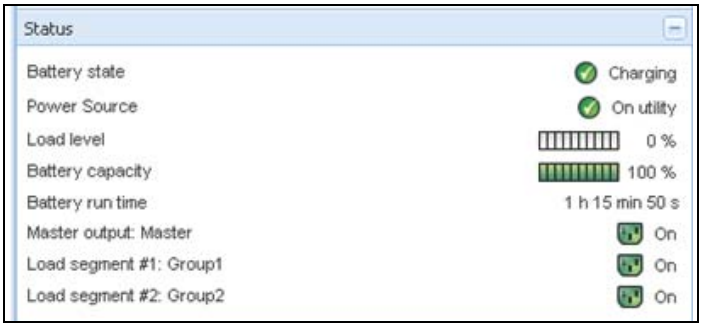

Figure 54. Status Panel

Outlets Panel

The following outlets status information displays for the selected ePDU in this panel (see Figure 55):

- Contextual information is provided when the mouse is over the outlet.
- When you select an outlet in this panel, the Graph panel displays the information for this outlet.
- You must also select Outlet information in the Graph settings dialog (accessible through the graph settings button in the Graph panel).

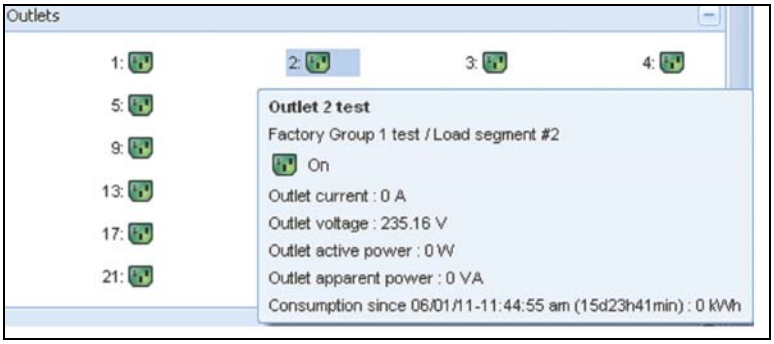

Figure 55. Outlet Panel

The outlet state is color-coded in the display (see Table 6).

Table 6. Outlet Color Codes

Icon	Color	Description
	Green	Powered (ON)
	Red	Not powered (OFF)
	Gray	Outlet status unknown

Measures Panel

This panel displays the selected device electrical parameters for single-phase or three-phase devices, depending on the node capabilities (see Figure 56 and Figure 57).

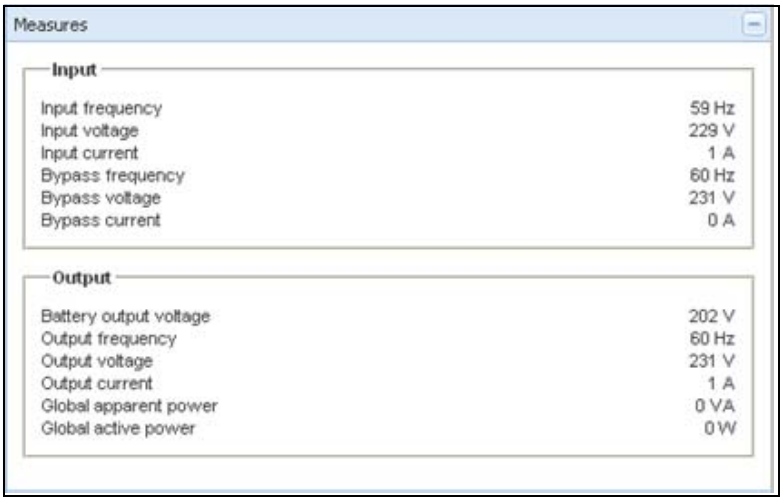

Figure 56. Measures Panel (Single-Phase)

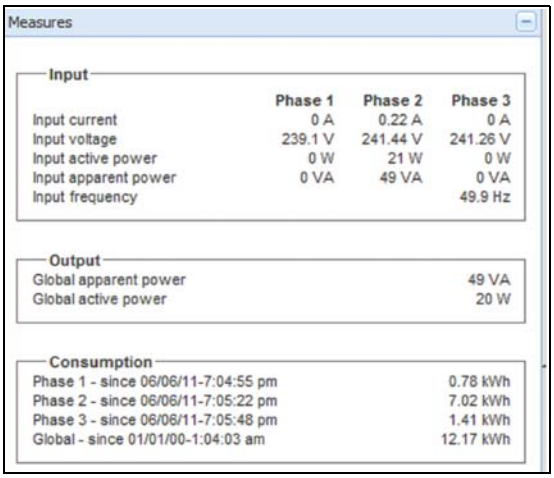

Figure 57. Measures Panel (Three-Phase)

Environment Panel

This panel displays the selected device sensor information if a device is attached (see Figure 58):

- **Temperature:** Temperature (in °C or °F)
- **Humidity:** Humidity level
- **Input #1:** Status of first contact (open / closed)
- **Input #2:** Status of second contact (open / closed)

NOTE For more information about the two optional input connections, please refer to the *Eaton Environmental Monitoring Probe (EMP) Quick Start Installation Manual*.

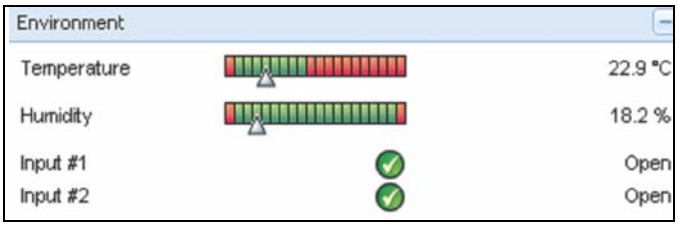

Figure 58. Environment Panel

Graph Panel

This panel displays the graph of the main measures of the selected device (see Figure 59):

- The button allows you to zoom in the graph.
- The button allows you to select the data you want to display in the graph.

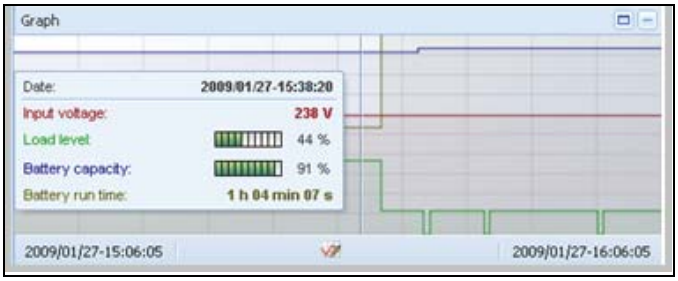

Figure 59. Graph Panel

Synoptic Panel

This panel displays the selected device synoptic (see Figure 60). A tool tip displays when you move the mouse over one of the functional block.

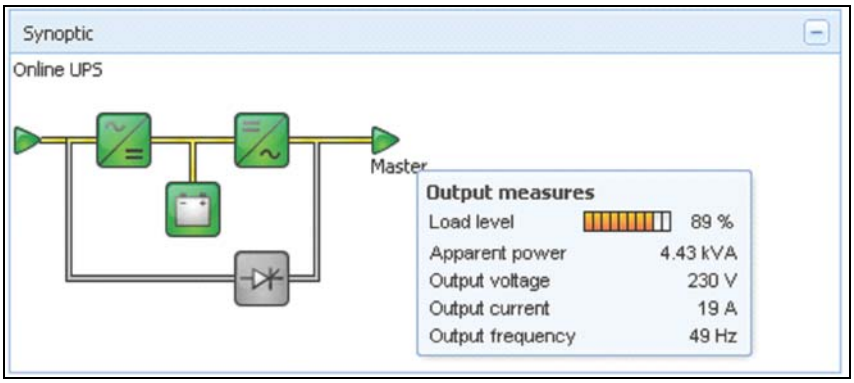

Figure 60. Synoptic Panel

The Synoptic color coded icons display for the following (see Table 7):

- UPS modules
- Battery modules
- Electrical flows
- Electrical power sources at UPS input
- Load at UPS output, with status linked to UPS output status
- Combined flow status and load status

Table 7. Synoptic Panel Icons

Symbol	Color	Description
UPS Modules		
AC/DC DC/AC Bypass 	Green	Status OK and Active
AC/DC DC/AC Bypass 	Red	Internal Fault and Inactive
AC/DC DC/AC Bypass 	Gray	Status OK and Inactive or Unknown
Battery Modules		
	Green	Status OK
	Orange	Battery charge is less than 50%

Table 7. Synoptic Panel Icons (Continued)

Symbol	Color	Description
	Red	Battery fault or End-of-backup
	Gray	Battery status unknown
Electrical Flows		
	Yellow	Current flow through the cable **NOTE** The object animation gives the direction of the current flow.
	Gray	No current flow through the cable

⚠ WARNING

Although there is no current flow through the cable, the cable may be under voltage.

Electrical Power Source at UPS Input		
	Green	Source powered. Status OK
	Gray	Source not powered or status unknown
Load at UPS Output		
	Green	Load powered and protected. Status OK
	Red	Load not powered
	Gray	Load status not known
Combined Color Code: Flow and Power Source Status		
	Green/Yellow	Electrical power source is powered and provides electrical flow
	Green/Gray	Electrical power source is powered and does not provide electrical flow
Combined Color Code: Flow and Load Status		
	Yellow/Green	Load powered and protected
	Gray/Red	Load not powered

Power Source

The Power Source panel displays information on the device that powers the selected application running on the server (see Figure 61).

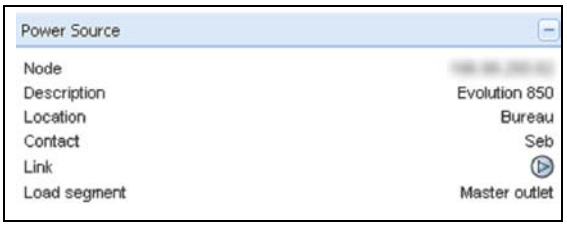

Figure 61. Power Source

Powered Applications

The Powered applications panel displays information for the software applications (shutdown agents on the servers) that are powered by the selected device (see Figure 62)"

- Status
- Name
- Shutdown diagram
- Shutdown duration
- Outlet group

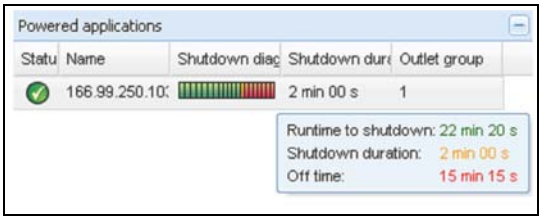

Figure 62. Powered Applications

Events Panel

This panel displays the events list of the selected node (see Figure 63). You can sort the events according to status, date, and message by clicking the column header.

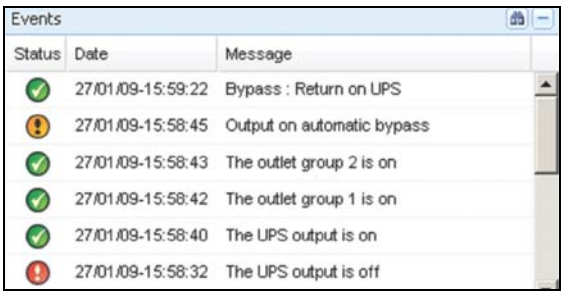

Figure 63. Events Panel

Statistics Panel

This panel displays the statistics of the selected node (see Figure 64). The button allows you to select the time interval for the statistics. You can adjust the time interval by clicking the two buttons with the "From" and "To" dates.

The statistics computed data is as follows:

- Active Consumption in Kilowatt-hour
- Average Active Power in Watts
- Power Failure Count
- Power Failure Cumulated Duration
- Battery Fault Count
- Internal Failure Count
- Overload Count
- Warning Alarm Count
- Critical Alarm Count
- Output Off Count
- Communication Lost Count

NOTE This information depends on device capabilities.

Figure 64. Statistics Panel

Power Components

Figure 65 illustrates the Power Components View. This panel displays the components of a redundant UPS system if the Redundancy feature is activated (see "Redundancy" on page 151).

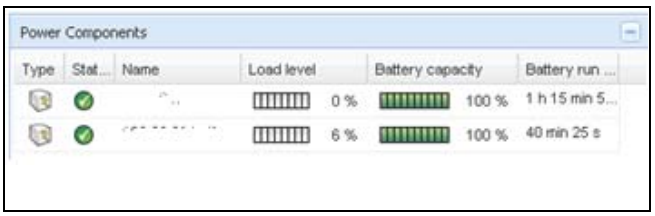

Figure 65. Power Component View (Subview of Power Source View)

Subviews

Defining Subviews

When you need to monitor large configurations, it is helpful to define several subviews and then filter the nodes or events in these categories. You can select many criteria in order to organize your tree.

To define a subview:

1. Select a view in the Views > Node ***List,*** such as Category: "Devices" or Location "HPO Finland" (see Figure 66).
2. Right-click this selection. The contextual subview menu displays (see Figure 67).
3. Click **Create a sub view from ...** and follow the instructions.

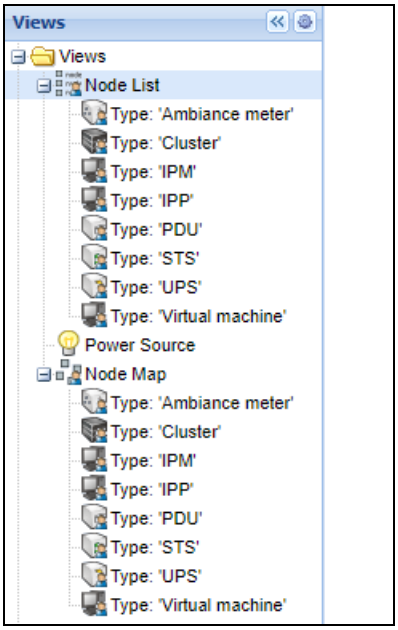

Figure 66. Views > Node List Example Hierarchy

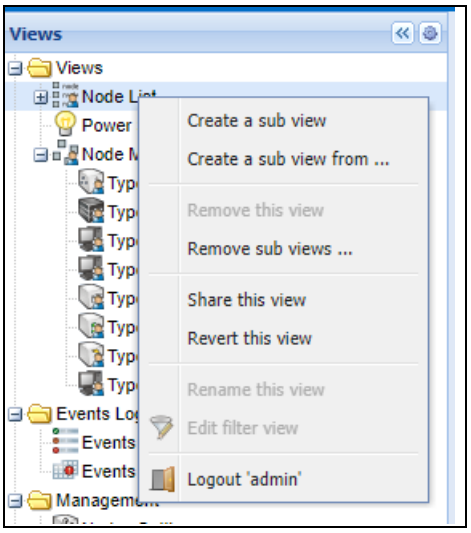

Figure 67. Contextual Subview Menu

To filter the nodes in this subview:

1. Select a view in the Views > Node ***List***, such as "Location: Computer Room" (see Figure 66).
2. Right-click this selection. The contextual menu subviews displays (see Figure 67).
3. Click **Edit a Filter View**. The View Filter Rules dialog box displays (see Figure 68).
4. Click **Add rule**, then type the Object, Operation and Values.

NOTE With the setup shown in Figure 68, this filtered view allows you to view the devices whose location field contains the value "Computer Room."

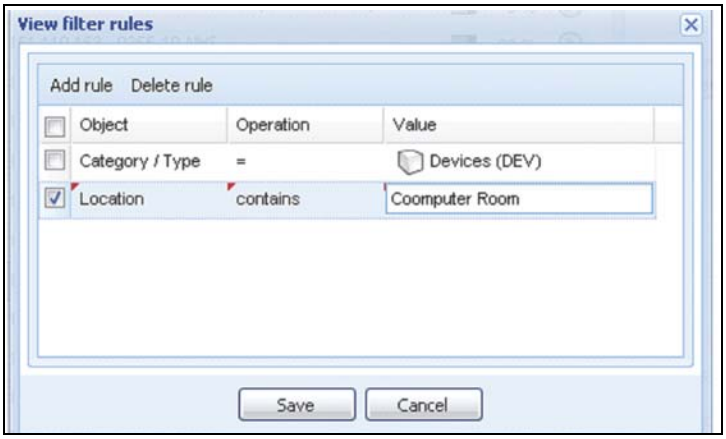

Figure 68. View Filter Rules Dialog Box

As the result of creating a subview, the following default information appears in the Applications List View page (see Figure 69).

- **Type:** Application
- **Status:** Status criticality of the server
- **Name:** Value configured in the Applications screen (by default this is an IP address or a DNS name)
- **Description:** Operating system
- **Policies:** Configuration policies list of the node (contact, location, IP address [Address IP of the node])
- **Power Source:** UPS that powers the Eaton IPP application/computer
- **Estimated Run Time to Shutdown:** Operating time in the event of a utility supply loss
- **Shutdown Duration:** Duration needed by the system to carry out its shutdown procedure (in seconds)
- **Link:** Link to the Web supervision interface of the Eaton IPP or Network Shutdown Module V3 module

NOTE The Eaton IPP or Network Shutdown Module V3 running on other computers in the network can be monitored in this view.

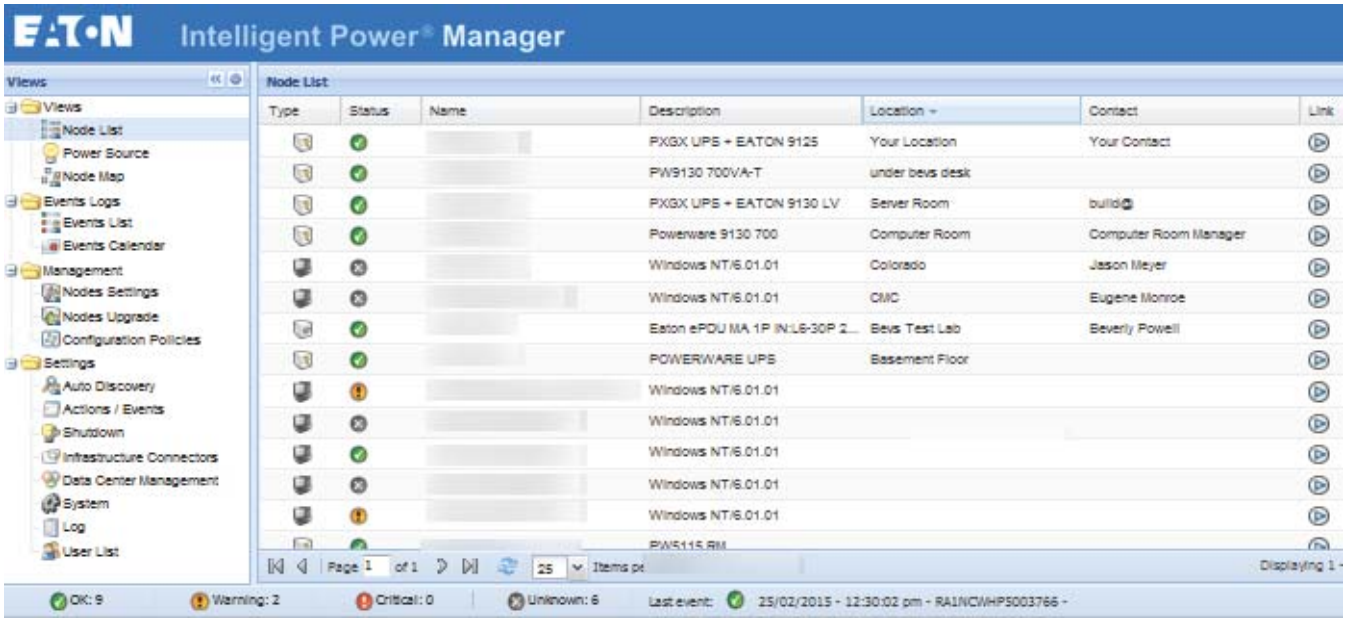

Figure 69. Applications List View Page

Sharing Subviews

A customized subview is "attached" to the user that created it. It is private. The customized subview is marked with a small man next to the icon of the subview (see Figure 70).

Figure 70. Shared View with Marker (left) and Public View without Marker (right)

If the owner of the subview wants to allow others to use the subview, he needs to share the view.

To share the view:

1. Right-click the view to open the contextual menu and click **Share this View** (see Figure 71).

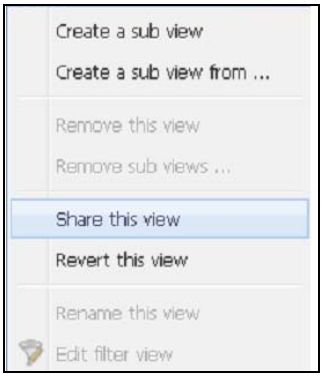

Figure 71. Contextual Subview Menu

NOTE Customizing a view cancels the sharing of this view. To allow all the users who were sharing this file to view it, the owner of the view must share it again.

Device Supervision

The bar at the bottom of the page provides the status of nodes being supervised. Note the following in Figure 72:

- 14 nodes are OK
- 4 nodes are in Warning status
- 2 nodes are in Critical status
- 0 nodes are in Unknown status

Figure 72. Bottom Bar for Device Supervision

Map View

This supervision map allows you to spatially represent your network nodes and uses "drag and drop" functionality.

NOTE Clicking a node icon updates the information for that node on the right-hand panel.

Create a Customized Map View

The customized map view is accessed on the left-side menu using the ***Views > Node Map*** selection. The map is automatically generated. (Icons are automatically placed on the Map and IP address assigned.)

The contextual tool button on the Node Map title bar provides tools to modify the map (see Figure 73):

- **Change theme** offers three kinds of icons representations (small tower icons, large tower icons, and large rack icons).
- **Manage backgrounds** allows you to import a new background image in the supervision tool (png, jpeg, and gif picture format types are supported). You can select a background already in the supervision tool for the map or remove the background images.
- **Regroup nodes** rearranges the icons position on the Map.
- **Add a label** allows to create a user-defined text and to place it on the Map through drag and drop.

NOTE To delete a label, right-click the label and then click **Delete**.

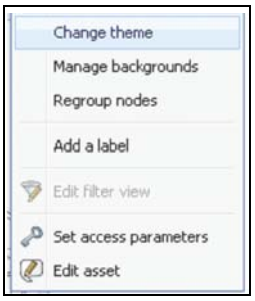

Figure 73. Contextual Tools Menu

Map Examples

This section provides examples of the following maps:

- World Map View
- Country Map View
- Server Room Map View

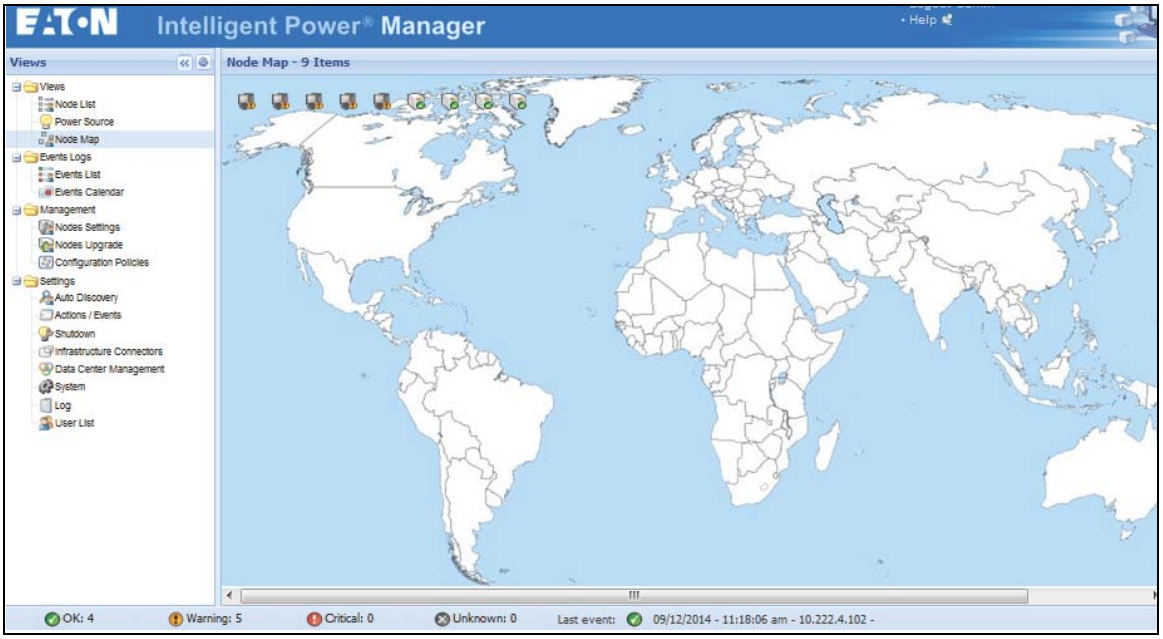

Figure 74. World Map View

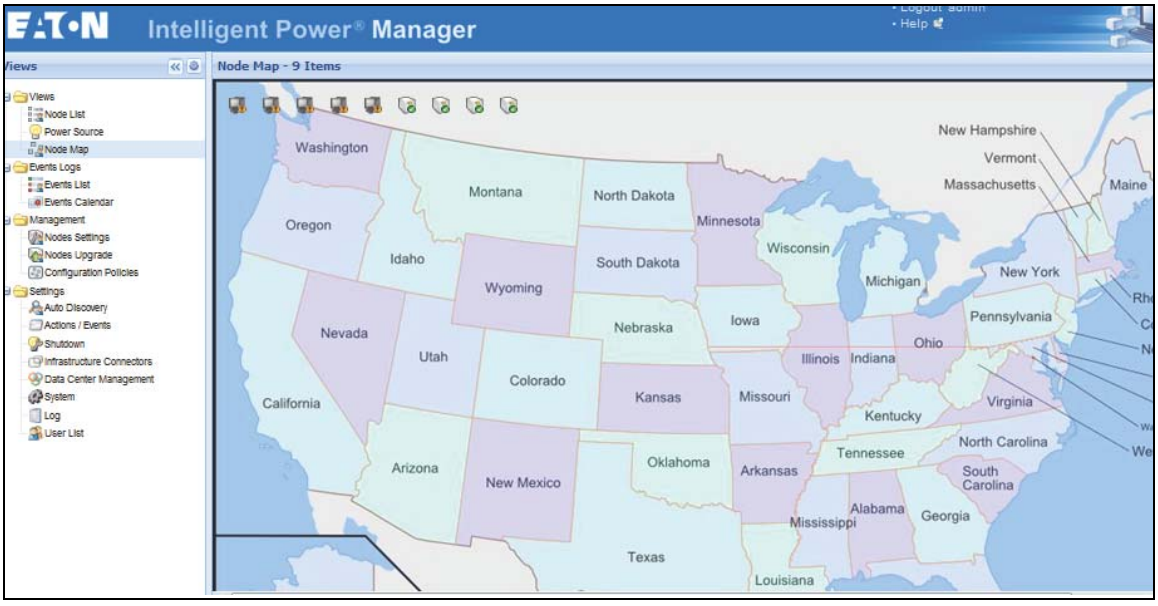

Figure 75. Country Map View

Figure 76. Server Room Map View

Events Logs

List Representation

Select **Events > Events List** to display the Events List page (see Figure 77). All new alarms are stored in this log. You can sort the alarms according to the Status, Date, Name, and Acknowledge (ACK) fields.

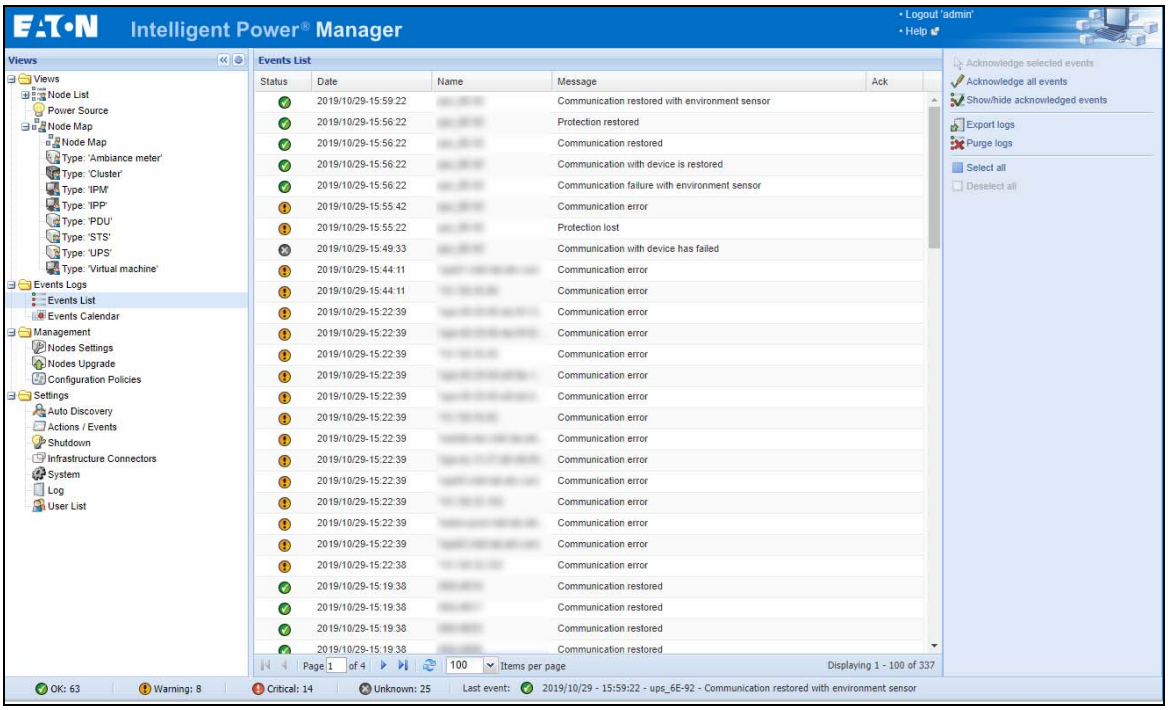

Figure 77. Events List Page

The following functions are available:

- **Acknowledge selected events**: Adds a checkbox in the Ack column for selected events.
- **Acknowledge all events**: Adds a checkbox in the Ack column for all events.

NOTE When an alarm is acknowledged, it is marked with a checkbox but it is still viewable in this Event list. The acknowledged alarms disappear in the ***Power Source > Event*** dedicated portal panel.

- **Export Logs**: Creates a logs.csv file with the following syntax:

```
"Date","Node","Type","Level","Object","Value","Message",
```

NOTE The export command may take several seconds before allowing the download in order to create the logs file.

- **Purge Logs**: Deletes all logs (specify a date)
- **Select all**: Selects all displayed events
- **Deselect all**: Deselects all selected events

Calendar Representation

Select Events > Events Calendar to display the Events Calendar page. In this matrix representation, each line is a week and each column is a day in the week. If you select a day or an interval (with the date-picker or using the shift+click command), the Events and Statistics panels provide all information for this selection and automatically refresh when new statistics are computed (see Figure 78).

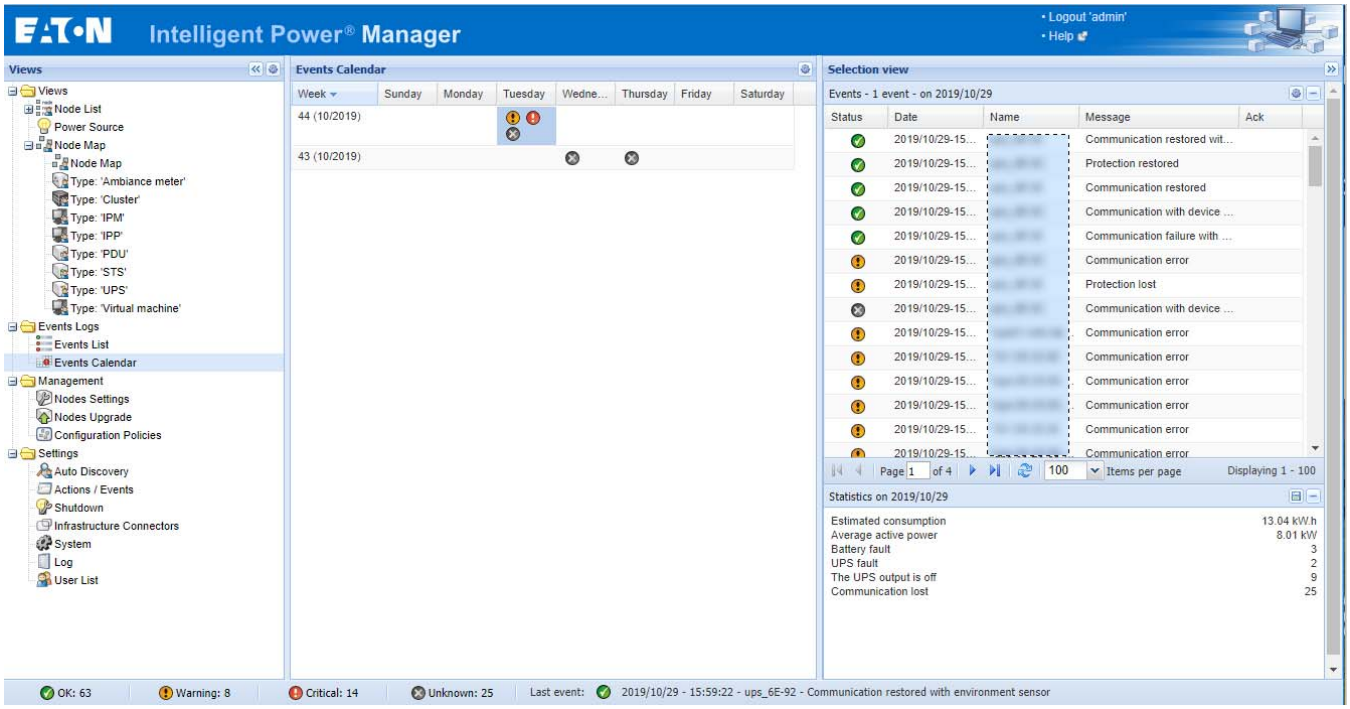

Figure 78. Event Calendar Page

Node Events List

The icons in the different views represent the event severity.

 NORMAL With this event, the UPS device is returning to a normal status.

Normal Event list (UPSs, ePDUs, Applications, or Generic devices):

- Communication with device is restored
- The system is powered by the utility
- The UPS output is on
- Battery OK
- UPS returns to normal load
- UPS OK
- Bypass: Return on UPS
- End of low battery alarm
- The outlet group 1 is on
- The outlet group 2 is on
- Communication failure with environment sensor
- Communication restored with environment sensor
- Humidity is in normal range
- Temperature is in normal range
- Input {x} on
- Input {x} off
- End of warning alarm
- End of critical alarm
- Redundancy restored
- Protection restored
- Reported communication restored
- Automatic bypass is in normal range
- Energy Saving Mode inactive
- Energy Saving Mode active

ePDU Normal Event List (Specific to ePDUs):

- The input current is in normal range
- The input current phase is in normal range
- Breaker group x reset
- The user group current x is in normal range
- End of configuration fault

ePDU Normal Event List (Specific to ePDUs):

- The input frequency is in normal range
- The input temperature is in normal range
- The input voltage is in normal range
- The input {x} is in normal load

- The section {x} current is in normal range
- The section {x} voltage is in normal range
- The outlet group {x} current is in normal range
- The outlet group {x} is in normal load
- The outlet group {x} is on
- The phase {x} output load is in normal range
- The output frequency is in normal range
- The output load is in normal range
- The output voltage is in normal range

WARNING A problem occurred on the UPS device. Your application is still protected.

Warning Event List (UPSs, ePDUs, Applications, Generic devices):

- The system is powered by the UPS battery
- Output on automatic bypass
- Output on manual bypass
- Humidity is below low threshold
- Humidity is above high threshold
- Temperature is below low threshold
- Temperature is above high threshold
- Warning Alarm (a generic Warning alarm is active on the device)
- Protection lost
- Redundancy lost
- Shutdown in <***time***>
- Remote Communication Error (remote communication or configuration issue is detected)
- Automatic bypass is out of range

CRITICAL A serious problem occurred on the UPS device. This problem requires an urgent action. Your application might NOT BE powered.

Critical Event List (UPSs, ePDUs, Applications, Generic devices):

- The UPS output is off
- The outlet group 1 is off
- The outlet group 2 is off
- Battery fault
- UPS overload
- UPS fault
- Low battery alarm
- Applications must stop immediately...
- System shutdown in progress...
- Critical alarm (a generic Critical alarm is active on the device)

ePDU Critical Event List (Specific to ePDUs):

- The input frequency is out of range
- The input temperature is above high threshold
- The input temperature is below low threshold
- The input voltage is above high threshold
- The input voltage is below low threshold
- The input {x} is overload
- The section {x} current is too high
- The section {x} current is too low
- The section {x} voltage is too high
- The section {x} voltage is too low
- The outlet group {x} current is too high
- The outlet group {x} current is too low
- The outlet group {x} is overload
- The outlet group {x} is off
- The phase {x} output is overload
- The output frequency is out of range
- The output is overload
- The output voltage is above high threshold
- The output voltage is below low threshold
- Breaker group x has tripped
- The user group current x is below low threshold
- The user group current x is above high threshold
- Configuration fault
- The input current is below low threshold
- The input current is above high threshold

 COMMUNICATION LOST Communication is lost.

Communication Lost Event List:

- Communication failure with Device or Application
- Reported communication error.

 DEVICE IS NOT MANAGED Device is not managed

- Your device is not managed due to license limitation. Use the Settings > System selection to enter a Silver or Gold license code.

Launching the Device Web Interface

From the Status panel, you can access the Web page for Eaton cards, including an on-board Web server. Click the associated Web link for http access (blue icon) or the https access (yellow icon).

Figure 79 provides examples of the opening view from different Web interfaces.

Figure 79. Opening View in Different Interfaces

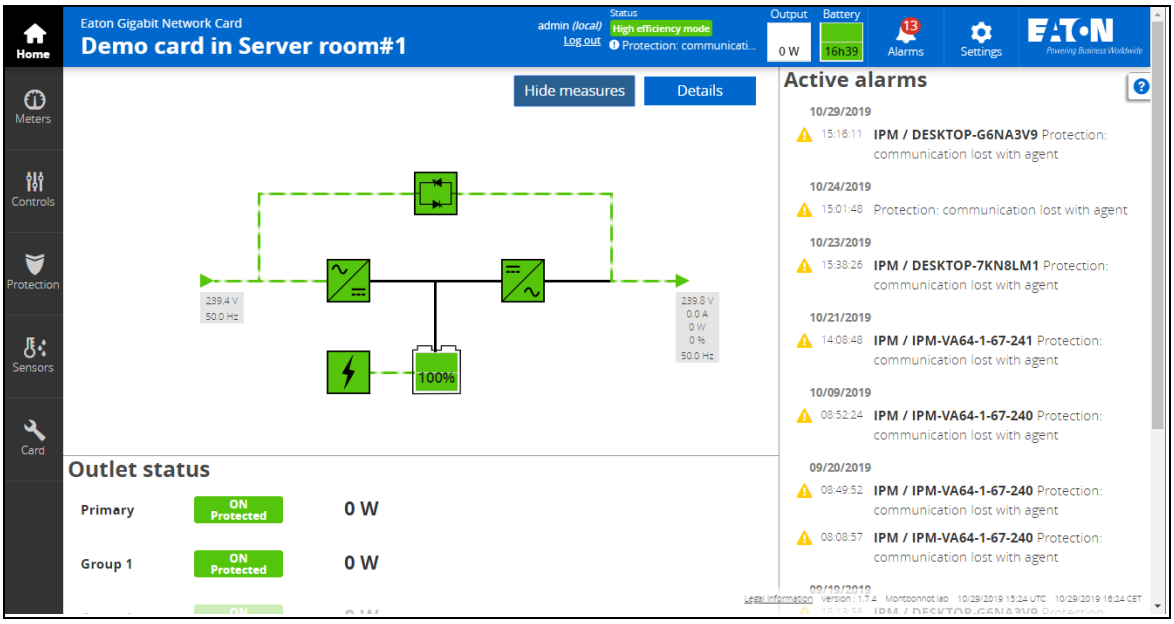

Figure 80. Opening View in Different Interfaces

Node List Export to CSV File

To export data displayed in the Node list, click the button in the top right corner of the Node list and select Export to CSV file (see Figure 81).

If some nodes are selected in the list, the exported file contains only data for the selected nodes. If no node is selected, the exported file contains data for all the nodes in the list. Only data from currently displayed columns are exported.

Figure 81. Export to CSV File

The function is also available from the ***Auto Discovery > Export to CSV file*** menu selection.

Chapter 6 Shutdown

The Eaton Intelligent Power Manager (IPM) provides local computer graceful shutdown when connected to a UPS through either an Eaton Gigabit Network Card, Network Management Card, USB port, or RS-232 port.

This shutdown feature can be enabled or disabled from the ***Settings > System > Modules Settings*** selection path.

NOTE 1 Refer to the *Eaton Intelligent Power Protector (IPP) User's Guide* for a detailed description of the Shutdown feature.

NOTE 2 When the Shutdown feature is enabled, the software displays a communication error until the Power Source is correctly configured as described in the following section, "Shutdown Configuration".

Shutdown Configuration

To access the shutdown configuration options and verify that the Shutdown Module is enabled (administrator access):

1. From the left-side **Views** panel of the Eaton IPM main interface window, select the ***Settings > Shutdown*** menu item.The Shutdown page displays (see Figure 82).

   The following configuration options are provided on the right-side panel of the Shutdown page:

   - Edit power source
   - Edit shutdown criteria
   - Edit advanced shutdown criteria
   - Edit UPS configuration
   - Test shutdown
   - Run battery test

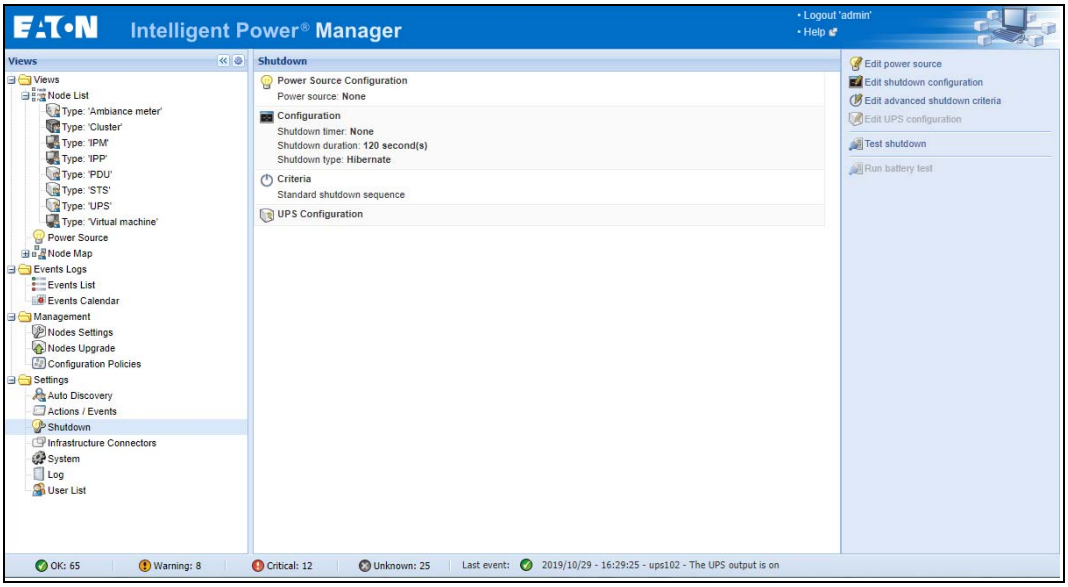

Figure 82. Shutdown Page

To configure shutdown, perform the following actions:

1. Click the **Edit Power Source** button.
2. In the Power source field, select the UPS that powers the computer hosting the Eaton IPM.
3. Select the UPS Load Segment that is powering the server.
4. Type the login and password if necessary (depends on the connectivity).
5. Click **Save**.

Shutdown Through Hibernate

If the hibernation feature is available with your operating system, there are a number of advantages to using it (available from Microsoft® Windows® 2000 and later versions). When the computer is shutting down, all system information (including work in progress) is automatically saved to the disk. The computer is also de-energized. When mains power returns, all the applications re-open exactly as they were before the computer shut down and you return to the application work environment.

The Hibernate function must first have been activated in the operating system in the power options on the Windows control panel Hibernate tab.

NOTE If you select hibernate, but your computer does not have this function, the Eaton IPM will still protect the system by carrying out the normal (default) shutdown action.

Power Source View

When the Shutdown feature is configured, select the ***Views > Power Source*** menu item to perform the following (see Figure 83):

- To supervise the information from the UPS that powers the Eaton IPM computer.
- To drag and drop the panels in this window to different locations to personalize your viewing preference.

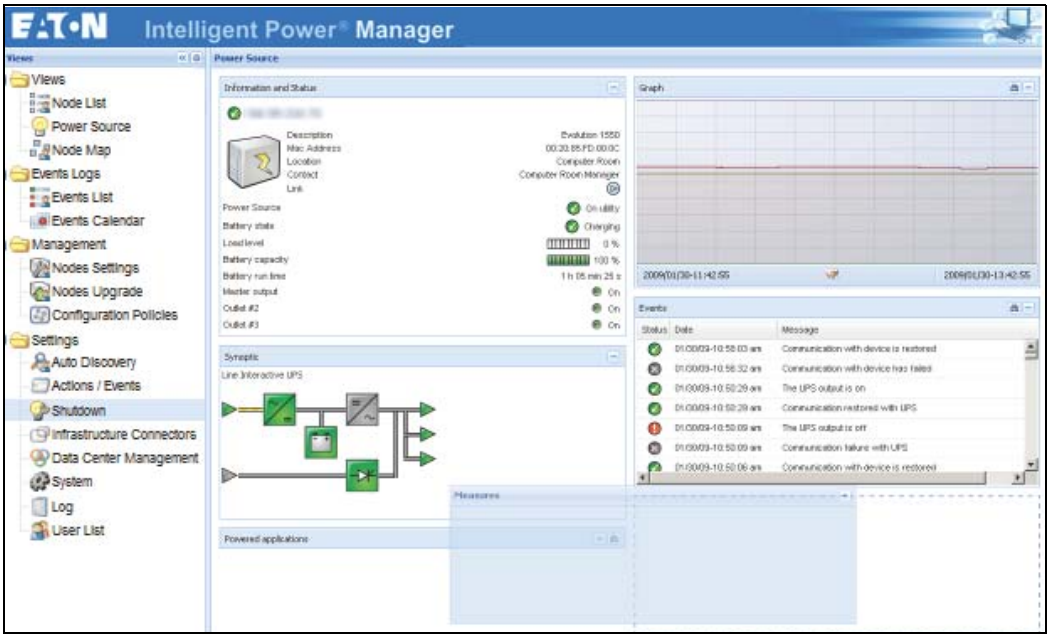

Figure 83. Power Source View

Shutdown Sequence

The Eaton IPM can acquire shutdown alarms from the Eaton IPP with the Shutdown Controller enabled.

NOTE Refer to the *Eaton Intelligent Power Protector (IPP) User's Guide* for more information about Shutdown sequence and Shutdown Use Case.

Chapter 7 Advanced Management

This chapter describes Eaton Intelligent Power Manager (IPM) advanced management features.

Nodes Settings

Single Node Configuration Display

The Eaton IPM can display the card and application configuration for other nodes on the network.

To display configurations for other nodes on the network (administrator access):

1. From the left-side **Views** panel of the Eaton IPM main interface window, select the ***Management > Nodes Settings*** menu item. The Node List page displays.
2. Select one node (card) from the Node List page (see Figure 84).
3. After a few seconds, on the right hand, the Node configuration panel is updated.
4. If you wish to save a standard node configuration (for example to deploy to other similar nodes), use the ***Configurations > Export Configuration*** file to export this configuration to a file.

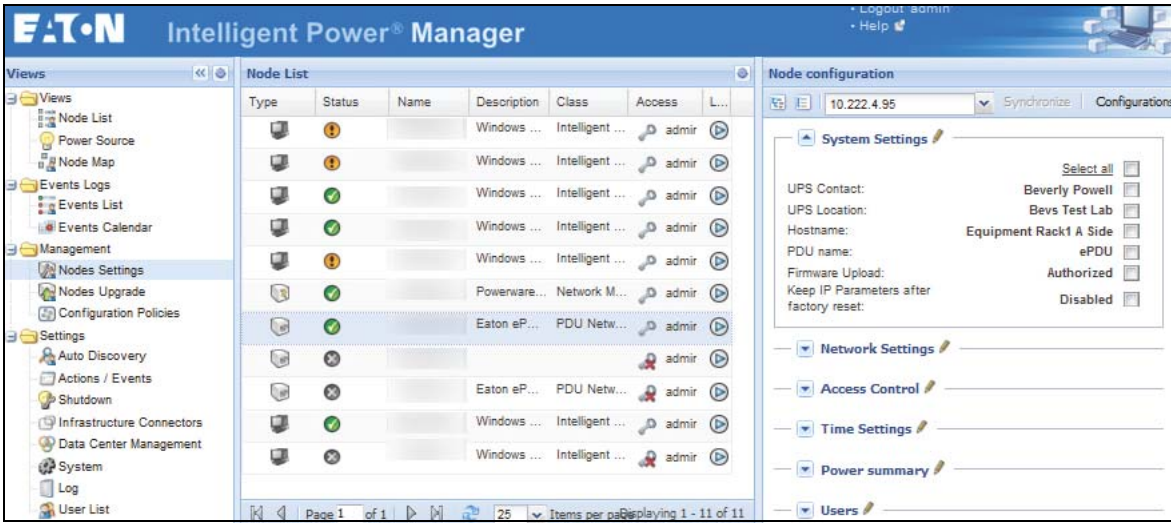

Figure 84. Nodes Settings View

Single Card Settings

Eaton IPM can configure a Network Management Card.

To configure a remote Network Management Card (administrator access):

1. From the left-side **Views** panel of the Eaton IPM main interface window, select the ***Management > Nodes Settings***.
2. Select one node (one card) from the Node List page (see Figure 84).
3. Click the **Node List** button , select **Set Login Parameters**, and enter the card Login and Password.

   The access status changes from Access Denied ( ) to Access OK ( ).

   After a few seconds, the Node configuration panel is updated.
4. Click on the Edit button , or load a previously saved configuration.

5. In the Network Settings Configuration dialog box, check the parameters you want to change and type the new values (see Figure 85).

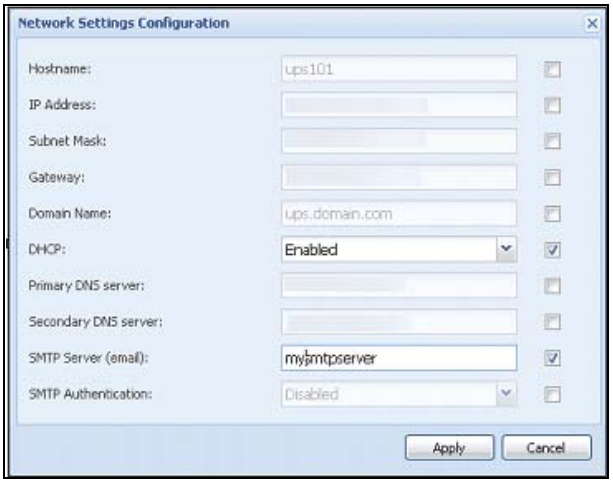

Figure 85. Network Section

6. Click **Apply** to apply to the selected node (card).

NOTE The parameters that have different card and configuration values (unsynchronized) are indicated by the ≠ sign.

7. Select the parameters you want to synchronize (with the checkbox).
8. Click **Synchronize.**

IMPORTANT

Some advanced parameter details are not displayed in the Network Settings Configuration dialog box. For these details, you will need to change the advanced parameters details directly on one device and then synchronize the configuration from this device to other devices (see Figure 86).

Figure 86 provides a typical example with PDU Power Schedule configuration. The details of Power Schedule 1 to Power Schedule 8 are available from the device Web interface. Checking all Power Schedule "***n***" advanced parameters synchronizes all the advanced parameter details of the category.

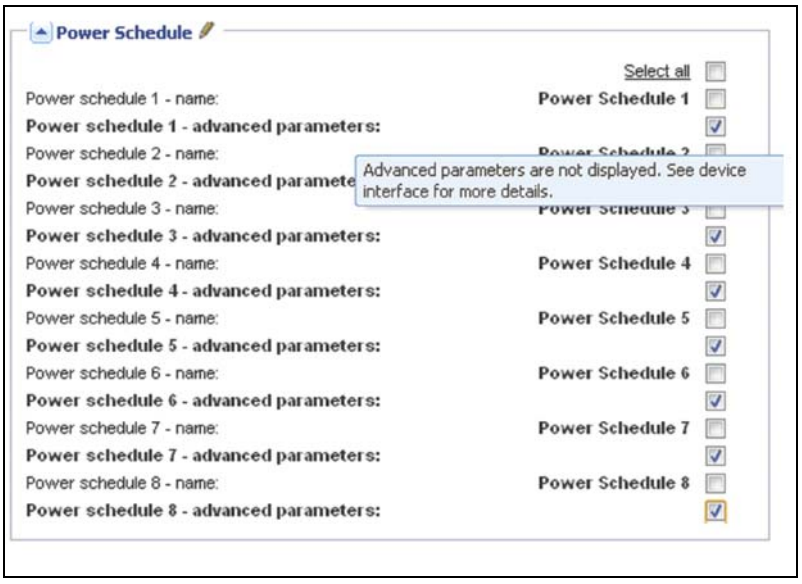

Figure 86. Advanced Parameters Not Displayed

Multiple Card Configurations Synchronization

The Eaton IPM can make changes to multiple Network Management Card configurations simultaneously.

To configure multiple Network Management Cards (administrator access):

1. From the left-side **Views** panel of the Eaton IPM main interface window, select the ***Management > Nodes Upgrade*** menu item.
2. Select the several cards on the Node List page.
3. Select the **Node List** button , select **Set Login Parameters** and enter the card login and password.

   The access status changes from: Access Denied ( ) to Access OK ( ).

   After a few seconds, the Node configuration panel is updated.
4. From the combo box, select the configuration that will be the model, or click **Edit** .

   The parameters that have different values on the cards are indicated by the "not equal" ≠ sign.
5. Select the checkbox associated with the parameters you want to synchronize.
6. Click **Synchronize**.

Nodes Upgrade

Upload Device Firmware

NOTE Refer to the Network Management Card's release notes to determine the latest firmware release compatible with the hardware revision.

To upload a device firmware:

1. From the left-side **Views** panel of the Eaton IPM main interface window, select the ***Management > Nodes Upgrade*** menu item.
2. Select the cards on the Node List page.
3. From the Node List button , select **Set Login Parameters** and enter the card login and password.

