Eaton® Intelligent Power® Manager (IPM)

User's Guide

Powering Business Worldwide

Class A EMC Statements

FCC Information

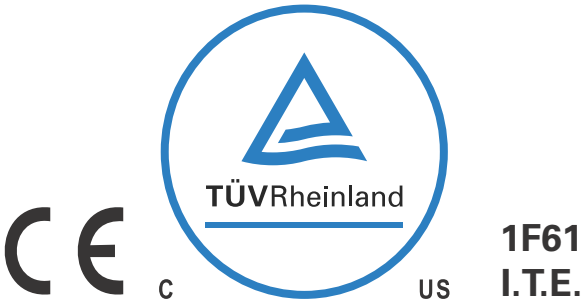
This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, 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.



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 Eaton Enclosure Power Distribution Unit (ePDU®), other manufacturer's 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:

- Discovers and supervises UPSs, PDUs, and ePDUs connected to the network either a card or a proxy. For the detailed list of compatible solutions, see "Compatibility" on page 2.
- Supervises the remote servers hosting the Eaton® Intelligent Power® Protectorr (IPP) or Network Shutdown Module V3 application.
- Provides advanced management feature (mass configuration and mass upload) with the Eaton® Network Management Cards (also called NMC): Network-MS (example, 66102/103006826) and Modbus-MS (example, 66103)
- Provides local computer graceful shutdown through Network or local connectivity, such as USB or RS-232 port
- Provides an agentless method for directly managing and controlling VMware® Hypervisors through the VMware® vCenter™ management platform
- Provides centralized management of Eaton IPP applications running on virtualized servers other than VMware vCenter (such as Microsoft® Hyper-V™ Hypervisor or Citrix® Xen®).

Figure 1 shows the Eaton IPM Node Map page.

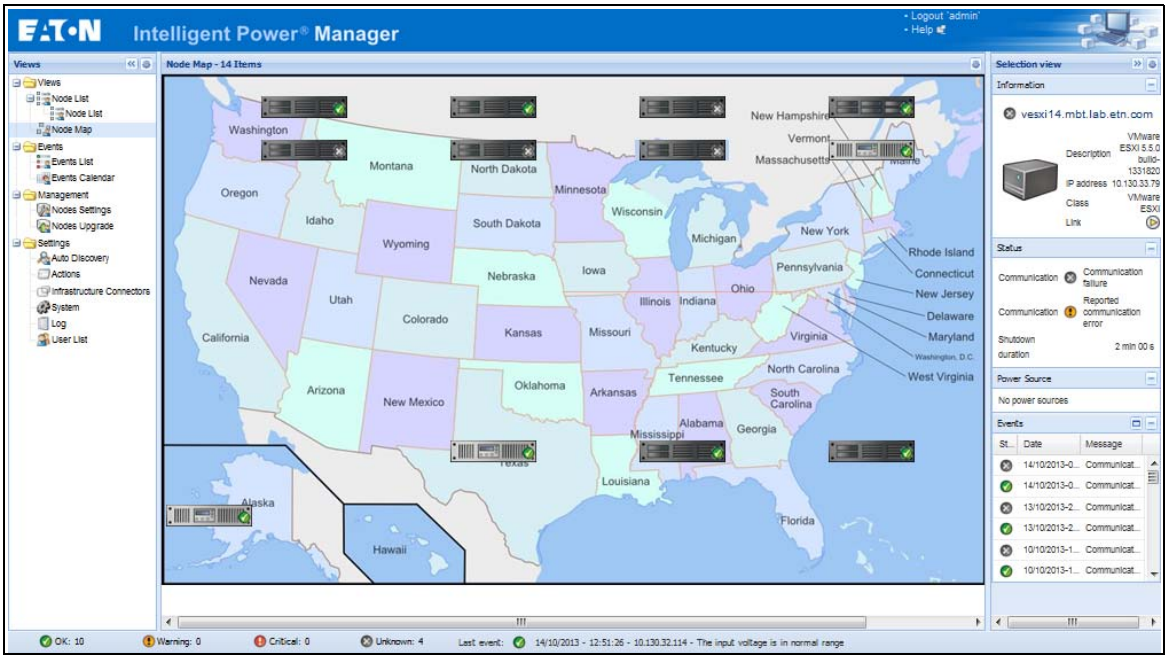


Figure 1. Eaton IPM Node Map Page

Compatibility

Eaton has tested the compatibility of the Eaton IPM with the following devices and applications.