   The access status changes from: Access Denied ( ) to Access OK ( ).
4. From the ***Firmware > Import Firmware File...*** list box, the uploading window displays.
5. Click **Browse** to select the firmware from a disk accessible from the computer.
6. Click **Import**.
7. Click ***Firmware > Upload Firmware to nodes***. The cards are updated with the selected firmware.

Upgrade Applications

To upgrade the applications (administrator access):

1. From the left-side **Views** panel of the Eaton IPM main interface window, select the ***Management > Nodes Upgrade*** menu item.
2. Select the applications in the Node List.
3. From the Node List button , select **Set Node Access Parameters** and enter the access login and password.

   The access status changes from: Access Denied ( ) to Access OK ( ).
4. From the Applications upgrade panel, click **Update**. The status of the applications (with respect to the version) is updated.

Chapter 8 Virtualization

The Eaton Intelligent Power Manager (IPM) Infrastructures Connectors module for VMware, Microsoft and Citrix virtualization requires a network shutdown environment. Enable the Infrastructures Connectors module to allow functionality related to third party products, including virtualization hypervisors.

NOTE The UPS must be connected through a network interface. Peer-to-peer interfaces between IPP and the UPS (USB/RS-232) communication protocols are not supported for virtualization applications.

To enable the Infrastructures Connectors module for virtualization (administrator access):

NOTE Some connectors are restricted to a license use. By default, it's possible to configure these connectors : VMware vCenter, VMware ESXi, Microsoft Hyper-V, and NetApp Storage. For Nutanix, HPE OneView, and Dell/EMC VxRail, a license key is mandatory to configure the connectors.

1. From the left-side **Views** panel of the Eaton IPM main interface window, select the ***Settings > System*** menu item. The System page displays (see Figure 88).
2. Click **Edit modules settings** in the right panel. The Edit modules settings dialog box displays (see Figure 87).
3. Ensure that the **Infrastructure Connectors** checkbox is selected (checked).
4. Click **Save**.

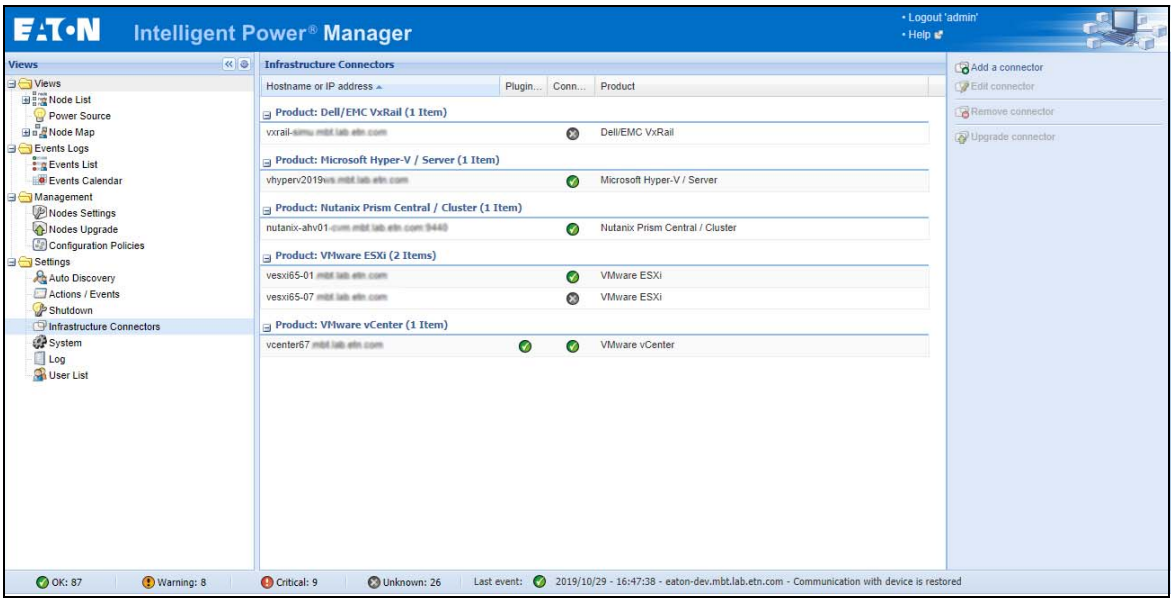

Figure 87. System Settings Page

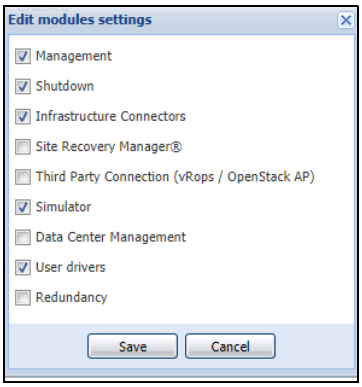

Figure 88. Enable Infrastructure Connectors Setting for Virtualization

When a user tries to add a connector by ***Settings > Infrastructure Connectors > Add a connector***, the sequence of screens show options available, depending of the JRE prerequisite (see Figure 89). The unselectable options are italic and grayed-out.

- If a JRE is installed on the system hosting Eaton IPM, VMware connectors are available (see "JRE Prerequisites" on page 8).

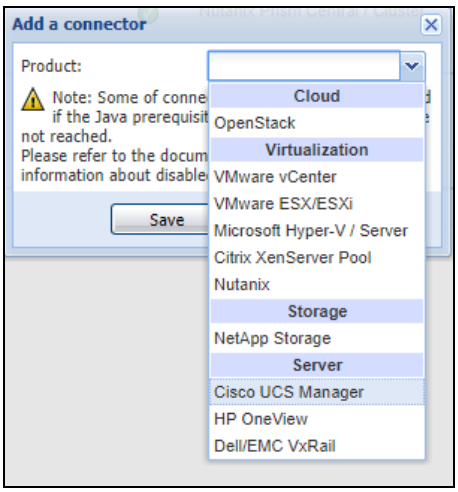

Figure 89. Selectable and Non-selectable Connectors

Eaton Solutions for VMware

Standalone Hypervisor and Local Solution

The standalone hypervisor and local solution requires you to have installed Eaton Intelligent Power Protector (IPP) and VMware vSphere Management Assistant (vMA). The architecture for this solution is illustrated in Figure 91.

NOTE For more information, refer to the *Eaton Intelligent Power Protector (IPP) User's Guide*.

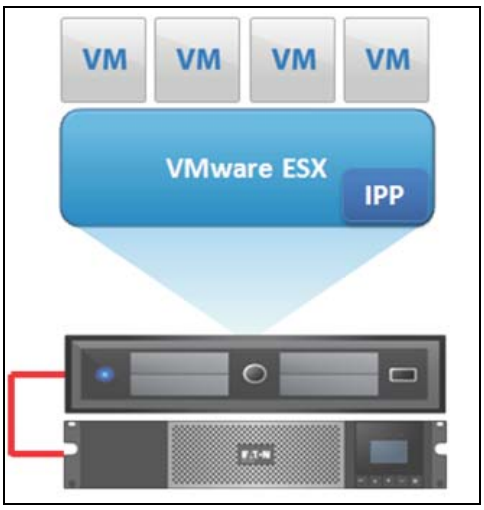

Figure 90. Eaton IPP Running on ESX Server

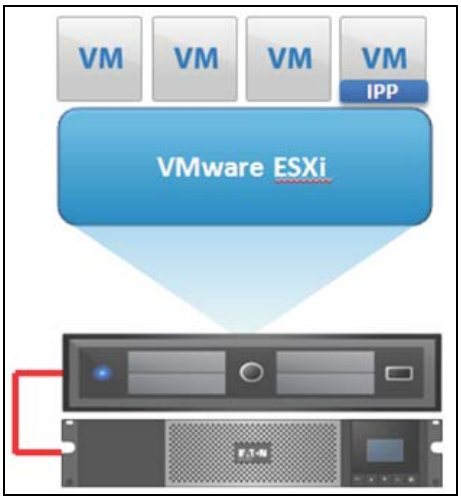

Figure 91. Eaton IPP Running on vMA

Multiple Hypervisor and Remote Solution

For multiple VMware hosts, it is possible to manage shutdown through IPM by either using or not using a vCenter plug-in. This solution is effective for large infrastructures working through the vCenter server and provides the following features:

- Remote graceful shutdown of multiple ESX/ESXi servers and hosted virtual machines (VMs)
- ESX/ESXi remote maintenance using VMware vMotion)
- Eaton IPM plug-in created in vCenter
- UPS events accessible through vCenter

These two solution architectures are illustrated in Figure 92 and Figure 93.

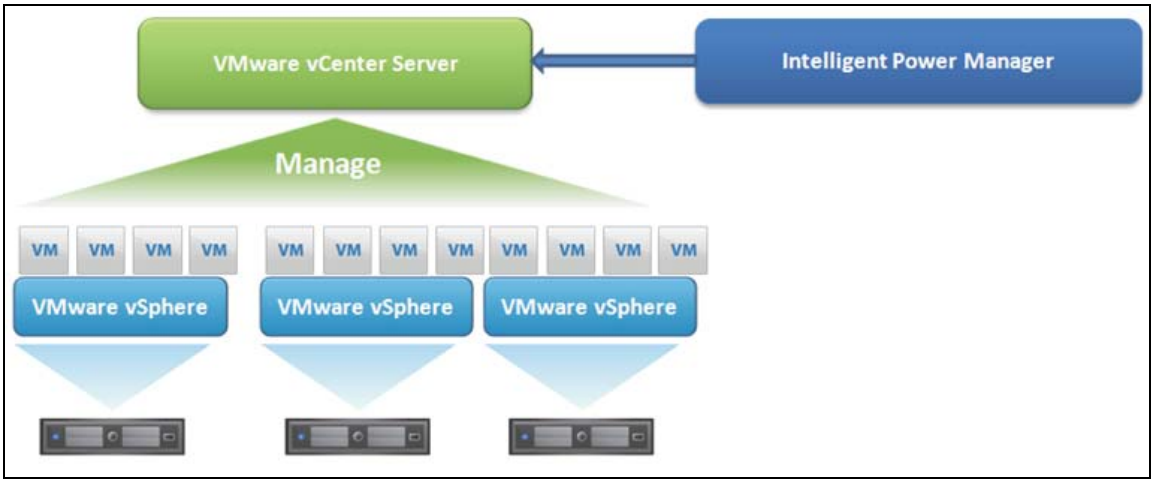

Figure 92. Eaton IPM Connected to vCenter to Protect VMware Infrastructure

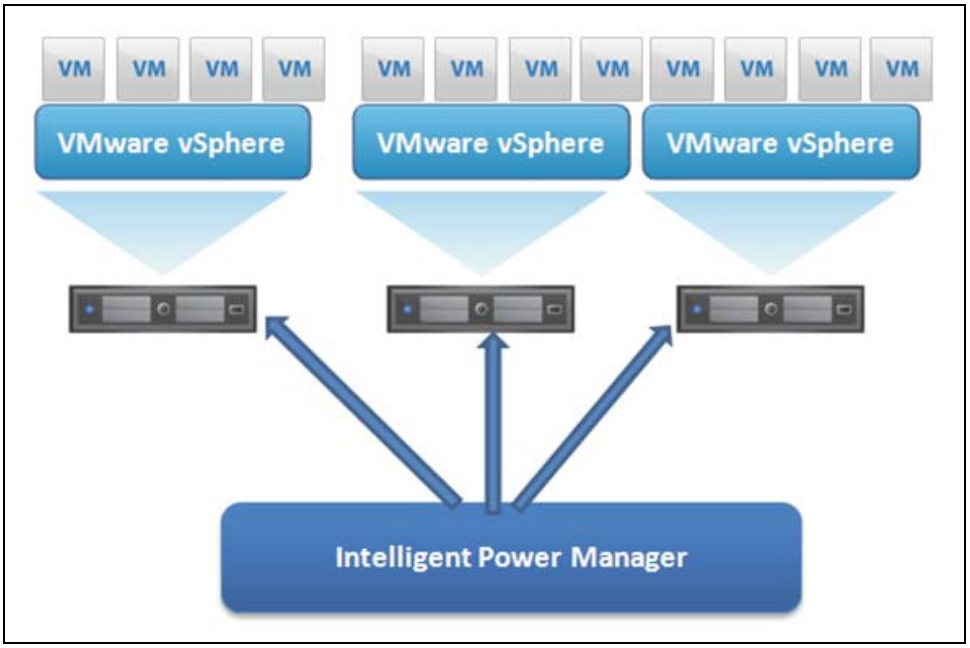

Figure 93. Eaton IPM Connected to ESX/ESXi to Protect VMware Infrastructure (Without vCenter)

Prerequisites

The Infrastructure Connectors module for virtualization requires the following prerequisites:

- VMware vCenter and VMware vSphere Client must be installed.

NOTE vCenter and Eaton IPM could be installed on the same system.

- To provide the virtual machine (VM) graceful shutdown, you must install VMware tools on each VM.
- You have knowledge and experience with Eaton IPM software and the VMware infrastructure.

In this solution, ESX and ESXi hosts are not controlled by vCenter (paid version only), which provides following features:

- Eaton IPP application is installed on VMware Infrastructure Management Agent (VIMA)/vMA for each host. VMware ESXI 6.7 local protection, based on VMA, is not supported by IPP 1.61 and higher.
- Eaton IPP configurations and actions can be managed centrally from the Eaton IPM client.
- Some command line programming is required.
- Remote graceful shutdown of multiple ESX/ESXi servers and hosted VMs.

Adding Infrastructure Connectors

To add Infrastructure Connectors (see Figure 94):

1. If you have not already enabled the Infrastructures Connectors module, use the Edit modules settings dialog in the ***Settings > System*** menu. The Infrastructure Connectors menu entry displays as a selection in the Settings menu.
2. Click **Infrastructure Connectors**.
3. Click **Add a connector** on the right-side panel. The Add a connector dialog displays.

NOTE To edit or remove connectors, you must first select a line in the center panel.

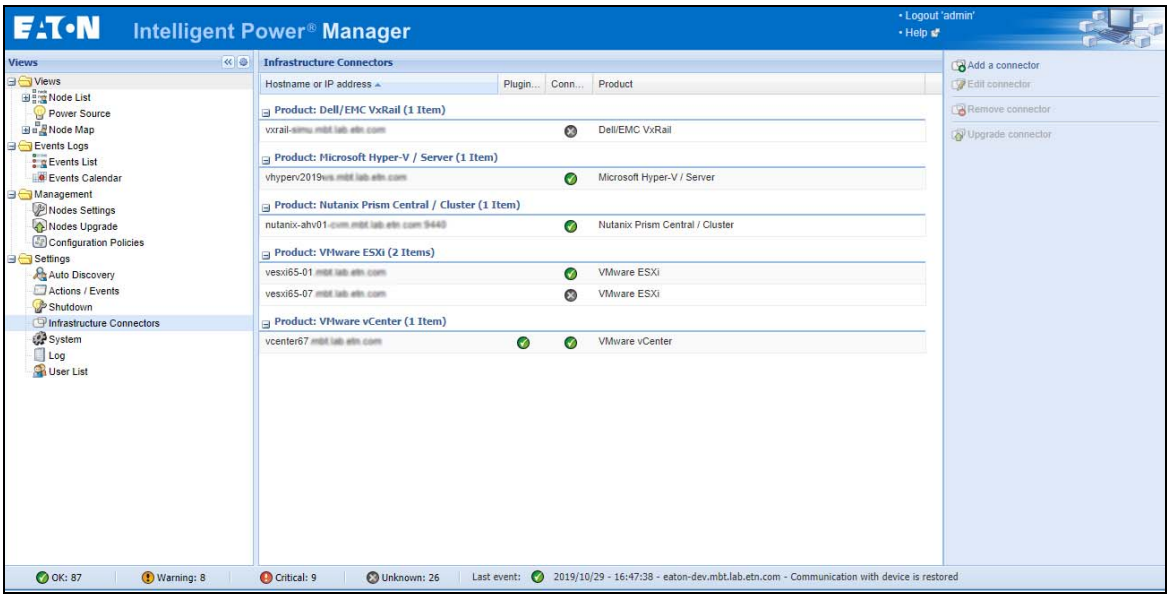

Figure 94. Infrastructure Connectors Page

Adding a vCenter Server Manager

To add a new VMware vCenter:

1. From the Add a Connector dialog, select VMware vCenter from the Product drop-down list (see Figure 95). A second Add a connector dialog displays for your product connector selection.

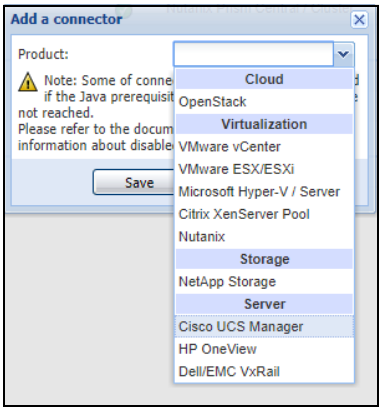

Figure 95. Add a Connector Product Selection Dialog

2. Add identification information for the selected connector (see Figure 96).
   - **Product:** Select VMware vCenter from the drop-down list
   - **Hostname or IP address:** Type VMware vCenter Host name or IP address
   - **Port:** Type the port number
   - **Username**: Type VMware vCenter Administrator Username
   - **Password:** Type VMware vCenter Administrator Password
   - **vCenter Plugin**: Select (check) the checkbox to install and configure the Eaton IPM Plug-in to vCenter

NOTE See "Configuring the Eaton IPM vCenter Plug-in and WebPlug-in" on page 179 when using this feature.

3. Click **Save** after the fields are updated. The VMware ESXi hosts are automatically added to the managed nodes.

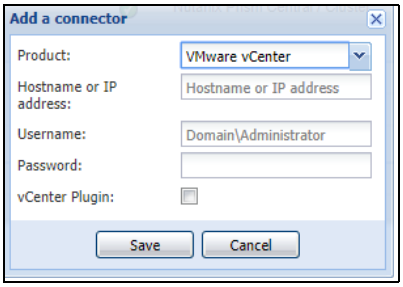

Figure 96. Add VMware vCenter

NOTE 1 The encrypted password is stored in the following configuration file ({Eaton IPM INSTALL DIRECTORY}\configs\vmconfig.js).

NOTE 2 When configuring the Login Username and Password, Eaton recommends using the Eaton IPM Web interface through https. Using http is also possible but the password is sent to the local or remote server in clear. The encrypted password is stored in the configuration file <IPM-Install-Dir>/configs/infraconfig.js

Adding a VMware ESX/ESXi Hypervisor List

In the case where you do not have a vCenter server manager, add VMware ESX/ESXi hosts individually.

To add a VMware ESX/ESXi hypervisor list:

1. From the Add a Connector dialog, select New VMware ESX/ESXi from the Virtualization drop-down list. A second Add a connector dialog displays for your product connector selection.
2. Add identification information for the selected connector (see Figure 97)
   - **Product:** VMware ESX/ESXi is already selected in the drop-down list.
   - **Hostname or IP address:** Type VMware ESX/ESXi Hostname or IP address
   - **Username**: Type VMware ESX/ESXi Administrator Username for the Administrator with admin rights on the ESXi
   - **Password:** Type VMware ESX/ESXi Administrator Password
3. Click **Save** after the fields are updated.

NOTE For more details you can also check the section "Configuring Maintenance and Shutdown".

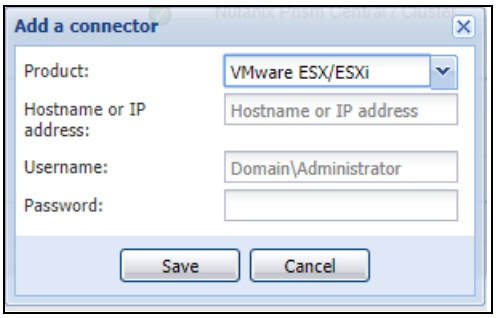

Figure 97. Add VMware ESX/ESXi

VM and vApps

Once you have connected IPM with a VMware vCenter or ESX/ESXi hypervisor, the VM and virtual applications managed by the VMware server are automatically discovered by IPM and added as new nodes.

If you click a VM node, you can see its power state and the ESX/ESXi which hosts it.

Changes on VM/vApp power state are logged in the "event popup window." With the "Advanced Event & Actions," you can trigger specific actions when such a change occurs.

See "VMware & VM Migrate on EMP" in Appendix A. VM and vApps are displayed only with a SILVER/GOLD license.

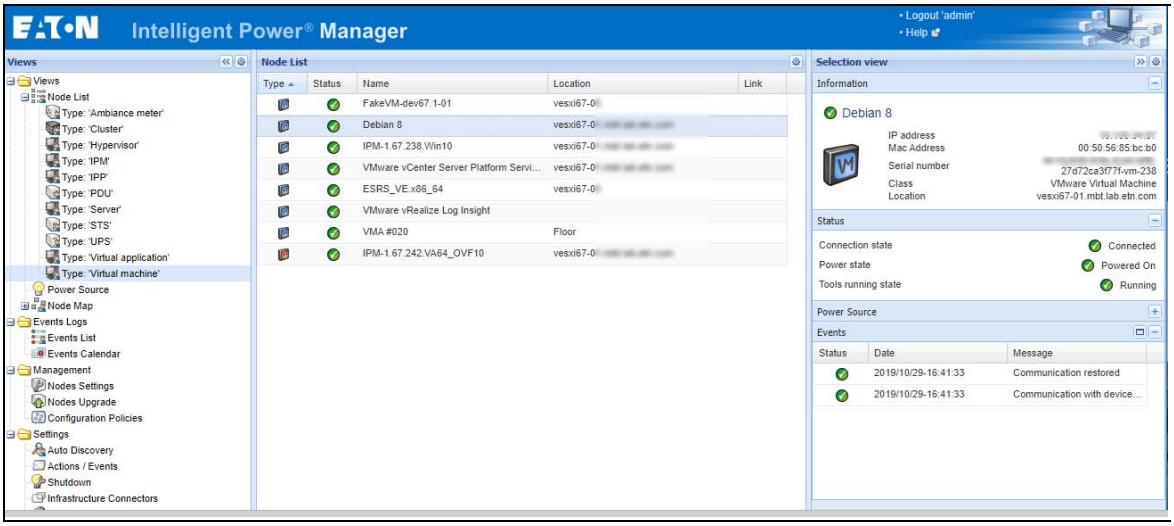

Figure 98. VMs Monitoring

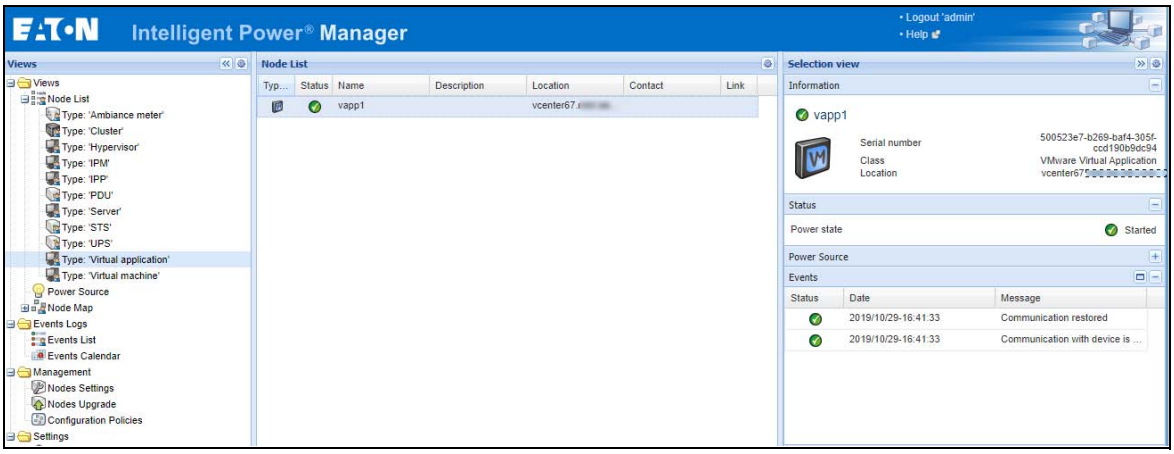

Figure 99. vApps Monitoring

VMware Site Recovery Manager

IPM is now fully integrated with VMware vCenter and VMware Site Recovery Manager. This integration provides the following benefits:

- **Starts recovery process on several different events:** IPM initiates the execution of recovery plan upon several different events.
- **Less down time for end users:** VMs will be down only for the amount of time required to transfer the latest snapshot and will restart once transfer is complete. The unprotected VMs will continue to run on the primary site.
- **Customization for end users:** You can customize the script included in the package as needed. For example, you may want to customize the SRM with IPM for low battery and protection loss features. You can trigger your customized SRM action when your customized event is triggered.
- **Unattended execution of recovery plan before server crash:** SRM with IPM provides recovery, even before the entire site crashes. When the SRM feature is used, the backup will be ready even before the crash, which keeps the site continually secured.
- See “Site Recovery Manager (SRM) with EMP” on page 232.

VMware Load Shedding Capabilities

During utility failure, load shedding can increase the effective runtime of highly critical devices because battery capacity is limited.IPM is now fully integrated with VWmare vCenter, it manages ESXi, VM and vApps of a vCenter as “application nodes.” You can trigger power actions (shutdown, startup) on each of these nodes when a power alarm is triggered. You can move VMs from a ESXi to another one on a shutdown alarm.

See “VMware & VM Load Shedding” on page 230.

Eaton Solution for Dell/EMC VxRail Cluster

IPM VxRail connector allows connection to one VxRail unit.

Through this implementation, the scope is to protect the entire cluster from power events.

When Eaton IPM is embedded in the VxRail Cluster, it's possible to configure a Cluster shutdown action based on a solution with the Eaton Gigabit Network Card.

To create a VxRail connector, the user only needs to provide the:

- VxRail Manager IP address / or hostname (FQDN)
- vCenter IP address / or hostname (FQDN)
- Credentials of vCenter or VxRail Manager

Once the connection is successfully created, a VxRail Cluster node is created, and monitored in IPM.

With VxRail Manager 4.7.0 and higher, Cluster shutdown is compatible with IPM:

- "Configuration policies" and "advanced events and actions" features of IPM can be configured to ensure the protection of VxRail environment, in case of a power or environmental event.
- For more details about the VxRail Cluster shutdown scenario, see "Cluster Shutdown" on page 45.

Settings Menu/System

Prerequisites for the Cluster shutdown feature with IPM:

1. IPM version 1.67 (or higher), IPM Virtual Appliance (OVA) package.
2. Optimize license is required to activate the VxRail Cluster shutdown feature.
3. Enable infrastructure connectors in modules settings.
4. VxRail Cluster protected by an Eaton UPS managed by an Eaton Gigabit Network Card (FW version 1.7.0 and higher); the shutdown script is relayed by the network card.
5. IPM is embedded into the cluster, IPM OVA is deployed on the same vCenter as the one managing the VxRail Cluster.
6. VxRail Software Manager version 4.7.000.
7. Containers are not supported by IPM for the Cluster shutdown sequence.

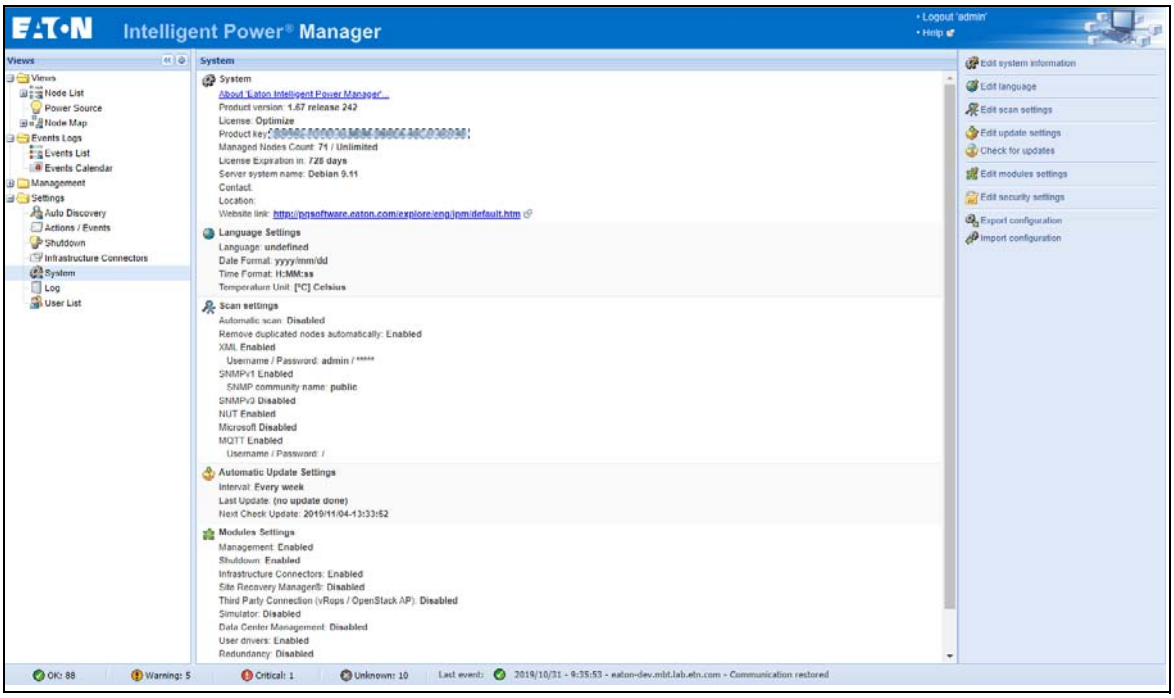

Figure 100. IPM System Menu Configuration

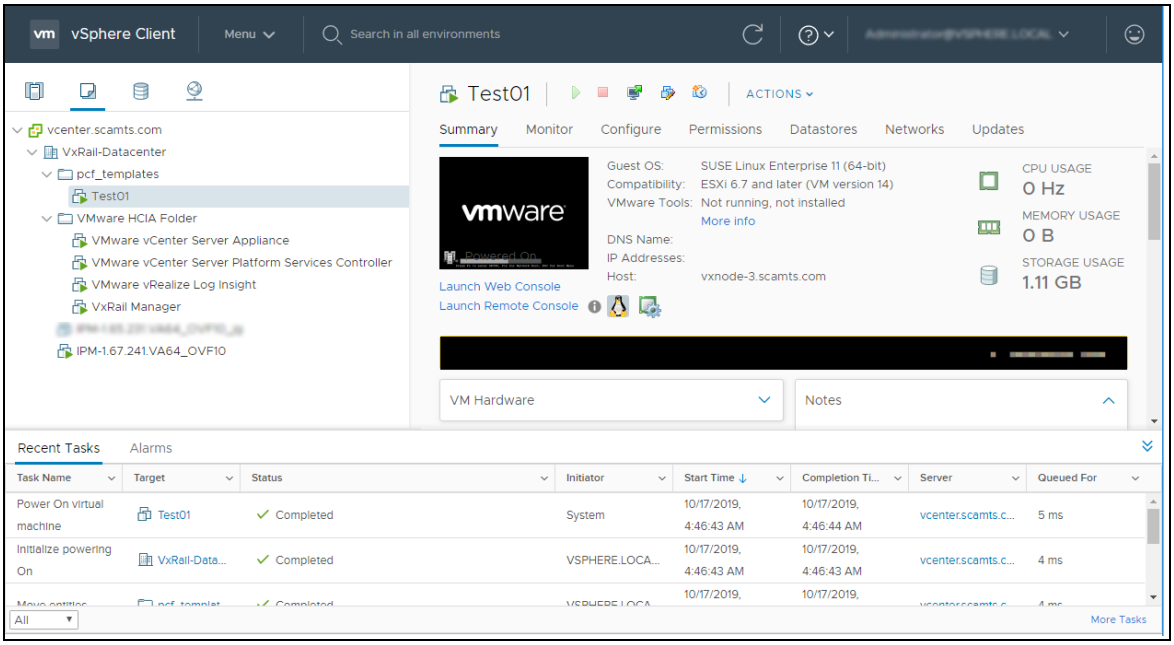

Figure 101. IPM OVA Deployed on VxRail vCenter

Configure VxRail Connector:

Open Settings menu / infrastructure connector, then select option "add connector" and select Dell/ EMC VxRail.

To set the connection with VxRail, the following information is required:

- Hostname or IP address: VxRail Software Manager
- Username
- Password
- vCenter Hostname

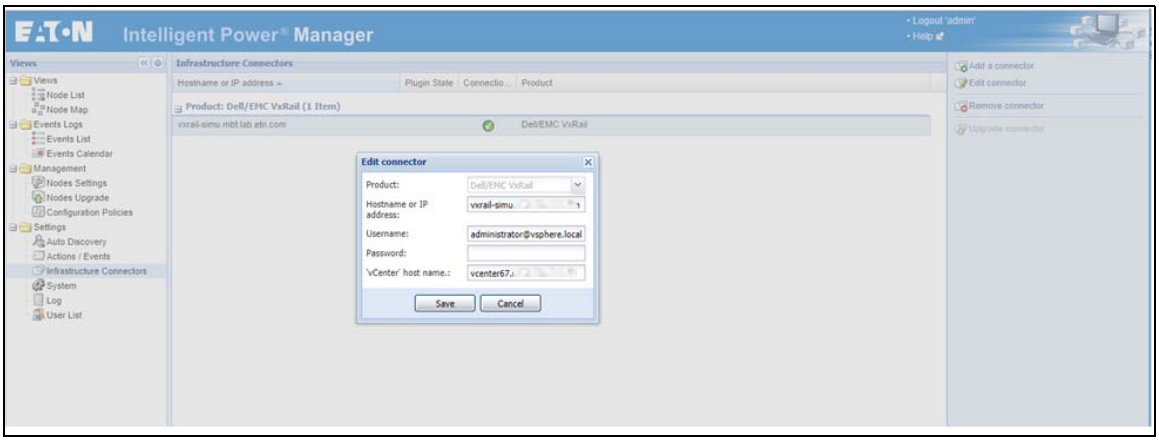

Figure 102. Edit Dell/EMC VxRail Connector

Once the configuration is done and connection is established with VxRail, the connector is displayed in the infrastructure connector with a green icon.

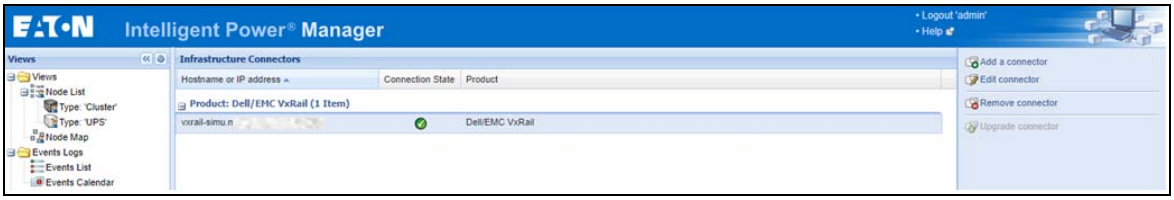

Figure 103. Dell/EMC VxRail Connector Configured

Cluster Monitoring:

Then in the node list, virtual assets managed by the VxRail Connector are retrieved and displayed in the node list. In this case, the VxRail Cluster.

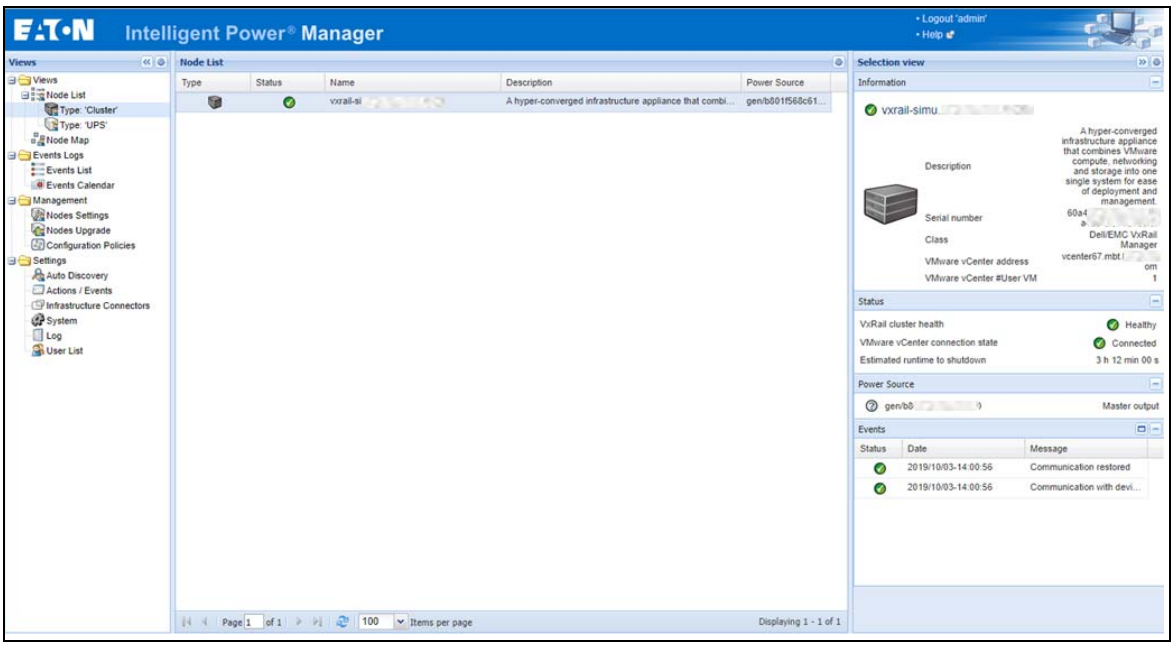

Figure 104. Dell/EMC VxRail Cluster Monitoring

Eaton Gigabit Network Card Settings:

Discover the card: settings / autodiscovery. If you know the IP address of the card, use the "Address Scan" option.

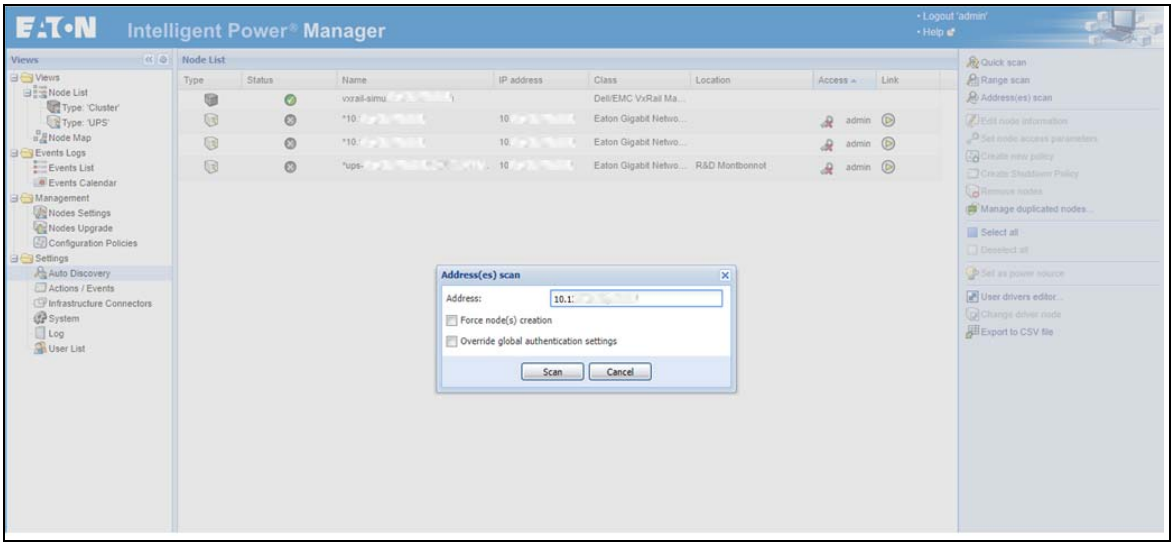

Figure 105. Discovering the Eaton Gigabit Network Card

Once the Eaton Gigabit Network Card is discovered, credential must be set. Select the card and click on "Set node access parameters" and set the card credentials.

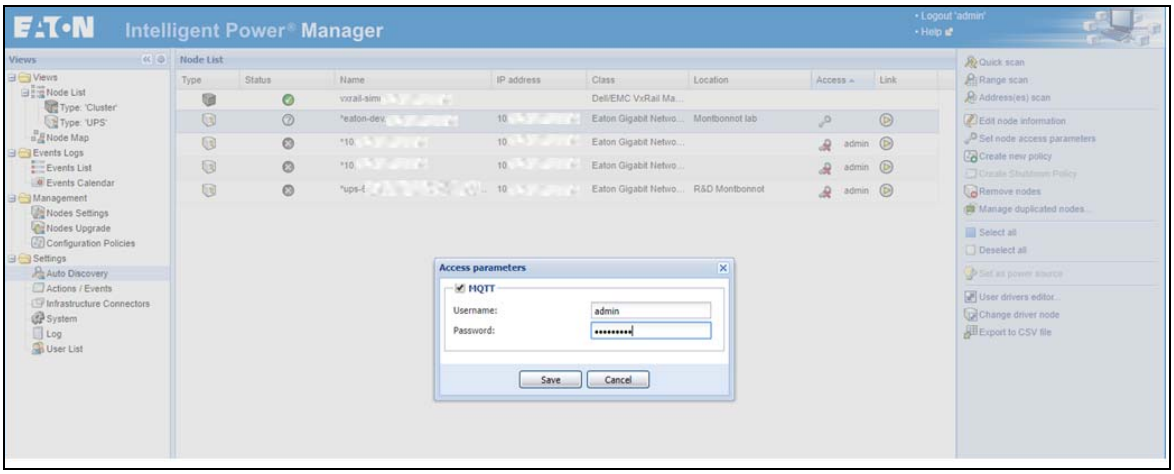

Figure 106. Setting Node Access Parameters for the Eaton Gigabit Network Card

After the access parameters are set, the connection with the Eaton Gigabit Network Card is complete.

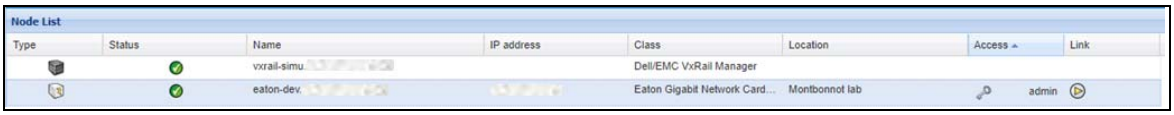

Figure 107. Eaton Gigabit Network Card Access Parameters Configured

The UPS managed by the Eaton Gigabit Network Card is now monitored by IPM.

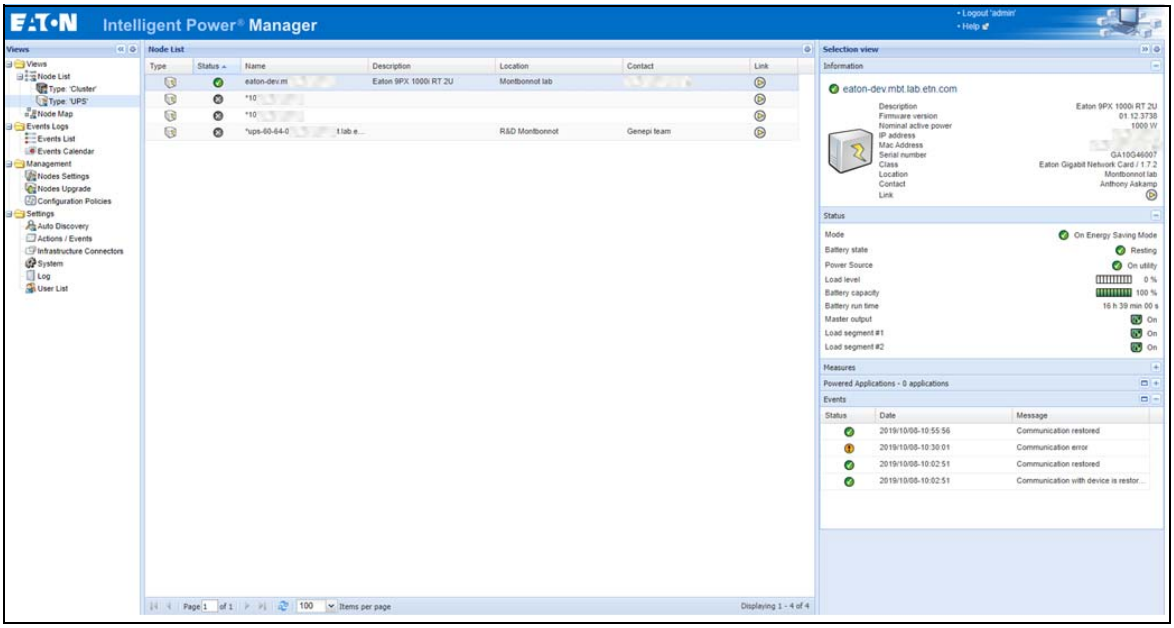

Figure 108. Monitoring of the UPS Managed by the Eaton Gigabit Network Card

Configuration Policy

Define a protection policy by targeting the VxRail Cluster and defining the power source of the cluster, the UPS managed by Eaton Gigabit Network Card.

On the node list:

- Select the cluster
- Right-click and select "Create new policy"

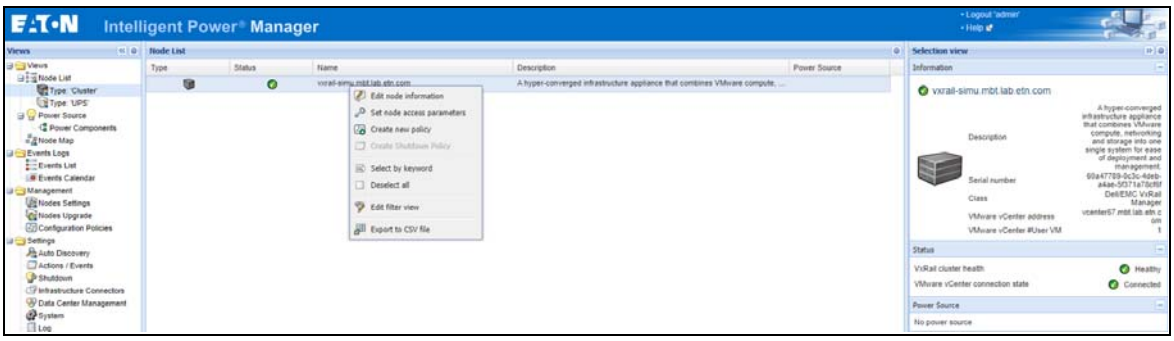

Figure 109. Create New Policy on the VxRail Cluster

Then configure the parameters:

- Target nodes = the VxRail Cluster to protect
- Class list = the power source
- Power source= the UPS protecting the VxRail Cluster

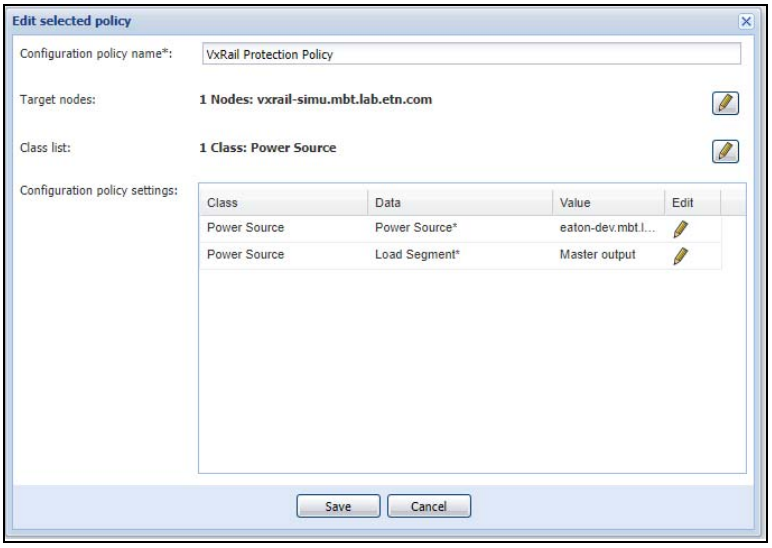

Figure 110. Edit Policy on the VxRail Cluster

Save the policy. The power source of the cluster is set.

IPM will propose to create a shutdown action: click on "yes."

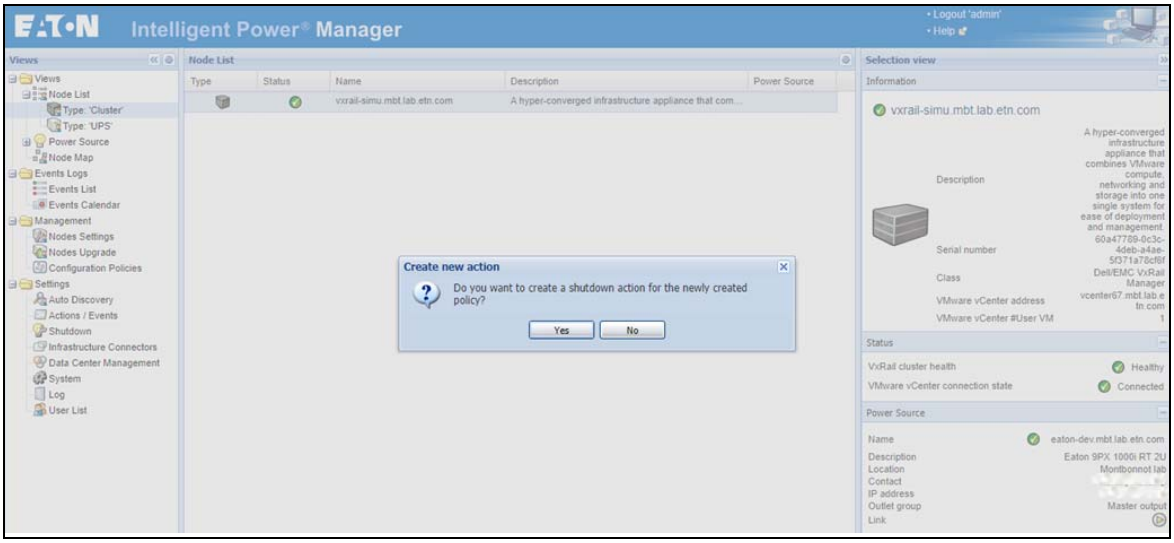

Figure 111. Create New Shutdown Action on the VxRail Cluster

Configure New Action: Cluster Shutdown

The modal opens and is based on the policy previously configured:

- Define the Action Name
- Define in the events list the trigger that will start the action (example: "power failure" on the UPS)
- Then select the action type: "Cluster Shutdown"
- In action settings, select the VxRail Cluster as Target of the action
- Configure timeout values
- Save action

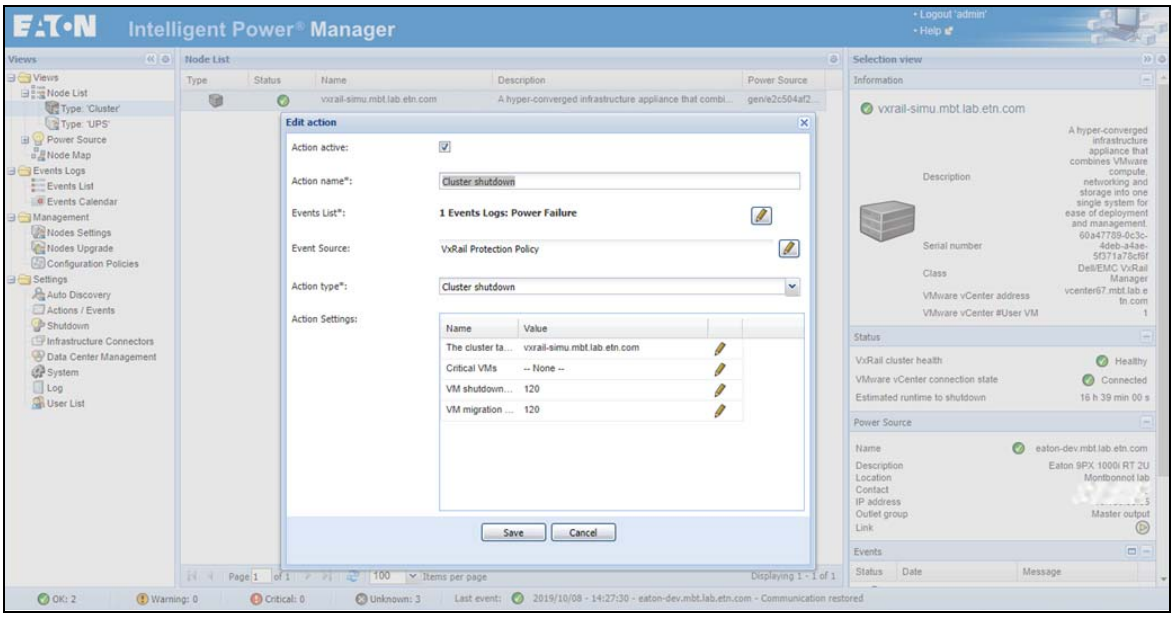

Figure 112. Edit Shutdown Action on the VxRail Cluster

The policy is saved and the power source of the VxRail is configured.

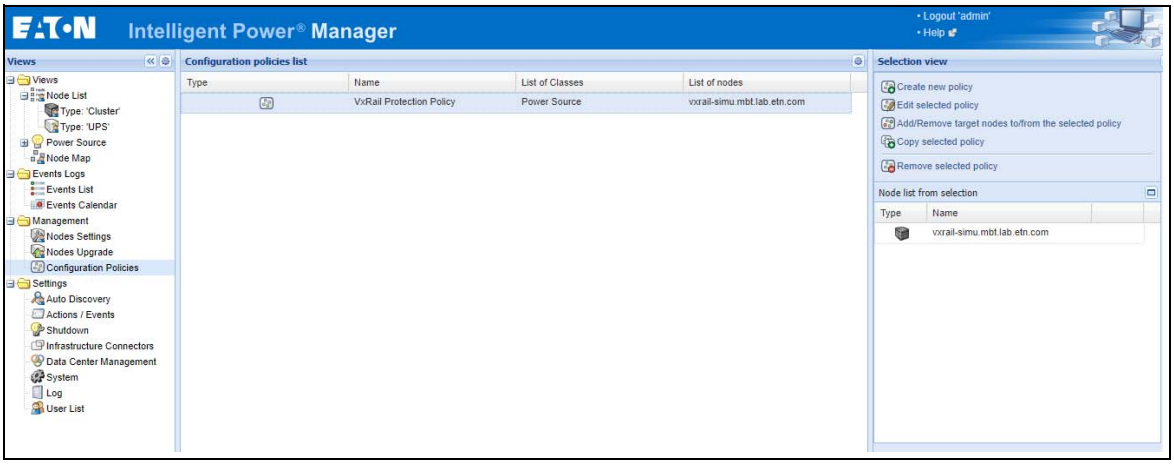

Figure 113. Policy Configured for the VxRail Cluster

Shutdown action is configured. Select the action and click on "test selected action" to trigger the action. It simulates a power event and starts the cluster shutdown action.

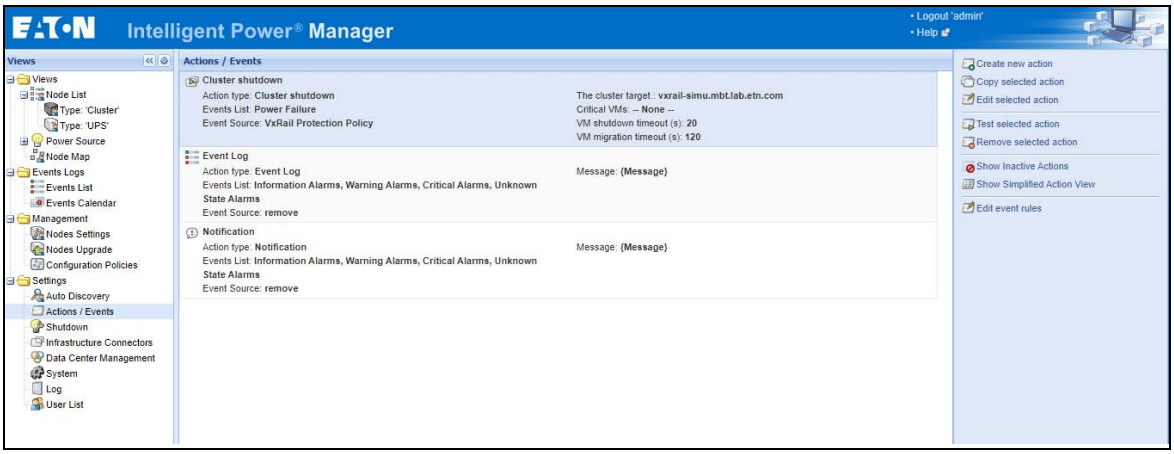

Figure 114. Action Configured for the VxRail Cluster

NOTE For more details about the VxRail Cluster shutdown scenario, see "Cluster Shutdown for Dell/EMC VxRail" on page 50.

Execution Logs for VxRail Cluster Shutdown

After a cluster shutdown, execution logs are available directly from the Eaton Gigabit Network Card:

- Card Menu/System logs/Download System logs/File name: System

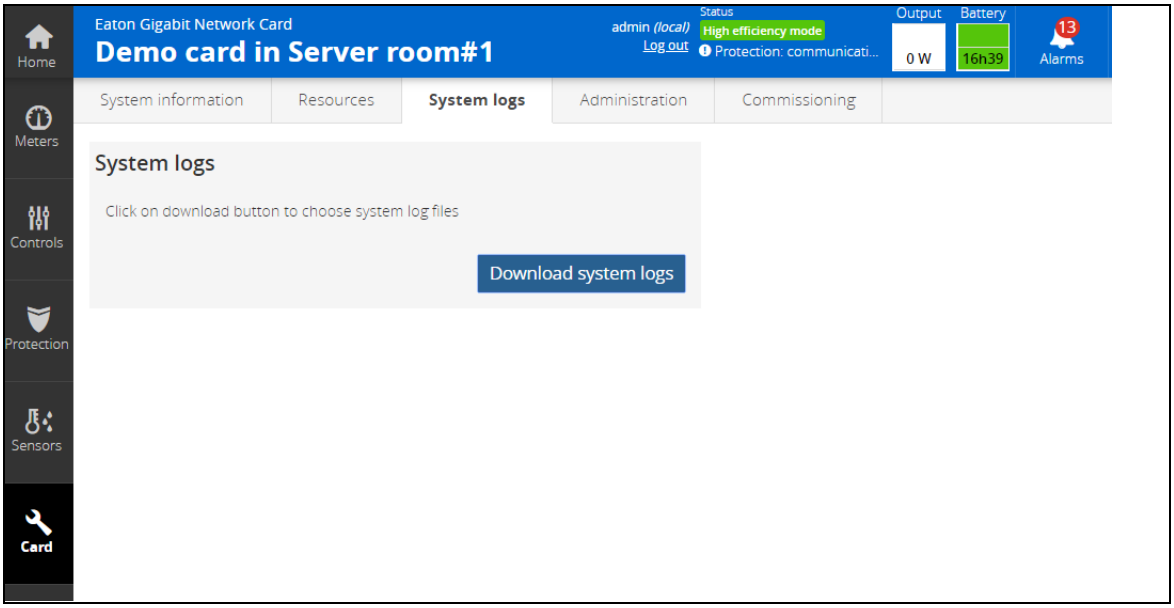

Figure 115. Download System Logs Window

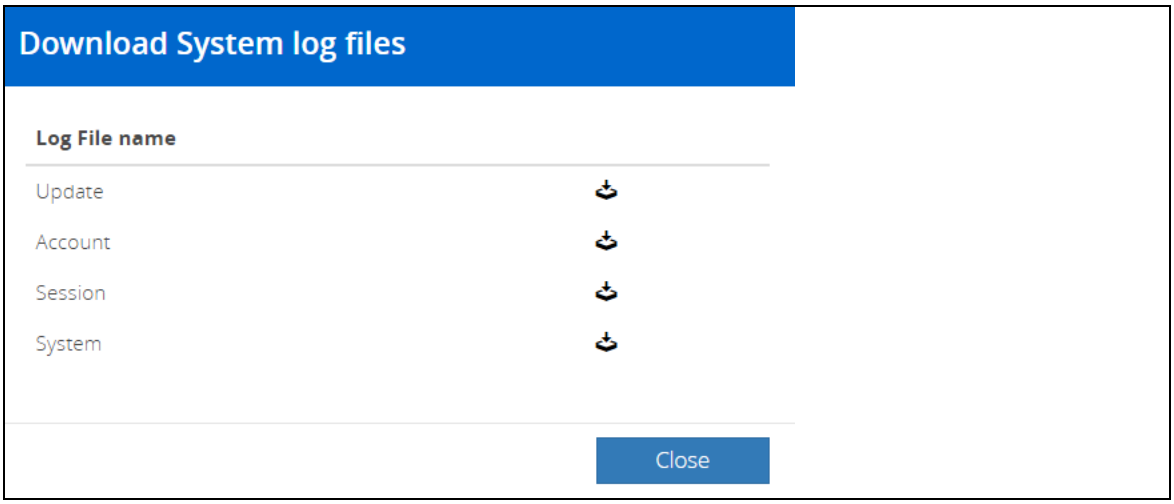

Figure 116. System Log Files Window

From the CSV file downloaded, these logs track the success of the cluster shutdown action.

Date Time(UTC)	Facility	Priority	Application	Message	User
2019-10-17T15:09:31	local4	info	protection	Start execution of script "Custom Shutdown Procedure". (0984d3f3-585f-56ec-abd6-b9c0f39af590)	system
2019-10-17T15:09:41	local4	info	logmessage	VxRail system is Healthy	system
2019-10-17T15:10:50	local4	notice	logmessage	VxRail is shutting-down with request c5d230cb-421e-4baa-b1bc-e5a0ab63ea1b	system
2019-10-17T15:11:54	local4	notice	logmessage	VxRail shutdown completed	system
2019-10-17T15:11:54	local4	info	protection	Execution of script "Custom Shutdown Procedure" succeeded. (0984d3f3-585f-56ec-abd6-b9c0f39af590)	system

Figure 117. Sample CSV File

Eaton Solutions for Microsoft

For Microsoft, Eaton IPM provides two solution architectures that are illustrated in Figure 118 and Figure 119. These solutions require Eaton IPP Windows. Refer to the *Eaton Intelligent Power Protector (IPP) User's Guide* for more information.

Standalone Hypervisor and Local Solution

The standalone hypervisor and local solution architecture for Microsoft is illustrated in Figure 118.

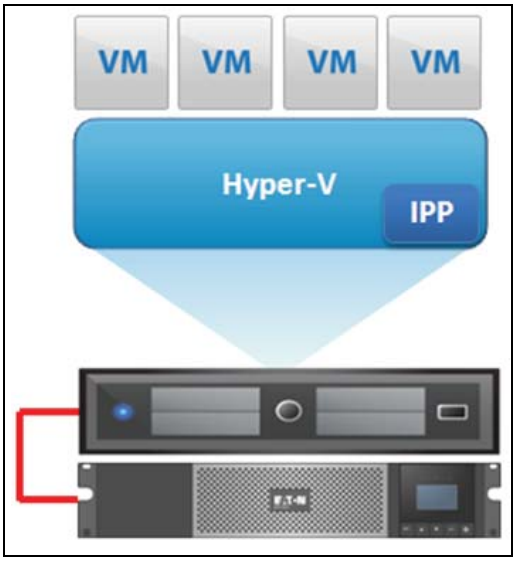

Figure 118. Eaton IPP Running on Hyper-V to Protect Hyper-V

Multiple Hypervisor and Remote Solution

For multiple hypervisor hosts, it is possible to manage shutdown through IPM by using System Center Virtual Machine Manager (SCVMM) or by using Hyper-V. This solution is ideal for large infrastructures working through an SCVMM server (see Figure 119).

This solution provides following feature:

- Hyper-V/Hyper-V server remote maintenance to trigger VM live migration.

NOTE For more information, refer to the *Eaton Intelligent Power Protector (IPP) User's Guide*.

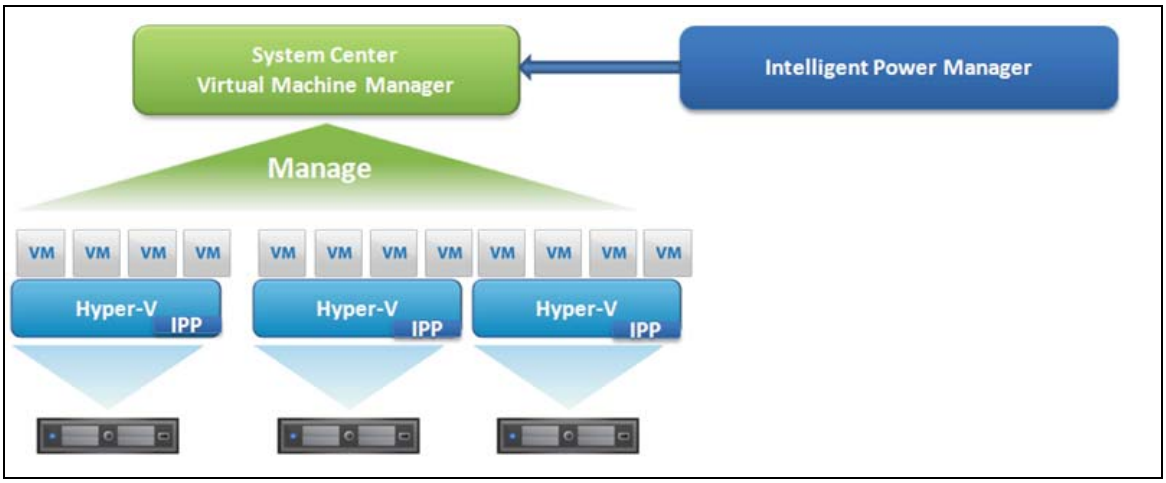

Figure 119. Eaton IPM Connected to SCVMM to Protect Microsoft Virtual Infrastructure

Prerequisites

The virtualization module requires the following prerequisites:

- The Powershell Snap-in for Microsoft SCVMM. Either install the VMM console on the machine hosting Eaton IPM, or install Eaton IPM on the machine hosting SCVMM.
- The server hosting Eaton IPM must be on the same Windows Domain as the SCVMM Server.
- The server hosting Eaton IPM must enable the execution of third party scripts on the local machine (minimum access "Remote Signed," for example, Set-ExecutionPolicy RemoteSigned).

Figure 120 illustrates the parameters that display for an example configuration. To save settings, click **Save** when the fields are updated.

NOTE When configuring the Login Username and Password, we recommend using the Eaton IPM Web interface through https. Using http is also possible, but the password is sent to the local or remote server in clear. In both cases, the encrypted password is stored in Eaton IPM and never again sent on the Client side.

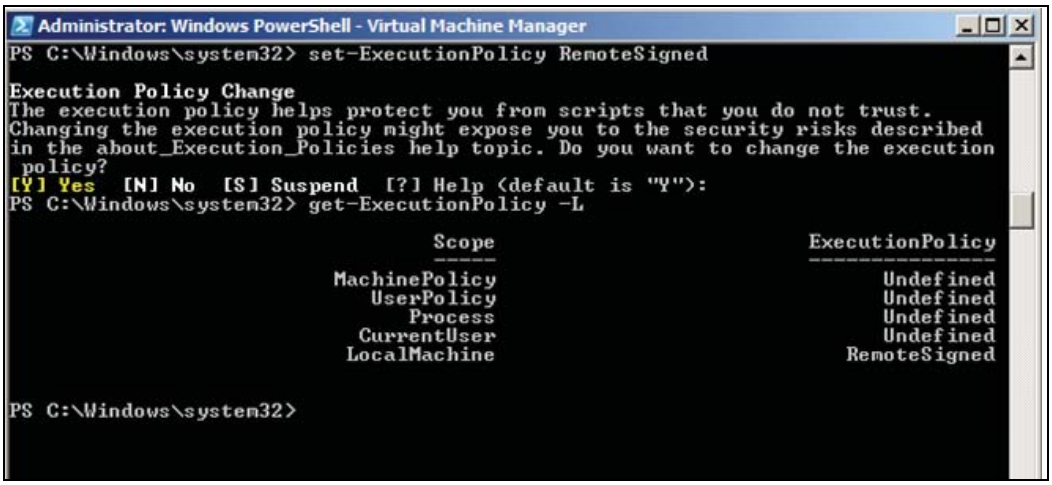

Figure 120. Windows PowerShell - Virtual Machine Manager

Adding an SCVMM Manager

Refer to the Eaton IPM Interoperability List for Microsoft SCVMM / Windows compatibility:

NOTE SCVMM connectors are no longer available in IPM 1.60. SCVMM connector configuration will still work after an upgrade but will not be configurable, it is replaced by the new MS Hyper-V Connector.

- Eaton Operating System Compatibility List

To add a new Microsoft SCVMM (see Figure 121):

1. From the Add a Connector dialog, select Microsoft SCVMM from the Virtualization drop-down list. A second Add a connector dialog displays for your product connector selection.
2. Add identification information for the selected connector (see Figure 97):
   - **Product:** Microsoft SCVMM (already selected in the drop-down list)
   - **Hostname or IP address:** Type Microsoft SCVMM Hostname or IP address
3. Click **Save** after the fields are updated.

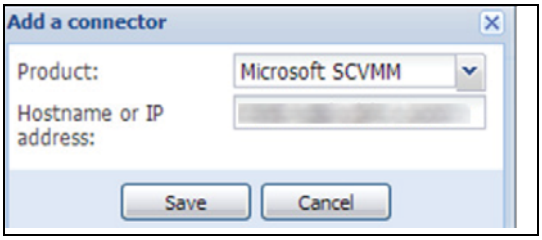

Figure 121. Add Microsoft SCVMM

Adding a Microsoft Hyper-V/Server Connector

Create Microsoft connector

1. Select the Infrastructure connector and click on **Add**

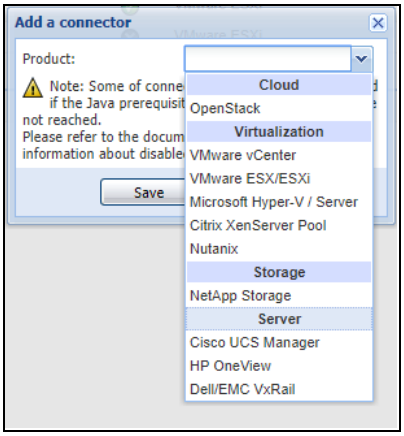

Figure 122. Select Infrastructure connector

2. Select **Microsoft Hyper-V/Server**
3. Configure it properly (for details, check the section Configure Microsoft Server authentication.

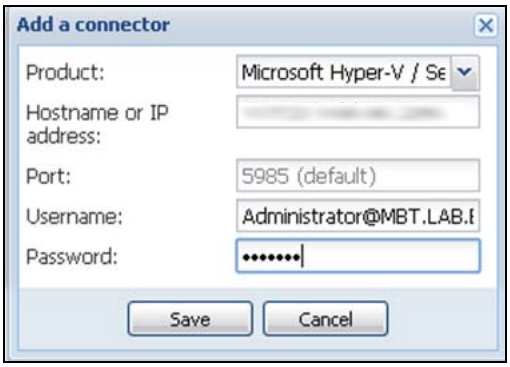

Figure 123. Select Microsoft Hyper-V/Server

4. Check that the communication is Ok

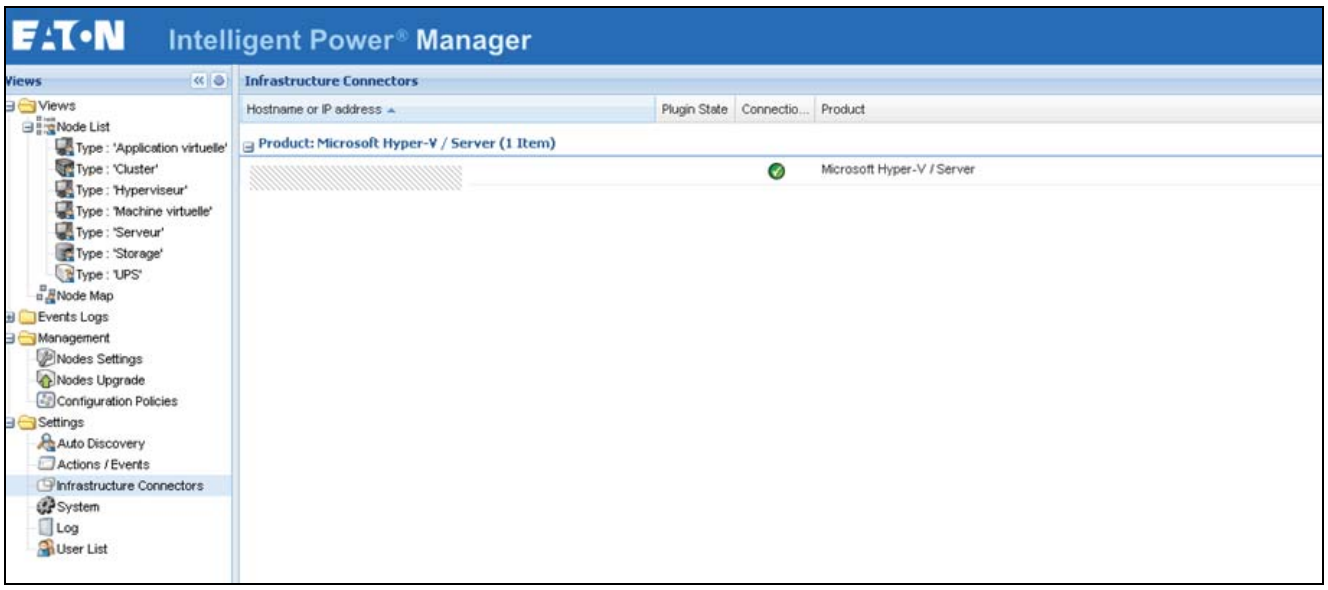

Figure 124. Check Server Communication

Display Data

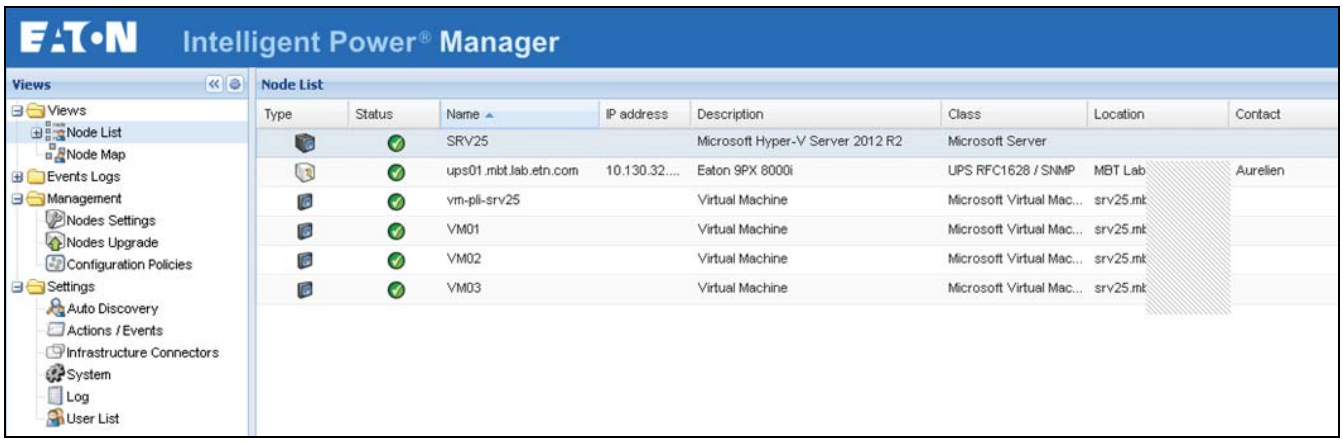

Figure 125. Node List Data Display

Configure Microsoft server authentication

Server Side

Configure Prerequisites

IPM is able to connect to the Microsoft server with two authentication configurations but requires some prerequisites:

WinRM service must be enabled:

```
winrm quickconfig
```

WinRM service AllowUnencrypted must be "true":

```
winrm set winrm/config/service '@{AllowUnencrypted="true"}'
```

Or remotely:

```
winrm set winrm/config/service/auth '@{Basic="true"}'
```

Kerberos Authentication

The default configuration is shown in Figure 126, there is no need to modify it.

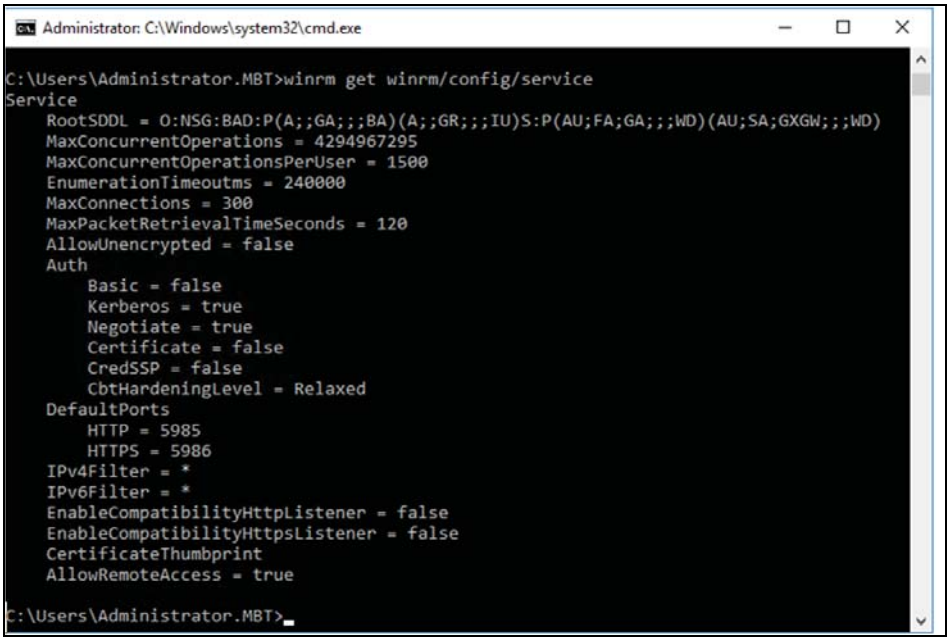

Figure 126. Kerberos Authentication Default Configuration

Basic Authentication

To allow the basic authentication you need to change the "auth" parameters:

```
winrm set winrm/config/service/auth '@{Basic="true"}'
```

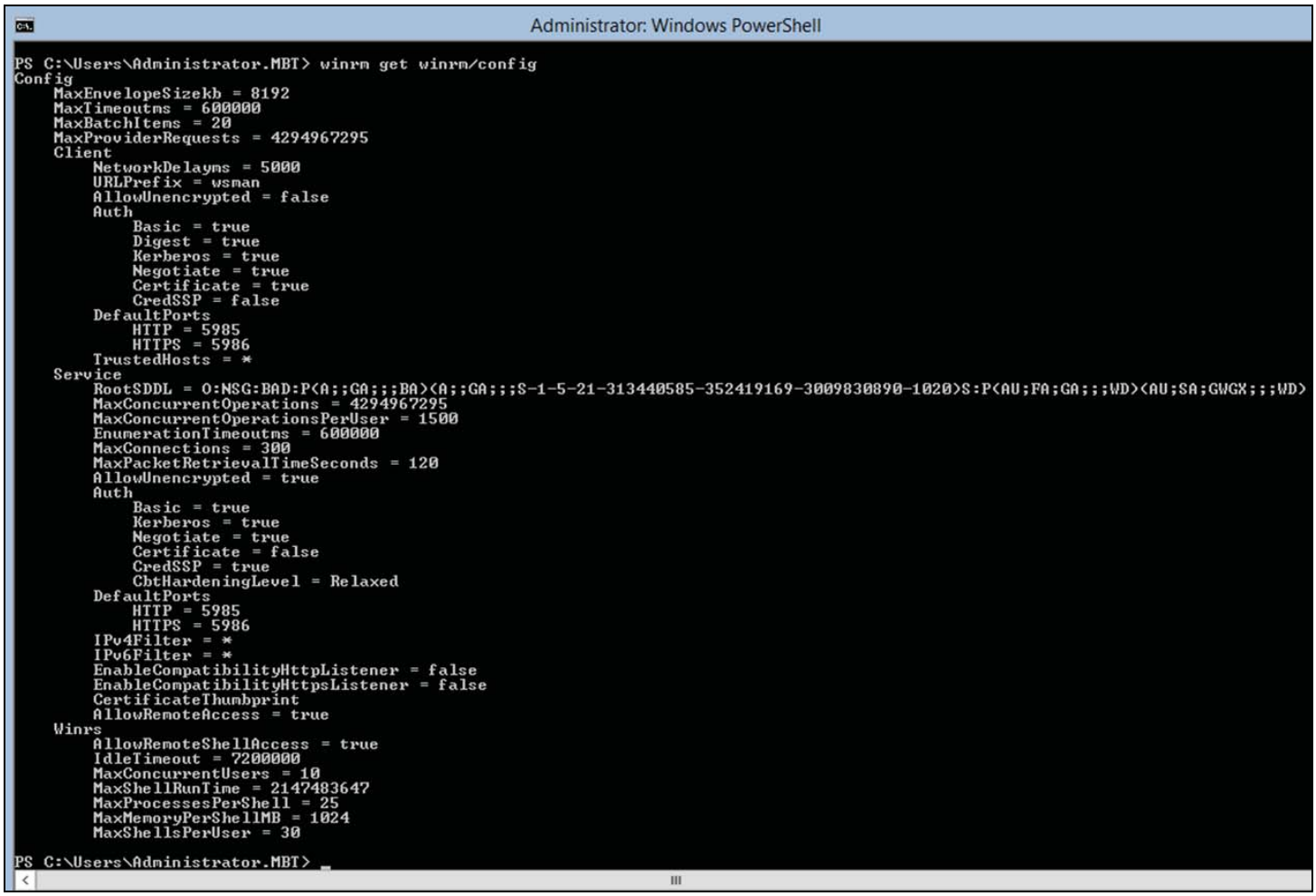

Figure 127. Basic Authentication Parameters

Client side (IPM hosted server)

Kerberos Authentication - Windows server:

- Configure the connector with the domain name e.g. "Administrator@DOMAIN.COM"
- The domain name must be in uppercase.
- The IPM will create a file named "krb5.conf" in "%%/IntelligentPowerManager/emc4j/etc/"

Virtual appliance

Modify the file "/etc/krb5.conf" as in Figure 128.

NOTE The domain name must be in uppercase.

```
vi /etc/krb5.conf

[libdefaults]

    default_realm = DOMAIN.COM

[realms]

    DOMAIN.COM = {

        kdc = kerberos.DOMAIN.COM

        admin_server = kerberos.DOMAIN.COM
```

Figure 128. Virtual Appliance Configuration

Eaton Solutions for Citrix

For Citrix, Eaton IPM provides two solution architectures that are illustrated in Figure 129 and Figure 130. These solutions require Eaton IPP Linux. Refer to the *Eaton Intelligent Power Protector (IPP) User's Guide* for more information.

Standalone Hypervisor and Local Solution

The standalone hypervisor and local solution architecture for Citrix is illustrated in Figure 129.

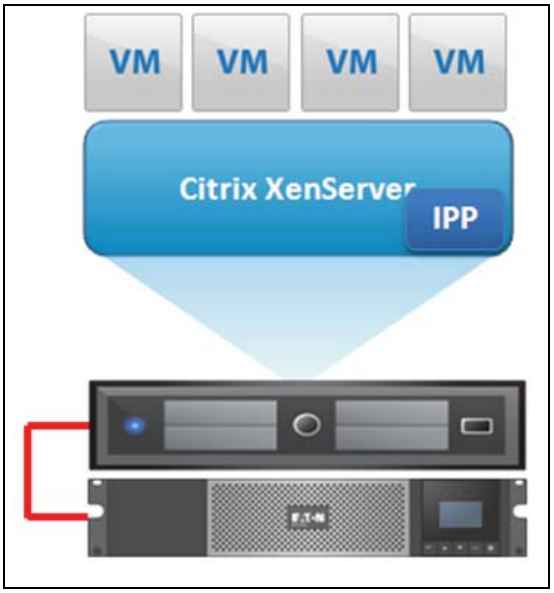

Figure 129. Eaton IPP Running on Citrix XenServer

Multiple Hypervisor and Remote Solution

For multiple hypervisor hosts, it is possible to manage shutdown through IPM by using System Center Virtual Machine Manager (SCVMM). This solution is ideal for large infrastructures working through XenCenter.

This solution is integrated into Eaton IPM and provides the following features:

- XenServer remote maintenance to trigger VM XenMotion
- XenServer remote shutdown

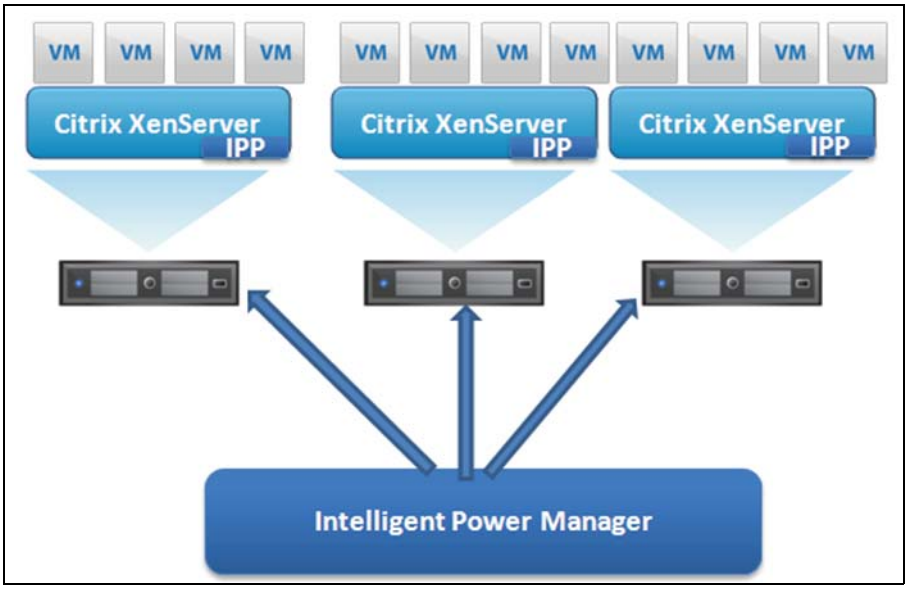

Figure 130. Eaton IPM Connected to XenServers (Triggers XenMotion and Eaton IPP Running on XenServer Infrastructure)

Figure 131 describes the recommended approach to protect your Citrix infrastructure. The latest Citrix infrastructure connector allows you to define configuration policies and use them in advanced events and actions schemes to address all your needs for business continuity. You can now install IPP on one IPM instead of installing it on each server.

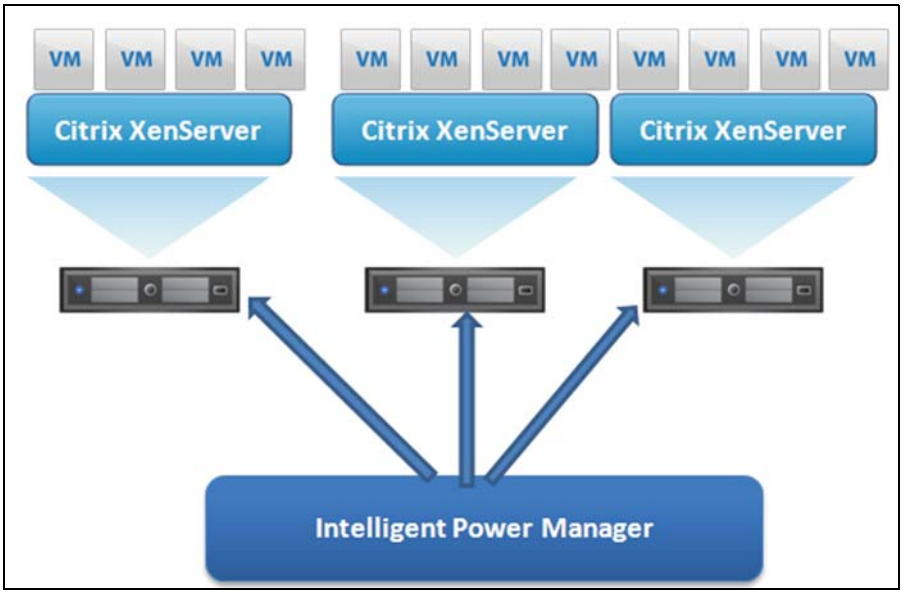

Figure 131. Eaton IPM Connected To XenServer to protect the XenServers

Prerequisites

The virtualization module requires the following prerequisites:

- XenCenter must be installed to manage the XenServers.
- To provide the VM graceful shutdown, you must install Xen tools on each VM.

Adding a Citrix XenServer Hypervisor List

To add a new Citrix XenServer List:

1. From the Add a Connector dialog, select Citrix XenServer from the Virtualization drop-down list. A second Add a connector dialog displays for your product connector selection.
2. Add identification information for the selected connector (see Figure 132):
   - **Product:** Citrix XenServer is already selected in the drop-down list
   - **Hostname or IP address:** Type Citrix XenServer Hostname or IP address
   - **Username**: Type Citrix XenServer Administrator Username
   - **Password:** Type Citrix XenServer Administrator Password
3. Click **Save** after the fields are updated.

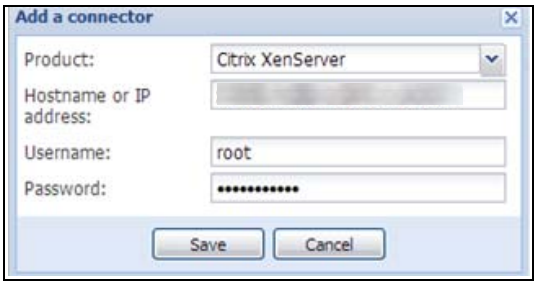

Figure 132. Add Citrix XenServer

Adding a XenCenter

Because Citrix XenCenter is a Client and not a Manager, you can install a plug-in on the system where XenCenter is installed (see Figure 133). This plug-in allows you to use Eaton IPM in XenCenter.

To add a new XenCenter:

1. From the Add a Connector dialog, select Citrix XenCenter from the Virtualization drop-down list. A second Add a connector dialog displays for your product connector selection.

1. Add identification information for the selected connector (see Figure 132):
   - **Product:** Citrix XenCenter is already selected in the drop-down list
   - **XenCenter Plugin:** Select the checkbox to use Eaton IPM in XenCenter
2. Click **Save** after the fields are updated.

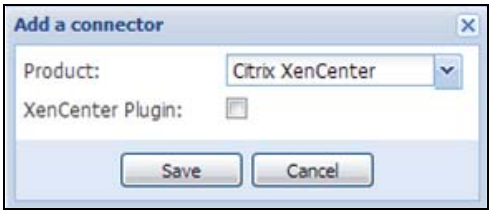

Figure 133. Add Citrix XenCenter

Eaton Solution for Red Hat

For Red Hat®, the Eaton IPM provides the solution architecture illustrated in Figure 134. This solution requires Eaton IPP Windows.

This solution provides the following feature:

- Provides graceful shutdown for KVM with Eaton IPP installed on each KVM system

NOTE For more information, refer to the *Eaton Intelligent Power Protector (IPP) User's Guide*.

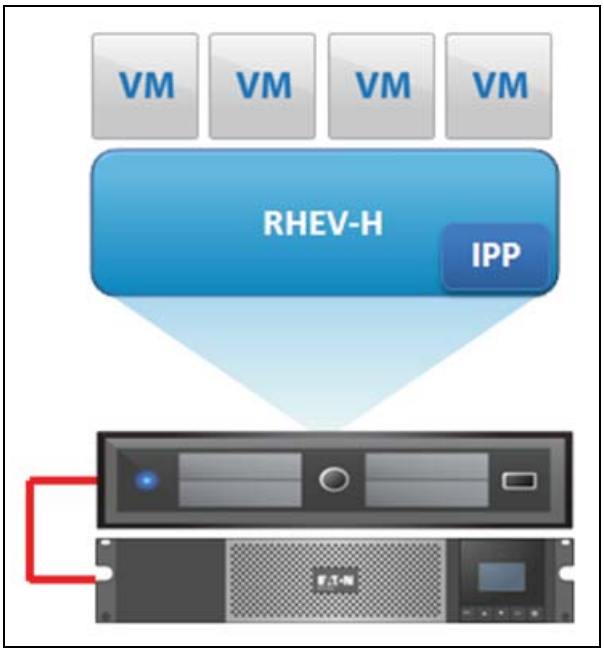

Figure 134. Standalone Hypervisor and Local Solution

NOTE For more information, refer to the *Eaton Intelligent Power Protector (IPP) User's Guide*.

Eaton Solutions for OpenSource Xen

For OpenSource Xen, the Eaton IPM provides a solution architecture that is illustrated in Figure 135. This solution requires Eaton IPP Windows. Refer to the *Eaton Intelligent Power Protector (IPP) User's Guide* for more information.

Standalone Hypervisor and Local Solution

For standalone hypervisor hosts, it is possible to manage shutdown through IPP installed on each Xen system. This solution is ideal for large infrastructures working through XenCenter.

This solution provides the following feature:

- Provides graceful shutdown for Xen with Eaton IPP installed on each Xen system

NOTE For more information, refer to the *Eaton Intelligent Power Protector (IPP) User's Guide*.

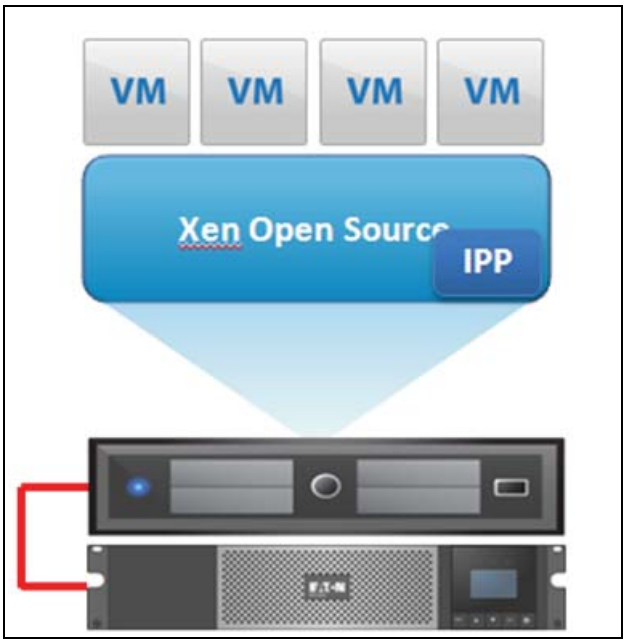

Figure 135. Hypervisor and Local Solution

Eaton Solutions for Nutanix

IPM Nutanix connector allows to connect to one Nutanix unit : Prism Central or Prism Element.

In this integration, the scope is to protect the User Virtual Machines or the entire cluster from power events.

Eaton IPM is set up to provide graceful shut down of the User Virtual Machines or to shutdown the cluster.

Eaton IPM uses a navigation panel to simplify the connection of IPM to the Nutanix infrastructure.

To create a Nutanix connector, the user only needs to provide the network address (or FQDN) of the Nutanix box and a valid login/password pair for the authentication. Once the connector is successfully created, a Nutanix node is created in IPM.

As soon as the connection is established, all clusters and all User Virtual Machines (UVM) are retrieved from the Nutanix box to be displayed in IPM as Cluster or Virtual Machine nodes.

"Configuration policies" and "advanced events and actions" features of IPM can be configured to ensure the protection of Nutanix environment, in case of a power or environmental event. Two types of policies are available:

- **Cluster shutdown**: The clusters are now monitored, and it's possible (from IPM) to perform a graceful shutdown.
- **VM management**: The UVM nodes are now monitored and IPM provides the ability to apply the following actions: On, Off, Suspend, guest shutdown on each individual UVM.

Nutanix DashBoard

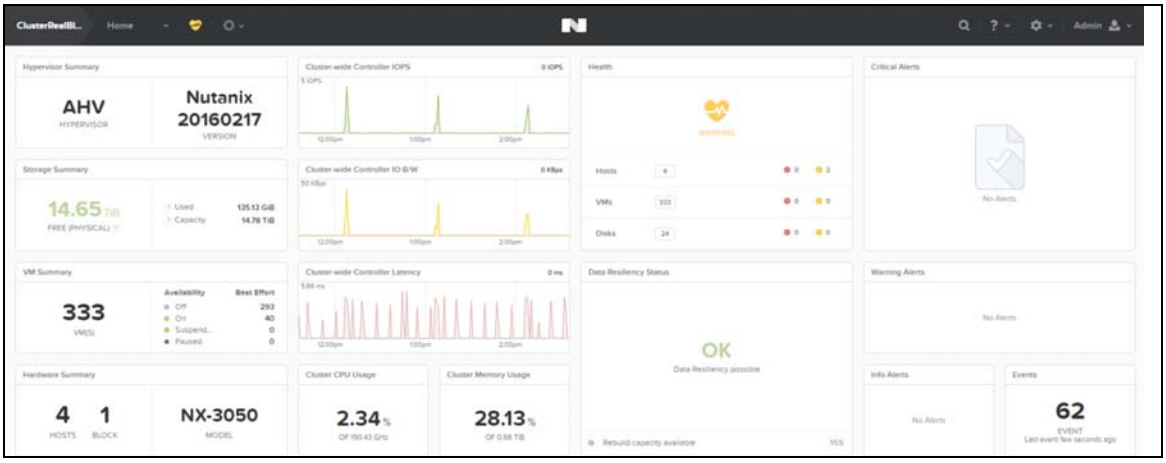

Figure 136. Infrastructure Connector Screen

Create Nutanix connector

1. From the left side navigation panel, select Infrastructure Connectors. Once you have selected Infrastructure Connectors a new screen will open. At the top right side of the page, click on Add a Connector.

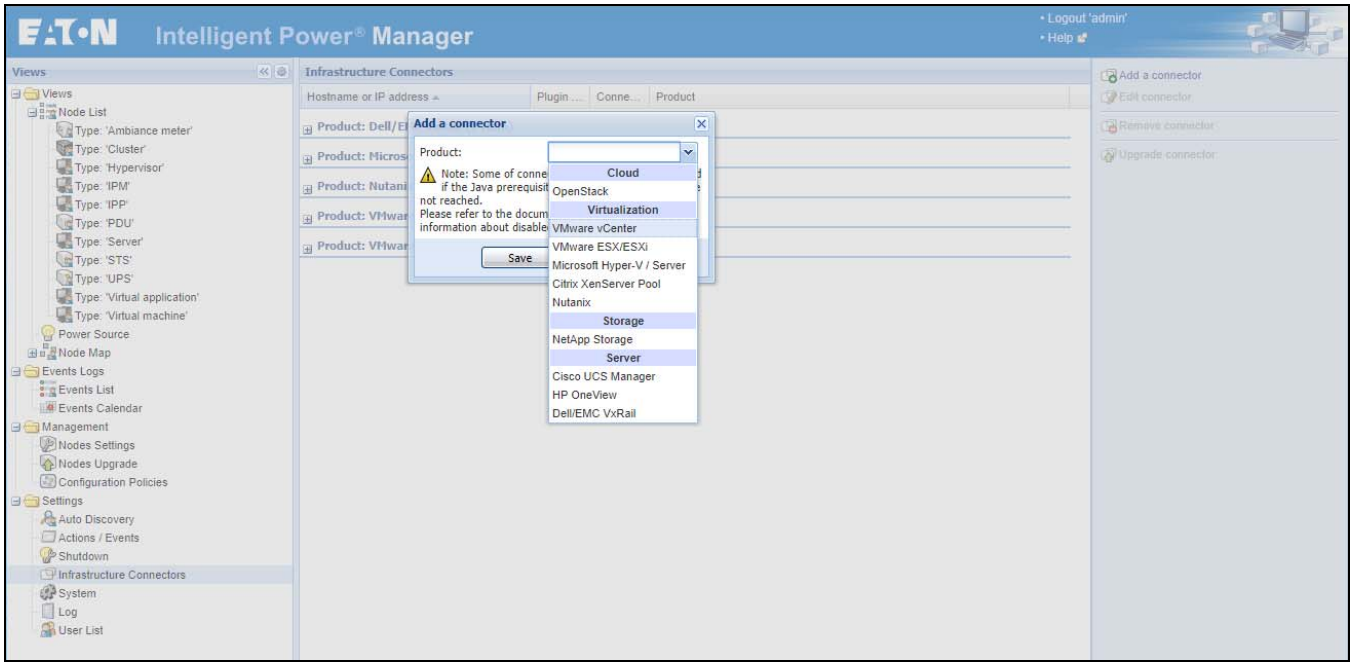

Figure 137. Add Connector Screen

2. Select Nutanix as shown on the screen shot directly above.
3. Configure it with host name, user name and a password of the Nutanix system.

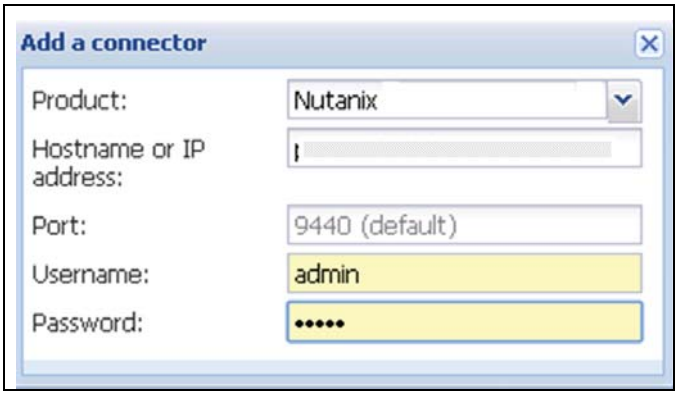

Figure 138. Add Connector User Name/Password

4. Check that the communication is Ok.

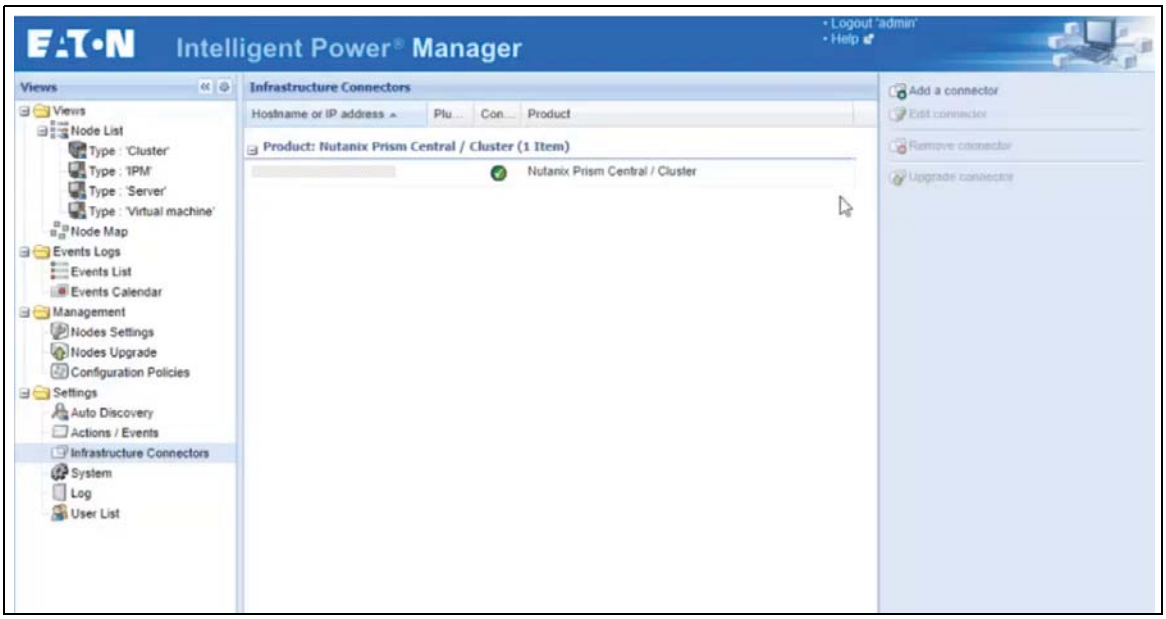

Figure 139. Communication Check

Display Nutanix Clusters and UVM Data

Select the Node List panel and create a filter by type, you will see the same list of VMs in the "Virtual Machine" filter that you see on the Nutanix UI.

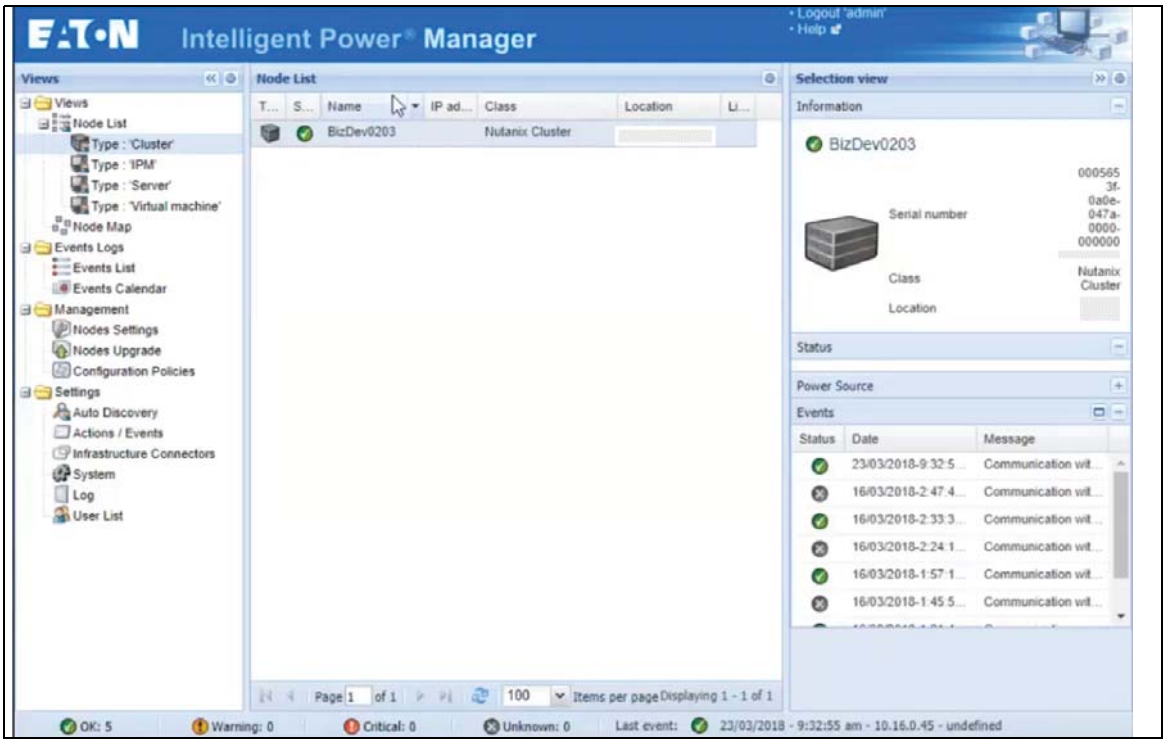

Figure 140. Node List Cluster Filter

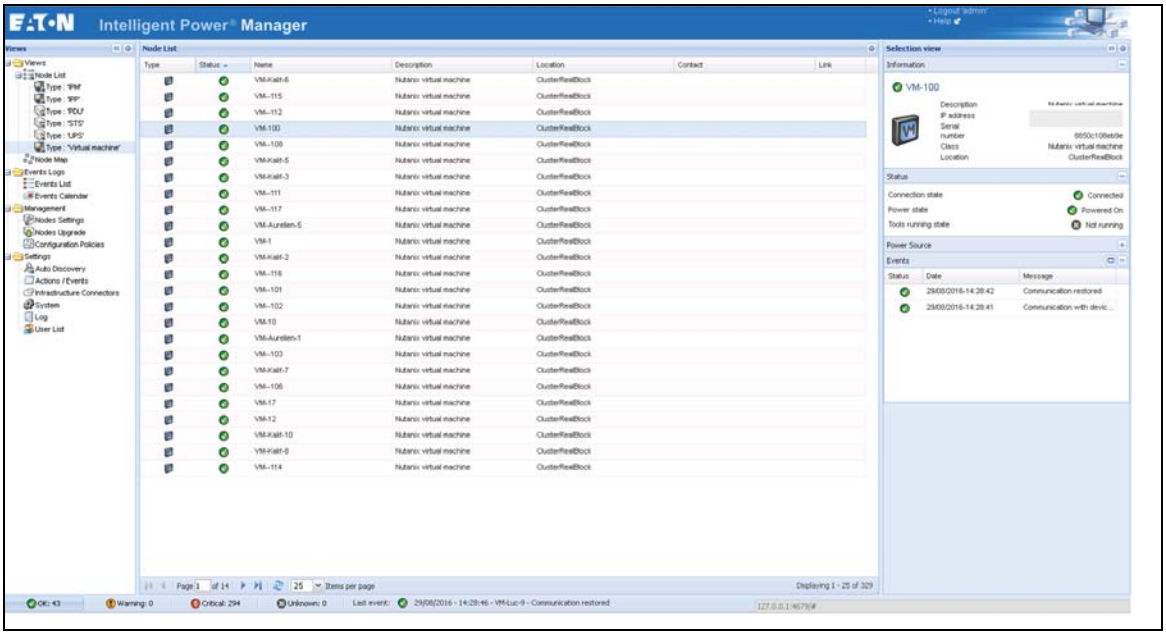

Figure 141. Node List VM Filter

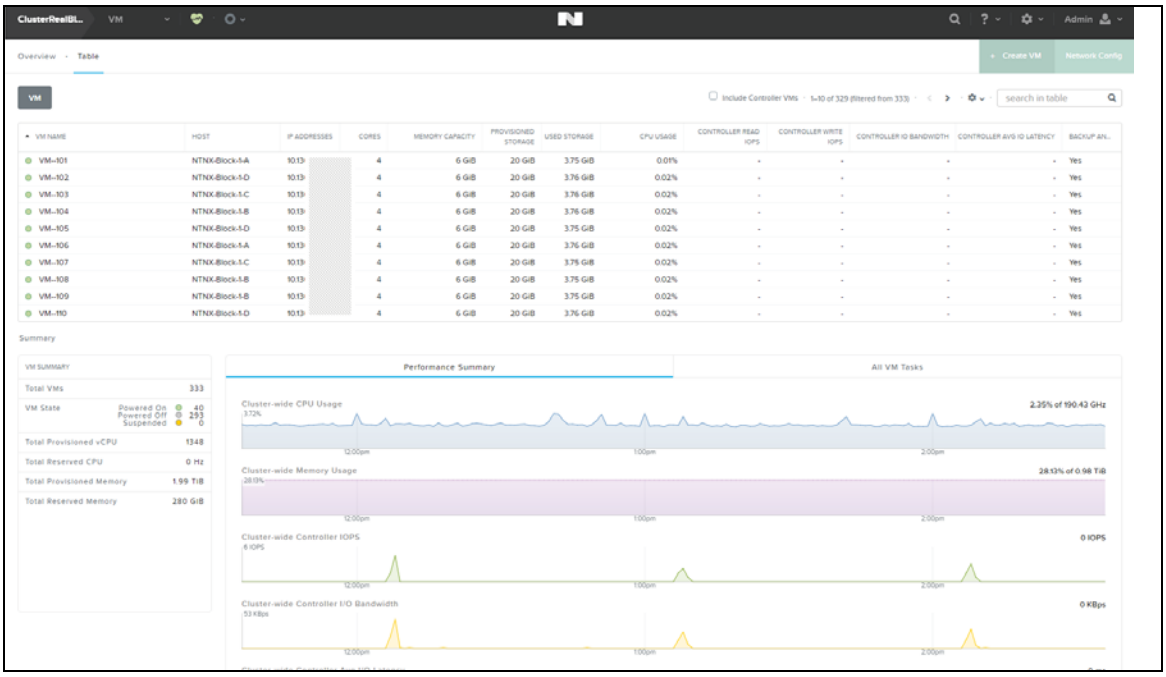

Figure 142. Node List VM Filter Nutanix

Configure Nutanix Actions

Before you configure a Nutanix action, you should become familiar with creating actions in IPM by reading the section Advanced events and actions.