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 Devices

Table 1. Eaton Devices

Eaton Equipment Designation	Type	Features	Protocols		
			XML	SNMPV1	SNMPV3
See NOTE Network Management Card Minislot SNMP / Web - Network-MS (ex 66102) and associated Environment Sensor	UPS Option Card Eaton Pulsar	Quick Scan Supervision Management Shutdown	•	•	•
See NOTE Network Management Card & Modbus / JBus -Modbus-MS (ex 66103) (through Ethernet Network) and associated Environment Sensor 66846	UPS Option Card Eaton Pulsar	Quick Scan Supervision Management Shutdown	•	•	•
NOTE SNMP is available for these devices, but IPM does not use it. IPM uses only XML protocol for this equipment.					
ConnectUPS- Minislot Network Management Card / Network-MS (ex 103006826)	UPS Option Card Eaton Powerware	Quick Scan Supervision Management Shutdown	—	•	•
ConnectUPS-BD Web /SNMP	UPS Option Card Eaton Powerware	Quick Scan Supervision Shutdown (**)	—	•	•
ConnectUPS-XSlot Web /SNMP/xHubCard (*)	UPS Option Card Eaton Powerware	Quick Scan Supervision Shutdown (**)	—	•	•
PXGX2000 (*)	UPS Option Card Eaton Powerware	Quick Scan Supervision Shutdown (**)	—	•	•
PXGX-UPS Card	UPS Option Card Eaton Powerware	Quick Scan Supervision Shutdown	—	•	•
Eaton Advanced ePDU® (Europe = Switched (SW), Advanced Monitored (AM) and Managed (MA) / US= Advanced Monitored (AM) and Managed (MA))	ePDU Integrated Communication Card	Quick Scan (v 1.20) Supervision (v. 1.20) Management (v. 1.25)	•	—	—
Eaton ePDU Monitored & Advanced Monitored	PDU Integrated Communication Card	Supervision	•	—	—
Eaton ePDU Managed	PDU Integrated Communication Card	Supervision	•	—	—
Eaton ePDU Switched	PDU Integrated Communication Card	Supervision	•	—	—
MGE Switched PDU NM - 68130 / 68134/56132/ 56134/56136/56138 MGE AmpMeter PDU NM - 68152/ 56134/56144	PDU Integrated Communication Card	Supervision	—	•	•

Table 1. Eaton Devices (Continued)

Eaton Equipment Designation	Type	Features	Protocols		
			XML	SNMPV1	SNMPV3
Computers (Windows - Linux) hosting the IPP Shutdown Controller	UPS Proxy (Shutdown Controller)	Quick Scan Supervision Management Shutdown	•	—	—
MGE Network Management Proxy (Windows) XML-Agent	UPS Proxy (legacy)	Supervision	•	—	—
Computers (Windows) hosting the application LanSafe Web View	UPS Proxy (legacy)	Supervision	•	—	—
MGE Network Management Card Minislot SNMP/ Web - 66244 and associated Environment Sensor	UPS Option Card (legacy)	Supervision	•	—	—
Network Management Card Transverse SNMP/ Web - 66074 and associated Environment Sensor	UPS Option Card (legacy)	Supervision	•	—	—
Aphel 1	ePDU Integrated Communication Card	Supervision	—	•	•
Aphel 2	ePDU Integrated Communication Card	Supervision	—	•	—

Serial Line Devices

The Eaton IPM is compatible with the following serial line devices (see Table 2).

Table 2. Serial Line Devices

Eaton Equipment Designation	Connectivity
Eaton 3105, 5110, 5115, 5130, 9130, 9135, 9140 and legacy 9120, 9125	USB or RS-232
Eaton BladeUPS, 5125, 9155, 9355, 9390, 9395	RS-232 only
Eaton Pulsar Series: Evolution 650 / 850 / 1150 / S 1250 / 1550 / S 1750 / 2000 / S 2500 / S 3000 Pulsar 700 / 1000 / 1500 / 1000 RT2U / 1500 RT2U (Intl. & US Models) Pulsar M / EX Eaton 5P, 5PX Pulsar MX & Pulsar MX Frame 16 U / MX Eaton 9PX	USB or RS-232
Eaton Pulsar Series: EX RT Comet EX RT 1:1 / 3:1 / EX 5 RT (Asia/Pacific)	RS-232 only

NOTE Ellipse ASR 600/750/1000/1500 USBS, Ellipse MAX, Protection Station, Protection Center, and NOVA AVR are currently supported by Personal Solution Pac software.

Other Network Devices

The Eaton IPM is compatible with the following other network device (see Table 3).

Table 3. Other Devices

Eaton Equipment Designation	Card Proxy	Features
HP UPS Network Module Minislot (AF465A)	Network Card	Quick Scan Supervision
Dell Network UPS Card (H910P)	Network Card	Quick Scan Supervision
IBM UPS Network Management Card (46M4110)	Network Card	Quick Scan Supervision
All IETF MIB enabled UPSs (RFC1628), such as Liebert (Standard IETF UPS MIB 1.3.6.1.2.1.33.xx)	—	Supervision
PowerDsine series 6000	Card	—
Servertech sentry models	PDU Integrated Communication Card	—
Storage • NETAPP® (FAS2040 Series, i.e: FAS 2040) • HP (X1400 G2 Network Storage) • Synology® (RS812+) • NETGEAR® (ReadyNAS® 2100) • QNAPt® (TS-559) • BUFFALOt® (LinkStation™, TeraStation™)	Generic Driver	—
Network UPS Tools (NUT) enabled devices	Generic Driver	Quick Scan Supervision

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 Eaton IPP upgrade

Performance Evaluations

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

Test with Machine 1 (server Dell PowerEdge 2900)

- CPU: Intel® Xeon® 5130 dual-core @2GHz
- Memory: 2Go DDR2 @666MHz
- HDD: 2 HDDs 67GB 7200 rpm RAID 0 (Mirroring)
- OS: Microsoft® Windows Server® 2008 64 bits

Test conditions during 40 hours:

- 1300 nodes (including ~50 real), mainly Eaton IPMs, and Network Management Cards.
- Average CPU load: 20~30%
- Memory load: 200~300MB

Test with Machine 2 (typical PC)

- 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 4 lists the network ports used by the Eaton IPM.

Table 4. Network Ports

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

NOTE PXGX2000, PXGX-UPS, Connect UPS BD, Connect UPS X-Slot, Network-MS

Troubleshooting

HTML pages

Cannot display the UPS properties page. HTTP 404 error with IE.

Solution:

Check the URL entered.

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

- or -

http://<name or IP of the computer hosting Eaton IPM>:4679/

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 as168.8.156.210.

OSGi

OSGi is a module system and service platform for the Java programming language that implements a complete and dynamic component model.

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.
- Open SSL
  - 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.

NOTE Please refer to the following installation information for operating system compatibility:
http://pqsoftware.eaton.com/install/common/eaton_os_compatibilities_aa.pdf

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 Microsoft® Windows 2000, Microsoft® Windows XP®, Microsoft® Windows Vista® 7, Microsoft® Windows 7 and 8, and on Microsoft® Windows Server® 2003, 2008 (including R2 revision), and 2012.

- 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 This is the previous Eaton software 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 7 and later

NOTE For optimal performance, Google Chrome or Firefox is recommended. For good performance, IE version 9 and later is recommended. IE6 performance is not optimal.

JRE Prerequisites

For all features correlated to the infrastructure connector (like VMware, UCS, NetApp) a JRE must be installed on the system hosting Eaton IPM (see "JRE Installation" on page 15). If this prerequisite is not installed, only virtualization features are available, such as the legacy API for VMware connectors.