Main features for Nutanix:

- **Cluster shutdown**: possibility to perform graceful shutdown.
- **VM power action**: The UVM nodes are now monitored and IPM provides the ability to apply the following actions: On, Off, Suspend, guest shutdown on each individual UVM.

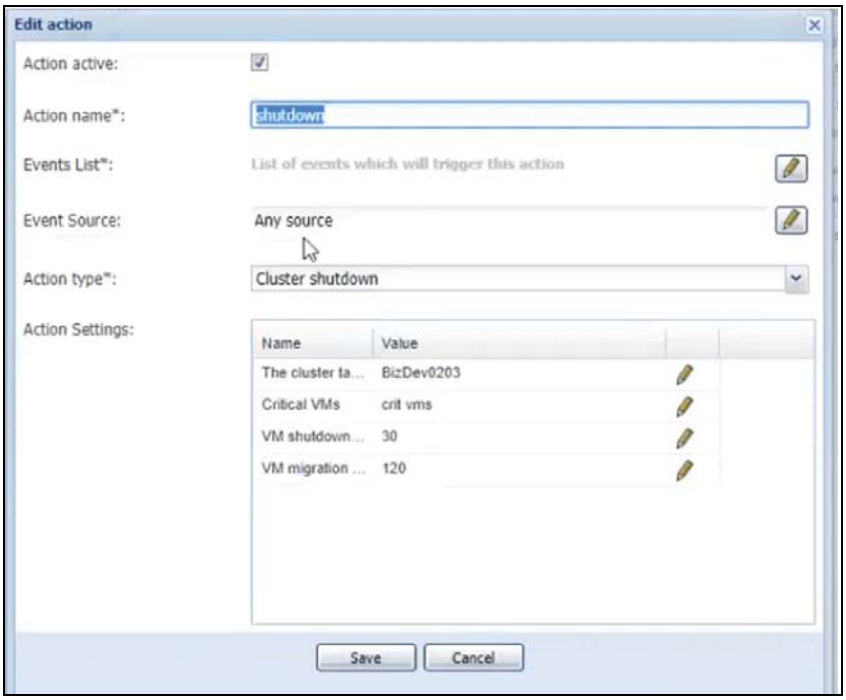

Figure 143. Cluster Shutdown

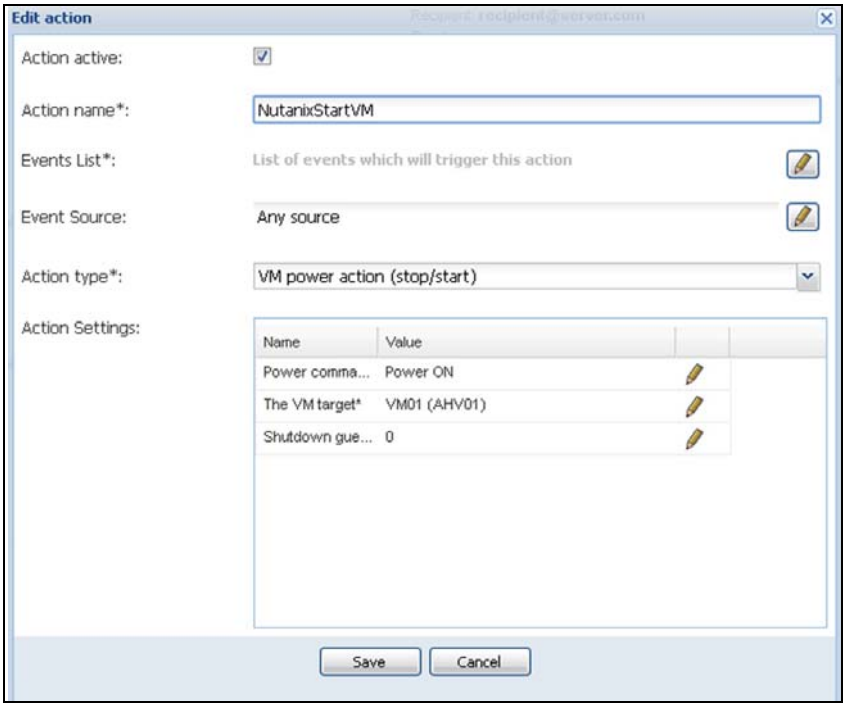

Figure 144. VM Power Actions

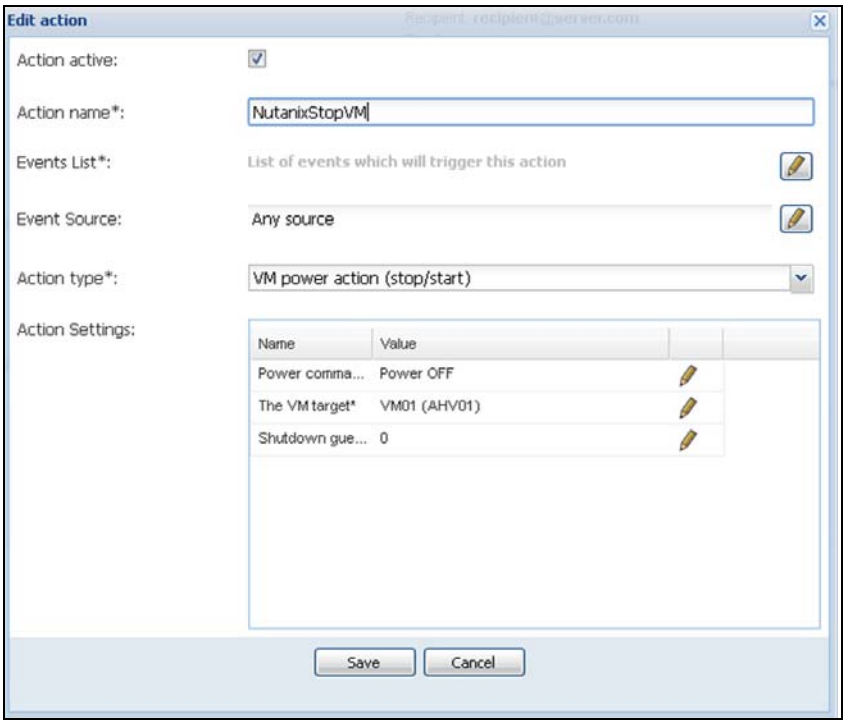

Figure 145. Configure Start and Stop Action

Eaton Solutions for OpenStack

IPM integrates infrastructure connector for OpenStack users. This connector brings the following new features:

- Supervise the following OpenStack components:
  - Physical hosts,
  - Virtual machines (on specific host),
  - Storage hosts,
  - Storage Volumes;
- Trigger the following actions on Power or Environmental events:
  - Virtual Machines Management through Nova (move, shutdown and start)
  - Storage volumes Migration through Cinder.

NOTE This infrastructure connector is available only to users having a GOLD license.

Create an OpenStack Connector

1. Go to "System" panel.
2. Enable the "Infrastructure Connectors" module.
3. Go to the "Infrastructure Connectors" panel.
4. Add a connector and select "OpenStack" as product type.

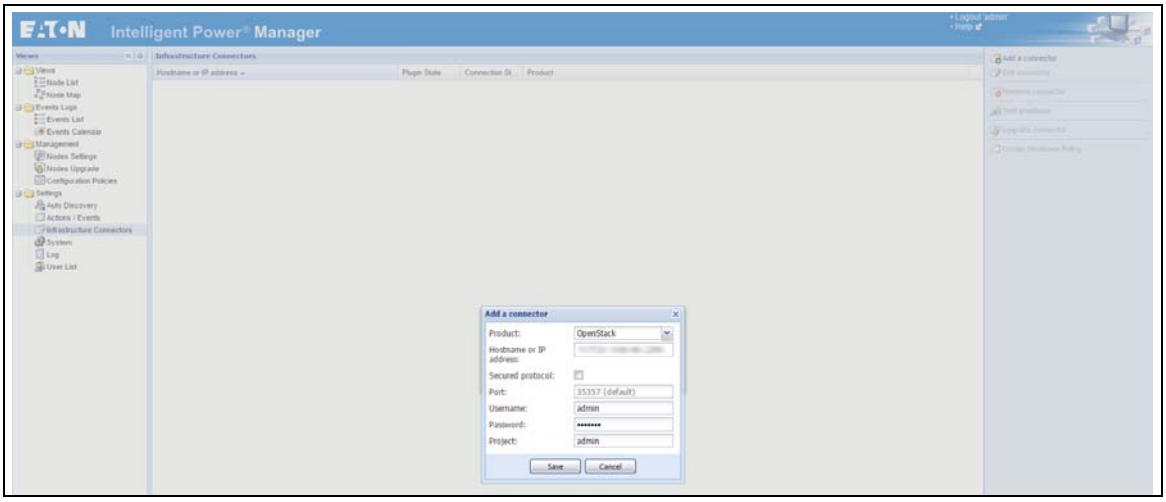

Figure 146. Add Connector Panel

5. Click on save.

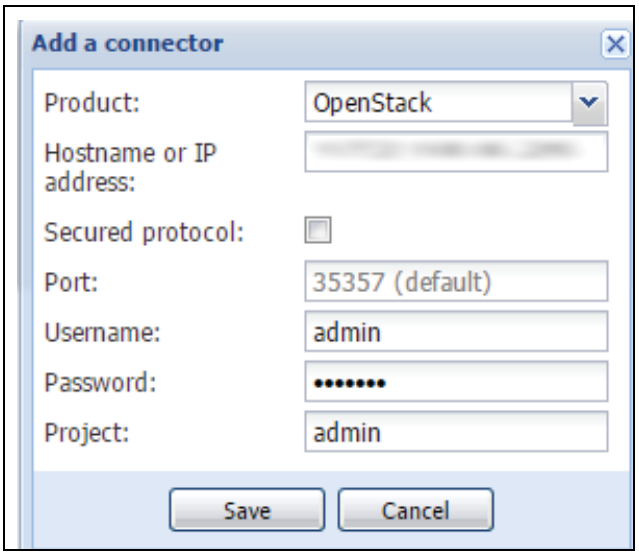

Figure 147. Save Connector

6. After the initialization delay, you should see the green icon telling you that the communication is established.

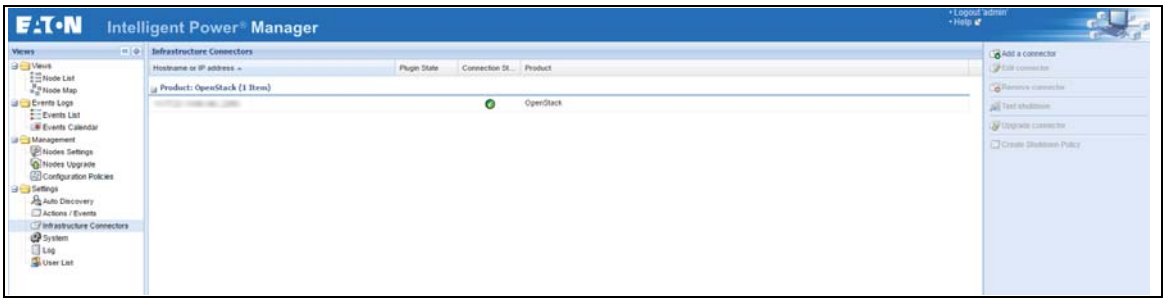

Figure 148. Communication Confirmation

7. You can go now check the Node List and see the new nodes that are appearing.

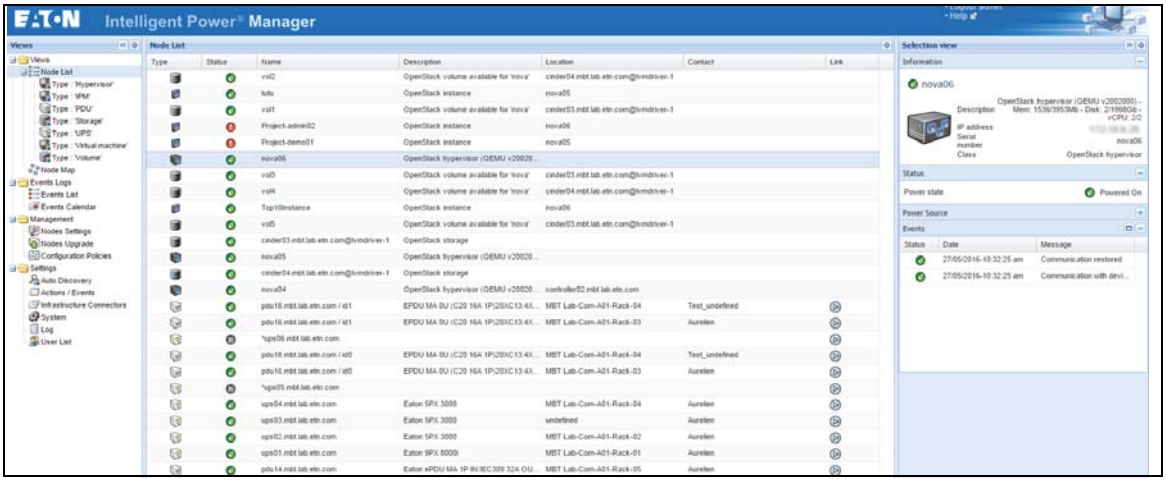

Figure 149. Node List

8. You can also create a filter and focus on some specific nodes.

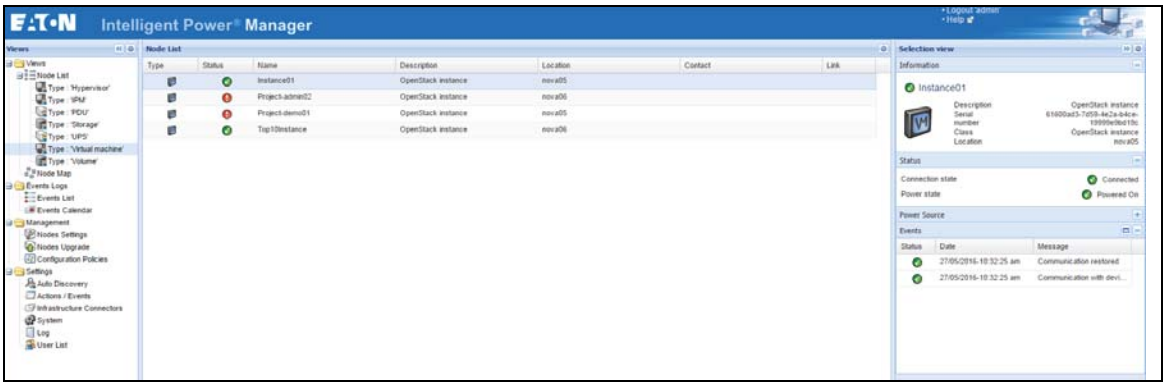

Figure 150. Node Filter

How-to use the OpenStack feature

Along with the OpenStack connector, some actions are available to manage the IT load behind.

To use and configure those actions, you need to follow the step by step procedure below.

1. Set up a configuration policy to define the scope of the future actions.
2. Define the events on which your actions will be launched.
3. Create the action regarding your needs:
    a. To shutdown OpenStack instances when the runtime threshold is reached:

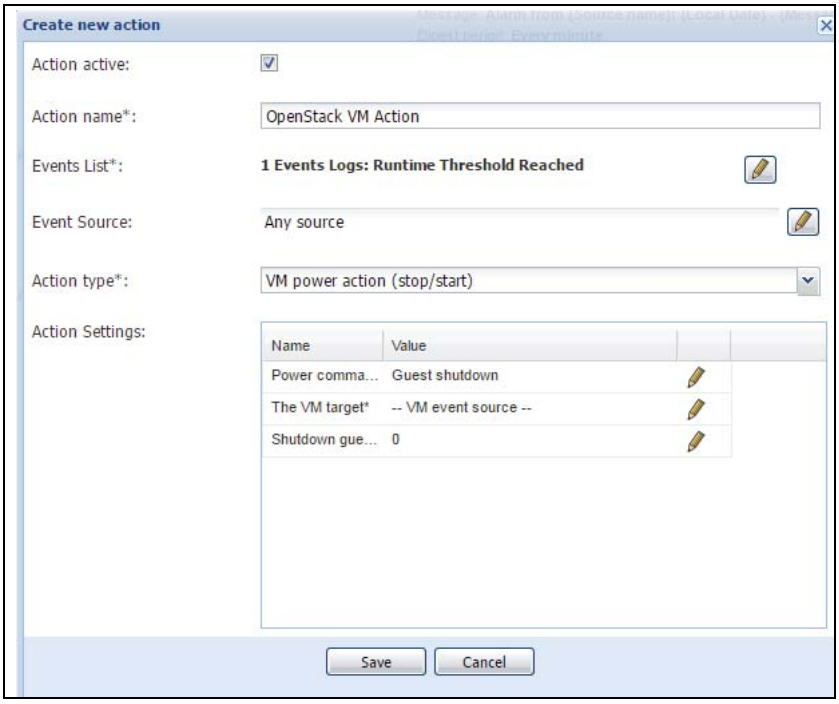

Figure 151. Create Shutdown Action

b. To migrate OpenStack instances when the power is lost:

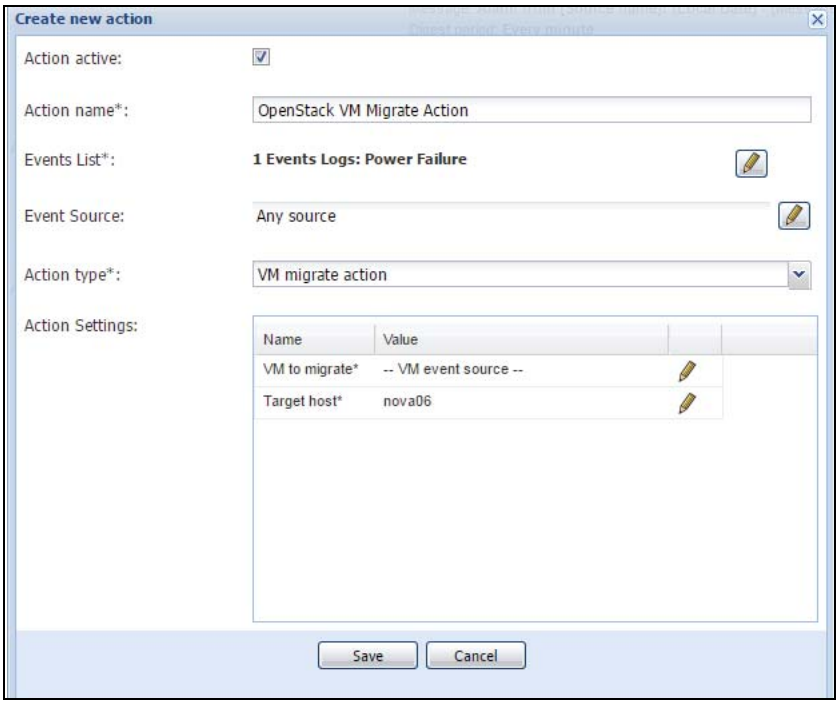

Figure 152. Create Migrate Action

4. Similarly, the following actions are also available:
   a. To start OpenStack instances;
   b. To migrate OpenStack volumes;
   c. To shutdown OpenStack Host (only the systems supported by OpenStack).

Eaton Solutions for HPE OneView

IPM integrates infrastructure connector for HPE OneView users. This connector retrieves in IPM all servers managed by one (or several) HPE OneView instance(s). HPE OneView provides the rack where each server is installed and IPM stores it as the location. Thanks to this spatial information, HPE OneView users can trigger the power capping ability of HPE servers on environmental events occurring in their rack.

Create an HPE OneView Connector

1. Go to "System" panel.
2. Enable the "Infrastructure Connectors" module.
3. Go to the "Infrastructure Connectors" panel.
4. Add a connector and select "HP OneView" as product type.

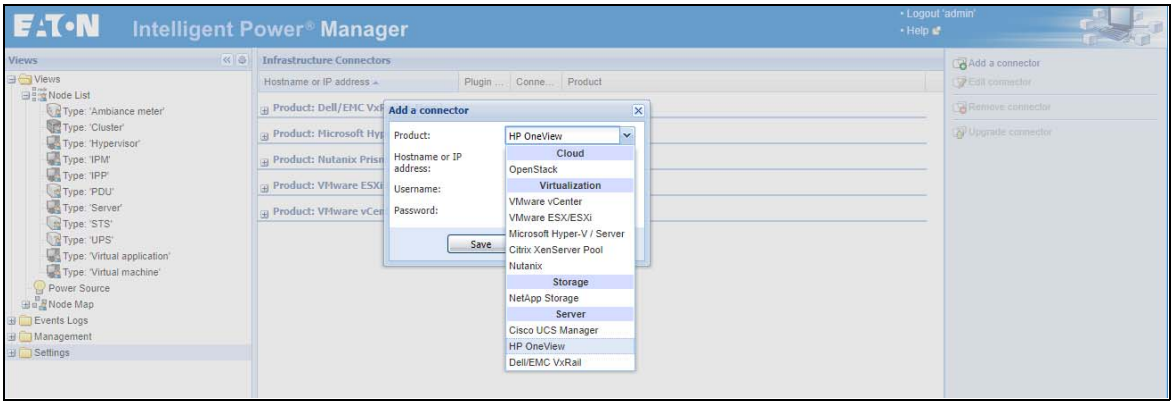

Figure 153. Add Connector Panel

5. Click on save.

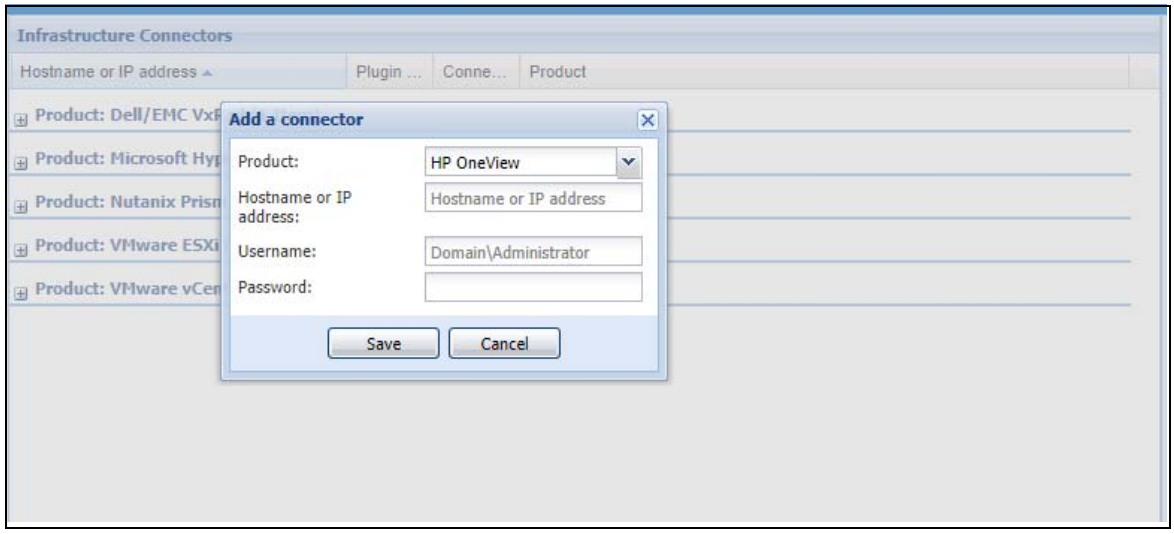

Figure 154. Add Connector Save

6. After the initialization delay, you should see the green icon telling that the communication is established.

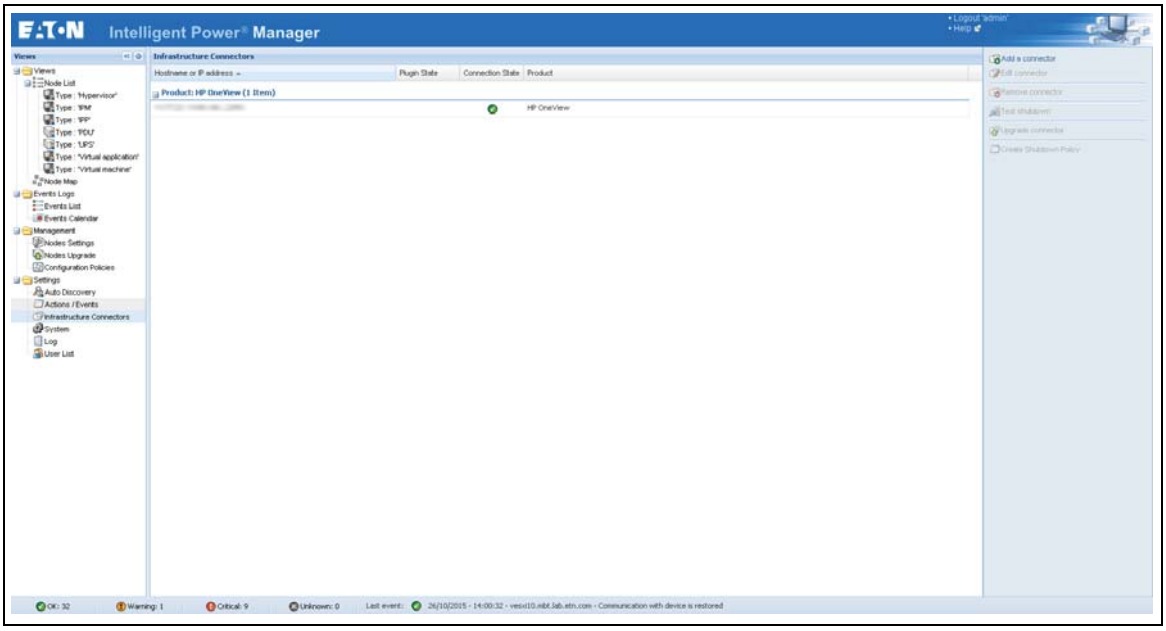

Figure 155. Communication Confirmation

How-to Use the HPE OneView Feature

Check for new nodes

Once the HP OneView connector is created and communication is established, the Node List reports the new nodes retrieved from HPE OneView.

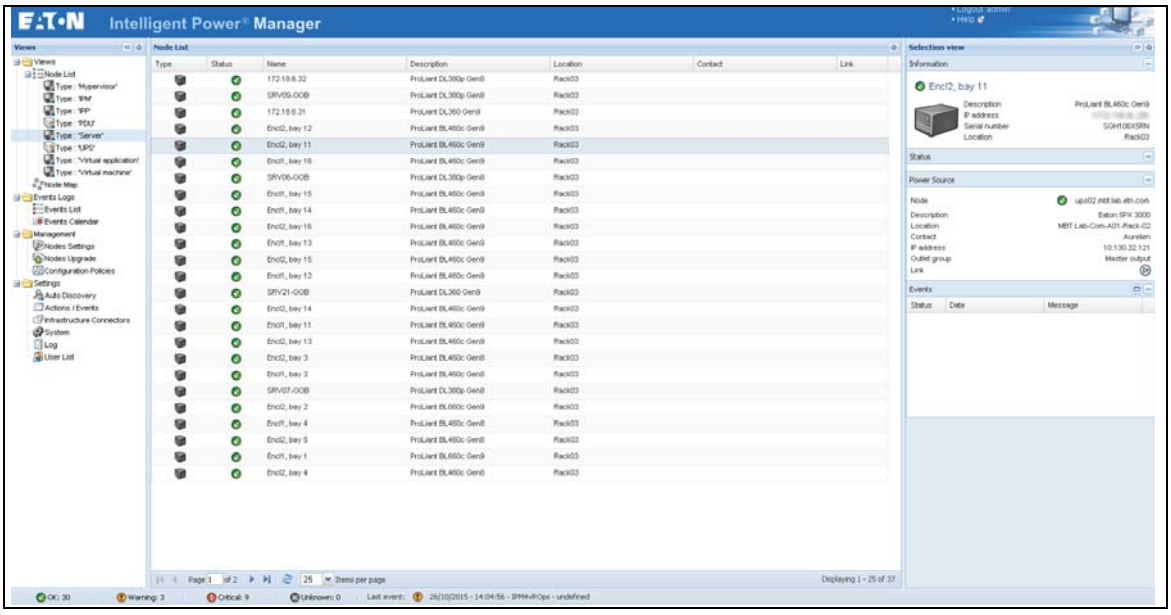

Figure 156. Node List

Create a filter by location

1. In order to focus on one rack, create a filter by location (Right click on Node List >> Create sub view from... >> Select "Location"). The sub-views created will be named according to the rack names provided by HPE OneView. Each sub-view will contain only the servers installed into the corresponding rack.
2. Select one of the views created by location.
3. In the list of servers, select the ones that have an active power capping feature.
4. Right click to create a new configuration policy.

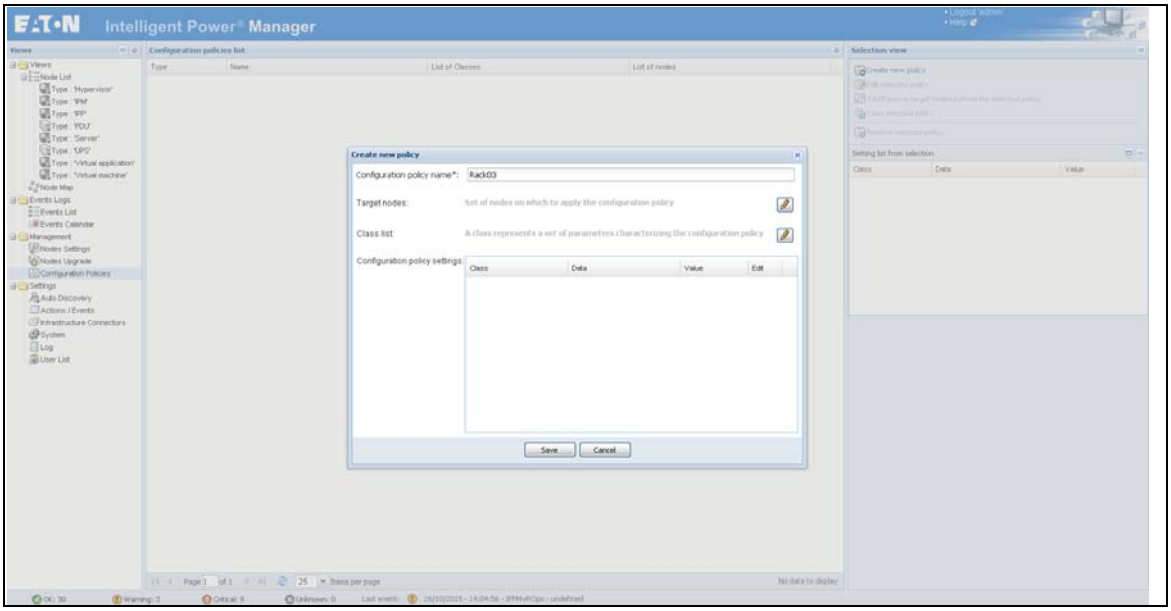

Figure 157. Create Configuration Policy

NOTE The target nodes are already set from to the previous selection.

5. Set the name to whatever you want, for example, "Rack03"

6. Select the class lists "Power Source" and "Runtime thresholds settings" and configure them:

- Timer: 5s;
- Shutdown Duration: 2s;
- Power source: select the UPS powering your rack.

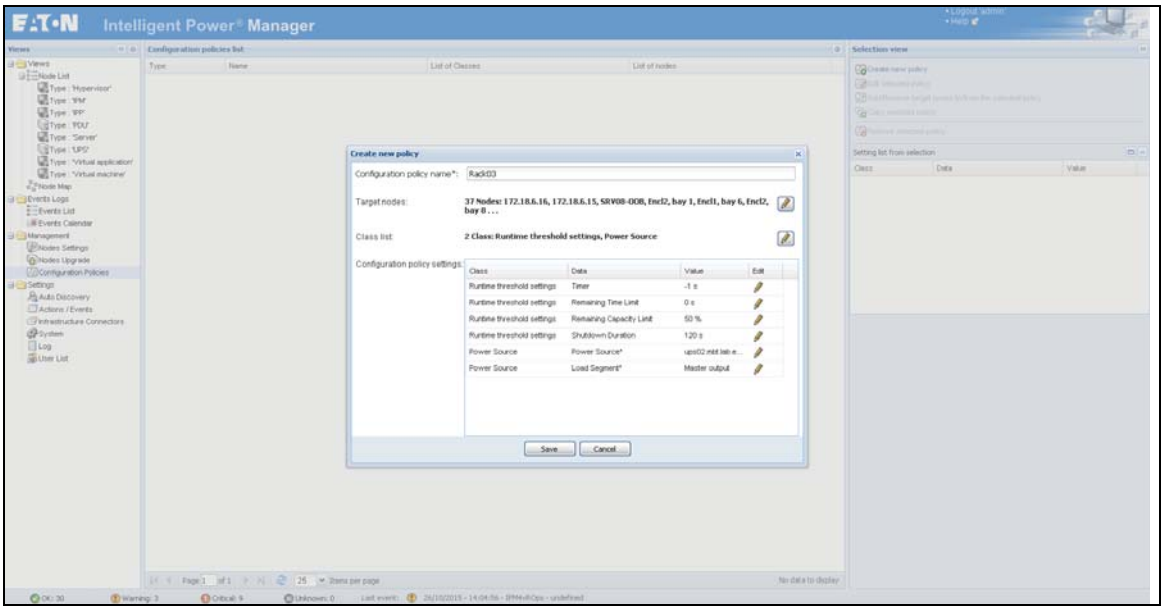

Figure 158. Class List Configuration

7. When prompted, accept to create a shutdown action.
8. In the following dialog:
    a. choose "Power Capping on Power event" for the action,
    b. change its type to "power capping"
    c. set the capping value (W) you want to apply when the event will trigger the action.

At that point, IPM will trigger the power capping at the desired value on all servers of the selected rack in case of a power event from the selected power source.

Configure the power capping on an environmental event

1. Create a custom event (Actions / Events > Edit event rules...)
    a. Name it "Over Temperature"
    b. Copy the name in the event message field
    c. Set its severity to "Warning"
    d. Add a new trigger
        i. Set the UPS card used as the source of the environmental data.

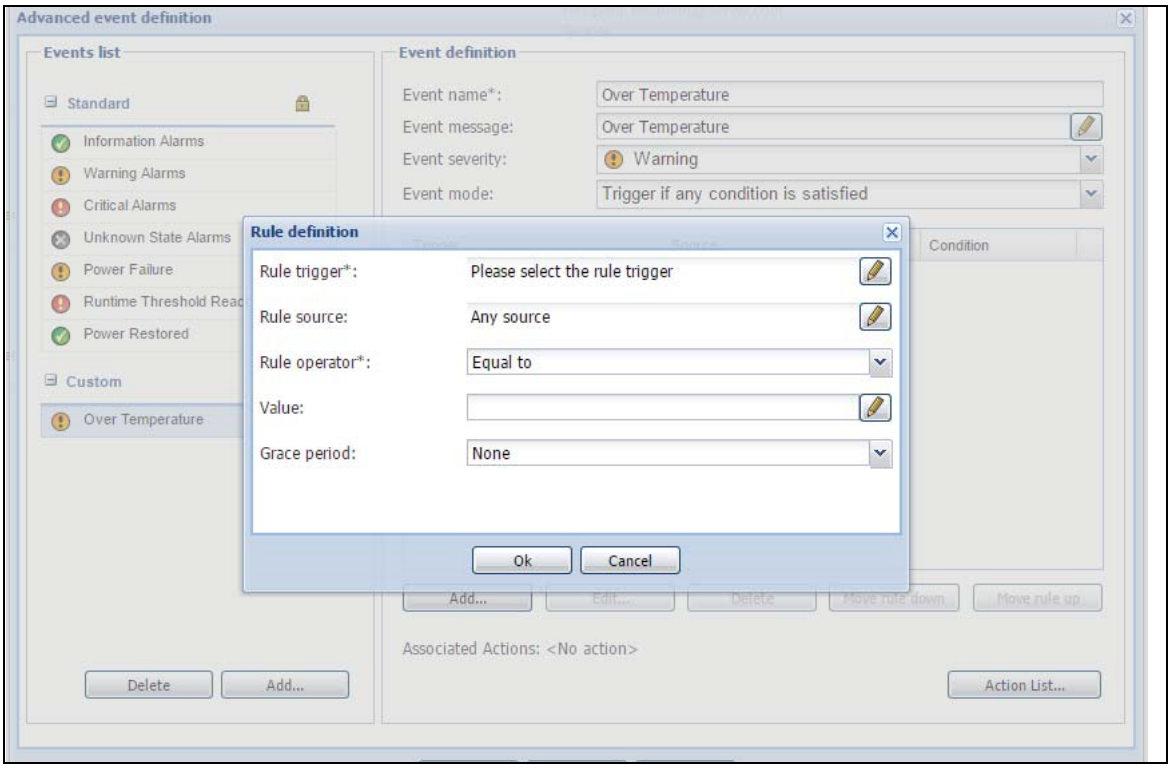

Figure 159. Set Environmental Source

ii. Pick the temperature reading for the rule trigger, and select the index value 1.

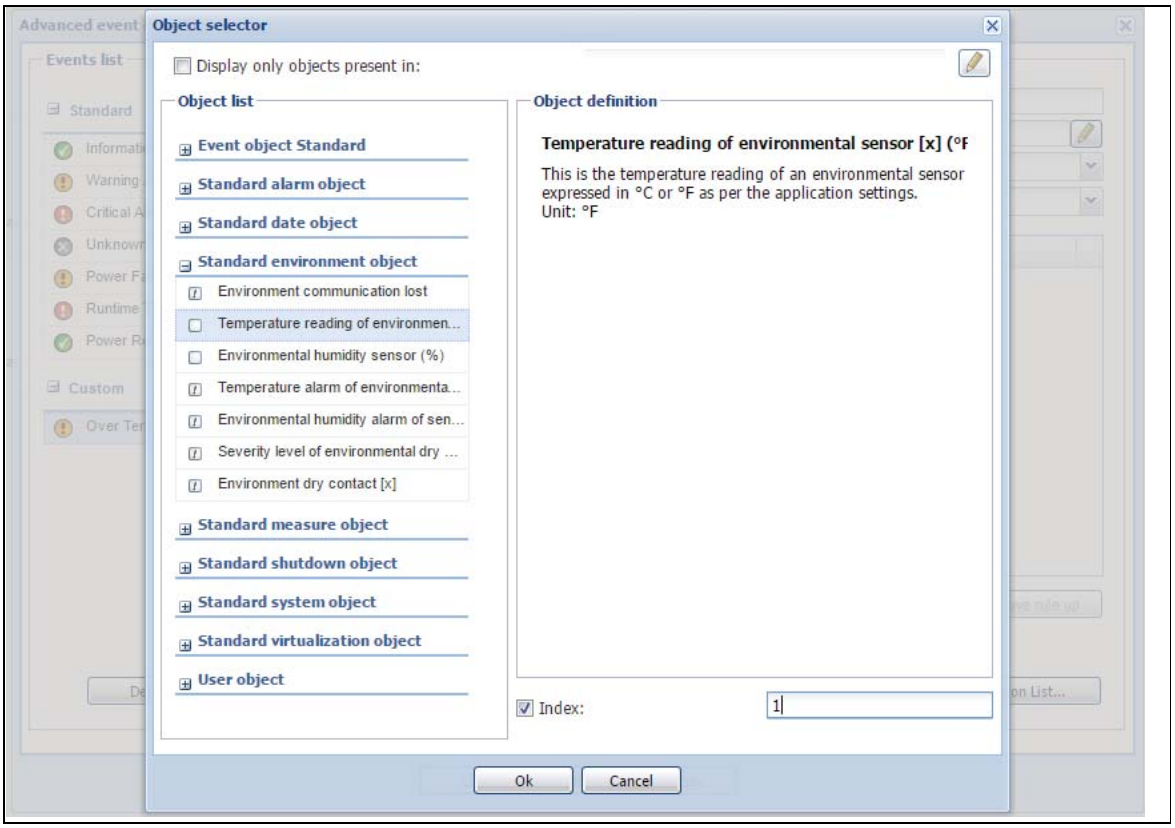

Figure 160. Power Capping Index

iii. Set the rule operator to "Greater than"

iv. Set the value to the desired threshold.

v. Set the grace period to 10s to trig the event only when the temperature is stabilized over the threshold.

vi. Set the rule operator to "Greater than"

vii. Set the value to the desired threshold.

viii. Set the grace period to 10s to trig the event only when the temperature is stabilized over the threshold.

2. Add it into the notification action:

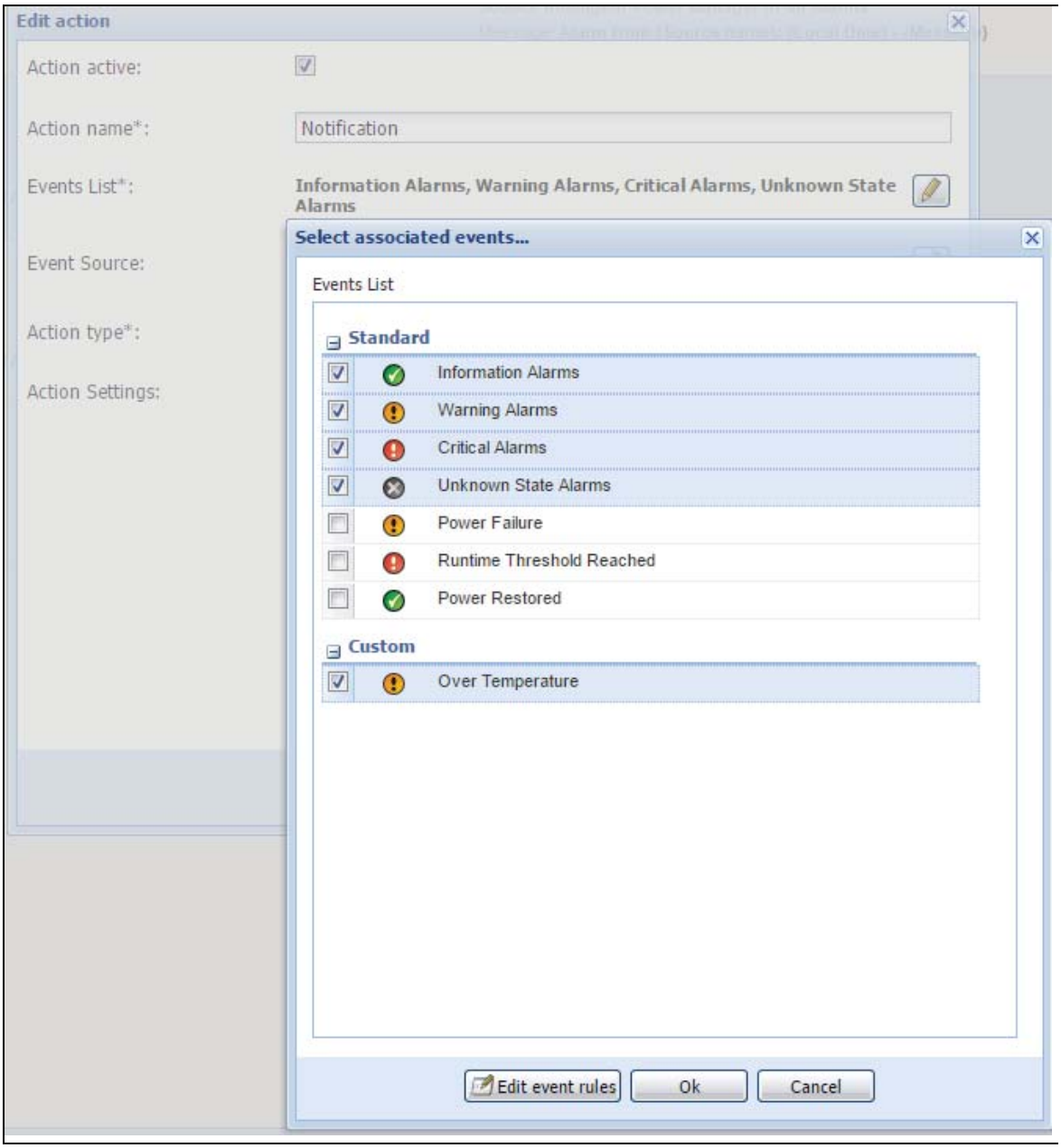

Figure 161. Notification Actions List

3. Create a new action for the power capping on Over Temperature (Actions / Events > Create new action).
   - "Action name": "Power Capping on Over Temperature"
   - "Event List" must contain the custom event "Over Temperature" created the step before
   - "Event source" is the UPS card the environmental data comes from
   - "Server target" is either an individual server or a configuration policy created earlier (like "Rack03" in the previous example).
   - "Value" is the Power Capping Value in Watts.

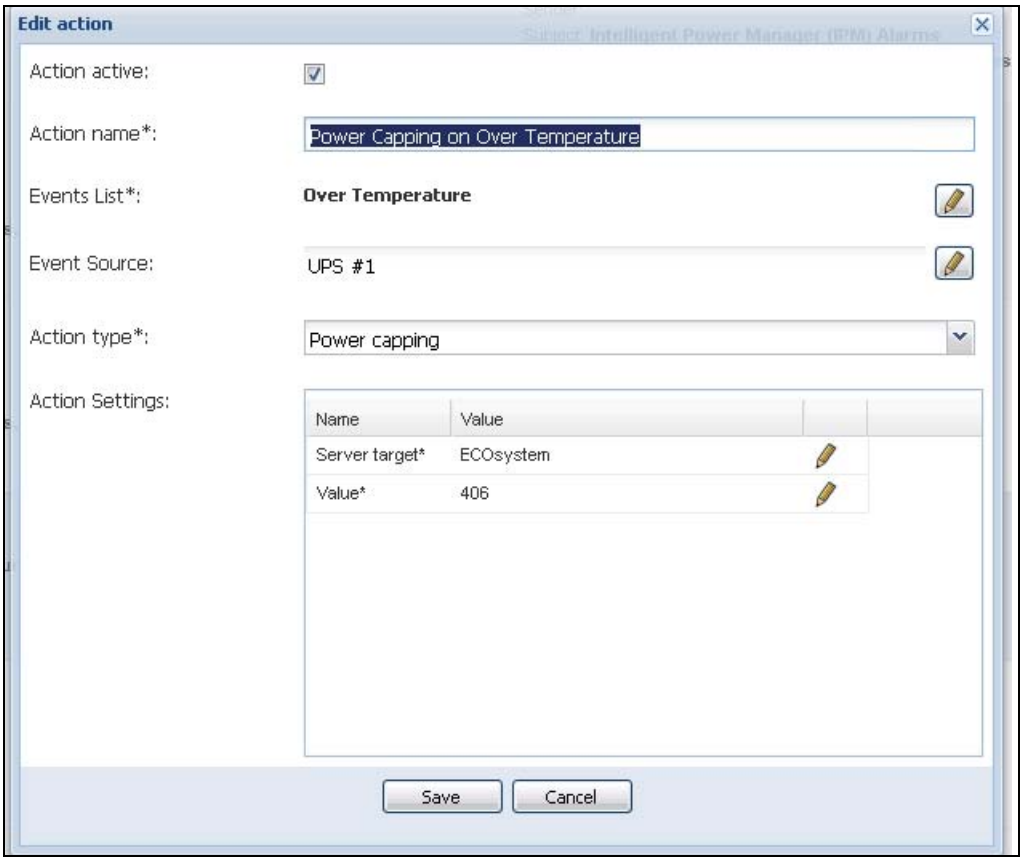

Figure 162. Power Capping on Over Temperature Action

4. At that point, IPM will trigger the power capping at the desired value on all servers of the selected rack in case of an over temperature event sent from the selected source. At the same time, an IPM notification will also be triggered.

Configuring Hypervisors

Descriptions of two methods for configuring hypervisors follow (see "Adding Infrastructure Connectors").

- If you previously "Added a Manager" in Eaton IPM:
  - After you have entered the correct information for the Manager, the Eaton IPM connects to the Manager (vCenter or Hyper-V). Refer to the following link: Eaton Operating System Compatibility List.
  - Eaton IPM automatically retrieves the VMHost information and creates new nodes in Eaton IPM for each VMhost.
  - Eaton IPM automatically creates two different types of nodes (you can see the new node in the Node List).
  - The next step is to configure Maintenance and Shutdown (see "Configuring Maintenance and Shutdown").
- If you previously "Added a Hypervisor List" in Eaton IPM:
  - After you have added a new hypervisor list, Eaton IPM creates new nodes and waits for credentials.
  - The next step is to configure the node credentials through the Infrastructure Connector.
  - After you have entered the correct information, IPM retrieves the hypervisor information.
  - Eaton IPM automatically creates two different types of nodes (you can see the new node in the Node List).
  - The next step is to configure Maintenance and Shutdown (see "Configuring Maintenance and Shutdown").

Configuring Maintenance and Shutdown

After you enter the correct credential information for your Managers and hypervisors, you must configure the Maintenance and Shutdown sequences according to the availability needs of your IT infrastructure when power fails.

There are two types of VMHost nodes:

- No Eaton IPP on VMHost
- Eaton IPP Running on the VMHost

The protection VMware infrastructures can be performed with a wizard.

1. Go into the Nodes list.
2. Select one or several ESXi (multi-selection is possible) that you want to protect and right-click on it. In the contextual menu, you can use the "Create shutdown Policy" command.

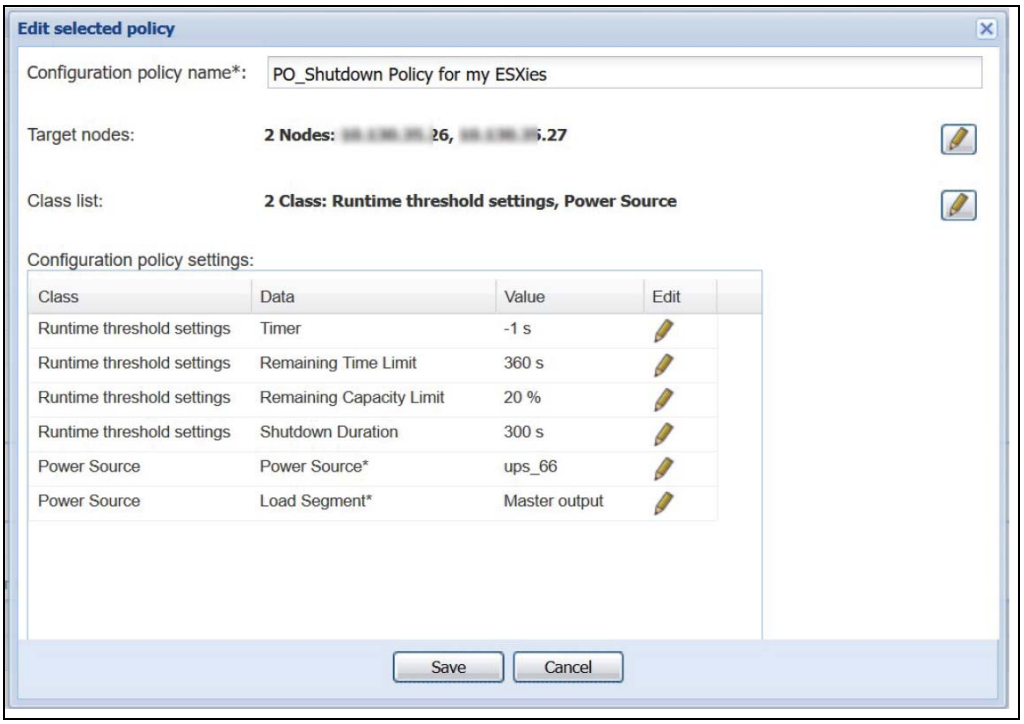

Figure 163. Policy

3. Select Save, the wizard prompts you about the creation of the required action.

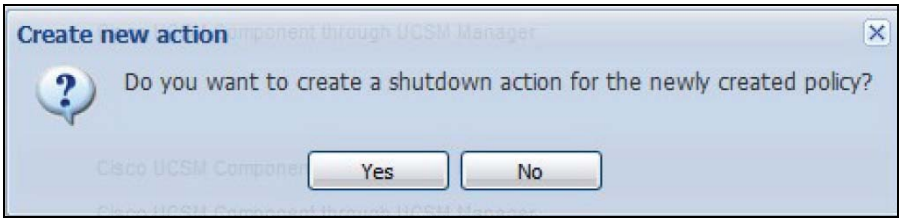

Figure 164. Create New Action

4. Select Yes and then define the action you want to perform; for example:

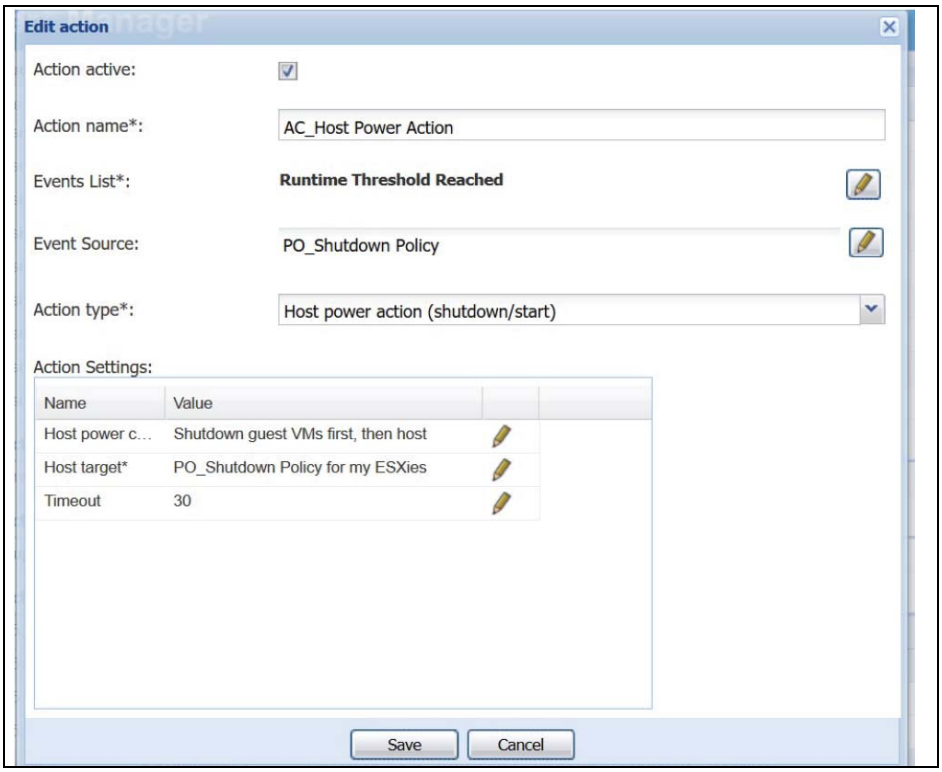

Figure 165. Edit Action

5. Select Save and the selected ESXi hosts are protected according to the triggers of the Policy and the action defined.

Eaton IPP Running on the VMHost

If Eaton IPP is installed on the server that is hosting the hypervisor (VM Host), Eaton IPP performs the shutdown. All the parameters are retrieved from Eaton IPP. Configure the Eaton IPP from Eaton IPM in the Node configuration panel. See "Nodes Settings" to use the configuration interface.

To configure the node:

1. From the ***Management > Nodes Settings*** menu item, click the host in the Nodes list (see "Nodes Settings").

2. In the Shutdown Settings panel on the right side of the page, select the applicable checkboxes to configure the required parameters (see Figure 166 and Table 8).

NOTE The shutdown settings that display vary depending on the node you select. In this example, the node contains both remote maintenance mode feature parameters and Eaton IPP shutdown parameters because the Eaton IPP performs the shutdown locally.

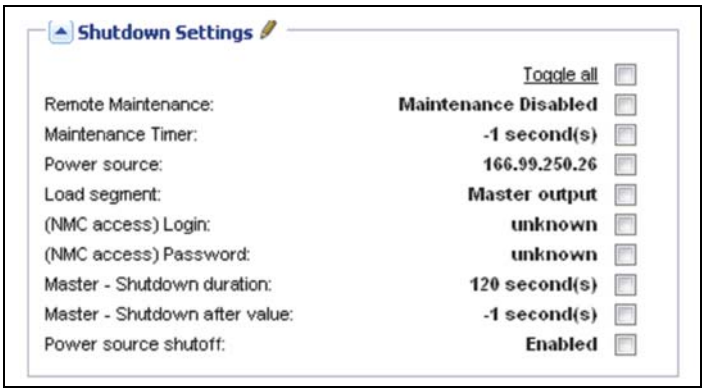

Figure 166. Shutdown Settings for VM Host with Eaton IPM

Table 8. Shutdown Settings with Eaton IPP on VM Host

Parameters	Values	Description
Remote Maintenance	Enabled or Disabled	When enabled, it allows the server management tool to move the VMs from this server to another server in case of "UPS on battery state" and Maintenance Timer elapsed.
Maintenance Timer	Type a value	This represents the time elapsed "on battery state" before the Eaton IPM script changes the state of the host to maintenance mode. The "-1 second(s)" value means that the timer is disabled. See "Configuring Maintenance Mode and vMotion with vCenter" on page 184 for more information.
Power Source	IP address of UPS	This parameter identifies the UPS powering this server. This node must already exist in Eaton IPM.
Load Segment	Master Load Segment 1 Load Segment 2	This parameter identifies the UPS load segment powering the server.
(NMC access) Login/ Password	Type a value	The Network Management Card Login/Password that allows IPP software to control NMC shutdown sequence.
Master - Shutdown Duration	Type a value	This runtime threshold defines the time needed for graceful host shutdown.
Master - Shutdown After Value	Type a value	This runtime threshold defines the time elapsed "on battery state" before graceful Shutdown. This timer must be greater than the maintenance timer.
Power Source shutoff	Enabled or Disabled	Typically Disabled. Enabled is used only for server connected with UPS though RS-232 or USB connection. Virtualization behavior requires Ethernet connectivity (NMC card).

NOTE Shutdown settings that display vary depending on the node you select.

IMPORTANT

If you install an Eaton IPP on the VM Host after the Eaton IPM node has been created, first delete the node in Eaton IPM. Then, rediscover the node with the "Address Scan" in the Auto Discovery panel. The Eaton IPM creates the correct node type and retrieves both the VM Host information and the Eaton IPP information.

Chapter 9 Redundancy

This chapter describes the Eaton Intelligent Power Manager (IPM) redundancy features.

The Eaton IPM can supervise composite devices. Composite devices are virtual nodes composed of two or more UPSs mounted with specific redundancy topologies and a dedicated redundancy level.

NOTE Specific redundance topologies include Redundant supplies, Hot standby, Static transfer switch (STS) for two components, and Parallel for two or more components.

Enabling Redundancy

This Redundancy feature is enabled from ***Settings > System > Modules Settings*** (see Figure 167). After the feature is enabled, the Eaton IPM performs the following:

- Supervise composite devices (if the Redundancy feature is activated)
- Shut down the Eaton IPM computer when a composite device is set as the power source and if the shutdown feature is also activated.

NOTE You can also shut down a remote server linked to the composite device through the infrastructure connector feature.

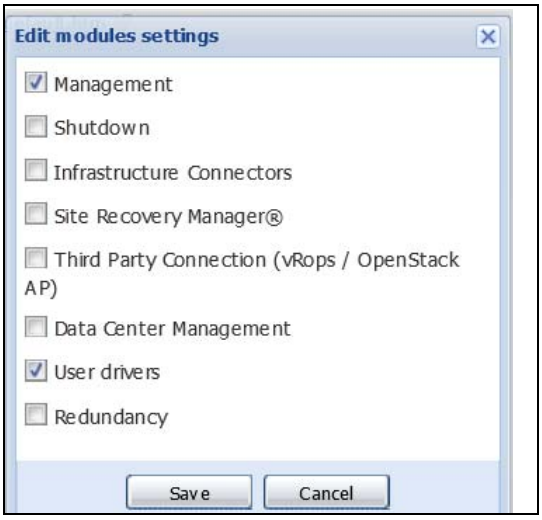

Figure 167. Edit Modules Settings Dialog

Electrical Redundancy Schemas

Figure 168 to Figure 171 illustrate the electrical redundancy topologies.

- **Redundant supplies (such as dual feeds or triple feeds):** Figure 168 illustrates a scenario when two UPSs provide power to one or several multiple-feed servers.

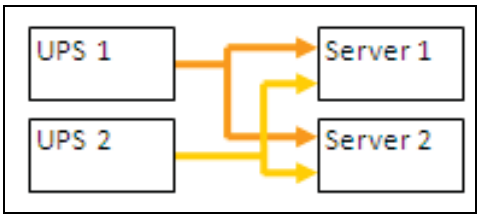

Figure 168. Redundant Supplies

- **Hot standby mode:** When the upstream UPS powers the load, the downstream UPS is on bypass (see Figure 169).

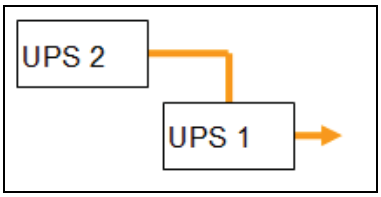

Figure 169. Hot Standby

- **Static transfer switch for two components:** For STS mode, there are several cases with single STS or multiple STSs (see Figure 170).

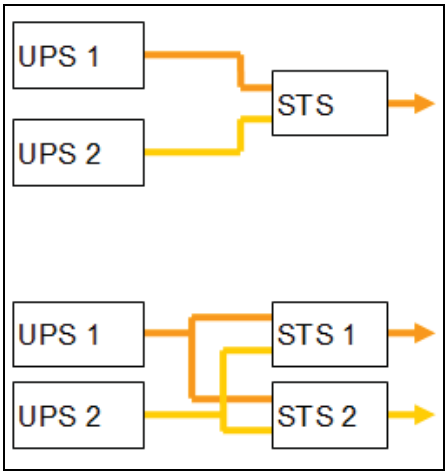

Figure 170. Static Transfer Switch

- **Parallel for two or more components:** All the UPSs power the load at the same time (see Figure 171).

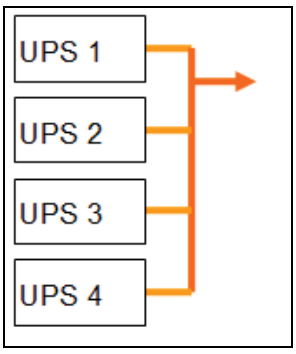

Figure 171. Parallel Redundancy Schema

Configuring Redundancy

To configure redundancy:

1. From ***Start > Programs > Eaton > Intelligent Power Manager***, select **Open Eaton Intelligent Power Manager** to start the main Eaton IPM graphical interface. Login with an administrator user profile.
2. Select the ***Settings > Auto Discovery*** menu item.
3. From the Nodes List page, select two or more nodes.
4. Click **Set composite device** in the right panel (see Figure 172).

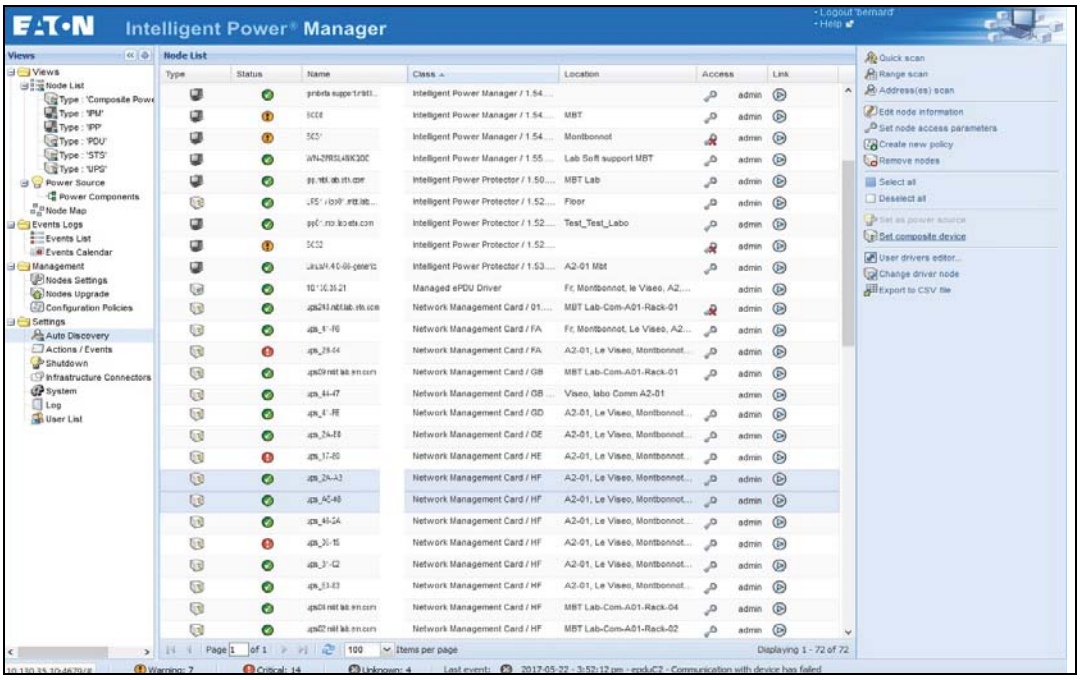

Figure 172. Selecting Set Composite Device for Nodes

5. In the dialog box, specify a device name, redundancy mode, and level (see Figure 173):
   - **Device Name**: Name of the composite device
   - **Redundancy Mode**: Parallel, Redundant Supplies, Hot Standby, or Static Transfer Switch
   - **Redundancy Leve**l: Minimal number of redundant UPSs powering your system (default value is 0)

NOTE If you set this parameter to a higher level, you will receive the "Redundancy Lost" alarm.

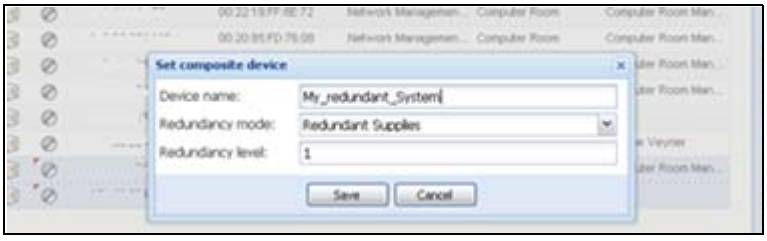

Figure 173. Set Composite Device Dialog Box

When the new node is created, it displays in the Node list.

Three actions you can perform on the new node are as follows (see Figure 172):

1. To select the new node as the power source:
   a. Select the new node in the discovery view.
   b. Click **Set as power source** in the right panel.

NOTE When created, a new virtual power source is counted as a node for the licensing node limitation.

2. To Edit composite device properties.
   a. Select the new node in the discovery view
   b. Click **Set composite device** in the right panel.
3. To retrieve properties of an existing composite device:
   a. Select components of a composite device.
   b. Click **Set composite device** in the right panel. The properties of the existing composite device display.

NOTE No new composite device is created by this action, so no composite device duplication is possible.

Redundancy Views

Selection View in Node List

When a composite device is selected in the node list, the Selection view panel provides the selection panels you check in the Select panels dialog (see Figure 174).

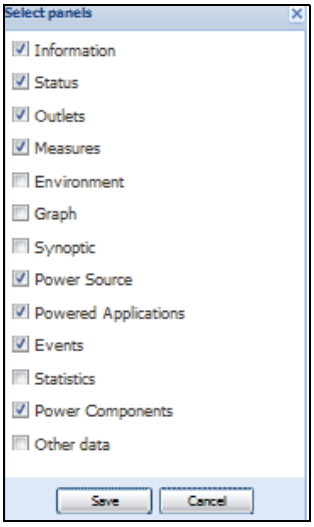

Figure 174. Select Panels for Selection View

Composite Device in Power Source View

When redundancy and shutdown modules are activated, a composite device can be selected as power source. From the ***Views > Power Source*** menu selection, the Power Source page displays. Four panels display with specific data for the device, including Information, Status, Events, and Power Components (see Figure 175).

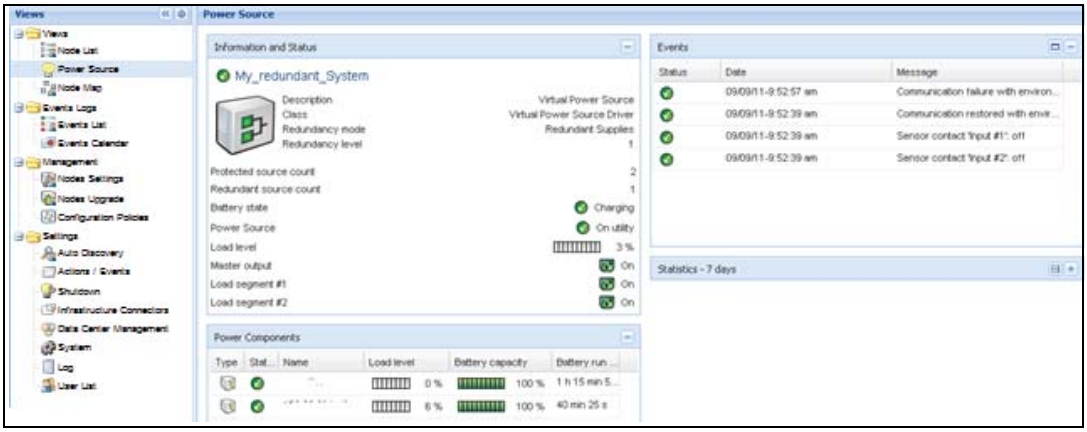

Figure 175. Composite Device Power Source View

Power Components Subview

When redundancy and shutdown modules are activated, a new power component view is also available as a subview of the Power Source view. From the ***Views > Power Source > Power Components*** menu selection, the Power Components display in the Node List. The Selection view displays properties of the power component selected in the Node List (see Figure 176).

NOTE This view shows only components of the selected power source if it is a composite device.

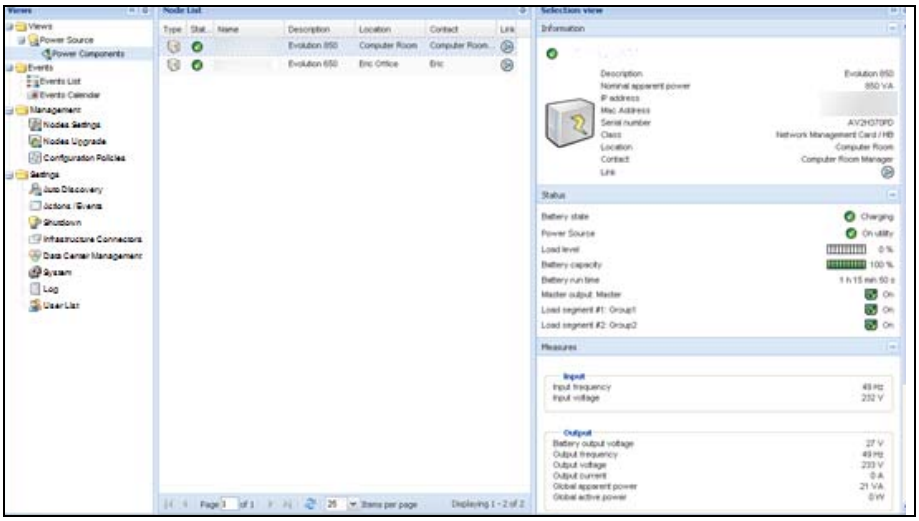

Figure 176. Power Components Subview

Redundancy Use Cases

This section describes several typical use cases to help you properly configure the redundant shutdown sequence according to your needs.

Use Case #1

You want to have the longest backup time with the redundant configuration. To do so, use the default IPM configuration.

- The IPM default configuration is available from ***Settings > Shutdown > Edit Shutdown Configuration*** (see Figure 177).
- For Network-MS and Modbus-MS, the default configuration for the Network Management Card shutdown configuration is available from ***UPS > Shutdown Parameters*** (see Figure 178).
- For ConnectUPS-BD or ConnectUPS-X network cards, the Network Management Card default shutdown configuration is available from ***Configuration > UPS Shutdown and Restart Settings*** (see Figure 179).

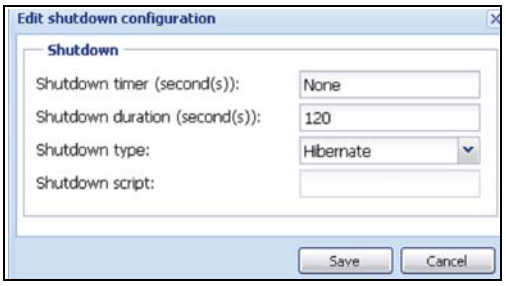

Figure 177. Edit Shutdown Configuration Dialog Box

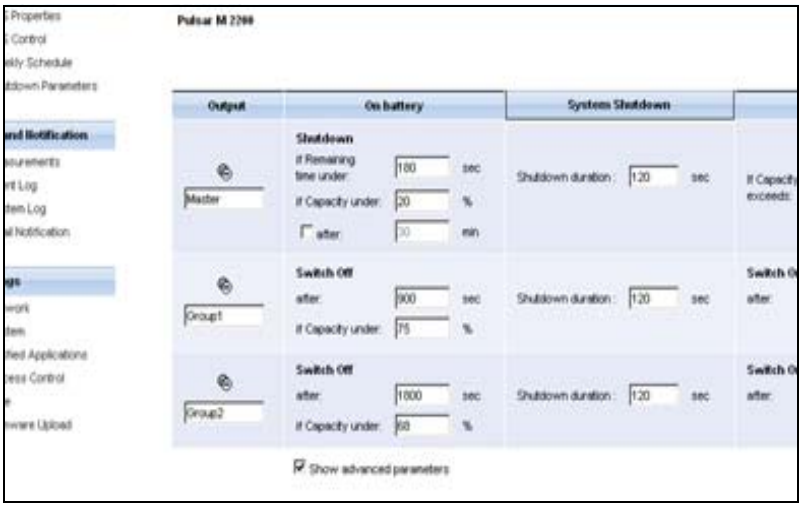

Figure 178. Network Management Card Web Interface

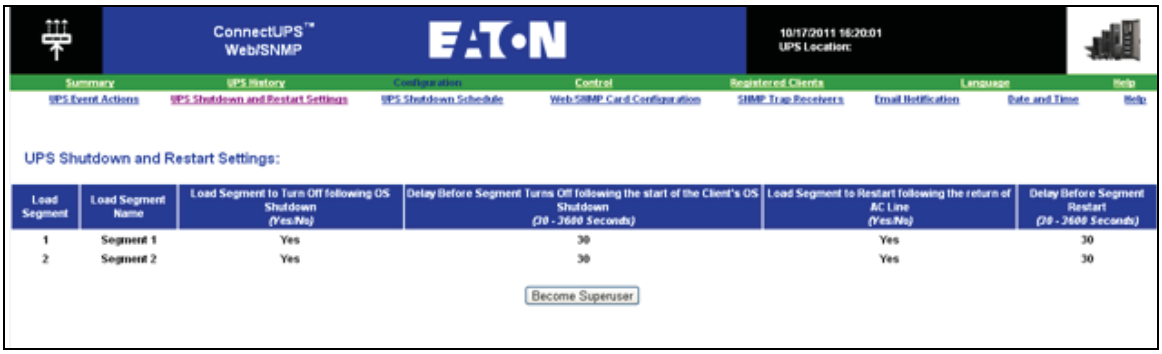

Figure 179. UPS Shutdown and Restart Settings

Use Case #2

You want to have a shutdown after a predefined time of 10 min. The shutdown must occur, even if only one UPS is on battery.

- The IPM default configuration is available from ***Settings > Shutdown > Edit Shutdown Configuration*** (see Figure 180).
- In this case, each server can have its own shutdown timer (10 min, 8 min, 6 min, and so forth). To set a predefined time of 10 min, configure the shutdown timer for 10 min in the Edit Shutdown Configuration dialog box.

NOTE This is the default configuration on the Network Management Card (see "Use Case #1" on page 156).

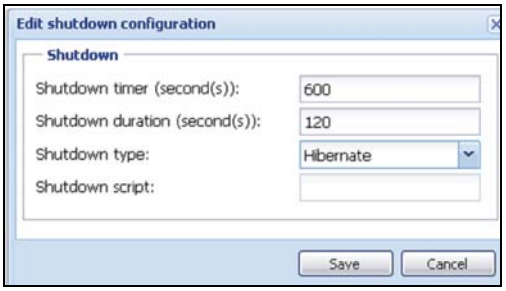

Figure 180. Edit Shutdown Configuration Dialog Box

Use Case #3

You want to start shutdown 10 min from the last detected Utility failure event. For this case, there are two UPSs, and one UPS is redundant. In addition, all servers are shut down at the same time.

- The Network Management Card Shutdown default configuration is available from ***UPS > Shutdown Parameters*** (see Figure 181).
- For ConnectUPS-BD or ConnectUPS-X network cards, the NMC default shutdown configuration is available from ***Configuration > UPS Shutdown and Restart Settings*** (see Figure 179)
- To configure this shutdown, you must set a shutdown timer of 10 min for all Network Management Cards. In this case, the last UPS sends the shutdown order after 10 min if it runs on battery. If the last UPS never runs on battery, the first UPS shuts down at the end of autonomy and the last UPS takes the load if it has the capacity. Otherwise, the shutdown occurs sooner.

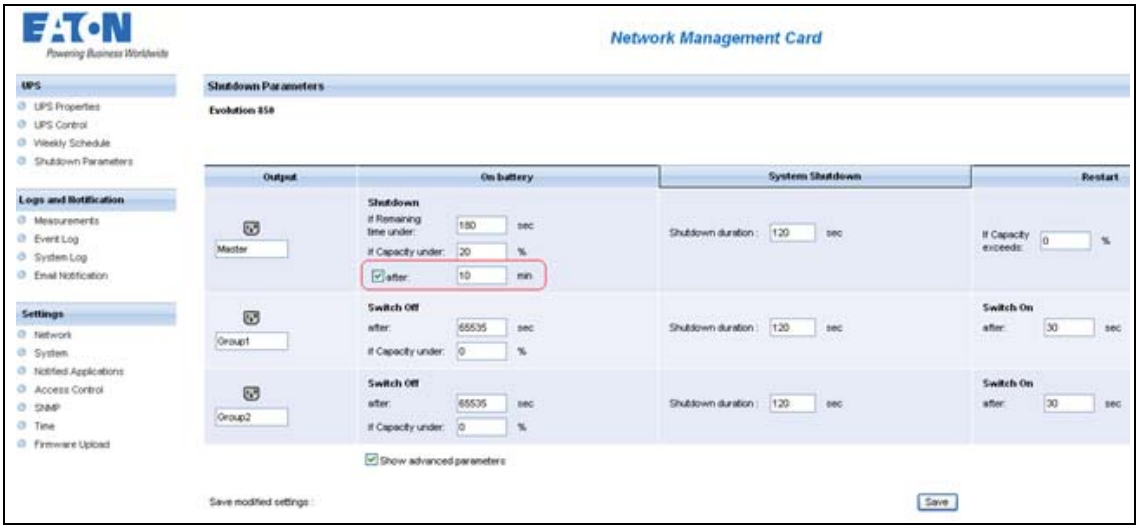

Figure 181. Network Management Card Shutdown Parameters

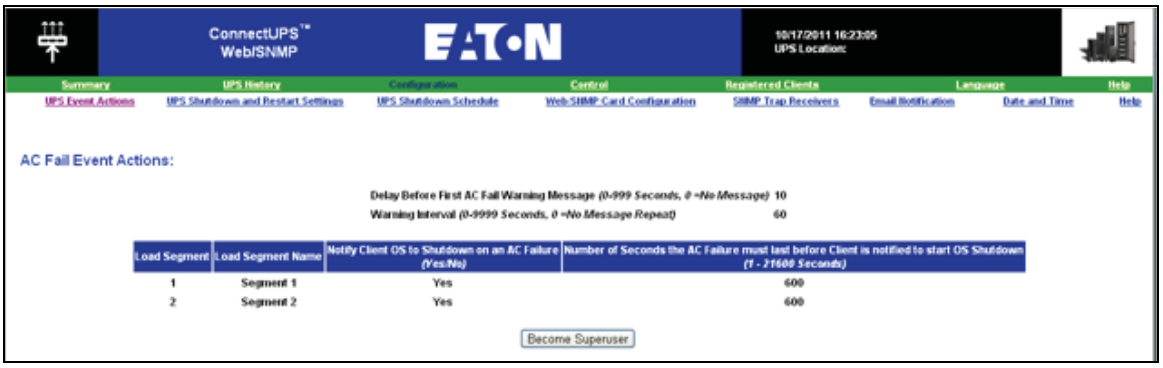

Figure 182. UPS Shutdown and Restart Settings

Use Case #4

You want to have a shutdown when 10 min remain for the last UPS. In this case, each server can have an individual shutdown duration, such as 10 min, 8 min, 3 min, and so forth.

- The IPM default configuration is available from ***Settings > Shutdown > Edit Shutdown Configuration*** (see Figure 183).
- You must configure a shutdown duration of 10 min in the Eaton IPM.

NOTE This is the default configuration on the Network Management Card (refer to "Use Case #3").

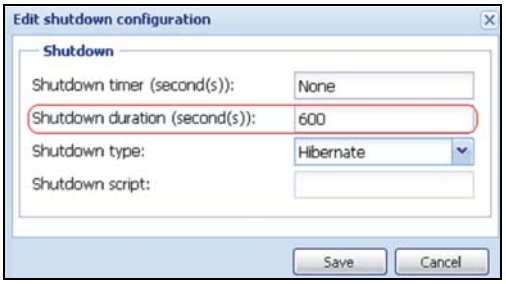

Figure 183. Edit Shutdown Configuration Dialog Box

- You must use the default Network Card Configuration. See "Use Case #1" on page 156 for more details.

Redundancy Advanced Behavior Example

The following example uses a configuration with four UPSs. Each UPS is 20 kW. For this parallel topology, the load can vary between 0 and 80 kW.

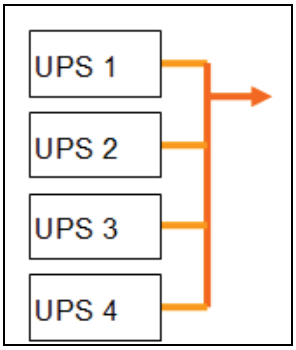

Figure 184. Example Topology

Redundancy Alarm Management with Four Modules

According to the Redundancy level and the Load settings, the following details are provided:

- R is the number of redundant UPSs
- Status of Redundancy Lost Alarm

Table 9 provides redundancy alarm management details.

Table 9. Redundancy Alarm Management

Load/Redundancy Level	Load < 20 kW	20 kW < Load < 40 kW	40 kW < Load < 60 kW	60 kW < Load < 80 kW
0	R=3	R=2	R=1	R=0
1	R=3	R=2	R=1	R=0 (Redundancy lost active)
2	R=3	R=2	R=1 (Redundancy lost active)	R=0 (Redundancy lost active)
3	R=3	R=2 (Redundancy lost active)	R=1 (Redundancy lost active)	R=0 (Redundancy lost active)

Protection Alarm Management with Four Modules

According to the Load and the Number of failed UPSs settings, the following details are provided:

- P is the number of UPSs protecting the load
- R is the number of redundant UPSs
- Status of Protection Lost Alarm

Table 10 provides protection alarm management details.

Table 10. Protection Alarm Management

Load/Failures	Load < 20 kW	20 kW < Load < 40 kW	40 kW < Load < 60 kW	60 kW < Load < 80 kW
No failure	P=4; R=3	P=4; R=2	P=4; R=1	P=4; R=0
1 failure	P=3; R=2	P=3; R=1	P=3; R=0	P=3; R=0 (Protection lost active)
2 failures	P=2; R=1	P=2; R=0	P=2; R=0 (Protection lost active)	P=2; R=0 (Protection lost active)
3 failures	P=1;R=0	P=1; R=0 (Protection lost active)	P=1; R=0 (Protection lost active)	P=1; R=0 (Protection lost active)
4 failures	P=0; R=0 (Protection lost active)	P=0; R=0 (Protection lost active)	P=0; R=0 (Protection lost active)	P=0; R=0 (Protection lost active)

Redundancy Compatibility

The following UPSs and topologies have been tested in redundant mode. Other topologies or UPSs may work, but have not been tested.

Table 11 provides a compatibility list for single-phase UPSs and Table 12 provides a compatibility list for three-phase UPSs.

Table 11. Redundancy Compatibility (Single-phase UPS)

UPS	Parallel	Multiple Feed	Hot Standby	STS
9120, 9130, 9135	n/a	NET, USB	n/a	NET, USB
Eaton 5P / 5PX / Evolution / Evolution S	n/a	NET, USB	n/a	NET, USB
Pulsar EX 700 / 3000	n/a	NET, USB	n/a	NET, USB
Eaton 9SX / 9PX	n/a	NET, USB	n/a	NET, USB
Pulsar MX 1+1	NET	n/a	n/a	n/a
Pulsar MX Frame 16 U	n/a	NET, USB	n/a	NET, USB
EX RT	n/a	NET	NET (*)	NET

- n/a = Not applicable
- NET = Acquisition through the network card
- USB = Acquisition through the USB
- NET (*) = Behavior has been implemented, but has not been tested

Table 12. Redundancy Compatibility (Three-phase UPS)

UPS	Parallel	Multiple Feed	Hot Standby	STS
Blade UPS	NET	NET	n/a	n/a
9x55 (9155 and 9355)	NET	NET	n/a	n/a
9390	NET	NET	n/a	n/a
9395	NET	NET	n/a	n/a
Eaton 9E Essential	n/a	NET	n/a	n/a
Pulsar MX 1+1	NET	n/a	n/a	n/a
Pulsar MX Frame 16 U	n/a	NET, USB	n/a	NET, USB
EX RT	n/a	NET	NET (*)	NET

- n/a = Not applicable
- NET = Acquisition through the network card

Chapter 10 User Drivers

The User Drivers feature allows the Eaton Intelligent Power Manager (IPM) to supervise any available Simple Network Management Protocol (SNMP) or Network UPS Tools (NUT) device. You can customize and adapt the Eaton IPM acquisition engine to many types of Data Center devices, such as HVAC, rack controllers, storage appliance, or DC power system controllers.

By default, the User Driver feature is activated. However, if you disable this function, previously discovered nodes that are using a User Driver are still managed.

NOTE This function is only accessible to Administrators.

User Drivers Editor

The User drivers editor dialog is used to integrate new devices in the IPM supervision application by using following objects:

- predefined common base objects
- user-specific objects

Predefined custom drivers that are managed by the application include:

- UPS RFC1628/SNMP: Manages the UPS which implements the SNMP mib RFC1628
- NAS BUFFALO®/SNMP: Manages the SNMP Buffalo Network Attached Storage (NAS)
- NAS HPE/SNMP: Manages the SNMP HPE NAS
- NAS NetApp/SNMP: Manages the SNMP NetApp NAS
- NAS Netgear/SNMP: Manages the SNMP Netgear NAS
- NAS Qnap/SNMP: Manages the SNMP Qnap NAS
- NAS Synology/SNMP: Manages the SNMP Synology NAS
- PDU/NUT Protocol: Manages the SNMP PDU using NUT
- UPS/NUT Protocol: Manages the SNMP UPS using NUT
- ATS Eaton 32A: Manage the SNMP EATON STS

NOTE NUT is open source software that provides control and management features for power devices, such as UPSs, through a control and management interface. Visit at: http://www.networkupstools.org

User Drivers Page

To supervise new devices with Eaton IPM:

1. From the left-side **Views** panel of the Eaton IPM main interface window, select the ***Settings > Auto Discovery*** menu item.
2. Select the User drivers editor... button from the right panel (see Figure 185). The User drivers editor page displays.

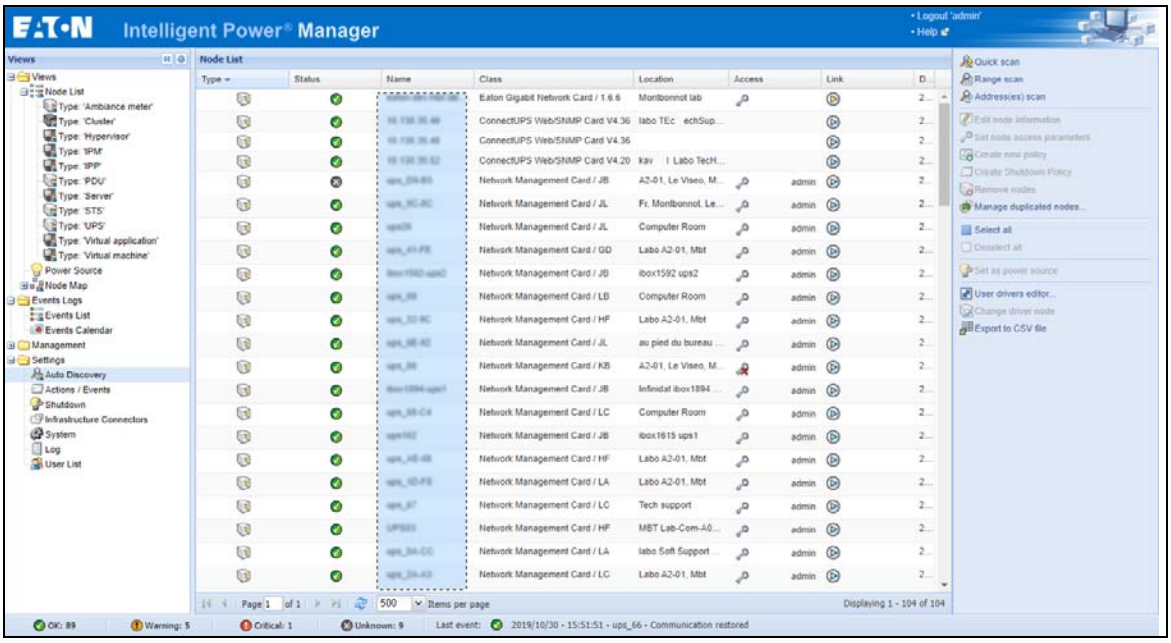

Figure 185. User Drivers Editor Selection

NOTE By default, the User Driver feature is enabled. You can enable or disable this function on the **Edit module settings** dialog by selecting or deselecting (checking or unchecking) the checkbox for the User Driver (see Figure 186).

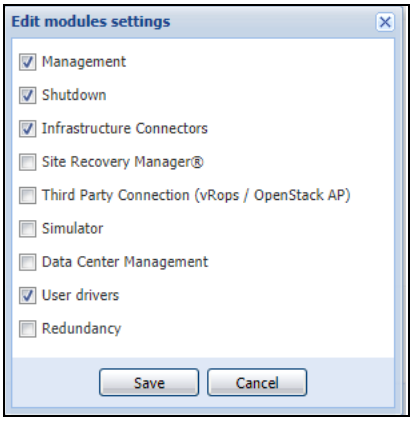

Figure 186. Enable or Disable User Drivers

User Driver Editor Dialog

When ***Settings > Auto Discovery*** is selected, the Nodes List page displays. Select the **User driver editor...** button to display the User drivers editor dialog.

The dialog provides the following data:

- The left panel lists the drivers.
- When a driver is selected in the left panel, the details of the selected driver are provided in the upper right window panel.
- Below the selected driver details, a table lists all rules defined for the selected driver.

NOTE A rule defines the relationship between a source object name and a destination object name.

- Buttons are provided at the bottom of the dialog to manage drivers and driver rules.

Figure 187 illustrates the User drivers editor dialog.

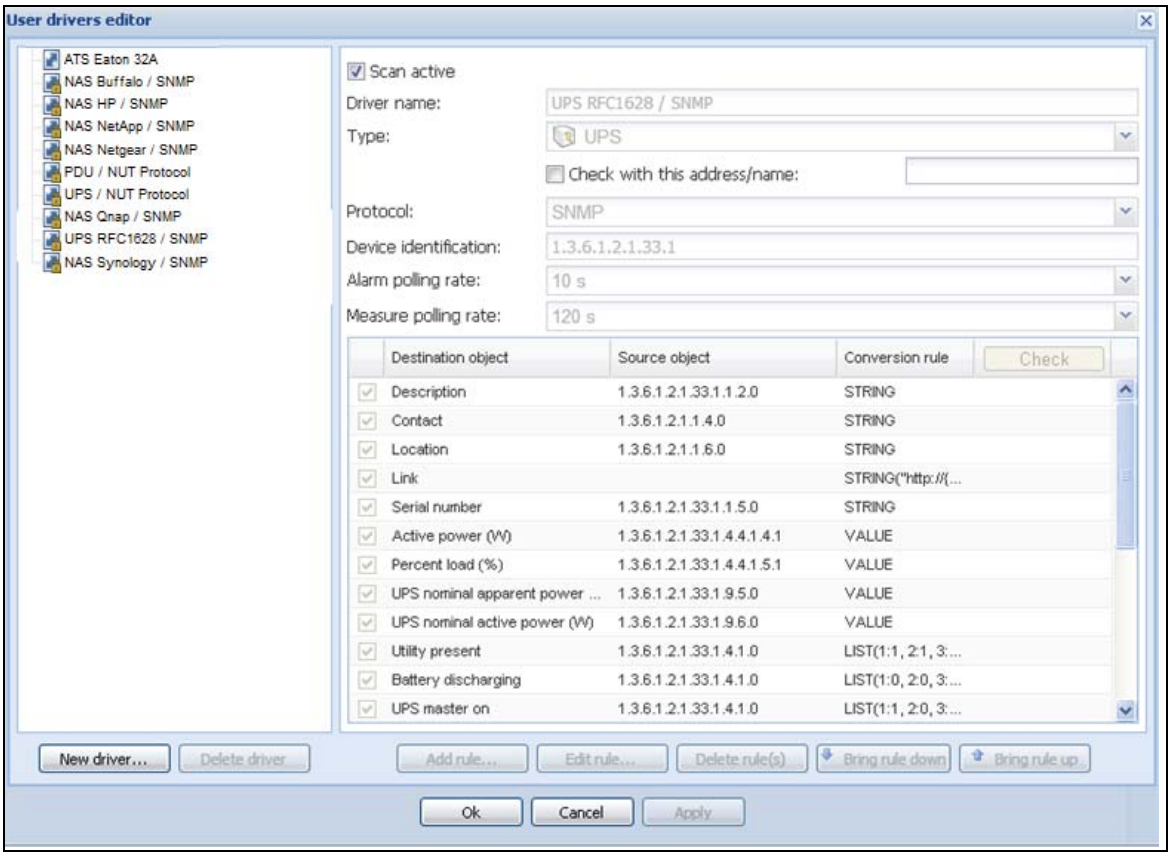

Figure 187. User Drivers Editor Dialog

Buttons

The following buttons allow you to manage drivers and rules.

- **New driver:** Click the New driver button to add a new driver to the list and define the properties for the driver. A new empty driver can be created or you can use a copy of an existing driver. Predefined drivers provided with the application are read-only and cannot be changed. They can only be deactivated or duplicated for customization purposes.
- **Delete driver:** The Delete driver button deletes the driver that is selected in the left panel.

NOTE When a driver is deleted after applying modifications, it is not possible to recover this driver.

To manage and define rules, use the following buttons:

- **Add rule...:** Add a new rule
- **Edit rule...:** Edit the selected rule
- **Delete rule(s)...:** Delete the selected rule(s)
- **Bring a rule down...:** Move the selected rule to a lower position in the table
- **Bring a rule up...:** Move the selected rule to a higher position in the table

You can enable or disable a rule by selecting (checking) or deselecting (unchecking) the checkbox in the first column. When a rule is disabled, the data defined in the rule is no longer acquired.

Driver Data

The right side of the page provides data for the driver selected in the left panel.

The top right data fields identify the selected driver and allow you to set actions to occur during discovery as follows:

- **Scan active**: This option provides the ability to activate or deactivate a driver. When this option is deselected (unchecked), the driver is filtered during discovery action. It allows using a modified copy of a driver instead of the default driver.
- **Driver name**: This name defines the unique friendly name of the driver. This name displays in the information **Class** column of the node view.
- **Type**: Type defines the driver type as follows:
  - UPS device
  - PDU device
  - Power meter
  - Power generator
  - DC controller
  - Power over Ethernet (PoE) appliance
  - Server
  - Storage appliance
  - Network appliance
  - Ambiance meter
  - Cooling system
  - Other device
- **Check with this address**: Allows you to check the rules result with an address or a device host name.
  - For SNMP protocol, it is the global scan settings you are using. If you need special access for the driver, you need to temporarily change these settings.
  - For NUT protocol, use <`IP address or host name`>/<`Device ID`>

  where <`Device ID`> = Name of the NUT device, such as, the section header name defined in the `ups.conf` file for a UPS.
- **Check button:** Enabled only if an address or a name is typed in the **Check with this address/name** entry box. See "Rule List" on page 167 for more information.
- **Protocol:** Protocol field, either SNMP or NUT:
  - SNMP: Provides support of SNMP v1 and v3 driver
  - NUT: Provides support of NUT client Interface

- **Device identification:** Defines the device identification used for device recognition during discovery. For SNMP device, use the SysOID value, or use the root OID of the device if the SysOID is not managed by the device.
- **Alarm polling rate**: Defines the polling rate for objects of type alarm. Information type data are acquired only once, at driver reset.
- **Measure polling rate**: Defines the polling rate for objects of measure type.

NOTE Measure data type polling can be performed simultaneously with alarm data type. In this case, only one task will be cyclically executed.

Rule List

The table on the right side of the User drivers editor dialog lists defined rules associated with the selected driver.

- **Source object name:** source object name of the data to acquire in the device
- **Destination object name:** internal object name managed by the IPM application

NOTE A destination object can be defined by several complementary rules. For a same destination object, if a rule is not applicable, it takes the next rule defined in the list.

The **Check** button in the Rule list table header is used to compute and display the result for each rule according parameters. The result is computed with the address or the name entered for **Check with this address/ name**.The **Check** button is enabled only if an address or a name is entered.

Rule Editor Dialog

The Rule editor dialog allows you to create (add), edit, or delete a rule. As part of defining the relationship between a source object name and a destination object name, conversion rules and parameters are selected and applied in this dialog.

To edit or create a rule on the Edit rule dialog, you need to enter the following:

- Destination object name
- Source object name
- Conversion rule and conversion parameters (conversion help files automatically display when a conversion rule is entered)

When the rule is created, you can test the rule using the **Check result** button. See the following section, "Buttons" for a description of the Check result button.

Figure 188 illustrates the Rule editor dialog.

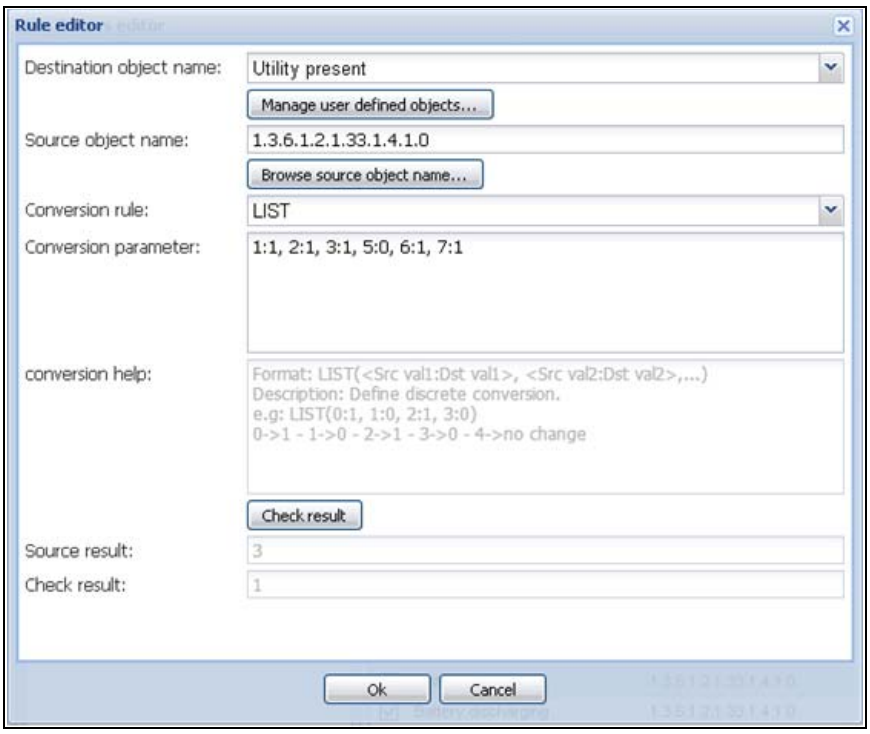

Figure 188. Rule Editor Dialog

Buttons

The following buttons allow you to create and test rules on the Rule editor dialog.

- **Manage user defined objects...:** Allows you to define your own object list to link for a specific device type
- **Browse source object name...:** Builds a list to help you to select the appropriate source object from a list of value
- **Check result:** Used to compute the rule result according the given parameters. The source result and the final rule result are both displayed.

NOTE The **Check result** button is enabled only if the address or name is entered for **Check with this address/name** on the User drivers editor dialog.

- **Ok:** Accept changes
- **Cancel**: Do not accept changes

Destination object name

This field defines the name of the destination object in the Rule editor dialog.

There are two ways to select the destination object name:

- Select a "well-known" and predefined object (which is a standard object managed by the IPM application) from the standard objects list in Table 13.
- Select a specific user-defined object when the needed object is not defined in the standard object list.

Table 13 lists the standard objects used by the Eaton IPM.

Table 13. Standard Objects

Information	Status	Input	Output	Battery	Environment
Name	Shutdown imminent	UPS input voltage (V)	Active power (W)	Battery charging	Environment communication lost
Description	UPS internal failure	UPS input current (A)	Apparent power (VA)	Battery discharging	Humidity reading of environmental sensor [x] (%
Contact	UPS overload	UPS input frequency (Hz)	UPS outlet #1 on	Battery low	Temperature alarm of environmental sensor [x
Location	UPS master on	UPS automatic bypass voltage (V)	UPS outlet #2 on	Battery fault	Environment dry contact [x]
Link	Utility present	UPS automatic bypass current (A)	UPS outlet #1 active power (W)	Battery capacity (%)	Level environment dry contact [x] opened
Serial number	Redundancy lost	UPS automatic bypass frequency (Hz)	UPS outlet #2 active power (W)	Battery runtime (s)	Level environment dry contact [x] closed
Communication description	Protection lost	PDU input voltage (V)	UPS power factor	Battery voltage (V)	Temperature reading of environmental sensor [x] (°C)
Platform	Automatic bypass in tolerance		UPS output voltage (V)		Humidity alarm of environmental sensor [x]
Mac address	On automatic bypass		UPS output current (A)		Environment communication lost
Version	On manual bypass		UPS output frequency (Hz)		
Manufacturer	UPS master shutdown delay (s)		PDU number outlet		
UPS nominal active power (W)	UPS outlet #1 shutdown delay (s)		PDU outlet [x] number		
UPS nominal apparent power (VA)	UPS outlet #2 shutdown delay (s)		PDU outlet [x] name		
UPS master switchable	UPS master startup delay (s)		PDU outlet [x] switchable		

Table 13. Standard Objects (Continued)

Information	Status	Input	Output	Battery	Environment
UPS outlet #1 switchable	UPS outlet #1 startup delay (s)		PDU outlet [x] on		
	UPS outlet #2 startup delay (s)		PDU outlet [x] voltage (V)		
	PDU outlet [x] shutdown delay (s)		PDU outlet [x] current (A)		
	PDU outlet [x] startup delay (s)		PDU outlet [x] apparent power (VA)		
	Communication Lost		PDU outlet [x] active power (W)		
	Communication error		PDU outlet [x] power factor		

You can also define your own object list to create links for a specific device type in the User defined object editor dialog. A new object can be defined by providing these properties:

- **Object name**: Unique object user name
- **Object index option ([x])**: Activate this option if the object needs to be indexed (e.g. value of type array).
- **Object type**: Information, Alarm or Measure
- **Object unit:** Optional unit which is displaying for the object
- **Object group**: Name of the group whose object is attached. This group is shown in the Other data panel. Objects with the same group name are represented in the same group.

Figure 189 illustrates the User defined object editor dialog.

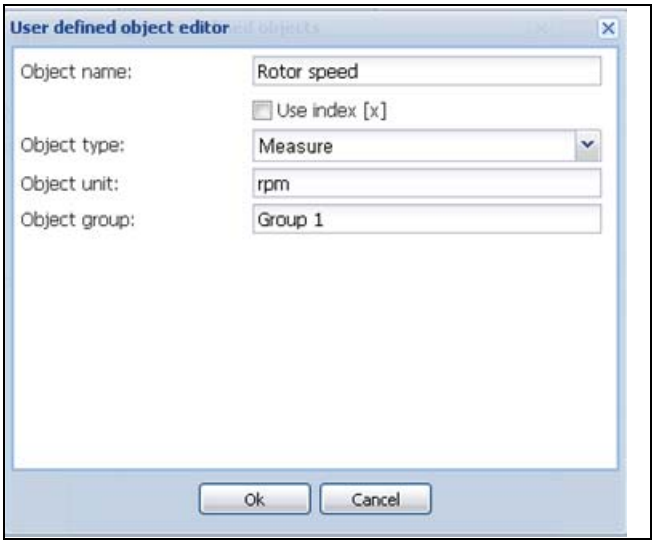

Figure 189. User Defined Object Editor

IMPORTANT

- The user-defined objects only display in a specific Node view panel named Other data (see Figure 190). These user-defined objects display as a raw list that is sorted by groups.
- The standard objects are NOT displayed in the Other data panel. These standard objects are defined in standard IPM panels (see Table 13).
- The user-defined object list is attached to the driver.
- Click the **Manage user defined objects…** button in the rule editor to manage user-defined objects.