Table 5. JRE Virtualization, Storage, and ServerCitrix XenCenter

Virtualization, Storage, or Server	Software	No JRE installed	JRE 1.6 or greater
Virtualization	New Vmware vCenter	—	•
	New Vmware ESX/ESXi	—	•
	Microsoft SCVMM	• see NOTE	• see NOTE
	Citrix XenCenter	•	•
	Citrix XenServer	•	•
	Vmware vCenter (legacy API)	•	•
	Vmware ESX/ESXi (legacy API)	•	•
Storage	NetApp Storage	—	•
Server	Cisco UCS Manager	—	•
NOTE	Only available if the system hosting is based on Microsoft operating system. See "Eaton Solutions for Microsoft" on page 85.		

JRE Installation

The installation of the Java Runtime Environment (JRE) is Operating System platform-dependent. All new Eaton components have been developed and tested for the Java version 1.6 or later. After installing the correct JRE, the IPM must be reloaded, to take account this new environment.

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.

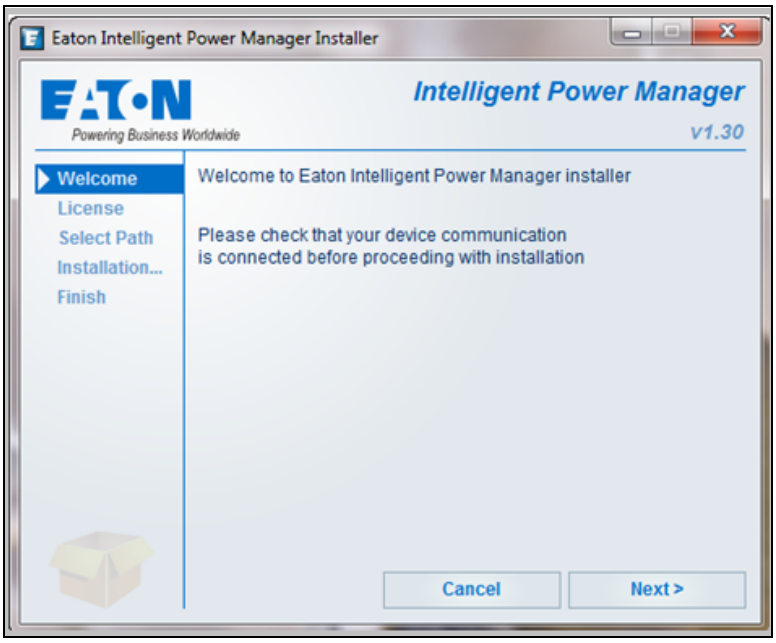


Figure 2. Welcome Screen

3. Read the application description. 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: Network Management Cards Network-MS (ex 66102 / 103006826) and Modbus-MS (ex 66103), PXGX2000, PXGX-UPS, ConnectUPS BD, ConnectUPS X, ConnectUPS MS, Intelligent Power Protector, Network Shutdown Module V3, new Eaton ePDU, new HP UPS Card, new Dell UPS Card, or new IBM UPS Card.
- Display the discovered nodes using ***Settings > Auto Discovery*** (see Figure 4).