Figure 190. Other Data Panel

Source Object Name

This feature defines the name of the source object that you need to acquire. The following notes apply when creating a source object name in the Rule editor dialog:

- If the destination object name is indexed (for a standard object or a user-defined object), use "x" in the source object name for the index position.
- For an SNMP device, the source object name corresponds to the object ID (OID) name of the data to acquire. The list is built from the device identification name which has been given. It corresponds to all OIDs available under the OID root or the SysOID value.
- For a NUT device, the source object name corresponds to the internal NUT object name.

If you provided a valid address in the check item of the driver, an interface is provided to help you to select the appropriate source object from a list of value.

To define the source object name:

1. From the Rule editor dialog, click on the **Browse source object name…** button. The object list is built automatically when the window opens.

NOTE You can pause the object list acquisition at any time using the **Pause** button.

2. The **Restart** button restarts the object list acquisition from the beginning.
3. The **Cancel** button aborts the object list acquisition.
4. Select the appropriate object in the list and then click **Ok**.

Conversion Rules

The following notes apply when defining the conversion rules in the Rule editor dialog:

- The rules are evaluated in the order of the rule list.
- Several rules can define the value of the same destination object.
- Several rules can use the same source object.

Table 14 provides a list of conversion rules.

Table 14. Conversion Rules

Rule	String
STRING	Format: STRING([<formatString>])
	Without parameters: No conversion
	Just transfers source object value as a string to destination object.
	With parameter, the destination object is created and its value is fixed.
	Normalized field can be used:
	STRING("My Device")
	STRING("http://{hostname}/default.html")
	STRING("{value}")
	Fields in brackets are replaced by correspondent value (if defined).
	Available fields are:
	{hostName}
	{ipAddress}
	{value}
	{object:UPS.PowerSummary.iProduct}
VALUE	Format: VALUE([<constantValue>])
	Without parameters: No conversion
	Just transfers object value as a number to destination object.
	With parameter, the destination object is created and its value is fixed by given value.
	VALUE(15)
	VALUE(-12.34)
	We can also use a javascript equation for special needs
	VALUE("{value} == -1 ? 0 : {value} + 1")
MULT	Format: MULT(<multiplier>)
	Multiply source value to the given factor before setting destination object.
	MULT(10), MULT(0.1), MULT(3.1415)...
LINEAR	Format: LINEAR(<srcVal1:dstVal1> , <srcVal2:dstVal2>)
	Example: conversion from °C to °F
	LINEAR(0:32, 100:212)
	Calculation:
	(dstVal2 - dstVal1) / (srcVal2 - srcVal1) * (value - srcVal1) + dstVal1

Table 14. Conversion Rules (Continued)

Rule	String
LIST	Format: LIST(<srcVal1:dstVal1>, <srcVal2:dstVal2>, ...)
	Define discrete conversion.
	If source value is not in the list, destination object is not changed.
	Example:
	LIST(0:1, 1:0, 2:1, 3:0)
	0 -> 1
	1 -> 0
	2 -> 1
	3 -> 0
	4 -> no change
	...
	Lists can also convert strings to numbers and numbers to strings.
STRFIND	Format: STRFIND(<searchString>, [<trueValue>], [<falseValue>])
	Returns <trueValue> if <searchString> was found or <falseValue> in the other case.
	If a result value is not defined, the destination is not changed.
	Example:
	STRFIND(“US”,1,2)
	STRFIND(“OL”,1)
	STRFIND(“OB”,,1)
BITCHECK	Format: BITCHECK(<bitPos>, [<trueValue>], [<falseValue>])
	Returns <trueValue> if bit at <bitPos> is true or <falseValue> in the other case.
	If a result value is not defined, the destination is not changed.

Chapter 11 Storage

The Eaton Intelligent Power Manager (IPM) can supervise storage devices. On the user interface, storage devices are seen as a "Storage Appliance" type with the following information displayed:

- Type
- Status
- Name
- Description
- Class
- Location
- Contact
- Link

Using the User Drivers feature, you can launch a Range scan with the IP address of your storage equipment (see "Range Scan" on page 18 and "User Driver Editor Dialog" on page 164). After performing a Range scan, you will have a list of storage managed by Eaton IPM.

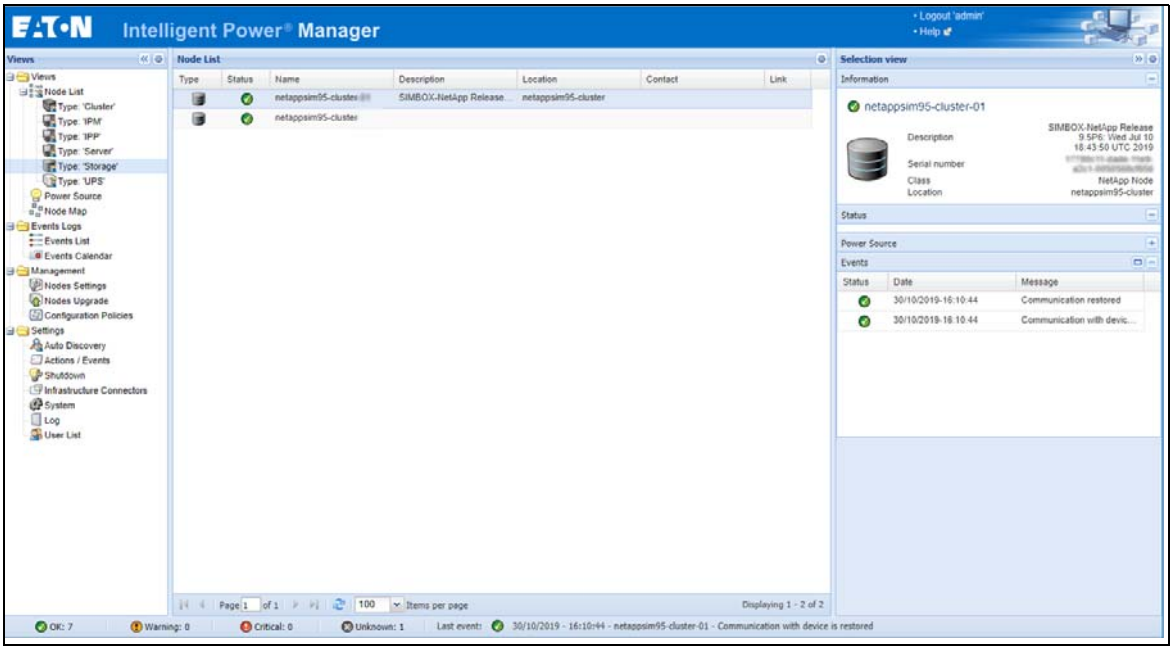

Figure 191. Storage View

Enable the Infrastructure Connectors Module

To enable the Infrastructure Connectors module for virtualization (administrator access):

1. From the left-side **Views** panel of the Eaton IPM main interface window, select the ***Settings > System*** menu item. The System page displays.
2. Click **Edit modules settings** in the right panel. The Edit modules settings dialog box displays (see Figure 192).
3. Ensure that the **Infrastructure Connectors** checkbox is selected (checked).
4. Click **Save**.

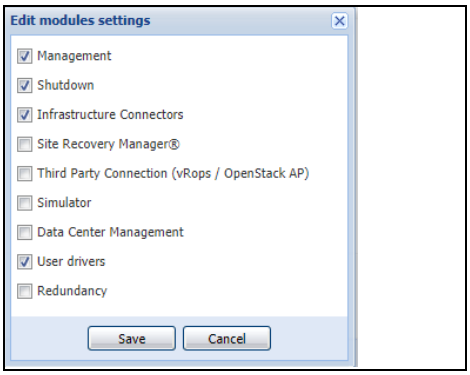

Figure 192. Enable Infrastructure Connectors Setting for Virtualization

5. Select **Settings > Infrastructure Connectors**. The Infrastructure Connectors Select Add a connector in the right panel. The Add a connector dialog opens (see Figure 193).
6. Add identification information for the selected connector
   - **Product:** Select NetApp storage from the drop-down list
   - **Hostname or IP address:** Type the NetApp IP address
   - **Username**: Type NetApp Administrator Username with admin rights on the NetApp
   - **Password:** Type NetApp Administrator Password
7. Click **Save** after the fields are updated.

Figure 193. Add NetApp

Create a Configuration Policy

The following procedure describes how to create a new configuration policy for storage protection.

To create a new configuration policy and define the protection (see Figure 194):

1. Name the new configuration policy.
2. Select the pen associated with Target nodes to add the storage device(s) to be protected.
3. In the configuration policy settings, configure the runtime threshold settings and power source.

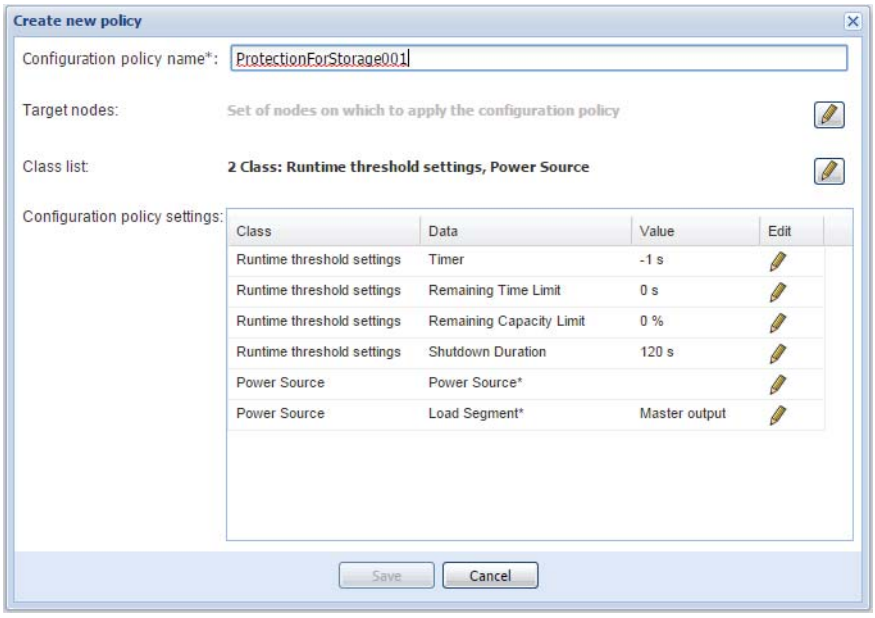

Figure 194. Create a New Configuration Policy

Shutdown

IPM manages the shutdown of storage through a simple and powerful shutdown action. For more information, see “Advanced Events and Actionswith” on page 31.

Chapter 12 Extended Functionality

This chapter describes extended functionality for the Eaton Intelligent Power Manager (IPM) including:

- Configuring the Eaton IPM vCenter Plug-in
- Configuring the XenCenter Plug-in
- Configuring Maintenance Mode and vMotion with vCenter
- VMware vCenter HA (High Availability)
- Configuring Maintenance Mode and LiveMigration with SCVM

Configuring the Eaton IPM vCenter Plug-in and WebPlug-in

The VMware® vCenter Server platform forms the foundation for virtualization management. It provides management of hosts and virtual machines (VMs) from a single console. To further unlock the power of VMware's management system, VMware has provided a facility to extend the functionality of VMware vCenter.

Various useful applications can be attached to vCenter to make it more useful. The vCenter Eaton Intelligent Power Manager Plug-in is also called the Eaton vCenter Plug-in. It is easy to deploy and to use the plug-in to manage the Eaton Intelligent Power Manager (IPM) from vCenter. This plug-in integrates the Eaton IPM with vCenter environment. After the plug-in is deployed, a tab in vCenter will open the Eaton IPM and allows you to configure and manage the Eaton IPM from the vCenter environment.

The VMware plug-in also allows the creation of new type of events that can be trigger type alarms (these are alarms that trigger an action).

Checking for vCenter Plug-in Registration

To verify that the Eaton IPM plug-in is registered in vCenter:

1. In the VMware vSphere Client, select the Plug-ins > Manage Plug-ins menu item (see Figure).
2. Locate the Eaton IPM Plug-in for vCenter in the Plug-in Manager (see Figure 196).

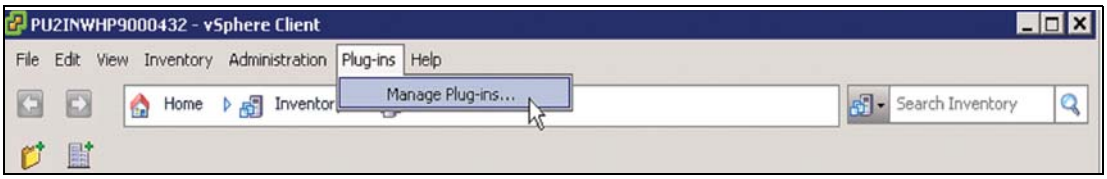

Figure 195. vSphere Client - Manage Plug-in Menu

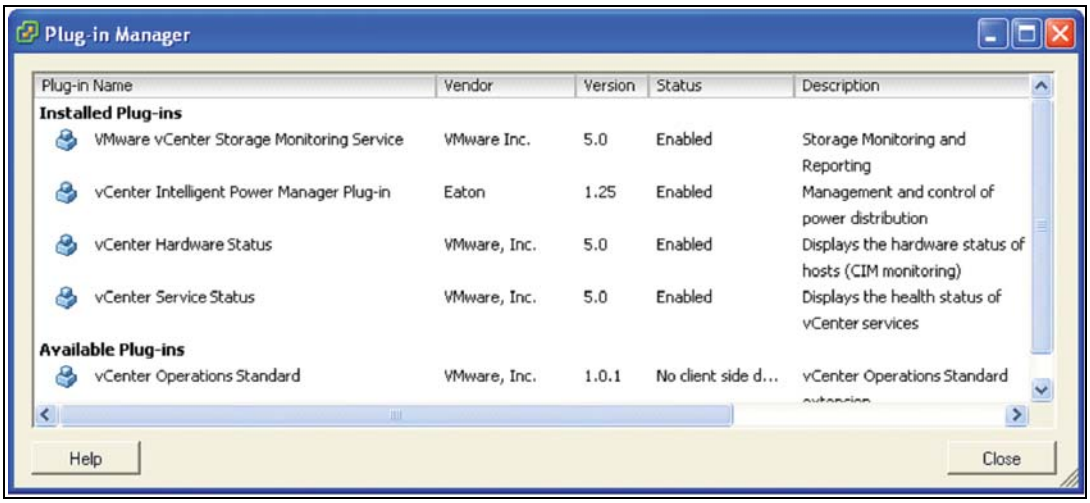

Figure 196. vCenter Plug-in Manager

Events and Alarms

After the vCenter Eaton Intelligent Power Manager Plug-in is registered, the Eaton IPM creates a new alarm "Host UPS PowerFailure (On Battery)" that is triggered from power event (see Figure 197).

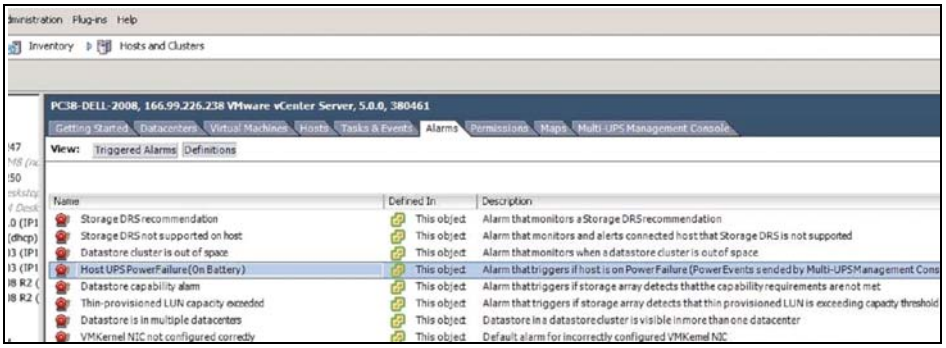

Figure 197. vCenter New Alarm from Eaton IPM

Using Eaton IPM through vCenter

The Eaton IPM tab is visible in the vCenter Server Console and in the root folder . The Eaton IPM is now available and is fully functional with the vSphere Client. Note that the Eaton Power Manager tab on the top is selected (see Figure 198).

Figure 198. vCenter Server Console

Using the Web Plug-in through the vSphere Web Interface

On the ***vCenter > DataCenter*** level, you will see a widget with the number of UPSs (devices) protecting your ESXi and a link to go directly on the IPM web interface (see Figure 199).

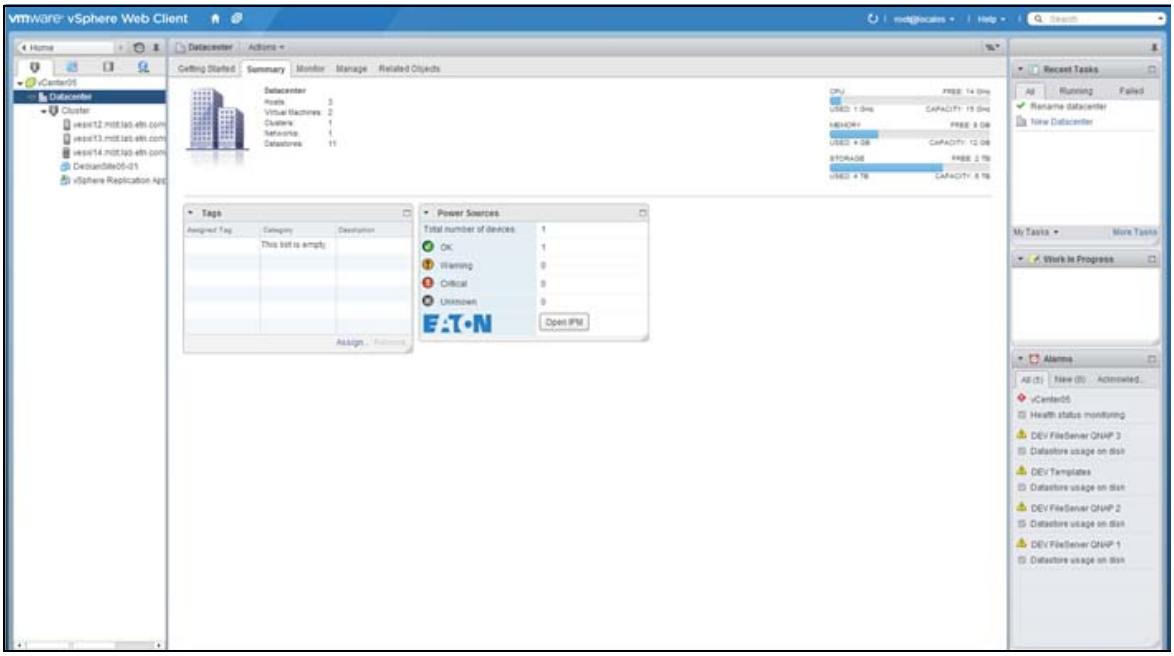

Figure 199. WebPlug-in DateCenter Level

On the Host level, you will see a widget with the UPS protecting your ESXi, and other information such as state, and a link to go directly on the IPM web interface.

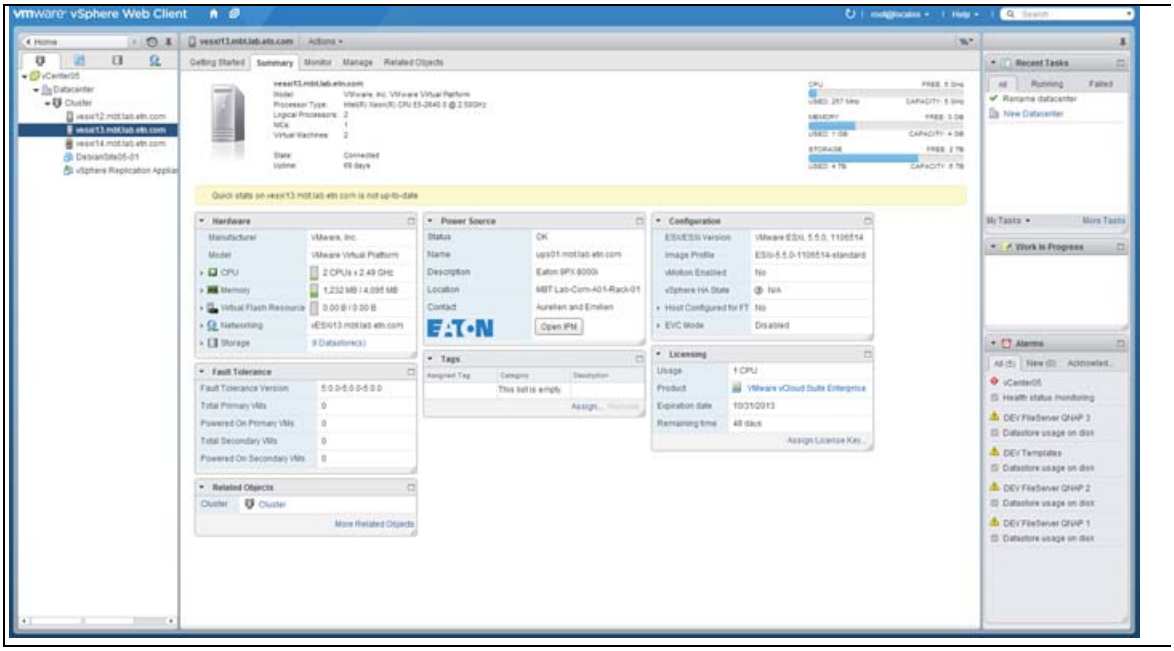

Figure 200. WebPlug-in Host Level

Configuring XenCenter Plug-in

Prerequisites

The Eaton IPM must be installed on the same machine as Citrix® XenCenter™.

Check XenCenter Plug-in Installation

- In the virtualization panel, check the box "XenCenter Plugin" to install XenCenter Plug-in (see Figure 201).
- You see the ***Plugin in XexCenter > Tools > Plugins***.
- If not, click **Re-scan Plugin Directory** (see Figure 202).
- Ensure that the Eaton IPM checkbox is selected.

Figure 201. Add Manager or Hypervisor List Dialog

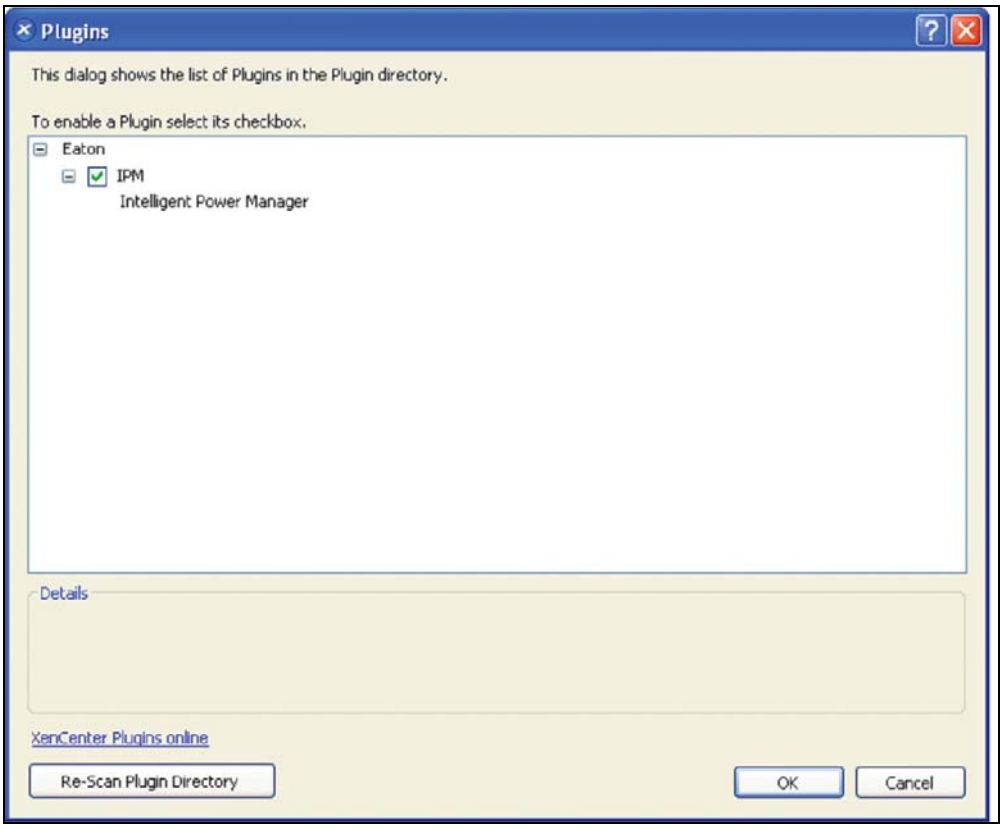

Figure 202. Plug-in Directory (Rescan)

Using Eaton IPM through XenCenter

After the plug-in is installed, you can see a tab named Eaton Intelligent Power Manager on the XenCenter level (see Figure 203).

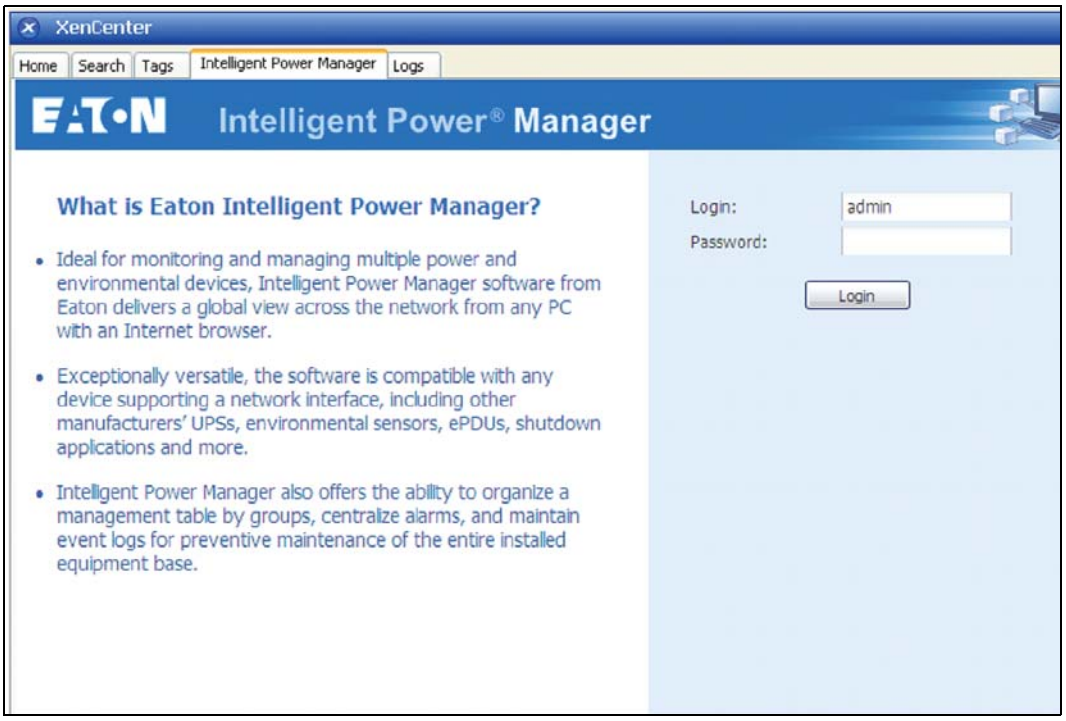

Figure 203. XenCenter Eaton IPM Tab

Configuring Maintenance Mode and vMotion with vCenter

Prerequisites

All VM images must be installed and configured on a file server.

NOTE For more information, see "VMware References" on page 187.

Introduction

The Dynamic Resource Scheduler (DRS) application from VMware is used to provide load balancing within the IT network. In particular, DRS is used to ensure the right resource capacity is available for the data center load. A second application called VMware vMotion (used in conjunction with DRS) will enact movement of VMs from physical server to physical server in order to provide the best load balance.

The Distributed Power Manager (DPM) application helps to maximize data center electrical power efficiency. It checks DRS for physical server utilization and then, using vMotion, moves VMs to servers in order to fully unload servers, idle them, or power them down for maximum power savings.

Eaton uses the same vMotion capability when a UPS is in a critical power situation to move VMs off of a server that has a critical power situation. Eaton IPM then writes alarms/alerts into vCenter, which, in turn, triggers vMotion.

VMware uses the term "setting a server into Maintenance mode" to trigger the vMotion. It is called this because before performing maintenance on server, the data center manager needs to clear the VMs from the server.

Understanding Maintenance Mode

Both standalone hosts, and hosts within a cluster, support the maintenance mode. Only VMware ESX/ESXi Server 3.0 and later supports maintenance mode for standalone hosts.

A host enters or leaves maintenance mode only as the result of a user request. If the host is in a cluster when it enters maintenance mode, the user is given the option to evacuate powered-off VMs. If this option is selected, each powered-off VM is migrated to another host, unless there is no compatible host available for the VM in the cluster. While in maintenance mode, the host does not allow deployment or "power-on" of a VM. VMs that are running on a host entering maintenance mode need to be either migrated to another host or shut down (either manually or automatically by DRS).

When no more operating VMs are on the host, the host's icon changes to include 'under maintenance' designation and the host's Summary panel indicates the new state. The default automation mode of a VM determines its behavior when the host (in a DRS cluster) it is running on enters maintenance mode:

- Any fully automated VM is migrated automatically.
- For a partially automated or manual VM, a recommendation for further action is generated and displays.

Configuring Maintenance Mode Behavior in vCenter

To configure the maintenance mode feature behavior, enable the DRS in "Fully Automated" automation level with following steps:

1. Open the vCenter server in a vSphere client.
2. Right-click and select ***Cluster > Edit Setting > Turn on VMware DRS***. Click **Next** and accept all default values.

NOTE With this example, you choose to move all the VMs from this server to another server of the same cluster. You can also define other behaviors according to your needs.

Configuration Test

To test the installation, please perform a power failure on the UPS and check on vSphere client that the corresponding ESX/ESXi host enters in Maintenance mode after the "Maintenance mode timer."

VMware vCenter High Availability

After the High Availability (HA) Cluster feature is enabled, VMware disables the automatic startup and shutdown functionality when a hypervisor is shut down.

Eaton IPM features for HA mode are as follows:

- Eaton IPM continues to move the VM from one server to the others, if all servers are powered by different UPSs with different power source (see Figure 204).

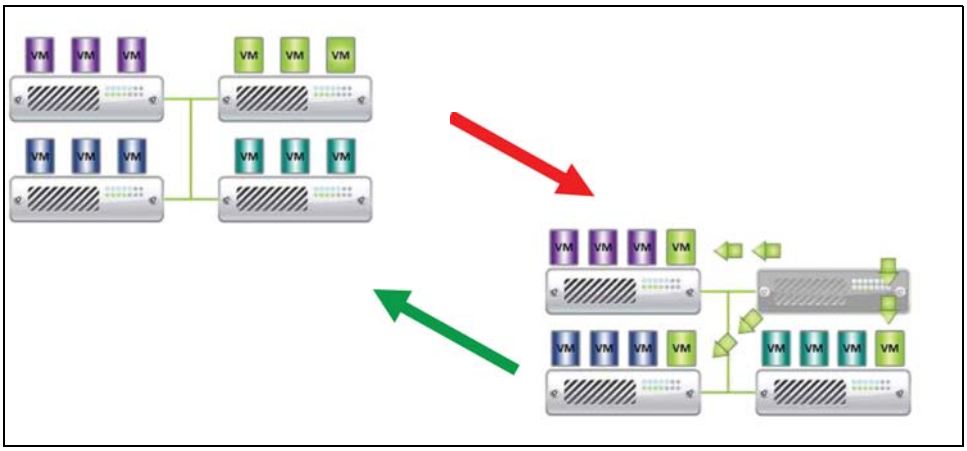

Figure 204. HA Mode with Eaton IPM

Eaton IPM continues to protect the hypervisor also when power fails.

Due to the deactivation of the automatic startup and shutdown, all VMs power-off at the end of utility failure sequence.

There are two solutions to prevent this VM from powering off:

- Configure the VMware ESX/ESXi nodes in Eaton IPM to shut down the VMs (remote shutdown of the VM setting).
- Install Eaton IPM on each VM, even if it is not an optimized solution. Take care to ensure that when VMs move, the Eaton IPM still links to the same UPS power source.

Table 15. Table Configuration/Behavior

Case	Remote Shutdown	VM Remote Shutdown Type	HA in vCenter	VM Action	Hypervisor Action	Comments
1	ENABLED	ENABLED	ENABLED	SHUTDOWN	SHUTDOWN	Valid Configuration
2	ENABLED	ENABLED	DISABLED	SHUTDOWN	SHUTDOWN	Valid Configuration (more reliable to let VMware shut down its own VMs)
3	ENABLED	DISABLED	ENABLED	CRASH	SHUTDOWN	Hypervisor shuts down without the VMs
4	ENABLED	DISABLED	DISABLED	CRASH/SHUTDOWN	SHUTDOWN	Depends on the VM startup/shutdown configuration
5	DISABLED	ENABLED	ENABLED	CRASH	CRASH	No action (IPM)
6	DISABLED	ENABLED	DISABLED	CRASH	CRASH	No action (IPM)
7	DISABLED	DISABLED	ENABLED	CRASH	CRASH	No action (IPM)
8	DISABLED	DISABLED	DISABLED	CRASH	CRASH	No action (IPM)

NOTE For more information about the deactivation of the Automatic Startup/Shutdown when creating a VMware HA Cluster, see links provided by "vSphere SDK for Perl" on page 187.

VMware References

Eaton and Virtualization

- http://www.eaton.com/virtualization

VMware ESX Configuration

- http://www.vmware.com/support

vCenter Server (VMware Supervisor)

- Visit http://www.vmware.com/products/vcenter-server for more information about download and installation of vCenter Server.
- Visit also http://www.vmware.com/products/vsphere/features/drs-dpm.html for more information about Distributed Resource Scheduler.

vSphere SDK for Perl

- For more information about download and installation of vSphere SDK for Perl, visit: http://www.vmware.com/support/developer/viperltoolkit/
- For more information about creating a vSphere HA Cluster., visit: http://pubs.vmware.com/vsphere-50/index.jsp?topic=%2Fcom.vmware.vsphere.avail.doc_50%2FGUID-E90B8A4A-BAE1-4094-8D92-8C5570FE5D8C.html

Microsoft Hyper-V References

Eaton and Virtualization

- For more information about virtualization, visit: http://www.eaton.com/virtualization

Microsoft TechNet Library

- For more information about Microsoft TechNet Library, visit: http://technet.microsoft.com/en-us/library

About Maintenance Mode

- For more information about Maintenance Mode, visit: http://technet.microsoft.com/en-us/library/ee236481.aspx

Requirements for Using Live Migration

- For more information about "Hyper-V Live Migration FAQ," visit: http://technet.microsoft.com/en-us/library/ff715313%28WS.10%29.aspx

VMware Icons and Diagrams

This document was created using the official VMware icon and diagram library. One or more VMware products are patented. Patents are listed at http://www.vmware.com/go/patents.

VMware does not endorse or make any representations about third-party information included in this document. The inclusion of any VMware icon or diagram in this document does not imply such an endorsement.

Manage the Cisco UCS Manager Component

NOTE Cisco UCS supports versions 2.x and 3.0.1a.

Enabling the Component

To enable the Infrastructure Connectors:

1. From the left-side **Views** panel of the Eaton IPM main interface window, select the ***Settings > System*** menu item. The System page displays.
2. Click **Edit modules settings** in the right panel. The Edit modules settings dialog box displays (see Figure 205).
3. Ensure that the **Infrastructure Connectors** checkbox is selected (checked).
4. Click **Save**.

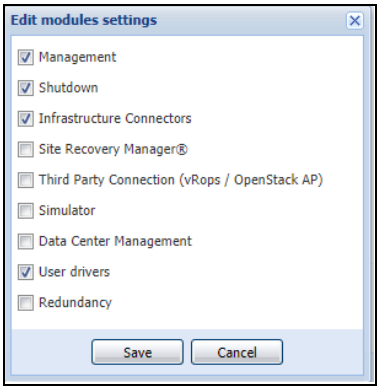

Figure 205. Edit Modules Settings - Infrastructure Connectors

Add the Component

To add a Cisco UCS Manager:

1. From the left-side **Views** panel of the Eaton IPM main interface window, select the ***Settings > Infrastructure Connectors*** menu item. The Infrastructure Connectorspage displays (see Figure 206).
2. Click **Add a connector** in the right panel. The Add a connector dialog box displays.

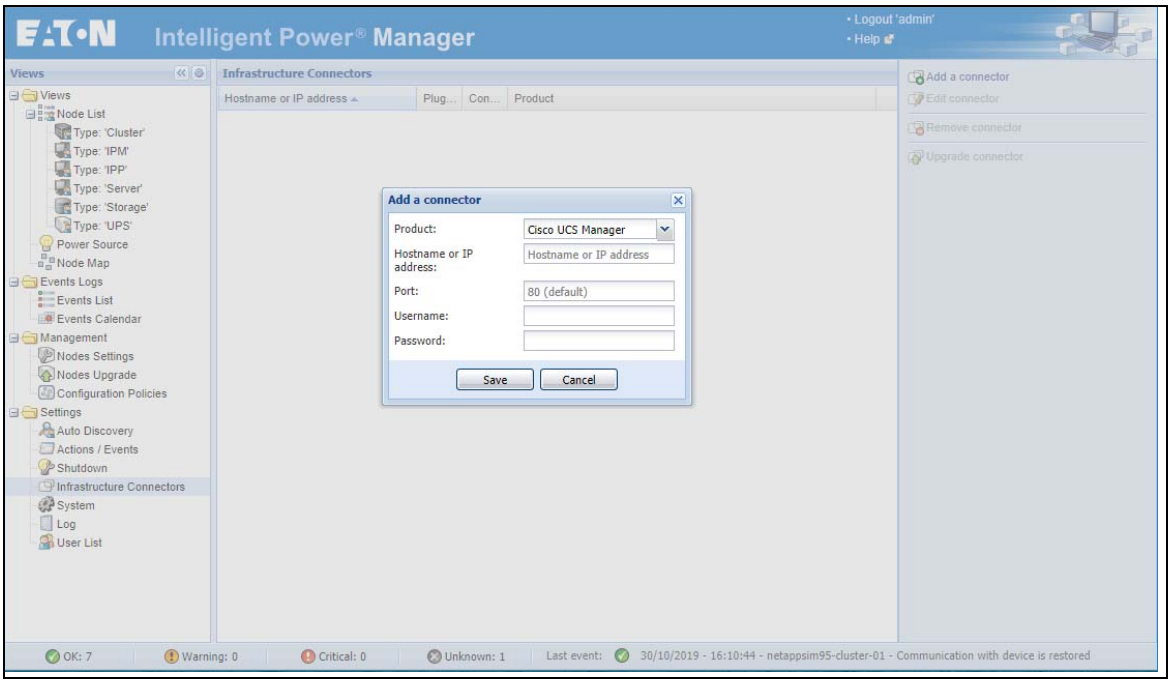

Figure 206. Select Add a Connector

3. From the Add a Connector dialog, select Cisco UCS Manager from the Product drop-down list.
4. Add identification information for the selected connector:
   - **Product:** Cisco UCS Manager is already selected in the drop-down list.
   - **Hostname or IP address:** Type Cisco UCS Manager IP address
   - **Port:** Port number
   - **Username**: Type Cisco UCS Manager Administrator Username for the Administrator with admin rights on the Cisco UCS Manager
   - **Password:** Type Cisco UCS Manager Administrator Password
5. Click **Save** after the fields are updated.
6. When the component is connected, the Cisco UCS Manager displays on the Infrastructure Connectors page (see Figure 207).
7. If the component does not display, refresh the page. Also, check the log to ensure the Event details display with an OK connection state (see Figure 208).

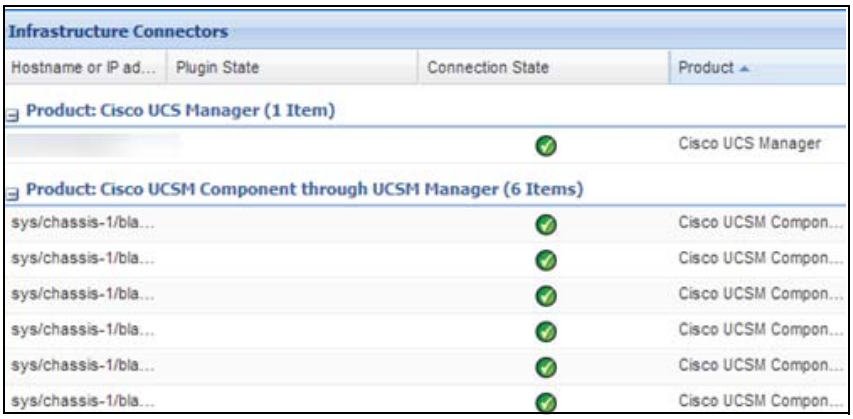

Figure 207. Cisco UCS Manager Component Added

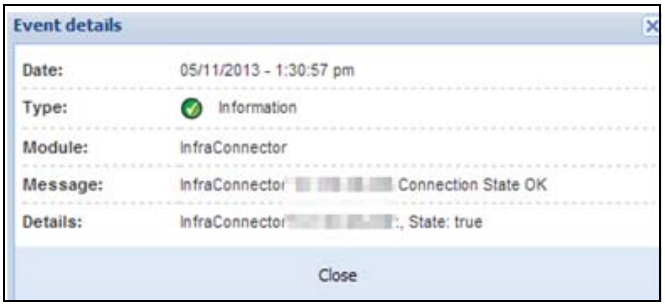

Figure 208. Event Details

Remove the Component

To remove a Component, right-click the component in the list. From the action box, click **Remove connector** (see Figure 209).

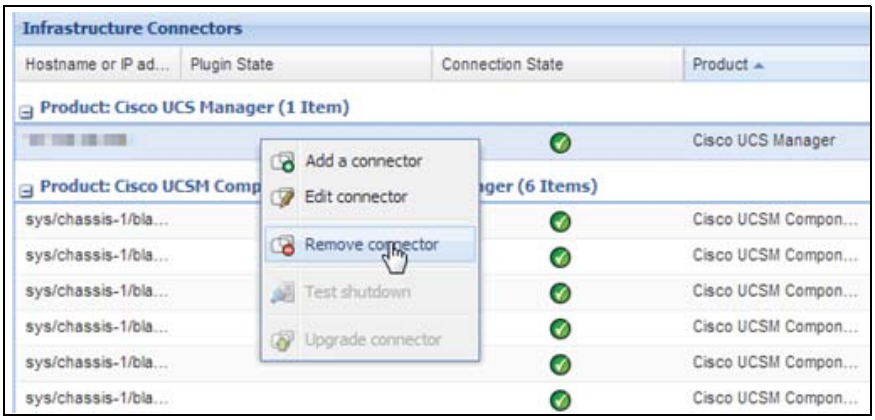

Figure 209. Remove a Connector

Edit a Component

To edit a Component, right-click the component in the list. From the action box, click **Edit connector** (see Figure 210). The Edit connector dialog displays.

NOTE IPM currently doesn't allow you to edit the IP address. To edit a new IP address, please remove the connector and add another connector.

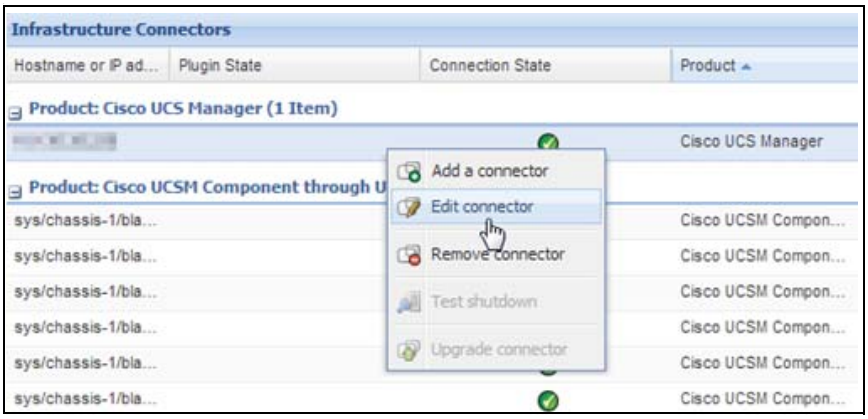

Figure 210. Edit a Connector

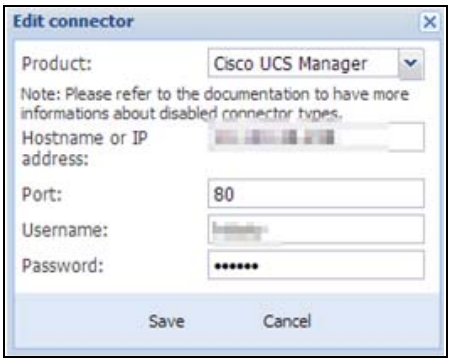

Figure 211. Edit Connector Dialog

Configure the Cisco UCS Manager Component

To set the UCS Manager component configuration:

1. Select ***Nodes Settings > "the UCS Manager component" > Shutdown Setting*** and click the pen icon (see Figure 212).

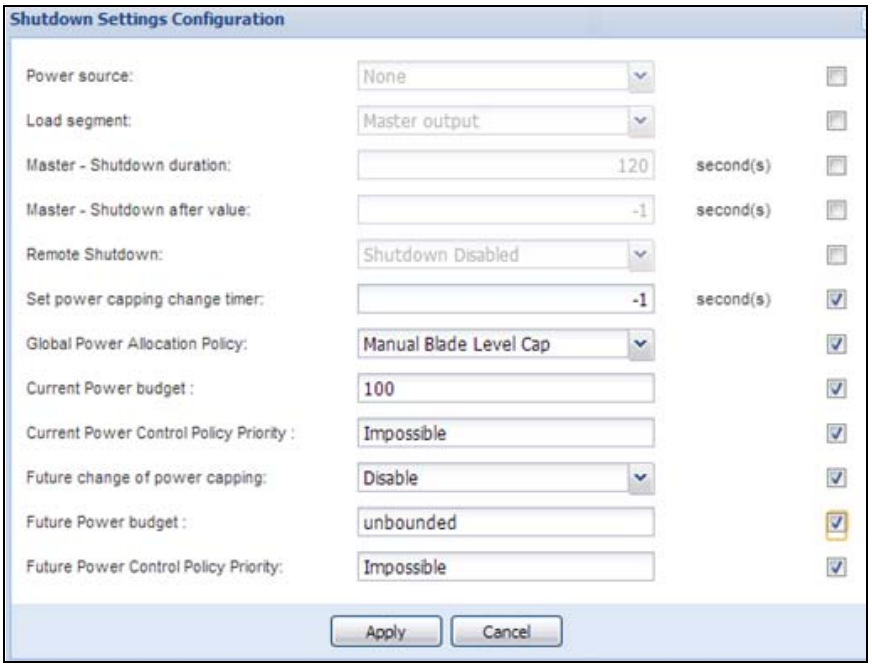

Figure 212. Shutdown Settings Configuration

Power source, Load Segment, Remote shutdown, Shutdown duration, and Shutdown after value are standard IPM options and are not described here. The following topics are discussed:

- difference between "current" and "future" options
- power capping timer
- global power allocation policy
- policy-driven power capping
- manual blade-level power capping
- power control policy and priority
- power budget

Difference Between "Present" and "Future" Options

The current Power Budget or Policy Priority are the values that are currently set in your UCS Manager (see Figure 213). Any change on those in IPM permanently sets the new values on UCS manager.

The future Power Budget or Policy Priority are the values that will be temporarily set in your blade. When the power failure occurs, the older values will be set back in your blade after the power come back.

Power Capping Timer

The power capping timer will set the Power Capping as specified by the duration (in seconds). See Figure 213. It launches immediately after a power failure. The value -1 signifies no timer set.

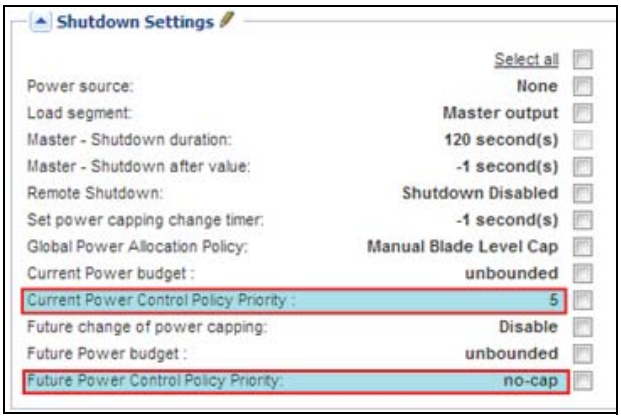

Figure 213. Shutdown Settings-Set Power Capping Change Timer

Global Power Allocation Policy

The global cap policy is a global policy that specifies whether policy-driven chassis group power capping or manual blade-level power capping will be applied to all servers in a chassis (see Figure 214).

Two global allocation policies in IPM are:

- policy-driven power chassis group power capping
- manual blade-level power capping

Policy-driven Chassis-level Power Capping

When policy-driven power chassis group power capping is selected in the global cap policy, Cisco UCS can, at the blade level, compute the amount of power allocated to a chassis based on priority (see Figure 214).

IMPORTANT

A service profile has to be attached to a blade to set priorities on a blade.

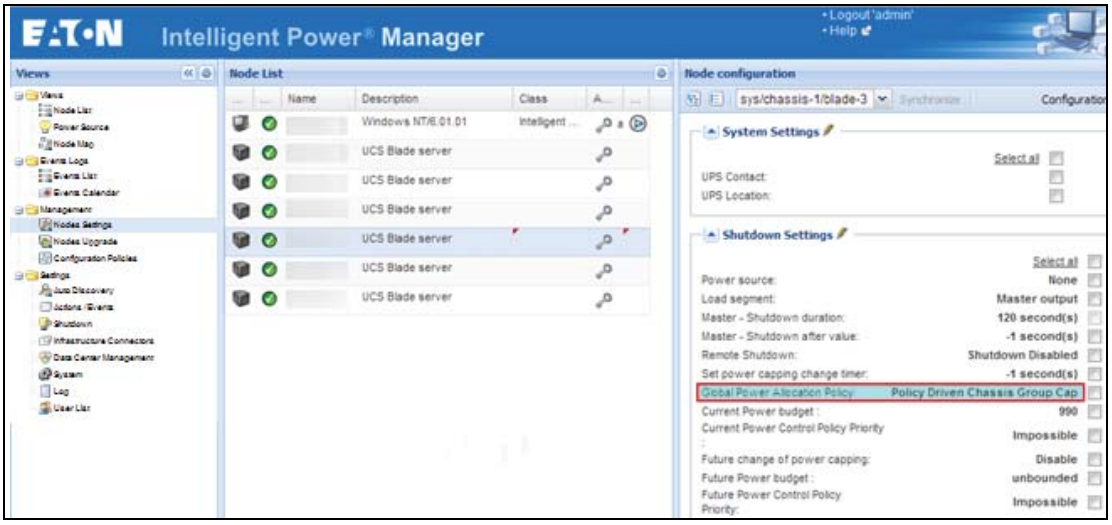

Figure 214. Policy-driven Power Chassis Group Power Capping

Manual Blade-level Power Capping

When manual blade-level power capping is configured in the global cap policy, you can manually set a power cap for each blade server in a Cisco UCS instance (see Figure 215).

If the server encounters a spike in power usage that meets or exceeds the maximum configured for the server, Cisco UCS Manager does not disconnect or shut down the server. Instead, Cisco UCS Manager reduces the power that is made available to the server. This reduction can slow down the server, including a reduction in CPU speed.

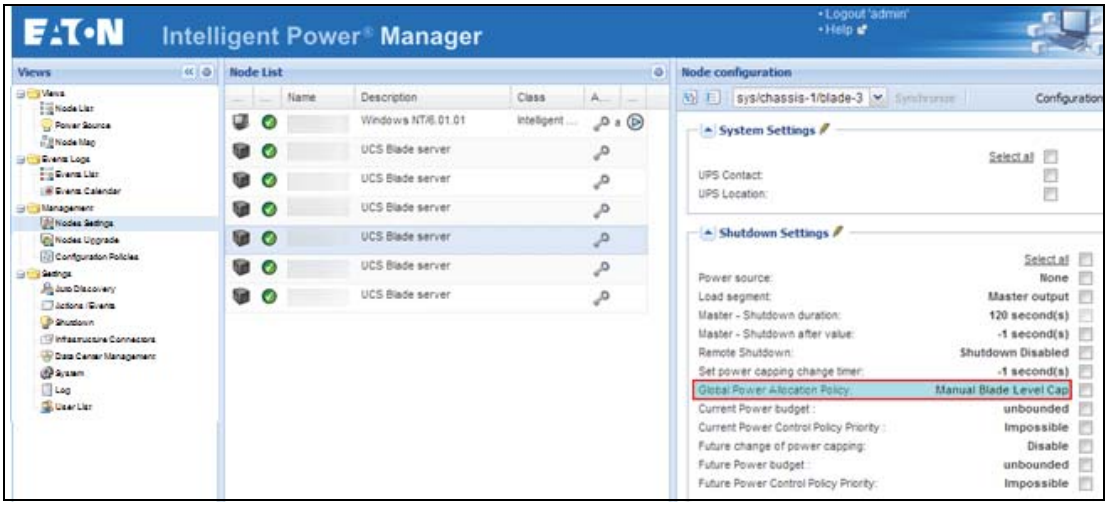

Figure 215. Manual Blade Power Capping

Power Control Policy and Priority

Cisco UCS uses the priority set in the power control policy, along with the blade type and configuration, to calculate the initial power allocation for each blade within a chassis. During normal operation, the active blades within a chassis can borrow power from idle blades within the same chassis. If all blades are active and reach the power cap, service profiles with higher priority power control policies take precedence over service profiles with lower priority power control policies.

Priority is ranked on a scale of 1-10, where 1 indicates the highest priority and 10 indicates lowest priority. The default priority is 5.

For mission-critical applications, a special power priority called no-cap is also available. Setting the priority to no-cap prevents a Cisco UCS from leveraging unused power from that particular blade server. The server is allocated the maximum amount of power that the blade can reach (see Figure 216 and Figure 217).