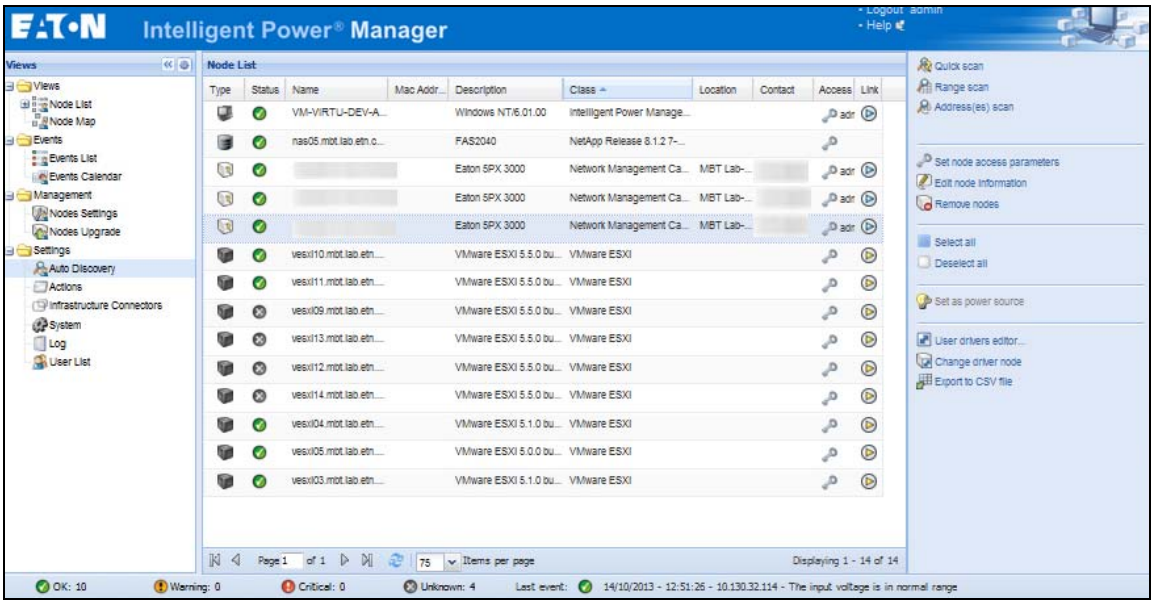


Figure 4. Quick Start - Auto Discovery Page

- 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***. 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).

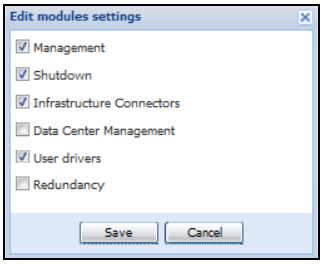


Figure 5. Edit Modules Settings Dialog

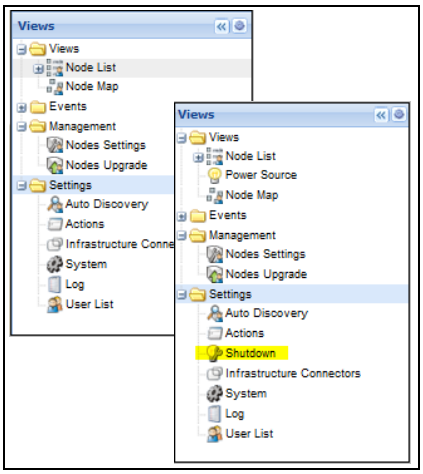


Figure 6. Shutdown Displays in the Settings Menu Hierarchy

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 monitors up to 10 devices (including UPS Web Card, ePDU, or Eaton IPP Shutdown Controller) without a license key.

If there are more devices to be monitored, an appropriate license is needed. The license can also be upgraded later without reinstallation.

Only for "Silver" or "Gold" paid versions:

1. In ***Settings > System > Edit System Information***, enter the license product key that is printed on the commercial CD booklet (inside the CD case):
   - ref 66925 Eaton IPM Silver License (11 to 100 device nodes)
   - ref 66926 Eaton IPM Gold License (101 to unlimited devices nodes)

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).