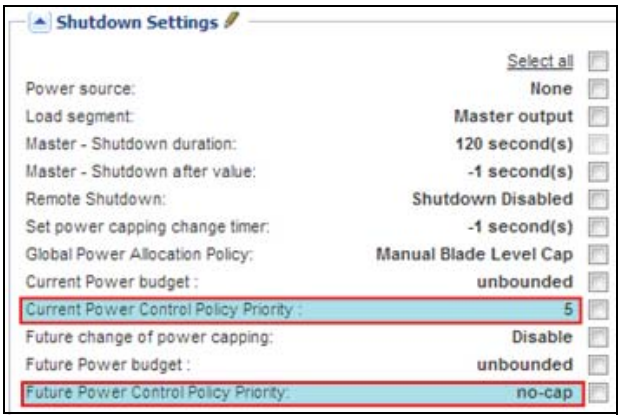

Figure 216. Shutdown Settings-Current Power Default Setting (Priority 5)

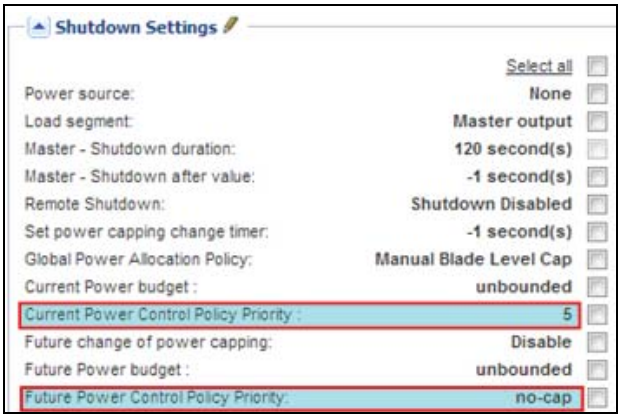

Figure 217. Shutdown Settings-Current Power Not Set Due to No-Cap Service Profile

Power Budget

Power budget allows you to specify the maximum amount of power (in watts) that the server can consume at one time.

If the value is set to "unbounded," no power usage limitations are imposed upon the server and the future temporary power budget is disabled (see Figure 218). The server can use as much power as it requires.

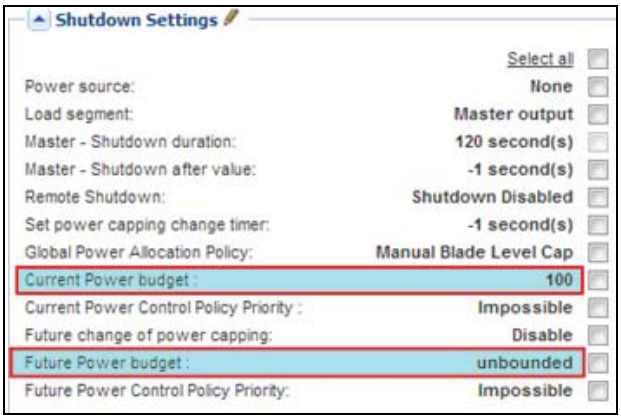

Figure 218. Shutdown Settings-Future Temporary Power Budget is Disabled

Common Errors and Notifications for the Cisco UCS Manager Component

1. You can't set a shutdown to a blade that doesn't have a service profile assigned (see Figure 219).

Figure 219. No Service Profile

2. You can't set a priority to a blade that doesn't have a service profile assigned (see Figure 220).

Figure 220. No Service Profile

3. IPM can't find a UCSM on the IP provided (see Figure 221).

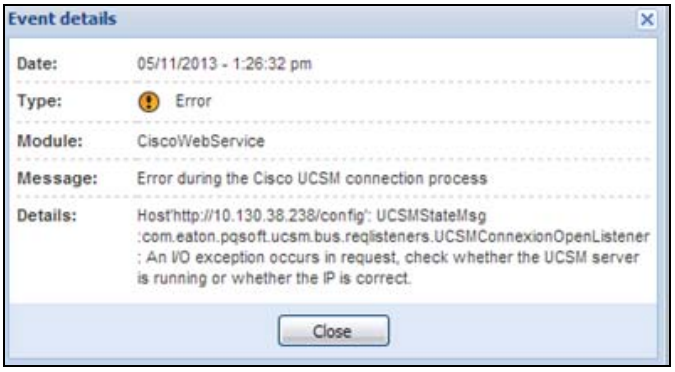

Figure 221. UCS Manager Not Found

4. A wrong value has been set for the power budget (see Figure 222).

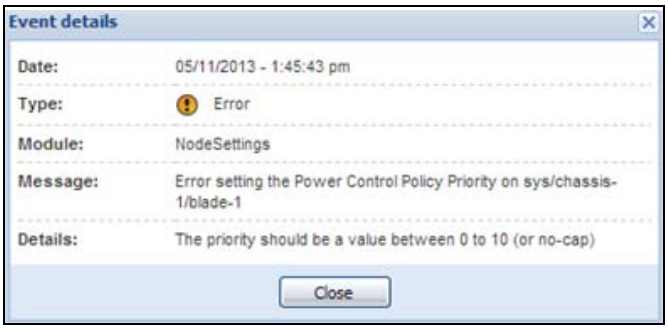

Figure 222. Wrong Power Budget Set

5. A new power budget has been requested by the client (see Figure 223).

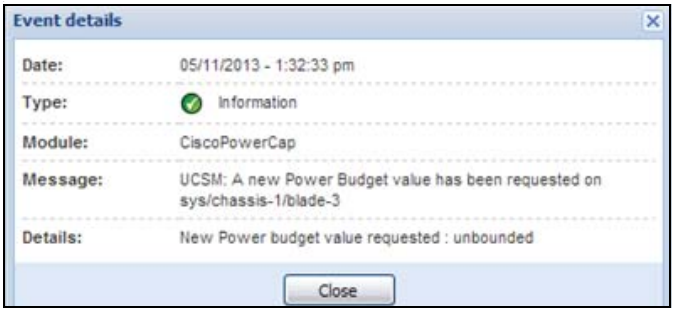

Figure 223. New Power Budget Requested

6. A new power budget has been successfully set by the server (see Figure 224).

Figure 224. New Power Budget Successful

Chapter 13 Virtual Appliance

This chapter describes deploying the Eaton Intelligent Power Manager (IPM) as a virtual appliance including:

- Deploying a Virtual Appliance in VMware vSphere
- Configuring a Virtual Appliance
- Security for the Virtual Appliance

Prerequisites and Requirements

Minimum System Requirements

The IPM virtual appliance can be installed on all hypervisors that support OVF/OVA templates.

- 14 GB data store
- 1GB free memory

NOTE Microsoft SCVMM feature is not supported on this virtual appliance.

Free Version Limitation

IPM as a virtual appliance is delivered as a "Basic" version with the limitation of 10 nodes (UPS/PDU devices). To install a new license, see"License Code" on page 12 for more information.

To supervise more than 10 nodes, please contact your sales representative.

Deploying a Virtual Appliance in VMware vSphere

To deploy the IPM virtual appliance:

1. Download the virtual appliance from one of the following links:
   - https://www.eaton.com/us/en-us/catalog/backup-power-ups-surge-it-power-distribution/eaton-intelligent-power-manager.html
   - http://powerquality.eaton.com/EMEA/Products-services/Power-Management/Software-Drivers/Intelligent-PM.asp?cx=101
2. Connect to the ESX/ESXi or vCenter from your client computer using vSphere.
3. Log in as a user who has permission to create, start, and stop virtual machines.
4. Choose ***File > Deploy OVF Template*** (see Figure 225).
5. Choose either Deploy from URL or Deploy from file, based on the location of OVA file.
6. Select the OVA file. Click **Next**.
7. Click **Next**.
8. Follow the instructions provided on the Deploy OVF Template (see Figure 225 and Figure 226).

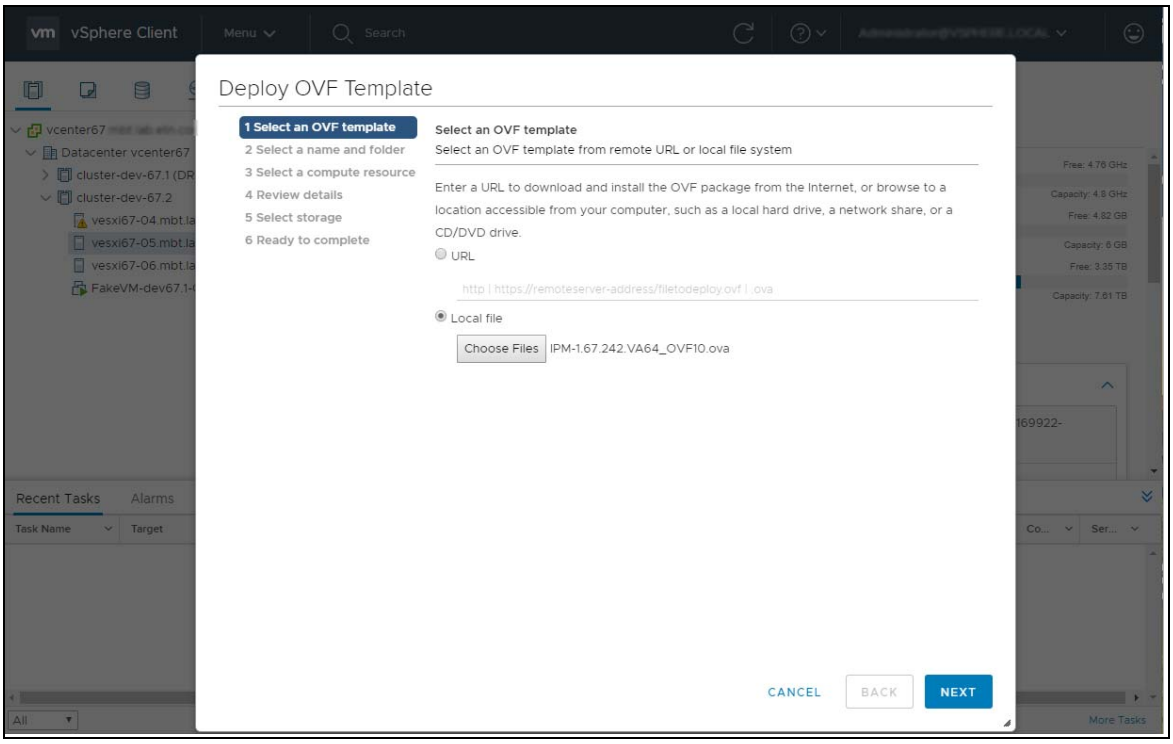

Figure 225. Deploy OVF Template

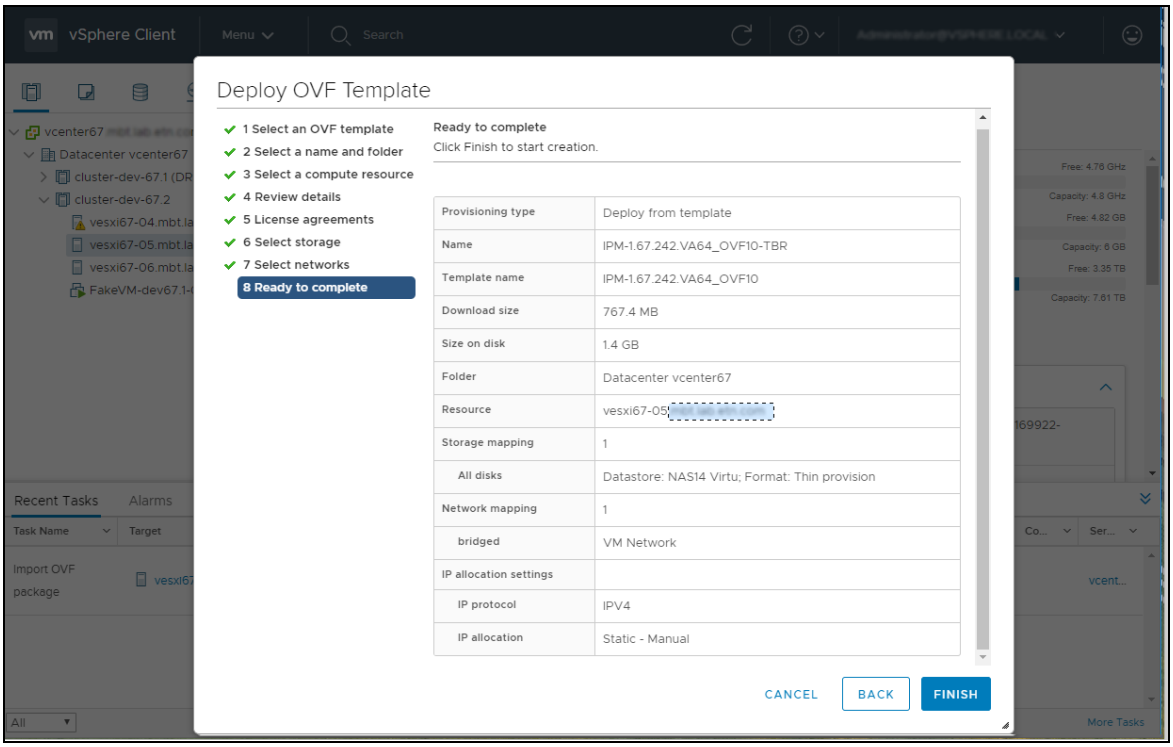

Figure 226. Deploy OVF Template

Configuring a Virtual Appliance

To log into the virtual appliance you can use:

- Standard Console of your hypervisor
- SSH Client

With a Standard Console, you will see the following screen (see Figure 227).

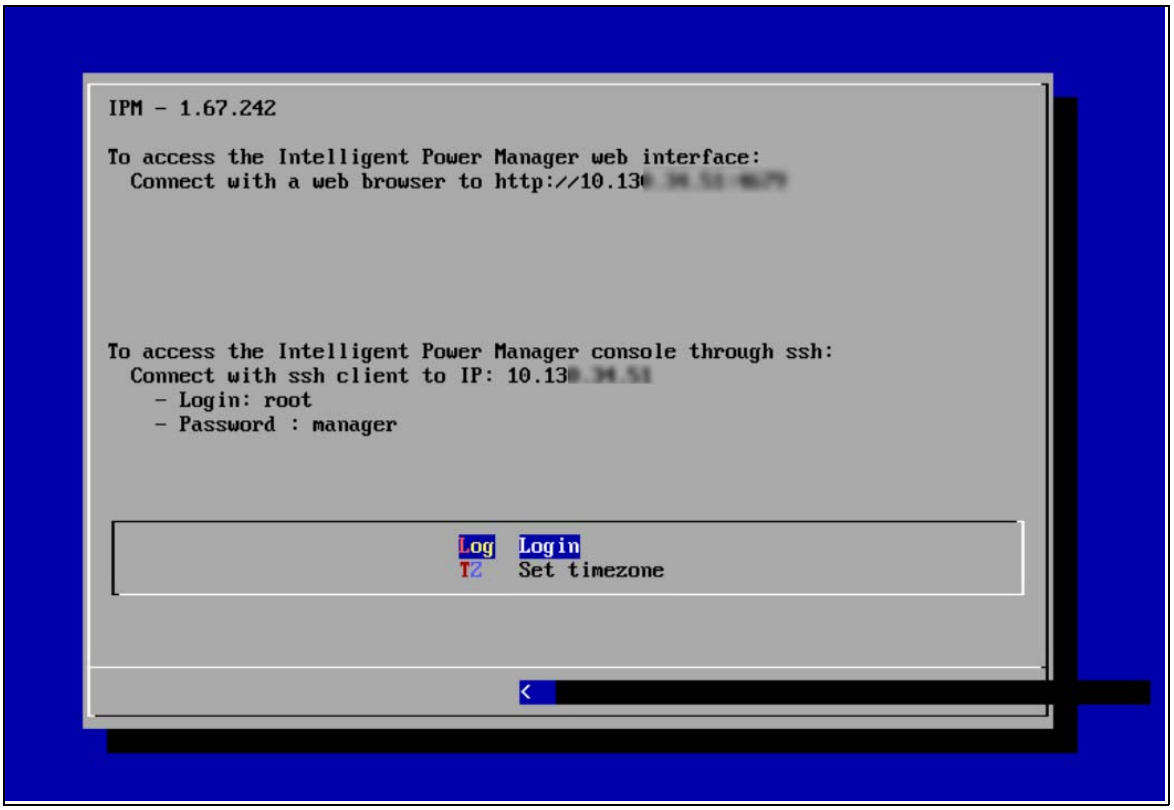

Figure 227. Standard Console

With SSH Client use the following credentials:

- Login: root
- Password: manager

NOTE To enable the first remote access, the root access is enabled for the SSH daemon. For security issues, you can disallow the connection of the root user in "/etc/ssh/sshd_config" and set "PermitRootLogin" to no.

Setting Security for a Virtual Appliance

To minimize security issue, Eaton has installed and pre-configured the firewall.

Basic Firewall Configuration

The firewall is pre-configured to drop all connection except SSH and Eaton web and devices connections.

You can only connect on the virtual appliance through Eaton Web Page or SSH connection. For example, the Virtual Appliance doesn't respond to "Ping" (an ICMP response is not allowed).

Advanced Firewall Configuration

If you want to customize the firewall configuration, you need to have:

- Knowledge of iptables
- Credentials to connect to the Virtual Appliance
- SSH Client

```
[root@localhost ~]# iptables -L -v
Chain INPUT (policy DROP 655 packets, 61197 bytes)
 pkts bytes   target     prot opt in     out     source    destination
127K   79M    ACCEPT     all  --  any    any     anywhere   anywhere     state RELATED,ESTABLISHED
  3   144     ACCEPT     tcp  --  any    any     anywhere   anywhere     tcp dpt:ssh
 1316 78424   ACCEPT     tcp  --  any    any     anywhere   anywhere     tcp dpt:mgesupervision
 0     0      ACCEPT     tcp  --  any    any     anywhere   anywhere     tcp dpt:mgemanagement
 7638   17M  ACCEPT     udp  --  any    any     anywhere   anywhere     udp dpt:mgesupervision
 3856  461K  ACCEPT     udp  --  any    any     anywhere   anywhere     udp dpt:mgemanagement
 0     0     ACCEPT  udp  --  any        any     anywhere   anywhere     udp dpt:bpcp-poll
 0     0     ACCEPT     udp  --  any    any     anywhere   anywhere     udp dpt:bpcp-trap
 0     0     ACCEPT     tcp  --  any    any     anywhere   anywhere     tcp dpt:61616
 0     0     ACCEPT     tcp  --  any    any     anywhere   anywhere     tcp dpt:rmiregistry

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 45494 packets, 12M bytes)
 pkts bytes target     prot opt in     out     source               destination
```

Figure 228. Firewall Configuration

To modify the default configuration, you need to edit the script in /etc/init.d/firewall.

You can see how the "firewall" is configured to be launched after each startup in Figure 229.

```
[root@localhost ~]#chkconfig --list
Eaton-IPM       0:off   1:off   2:on    3:on    4:off   5:on    6:off
firewall        0:off   1:off   2:on   3:on    4:off   5:on   6:off
.
.
sshd            0:off   1:off   2:on    3:on    4:on    5:on    6:off
.
vmware-tools    0:off   1:off   2:on    3:on    4:off   5:on    6:off
```

Figure 229. Modify Default Configuration

To Start or Stop the Firewall

To start the firewall:

```
[root@localhost ~]# /etc/init.d/firewall start
```

To stop the firewall:

```
[root@localhost ~]# /etc/init.d/firewall stop
```

NOTE After upgrading IPM software (1.28 to 1.40 for example) you must add these two rules in the firewall:

```
/sbin/iptables -A INPUT -p tcp --dport 61616 -j ACCEPT #EMC4J MessageBus
/sbin/iptables -A INPUT -p tcp --dport 1099 -j ACCEPT #rmiregistry
```

Configuring IPM

To configure IPM, see "Configuring IPM".

VMware Studio References

Virtual Appliance on VMware Website

- Visit http://www.vmware.com/support/developer/studio for more information on Virtual Appliance on VMware website

Firewall (iptables)

- Visit the iptables project on the NetFilter website
- Project - http://www.netfilter.org/projects/iptables/index.html
- Documentation - http://www.netfilter.org/documentation/index.html

Chapter 14 Service and Support

If you have any questions or problems with the Eaton Intelligent Power Manager (IPM), call your **Local Distributor** or the **Help Desk** at one of the following telephone numbers and ask for a technical representative.

United States:	**1-800-356-5737**
Canada:	**1-800-461-9166 ext 260**
All other countries:	**Call your local service representative**

Please have the following information ready when you call the Help Desk:

- Model number
- Serial number
- Version number (if available)
- Date of failure or problem
- Symptoms of failure or problem
- Customer return address and contact information

If repair is required, you will be given a Returned Material Authorization (RMA) Number. This number must appear on the outside of the package and on the Bill Of Lading (if applicable). Use the original packaging or request packaging from the Help Desk or distributor. Units damaged in shipment as a result of improper packaging are not covered under warranty. A replacement or repair unit will be shipped, freight prepaid for all warrantied units.

NOTE For critical applications, immediate replacement may be available. Call the **Help Desk** for the dealer or distributor nearest you.

Chapter 15 Appendix A

Web Interface and Cryptography

The web interface of Eaton Intelligent Power Manager is available in plain text at http://<host>:4679/ or through a secure channel at https://<host>:4680/, where <host> is the host name or IP address of the machine hosting the Eaton IPM.

For cybersecurity reasons, by default, the plain text page redirect to secured one. To manually activate unsecured plain text pages, go to Settings > System > Security settings and uncheck the option "Force HTTPS mode to access to the interface".

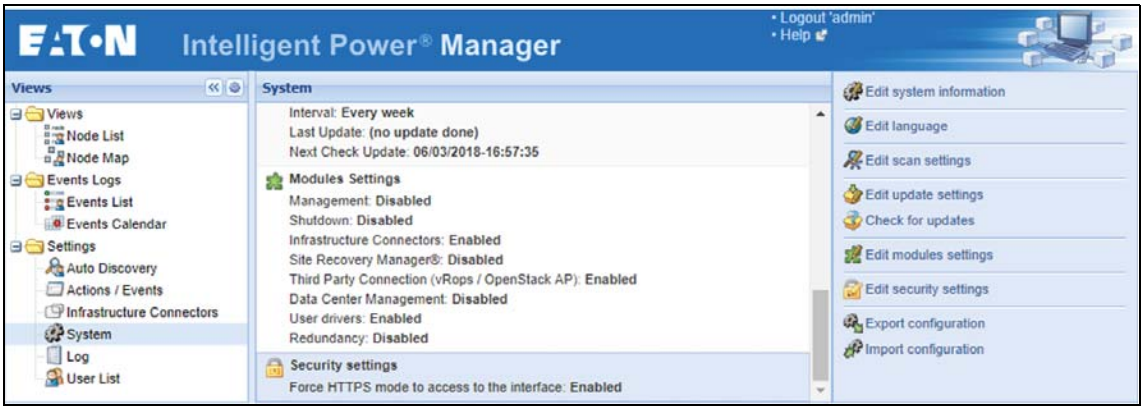

Figure 230. IPM Security Settings

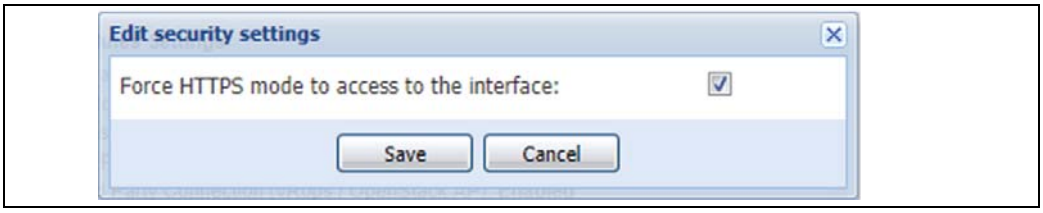

Figure 231. Save Security Settings

By default, when a client connects to the secured interface, IPM uses an RSA-2048 key and a self-signed certificate. A security certificate alert message is likely to appear from the Web browser. You can go through by selecting "Continue to this website", directly available or through an advanced settings section depending of the browser.

NOTE If you deactivate the option, you have to clear the browser cache and to refresh the web page.

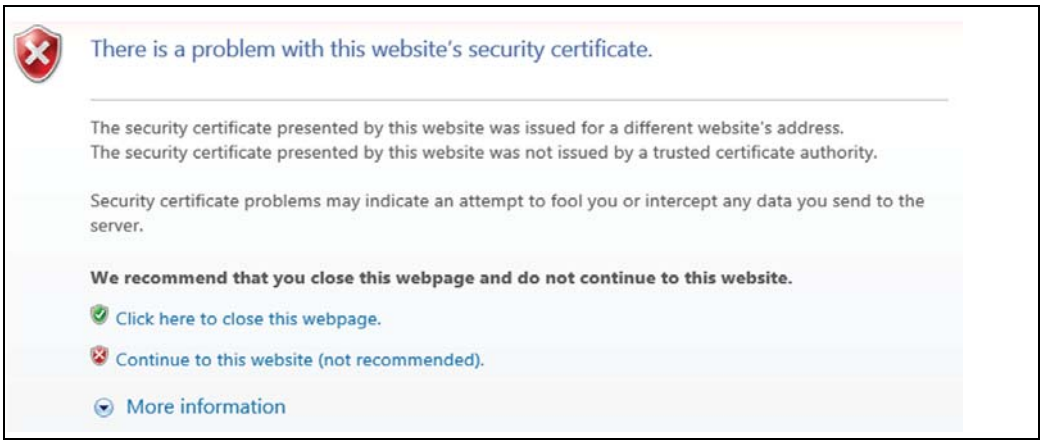

Figure 232. Security Alert Message

An administrator can set their own private key and certificates by putting them in respectively key.pem and cert.pem files in the "bin" subdirectories of the installation directory (typically C:\Program Files (x86)\Eaton\IntelligentPowerManager\bin). They will be taken in account after a restart of the Eaton Intelligent Power Manager service.

For more details about Cybersecurity recommendations please review this document "IPM Recommended Secure Hardening Guidelines"

Available in "White papers" section on eaton website :

http://www.eaton.com/us/en-us/catalog/backup-power-ups-surge-it-power-distribution/eaton-intelligent-power-manager.resources.html

Create an Action

Prerequisites

None

Example Procedure

1. Select ***Settings > Actions / Events***.
2. In the right panel, click Create a new action.
3. Select the Action type you want to perform (E-mail, VM Host Power action, and so forth).
4. Select the Event on which you want the action to be launched.
5. Configure the Settings of the Action (see Figure 233).

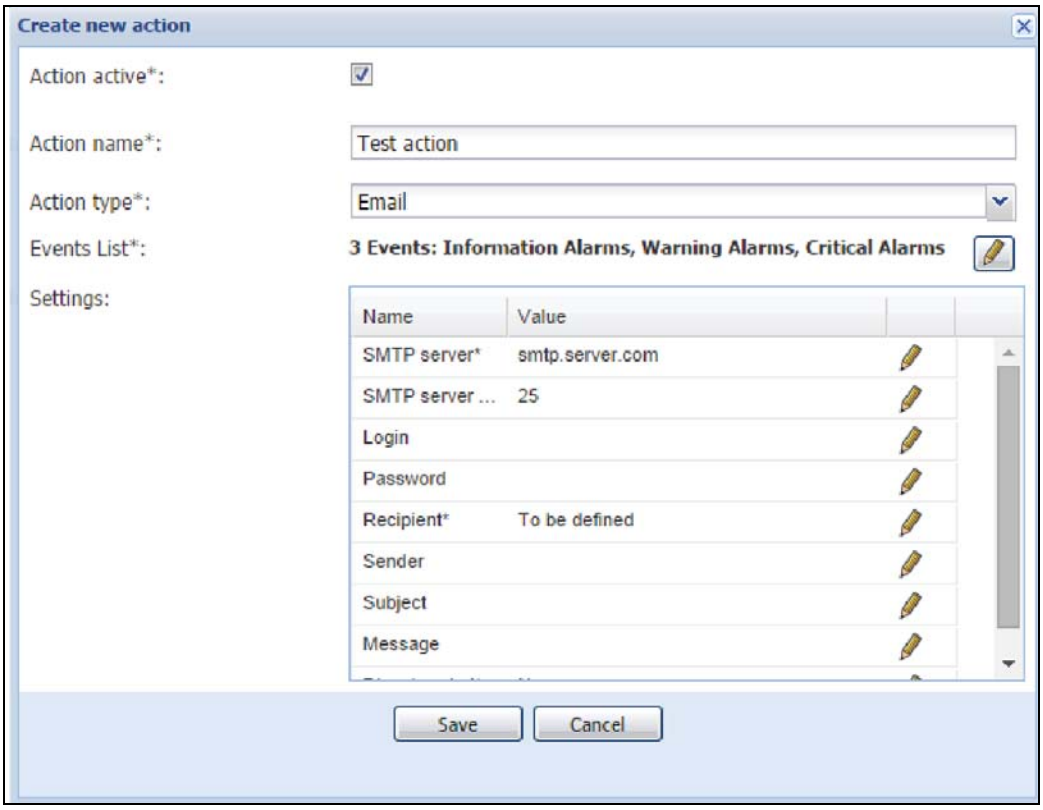

Figure 233. Create New Action

Create a Configuration Policy

Prerequisites

None

Example Procedure

1. Select ***Management > Configuration Policy***.
2. In the right Selection view panel, click Create new configuration policy. The Create new configuration policy dialog displays (see Figure 234).

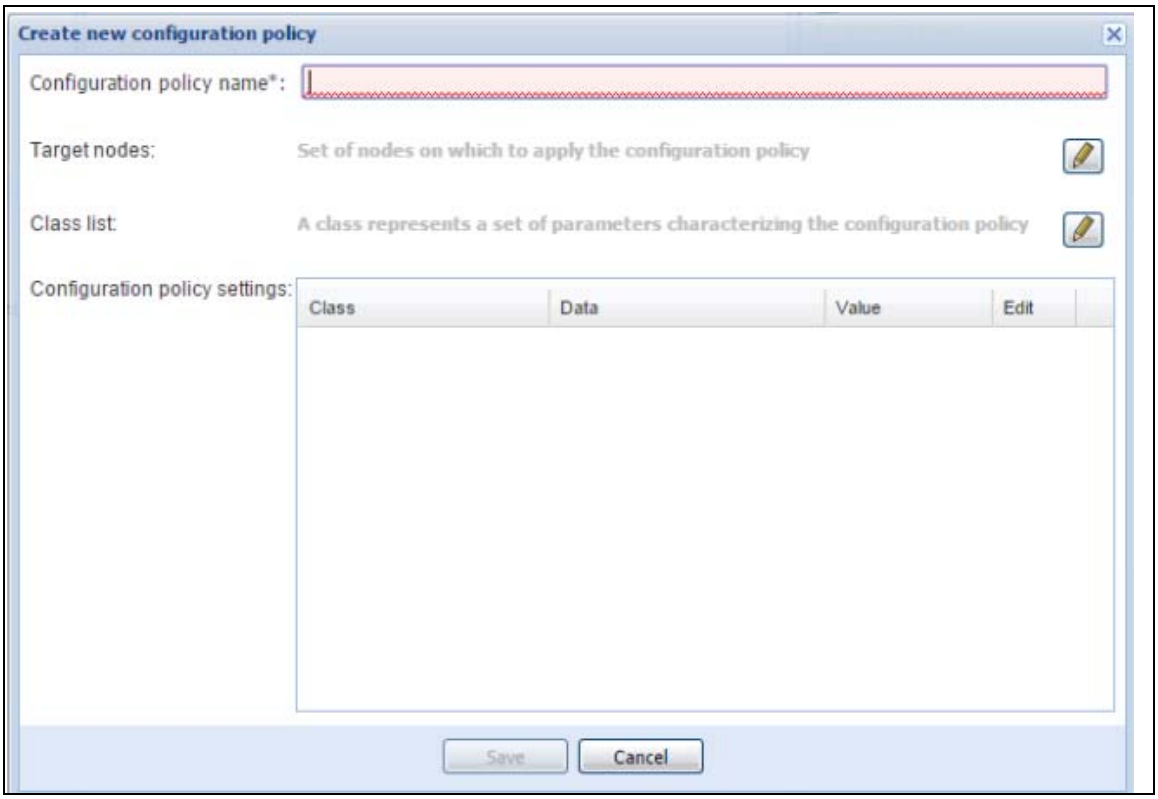

Figure 234. Create New Configuration Policy

3. Select the pen icon for **Class list** to enable the configuration of:
   - Asset Information
   - Runtime threshold settings
   - Power Source
   - User Settings
4. In this example case, select (check) the **Power Source** checkbox to add the Power Source class, and then click **Ok** (see Figure 235).

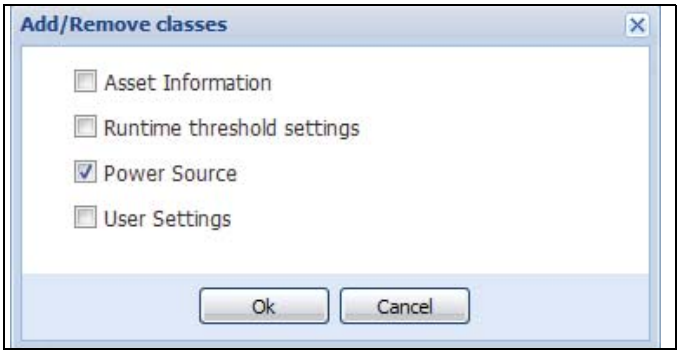

Figure 235. Add/Remove Classes

5. Select the pen associated with Target nodes to add or remove classes in the configuration policy.

6. In this example, select nodes from the "Available nodes list" and transfer them to the "Selected nodes list" using the right arrows, and then click **Ok** (see Figure 236).

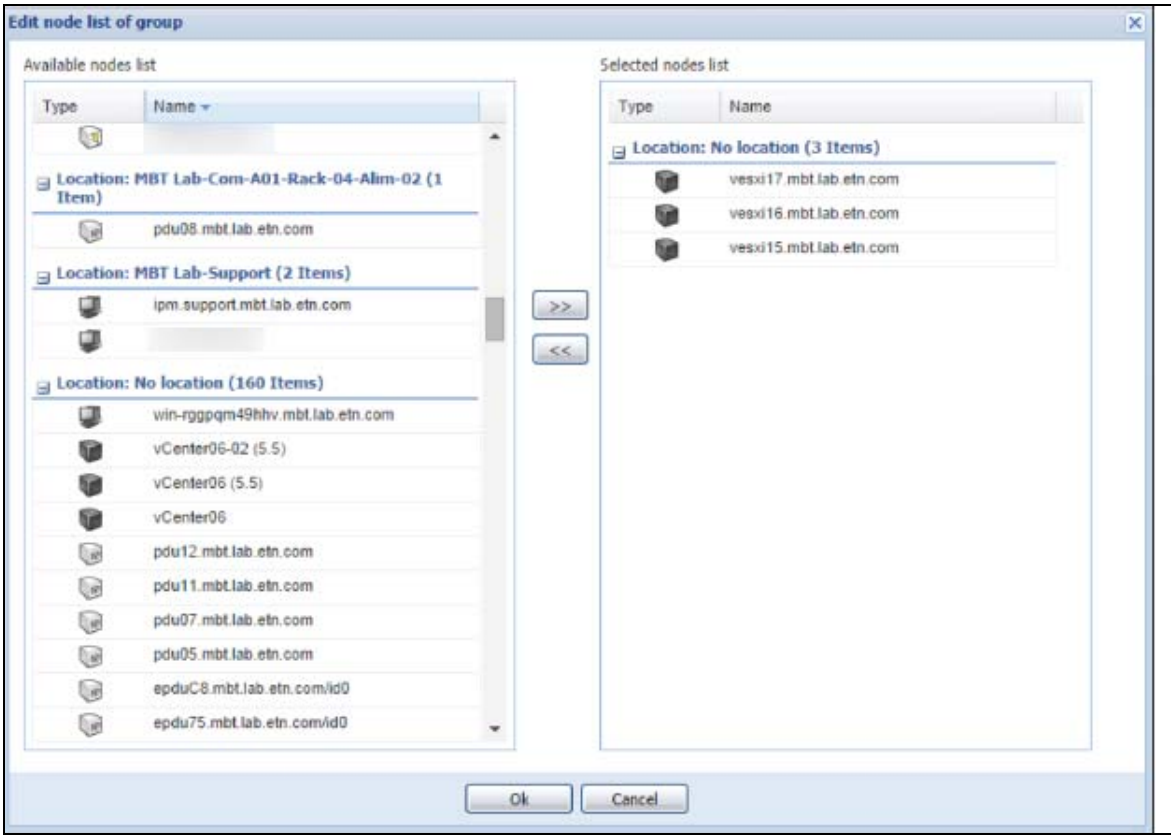

Figure 236. Edit Node List of Configuration Policy

7. Then, in the "Configuration policy settings", configure the correct power source (see Figure 237).

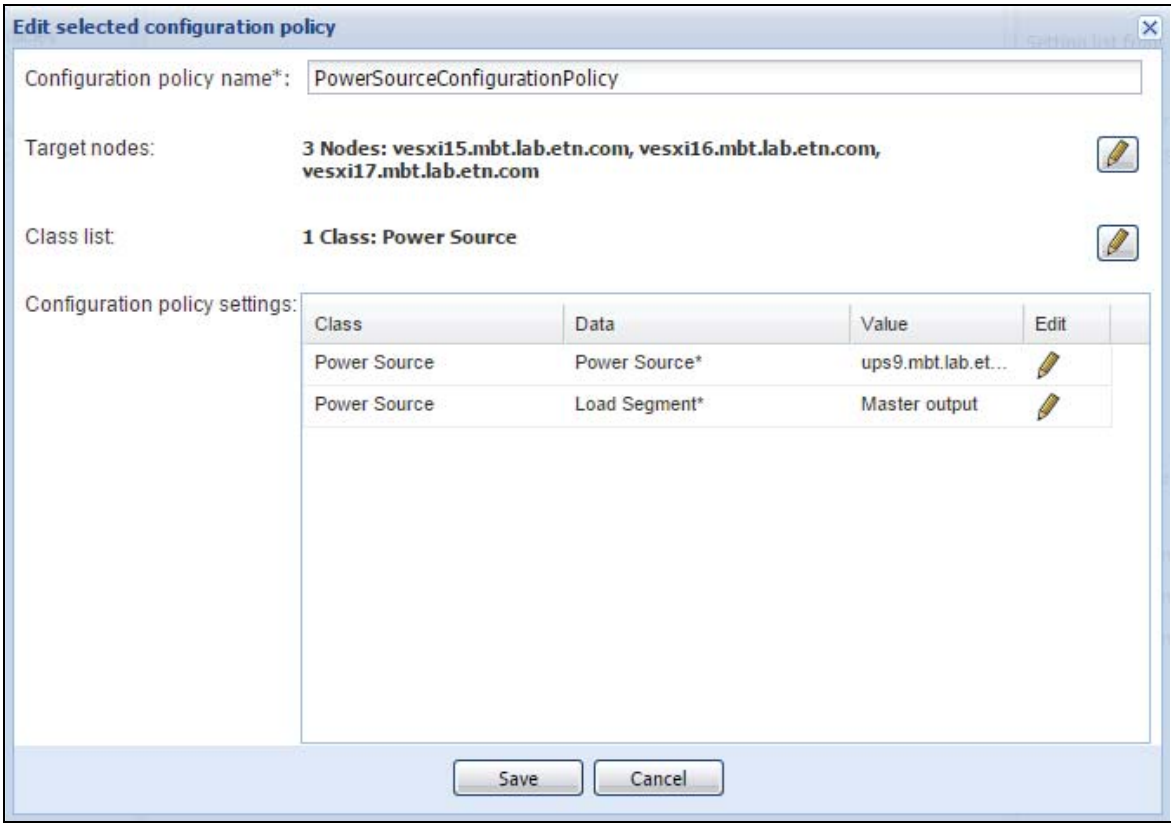

Figure 237. Edit Selected Configuration Policy

8. With this configuration, the three ESXi selected have the Power Source ups09.mbt.lab.etn.com.

Add a VMware vCenter Connector

Prerequisites

None

Example Procedure

1. Select ***Settings > System***.
2. In the right panel, select Edit modules settings and enable Infrastructure Connectors.
3. Select ***Settings > Infrastructure Connectors***.
4. In the right panel, select Add a connector. In the Add a connector dialog, select product type VMware vCenter (see Figure 238).

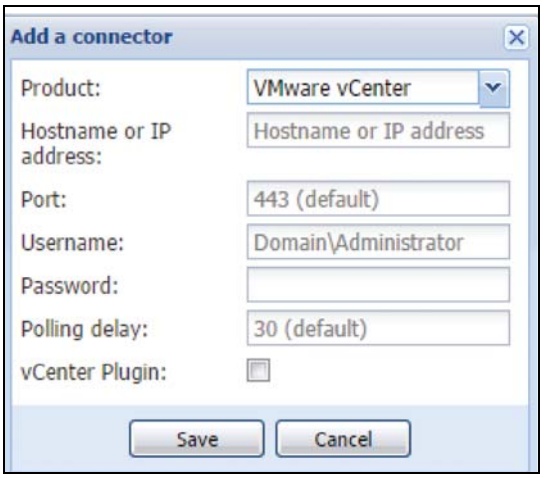

Figure 238. Add a Connector

5. Check that the connection is listed in the Infrastructure Connectors panel (see Figure 239).

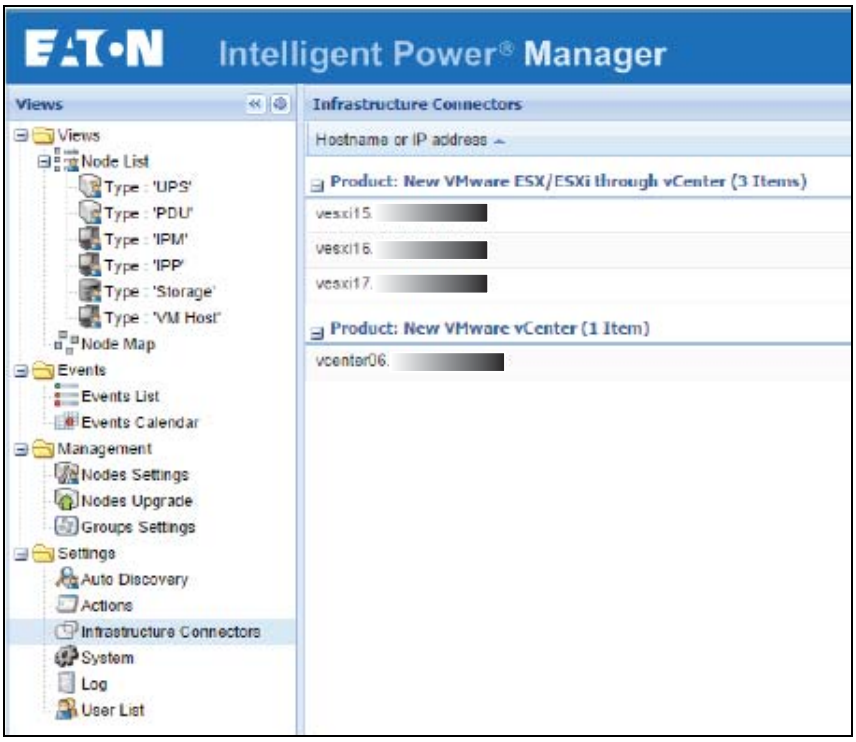

Figure 239. Infrastructure Connectors

Create a Filter

Prerequisites

None

Example Procedure

You can create a subview from Type to filter the VMHost, VMs, and vApps.

1. Select ***Views > Node List*** or click the configuration icon.
2. Right-click and select Create a sub view from (see Figure 240).
3. From the Criteria drop-down list on this dialog, select Type.

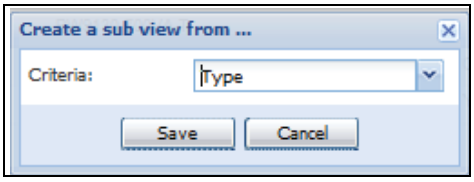

Figure 240. Select Type

4. You should see several new filters, depending on the nodes you have.

VMware & VMHost Shutdown

The following procedure describes how to make configuration policies and configure the IPM to shut down VMware ESXi after a UPS power failure.

Prerequisites

- Know VMware vCenter and VMware ESXi
- Know how to Add a VMware vCenter Connector
- Know how to Create a filter (Optional)

Example Procedure

1. Select ***Management > Configuration Policies***.
2. Create a new configuration policy with the Class Power Sources Identification in the configuration policy name field and class shutdown settings (see Figure 241).

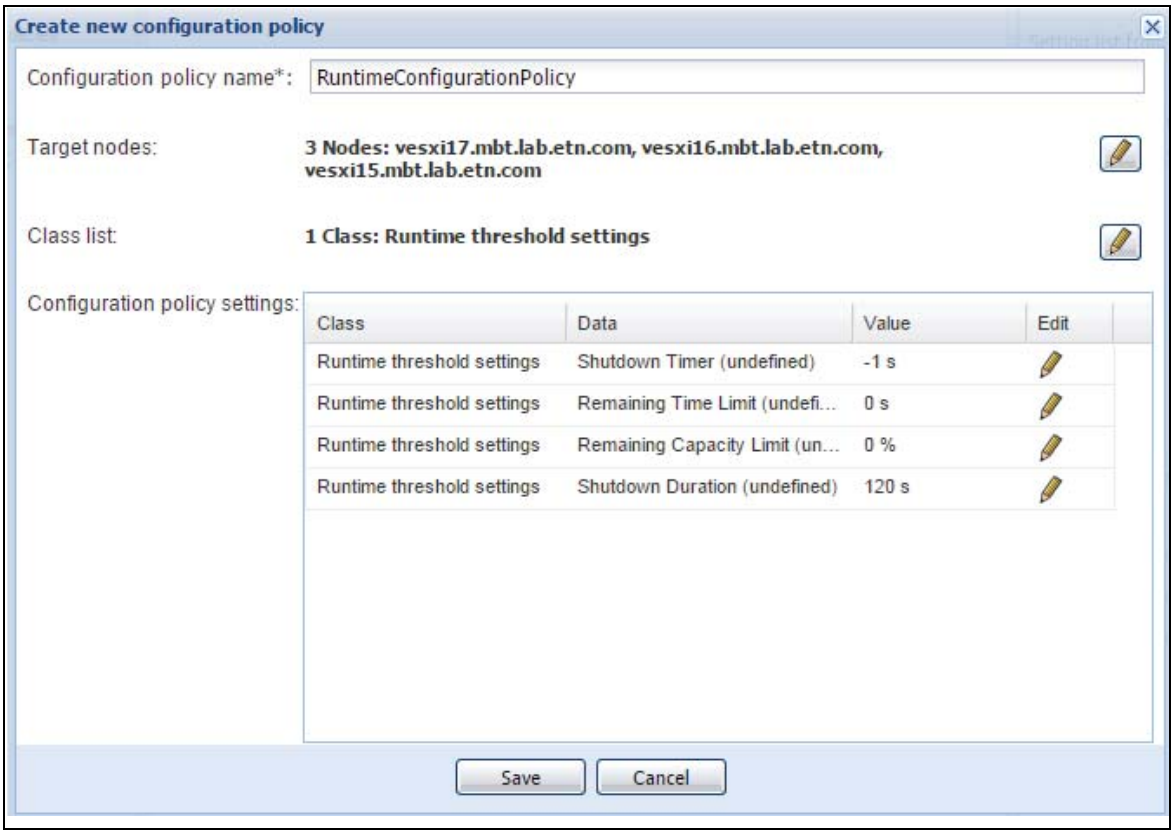

Figure 241. Create New Configuration Policy

3. Select ***Settings > Actions / Events***.
4. From the right panel, select Create new action with settings (see Figure 242).

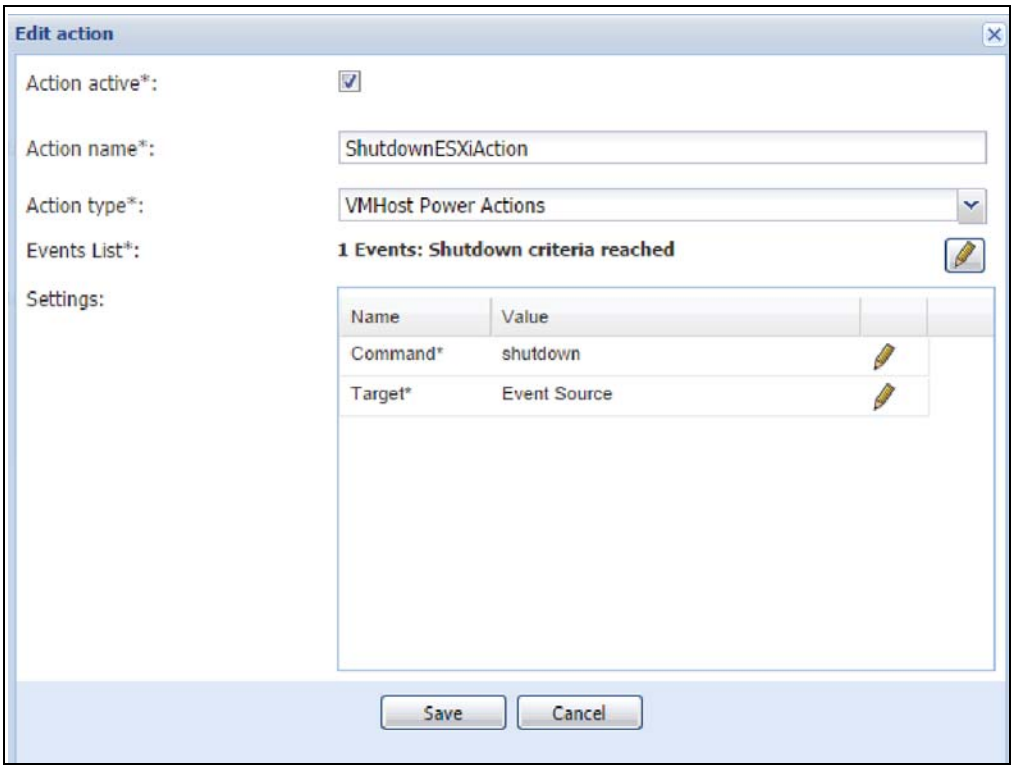

Figure 242. Create Shutdown ESXiAction

5. After the runtime threshold is reached, the action will be launched on each VMHost (shutdown in this case).

VMware & Maintenance Mode

The following procedure describes how to put a VMware ESXi in Maintenance mode as the result of a specific event.

Prerequisites

- Know how to install and connect on IPM web interface
- Know VMware vCenter and VMware ESXi
- Know how to Add a VMware vCenter Connector
- Know how to Create a filter (Optional)

Example Procedure

1. Select ***Settings > Actions / Events***.
2. In the right panel, select Edit event rules.
3. Add a custom event (see Figure 243 and Figure 244).

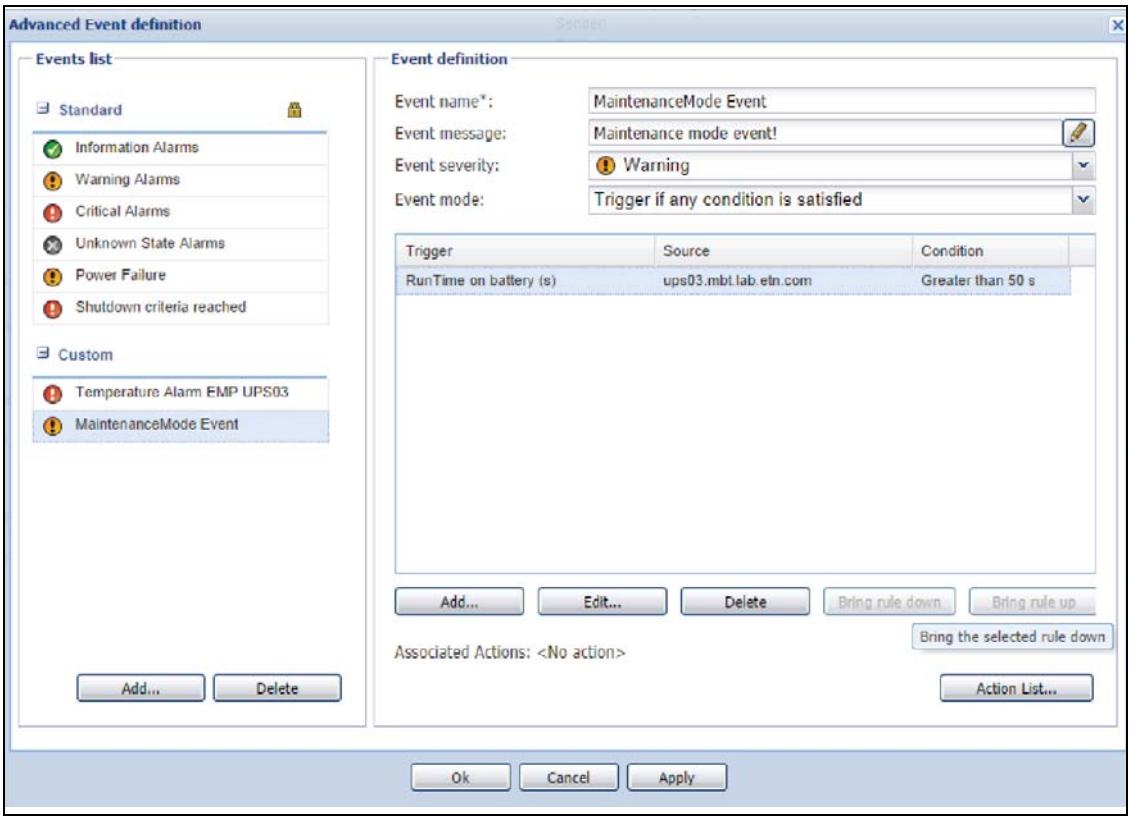

Figure 243. Advanced Event Definition

NOTE Before version IPM 1.50, a maintenance timer was used to match this object.

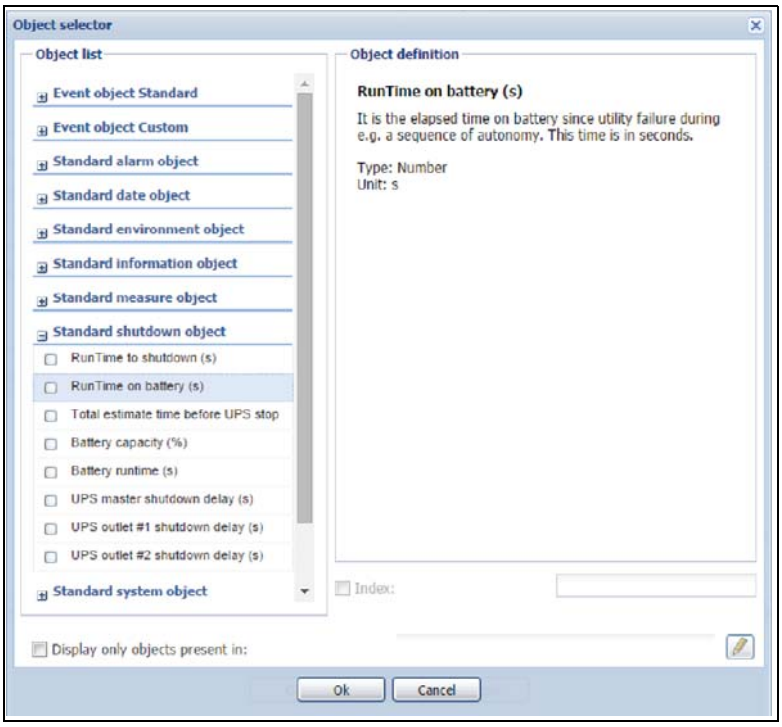

Figure 244. Object Runtime on Battery

4. On the Rule definition dialog, select the source and the value (see Figure 245).

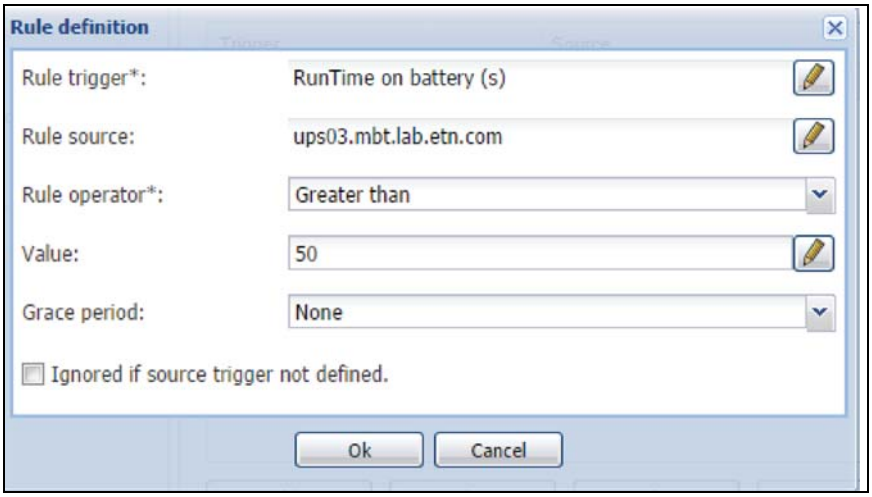

Figure 245. Rule Definition

5. Select ***Settings > Actions / Events***. In the right panel, click Create a new action.
6. From the Create new action dialog, select the Action type Host Power action. Click **Save** (see Figure 246).

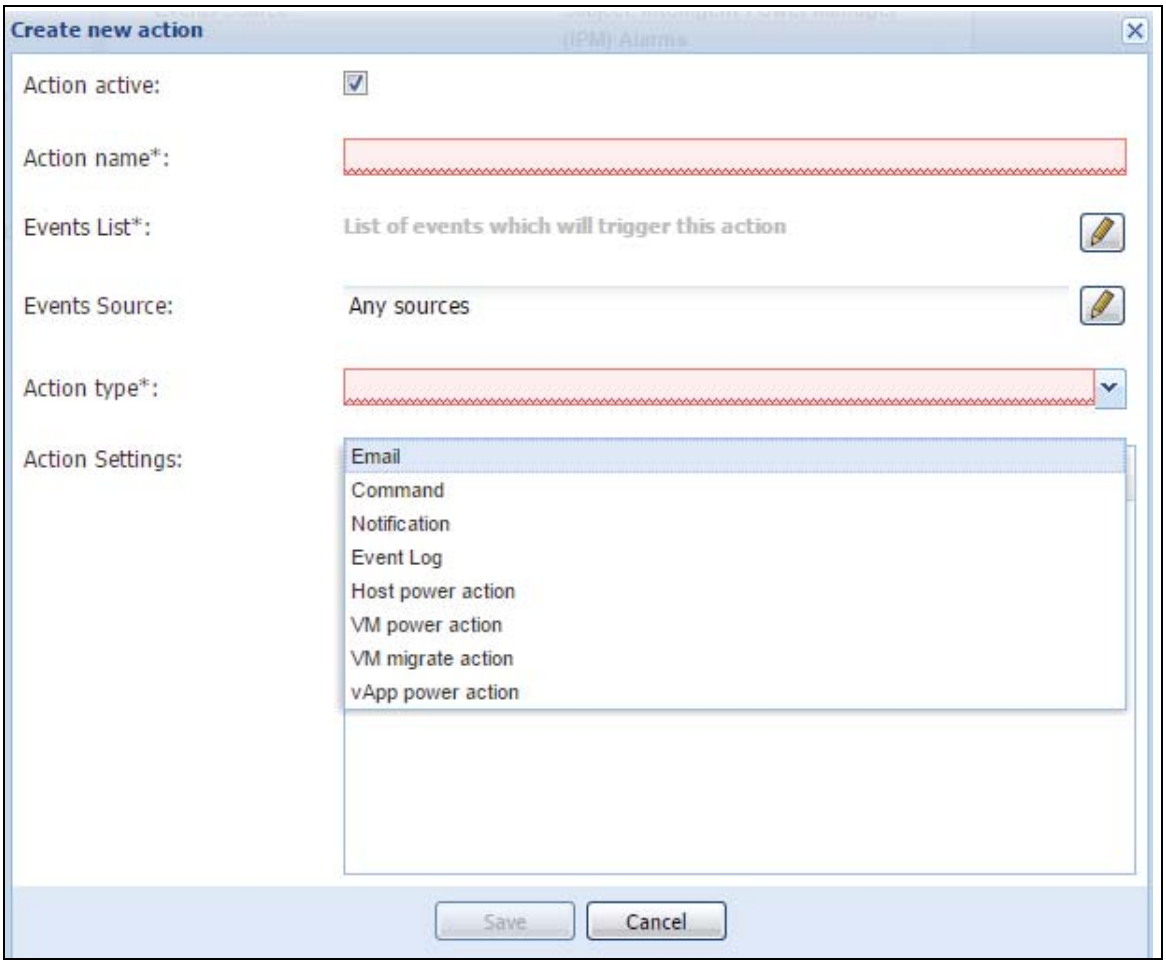

Figure 246. Create New Action

7. From the Create new action dialog, select the Events List (see Figure 246).

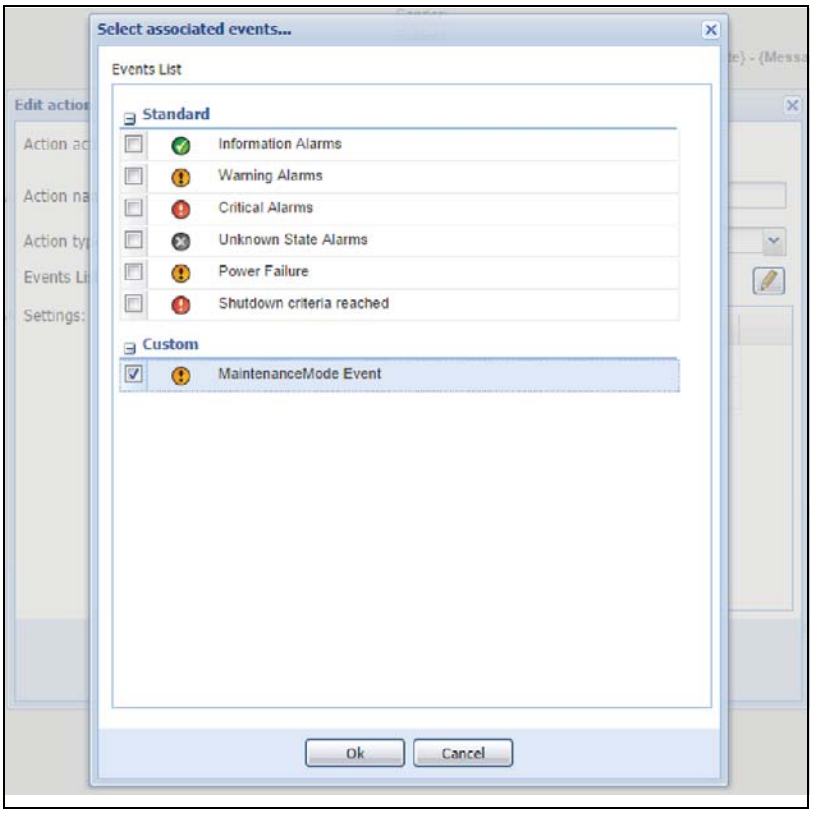

Figure 247. Events List for Select Associated Even

8. From the Select associated events pop-up, check the Custom box for MaintenanceMode Event. Click **Ok** (see Figure 247).
9. From the Edit Action screen, select the command, "EnterMaintenanceMode" (see Figure 248).

10. From the Edit Action dialog, select the Target.
11. Click **Save**.

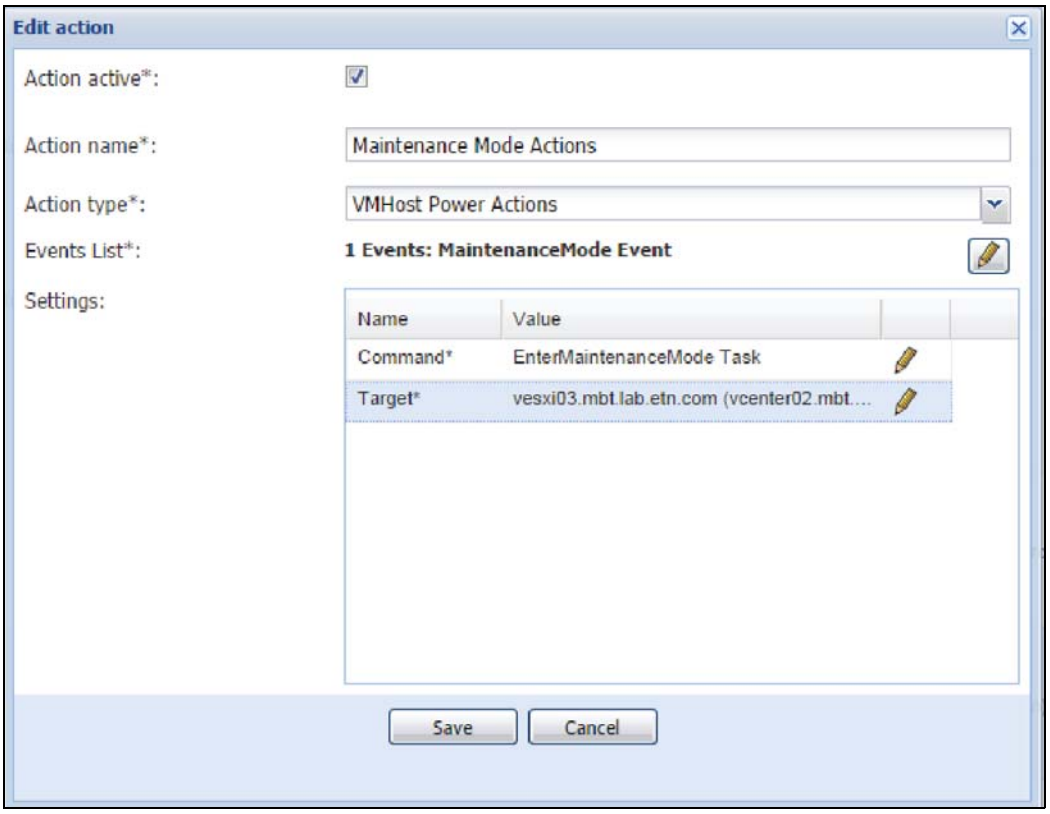

Figure 248. Select Target on Edit Action

12. If you want to have this action launch on several servers, you can create a configuration policy with them and launch the command on the configuration policy.

VMware & VM Migrate on EMP

The following procedure describes how to migrate virtual machines from an environment event.

Prerequisites

- Know VMware vCenter and VMware ESXi
- Know how to Add a VMware vCenter Connector
- Know how to Create event from EMP Temperature
- Know how to Create a filter (Optional)

Example Procedure

1. Select ***Settings > Action / Events***.
2. Create a new action with action type, "VM migrate action."
3. Select the Temperature Event created previously. Click **Ok** (see Figure 249).

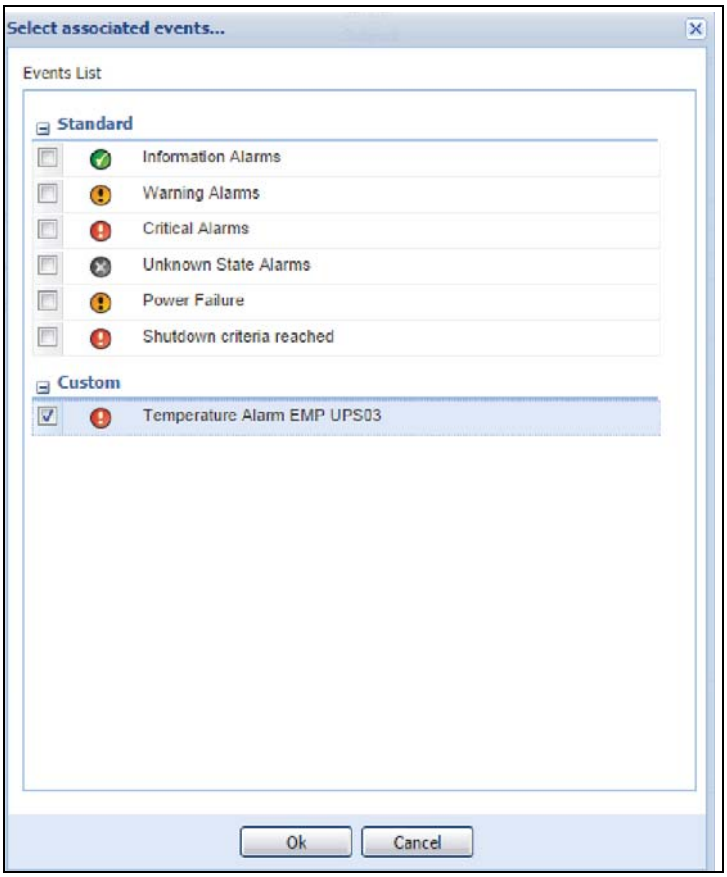

Figure 249. Select Temperature Event

4. From the Edit action dialog, configure the settings (see Figure 250).
5. Select the VMs to migrate (VMs or configuration policy containing VMs).
6. Select the target Host.

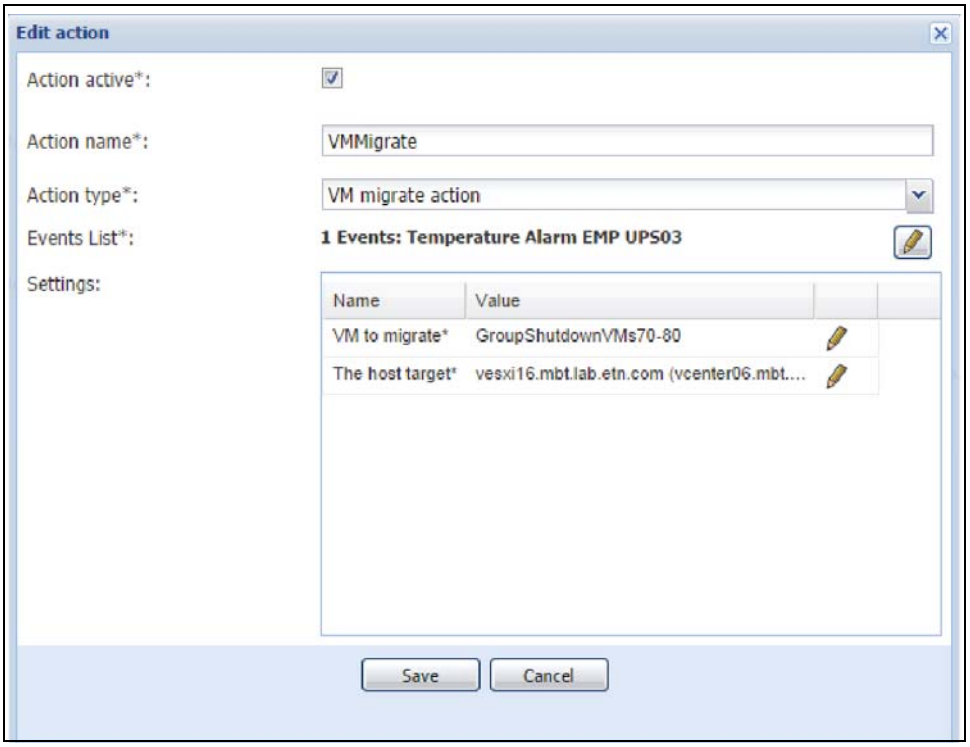

Figure 250. Select Target Host on Edit Action

7. Click **Save** and the configuration is completed.

Create Event from EMP Temperature

Prerequisites

None

Example Procedure

1. Select ***Settings > Action / Events***.
2. Click Edit event rules in the right panel.
3. Add a custom event (see Figure 251).

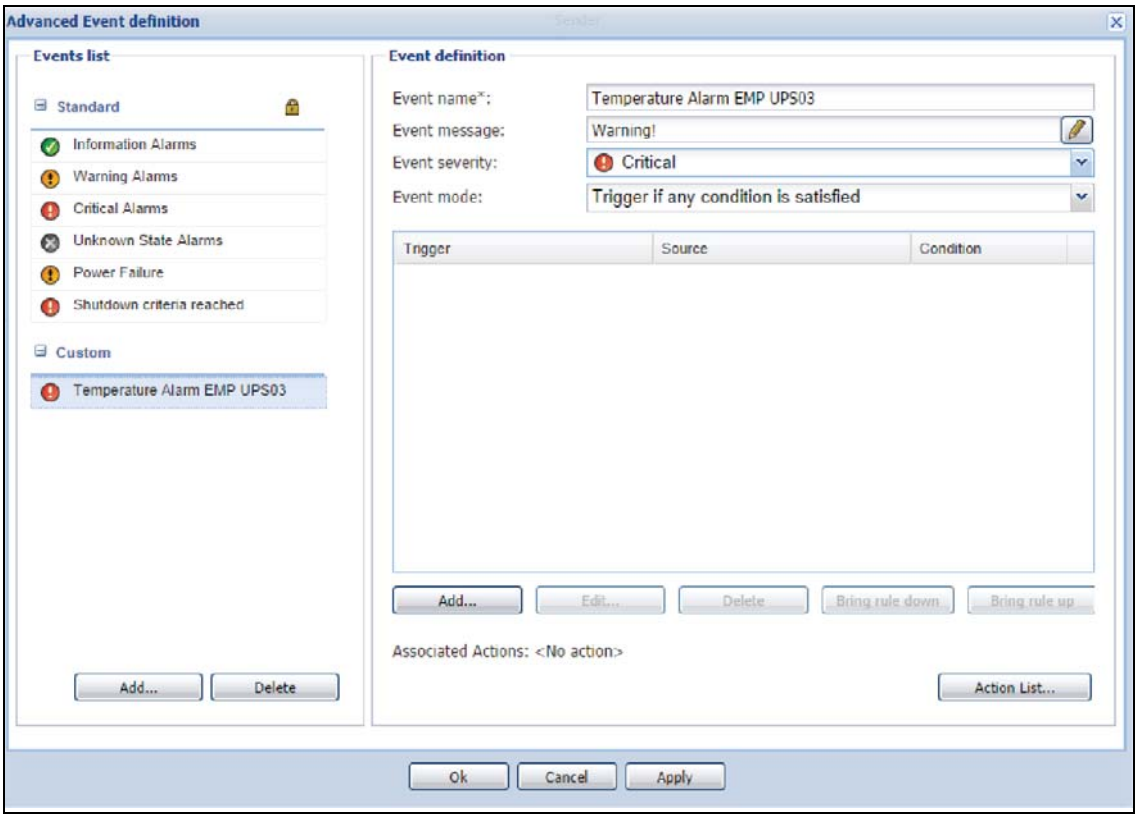

Figure 251. Advanced Event Definition

4. Add a Trigger.
5. Select the Rule trigger on the environment Object "Temperature."
6. Select the Source if you want to check only one EMP.

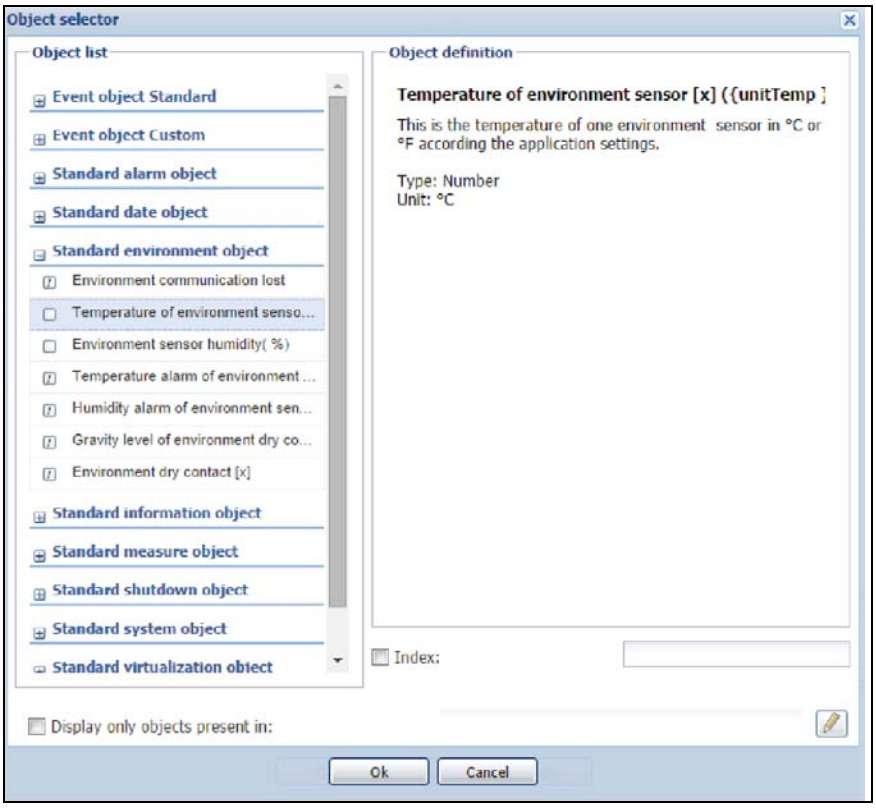

Figure 252. Object Selector

7. Select the value and click **Ok** (see Figure 252 and Figure 253).

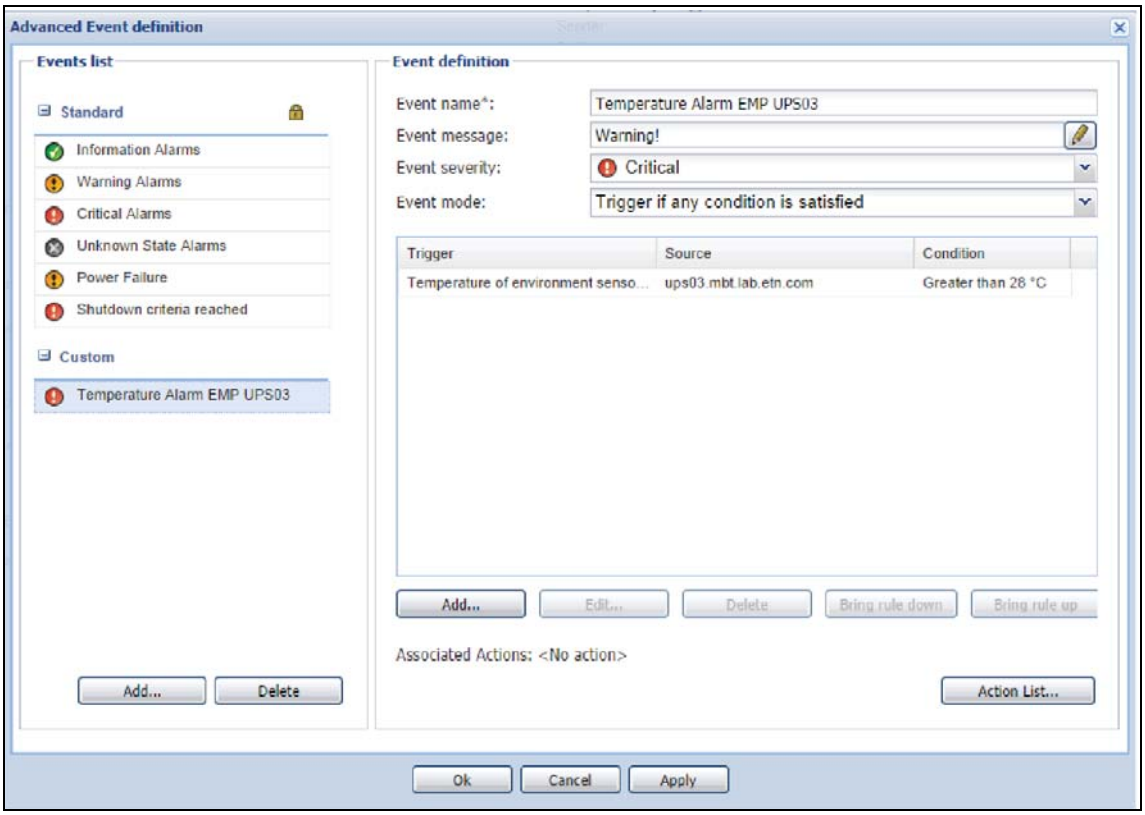

Figure 253. Advanced Event Definition

Site Recovery Manager (SRM) with IPM

VMware Documentation and Packages

- SRM documentation (Installation, Configuration)
- VMware SRM 6.5 to 6.7

SRM Packages

- SRM 6.5
- SRM 6.7

Prerequisites

- Java installed
- Knowledge of IPM Infrastructure Connectors
- Knowledge of VMware vCenter and VMware SRM
- Requires a Silver or Gold license to activate the IPM SRM module

Example Procedure

1. Select ***Settings > System***.
2. Click Edit Modules Settings in the right panel.
3. From the Edit modules settings pop-up, check the box for Site Recovery Management and click **Save** (see Figure 254).

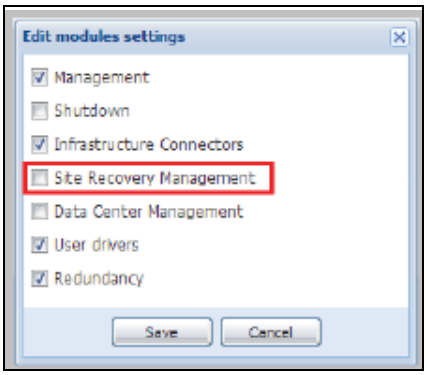

Figure 254. Edit Modules Settings

NOTE The Site Recovery Management selection is disabled with a Basic license.

4. You should now see a new column for SRM state in the Infrastructure Connectors panel (see Figure 255).

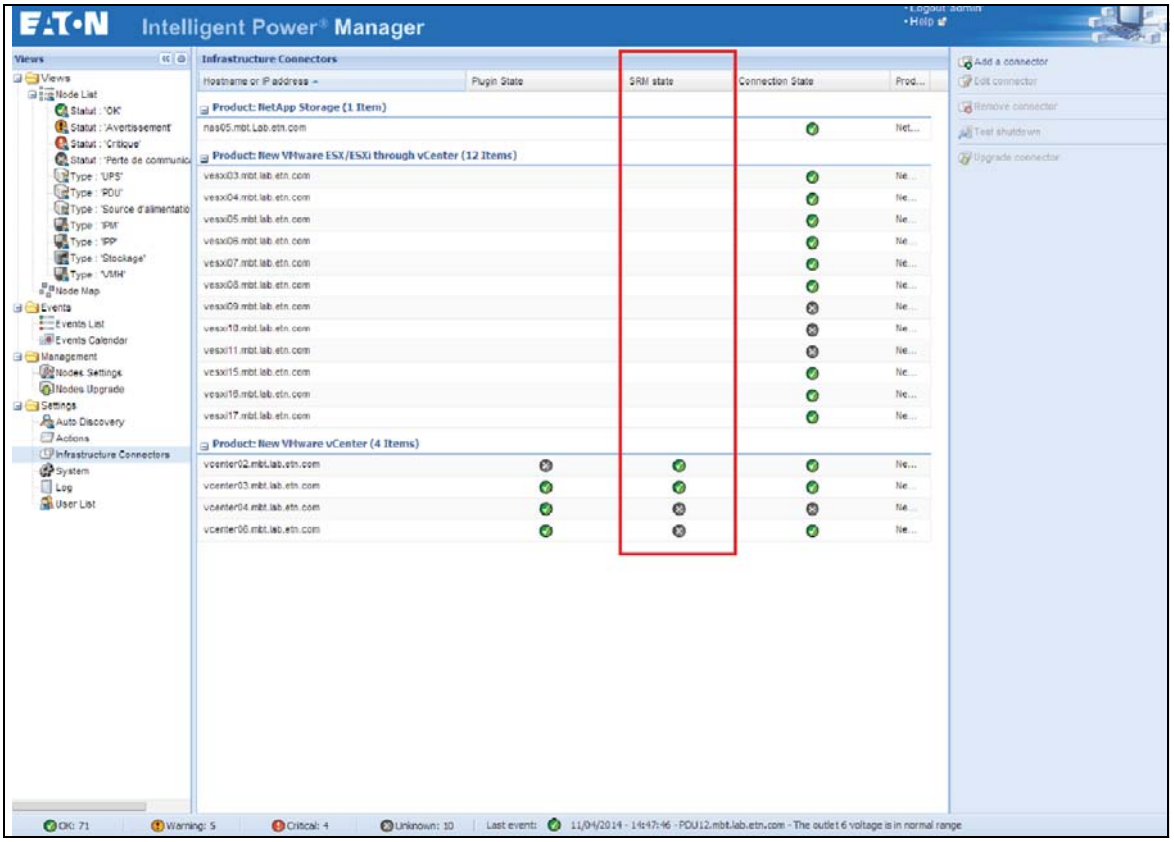

Figure 255. Infrastructure Connectors

NOTE IPM automatically discovers the IP address of the SRM server through the ExtensionManager and connects to it using the vCenter credentials.

Configure SRM Actions

Once you have this working, you can go to the action panel and add a new SRM action:

1. Select ***Settings > Action / Events***.
2. Click Create new action in the right panel.

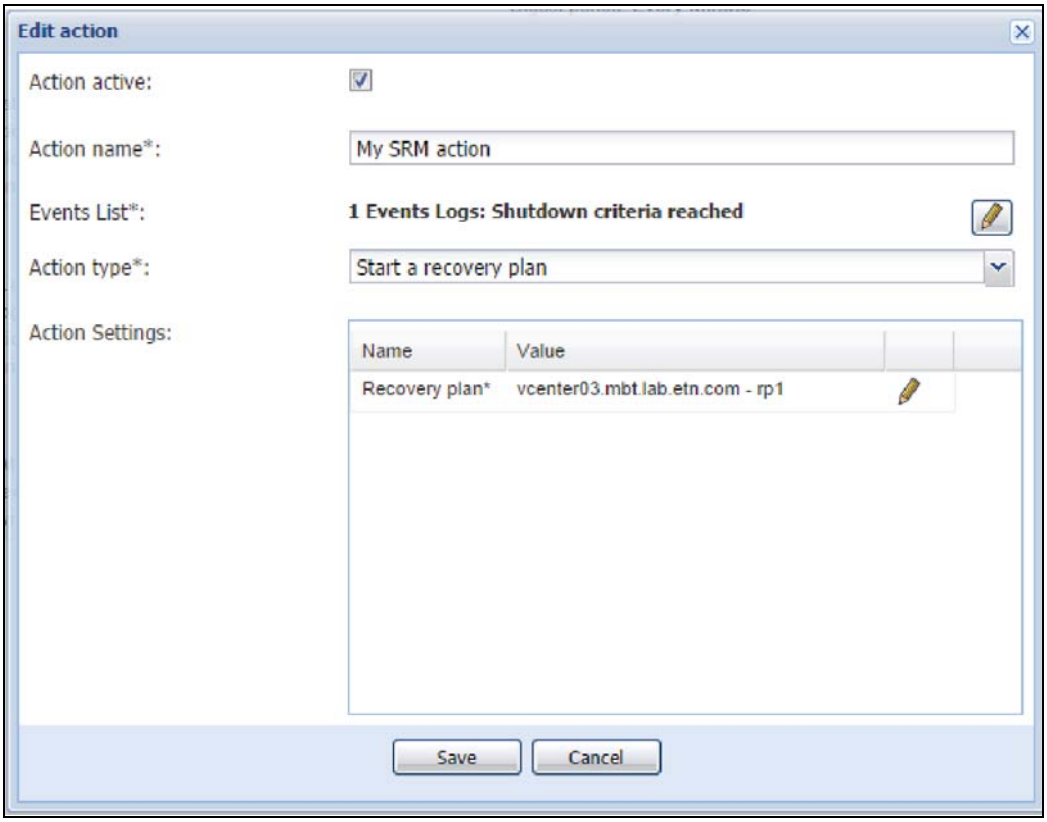

Figure 256. Edit Action

3. From the Edit action dialog, complete the fields for your SRM action (see Figure 256).
   - **Action name**: the action name (String field)
   - **Events List**: the events that will trigger the SRM Recovery Plan, in the above example, a "Runtime Threshold reached" event is selected.
   - **Action Settings**: the action specific parameters
     - **Recovery plan**: the recovery plan that will be launched (Failover Mode)

NOTE All fields followed by an asterisk "*" are mandatory. See the "Advanced Events and Actionswith" on page 31 for more informations.

4. After you are satisfied with your settings, you can save the configuration (see Figure 257).

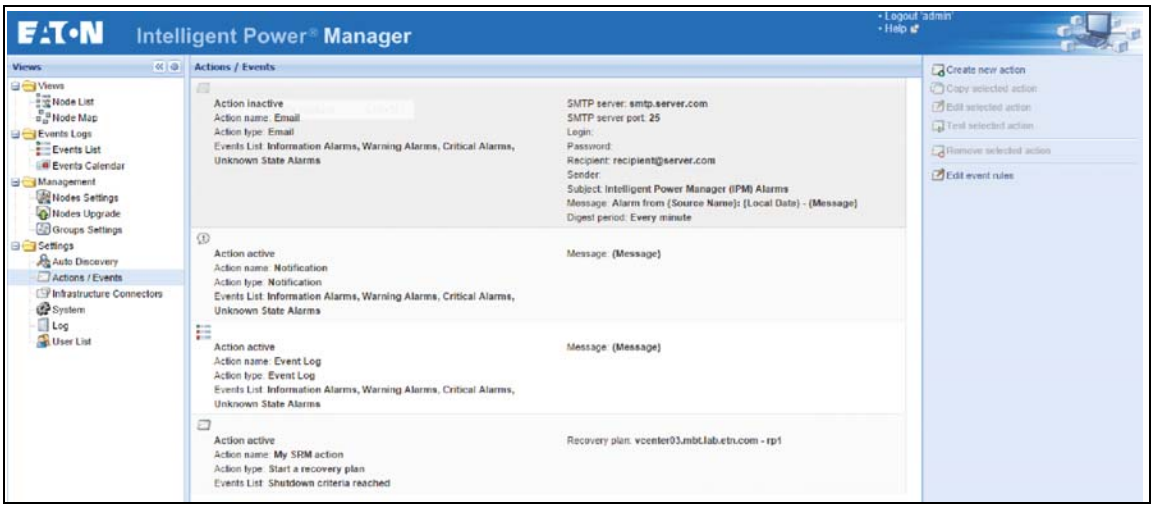

Figure 257. Actions / Events Panel

Monitoring Events and SRM Actions

After the expected event executes and the corresponding recovery plan is started, you can view event details by selecting ***Settings > Log*** (see Figure 258).

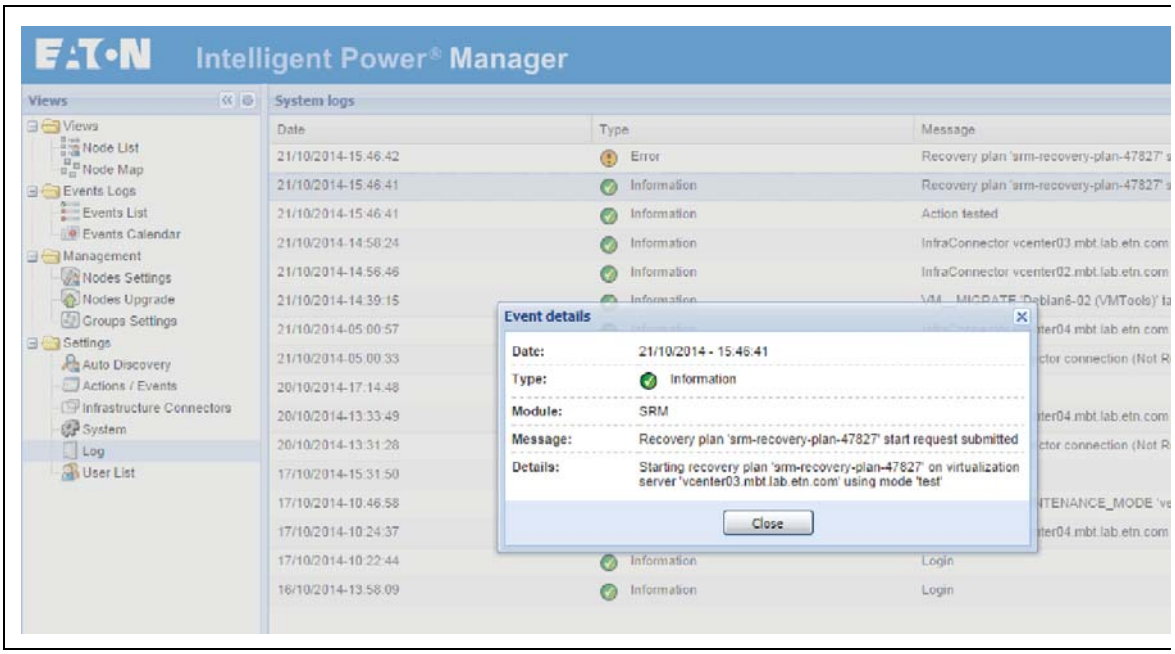

Figure 258. System Logs

VMware & VM Load Shedding

The following procedure describes how to shutdown VMs after a UPS power failure in a specific order of configuration policies.

Prerequisites

- Know VMware vCenter and VMware ESXi
- Know how to Add a VMware vCenter Connector
- Know how to Create a filter (Optional)

Example Procedure

1. Select ***Management > Configuration Policies***.
2. Click Create a new configuration policy in the right panel.
3. From the Create new configuration policy dialog, create a new configuration policy with the Class, including Runtime Threshold Settings and Power Sources Identification (see Figure 259).
4. Select the Node to add in this configuration policy.
5. Configure the configuration policy settings with remaining capacity limit on 70%.
6. Click **Save**.

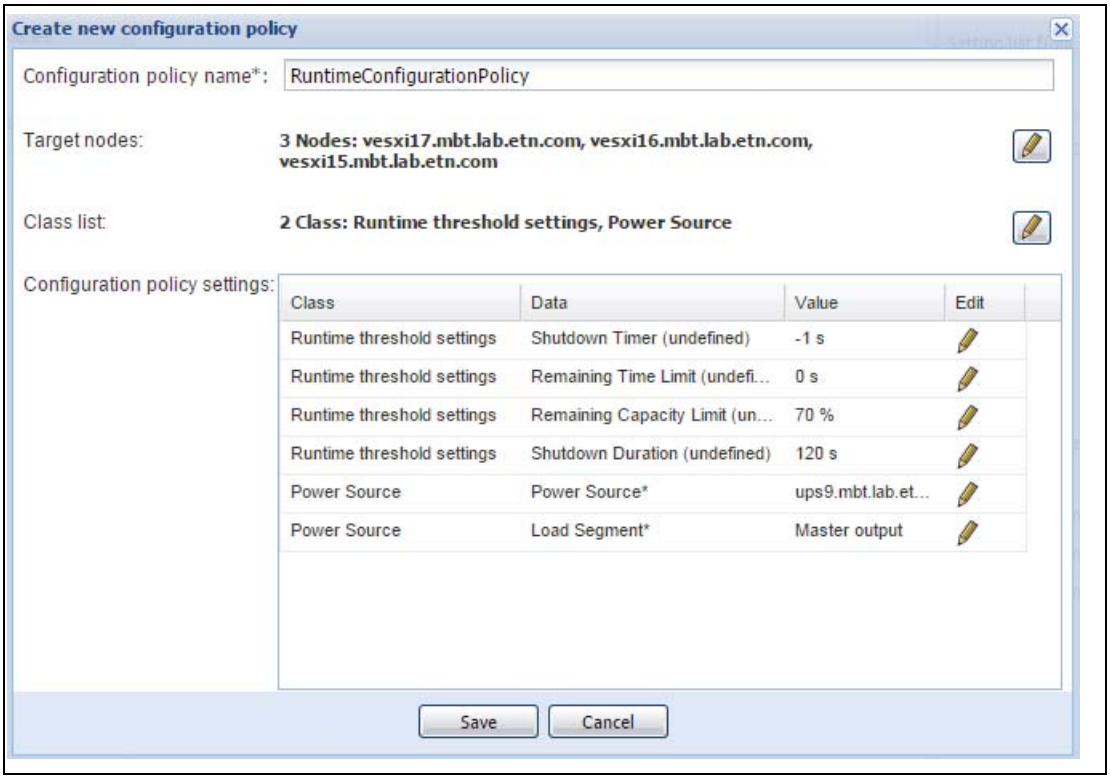

Figure 259. Create New Configuration Policy

7. Copy the configuration policy and modify the Nodes List and the configuration policy settings to match your environment constraints (see Figure 260).

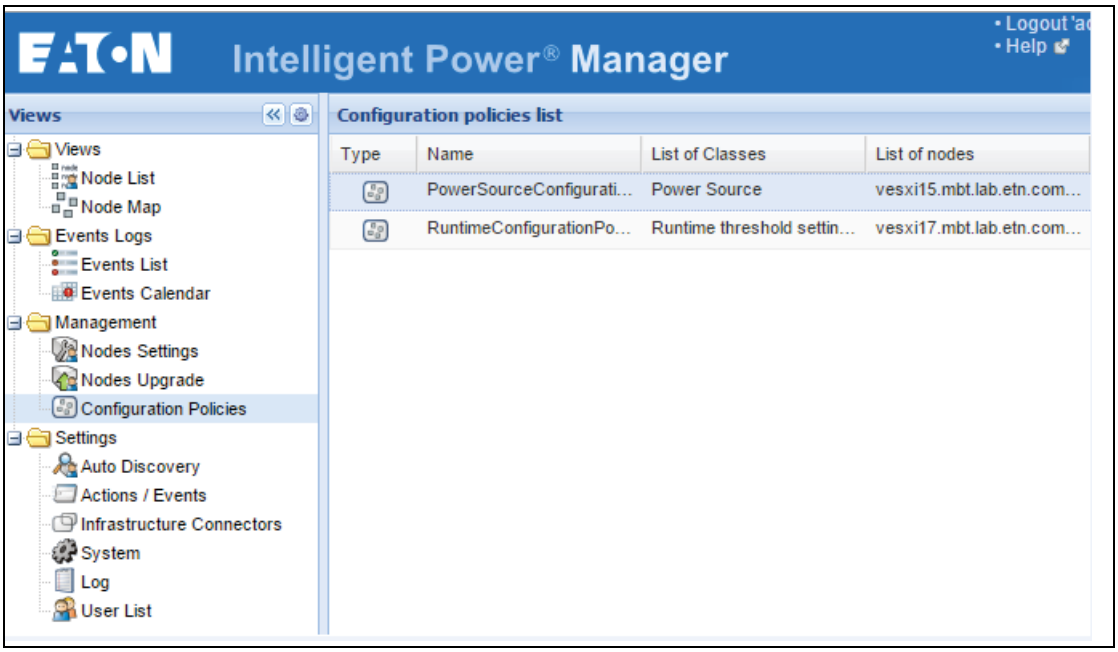

Figure 260. Configuration Policies List

8. Select ***Settings > Actions / Events.***
9. Click Create a new action in the right panel (see Figure 261).
10. Select Action type: Power Action
11. Choose the event on which the action will be triggered, which is "Runtime Threshold reached" in this example.
12. Configure the following settings:
    - **Action setting:** Shutdown
    - **Target selector:** Select Event Source

Figure 261. Actions

Result after a Power Issue

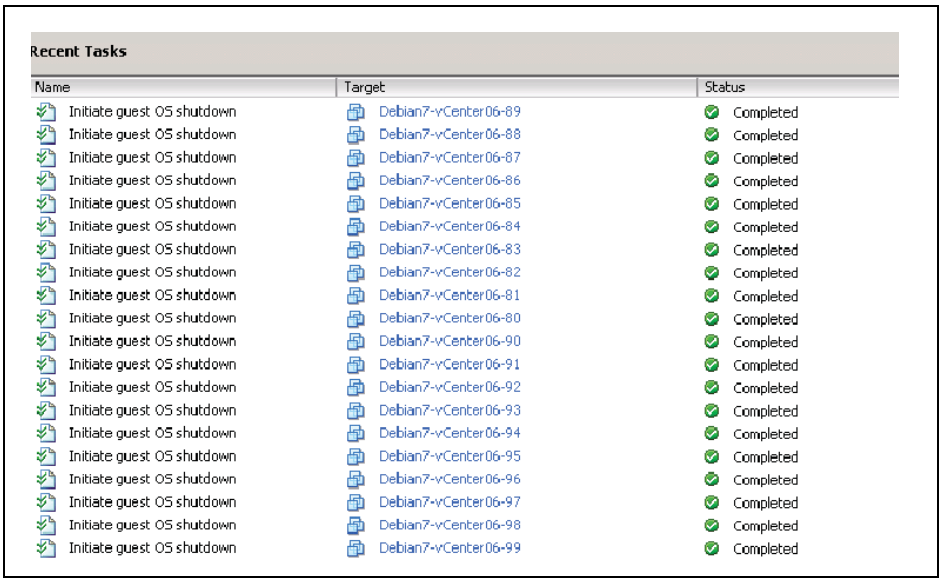

Figure 262. Recent Tasks

Site Recovery Manager (SRM) with EMP

The following procedure describes how to launch a VMware Site Recovery Plan from an environment event.

Prerequisite

- Know how to install IPM
- Know how to configure VMware Site Recovery Manager
- Know how to Create event from EMP Temperature

Example Procedure

1. Select ***Settings > System***.
2. Click Edit modules settings in the right panel and enable Infrastructure Connectors and Site Recovery Manager.
3. Click **Save**.
4. Select ***Settings > Infrastructure Connectors*** (see Figure 263).
5. In the right panel, click Add a connector. Select product type VMware vCenter
6. After it is created, make sure the SRM state column is in the Infrastructure Connector panel.

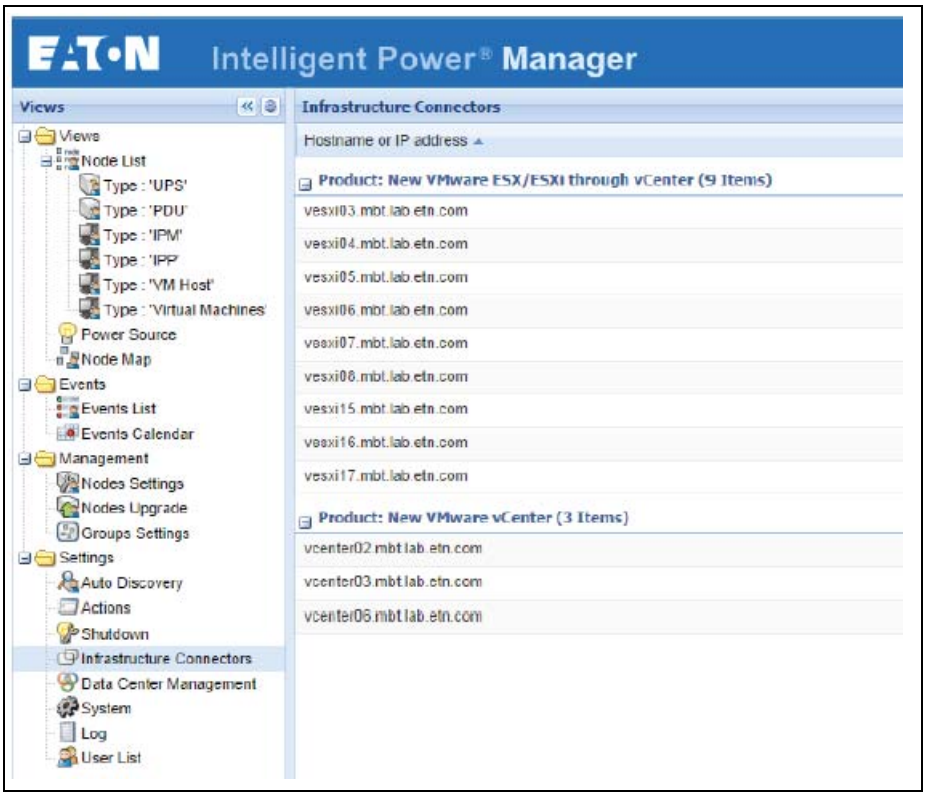

Figure 263. Infrastructure Connectors

7. Select ***Settings > Actions / Events***.
8. In the right panel, select Create a new action with SRM action. The Edit action dialog displays (see Figure 264).
9. From the Edit action dialog, select the Events list.

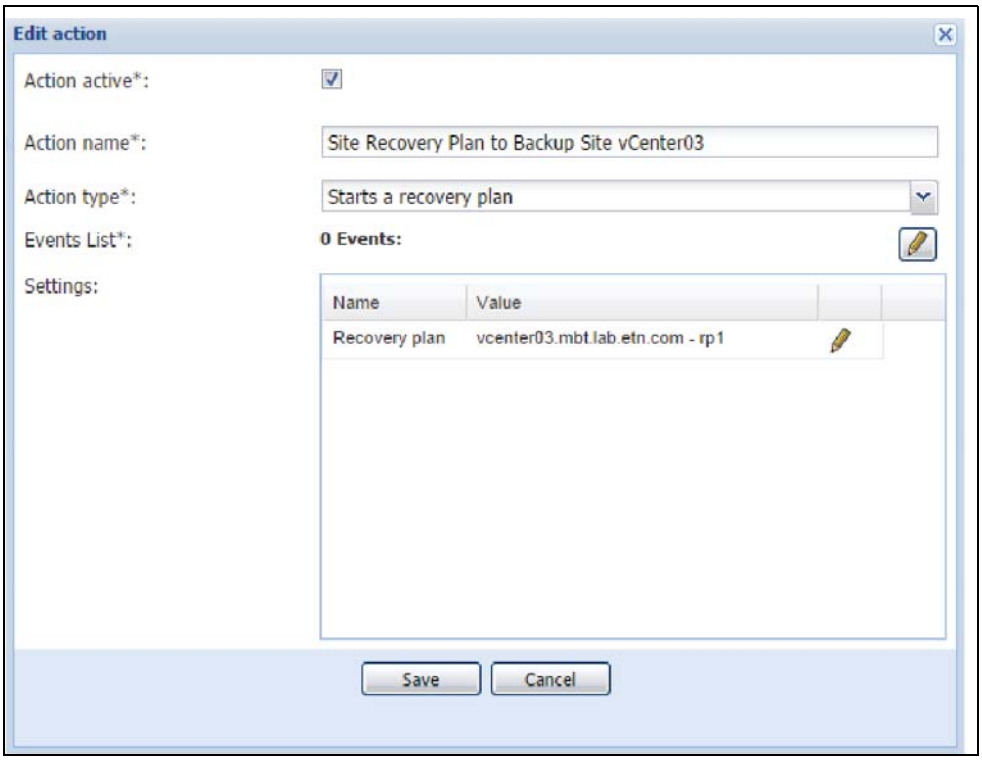

Figure 264. Edit Action

10. Select the event you configured previously (see Figure 265).

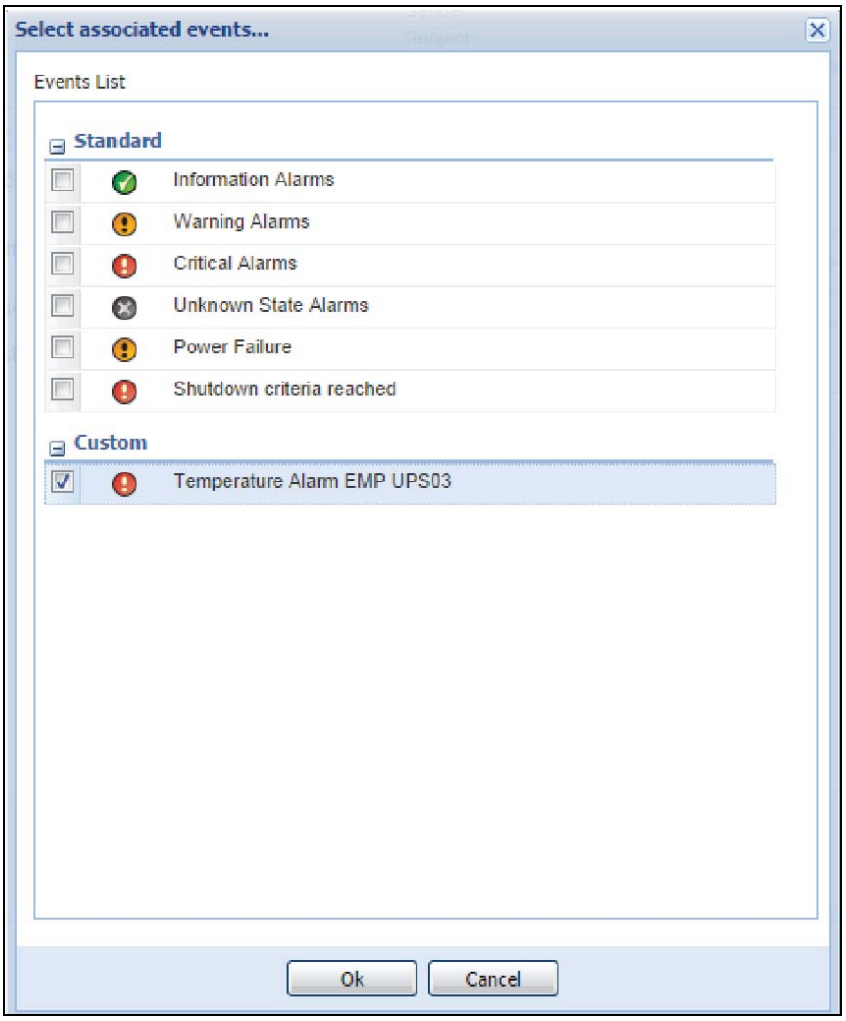

Figure 265. Select Associated Events

11. Click **Ok** to complete the configuration.

Appendix A