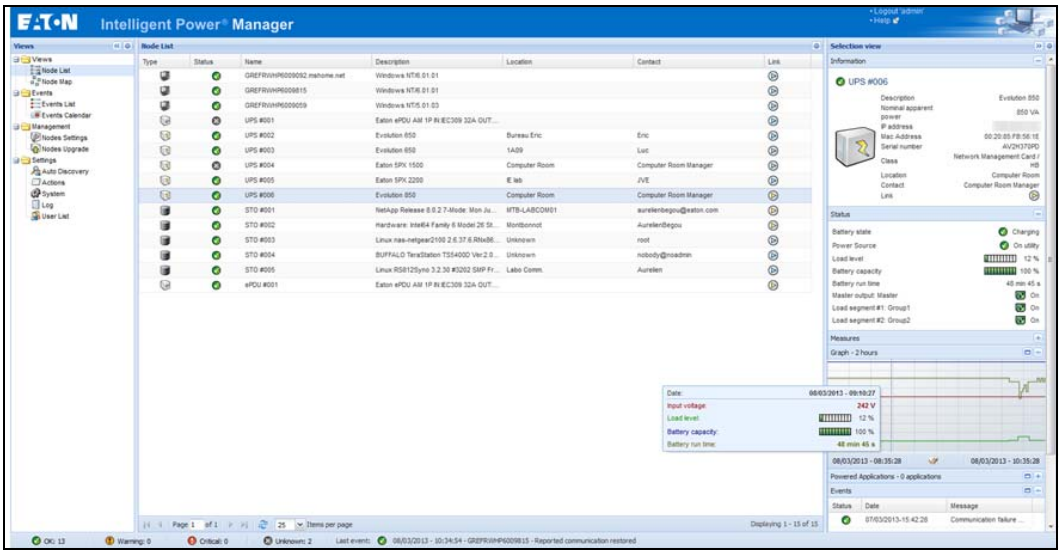


Figure 7. Node List Main Page

- [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 74 for upgrade information. Also see "System Settings" on page 29 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 Install 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.

JRE Installation

The installation of the Java Runtime Environment is Operating System platform dependent. All new Eaton components have been developed tested for the Java version 1.6 or later. After installing the correct JRE, the Eaton IPM must be reloaded to take account this new environment (see "JRE Prerequisites" on page 10).

Chapter 3 Configuration

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

Configure Nodes

Each node (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 Scan button

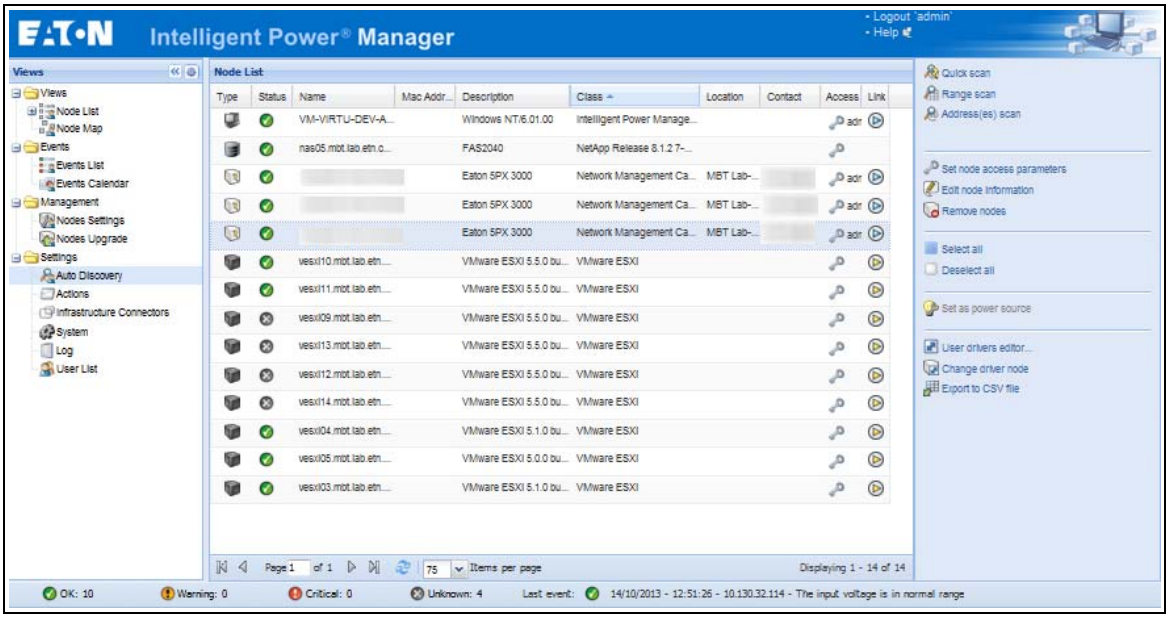


Figure 8. Node List Page

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:

- Network Management Cards Network-MS (example, 66102 / 103006826) and Modbus-MS (example, 66103)
- PXGX2000, PXGX-UPS, ConnectUPS BD, ConnectUPS X, or ConnectUPS MS
- ePDUs
- 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 check (select) the Override global authentication settings checkbox to specify authentication parameters that are different from global scan settings (see Figure 9).

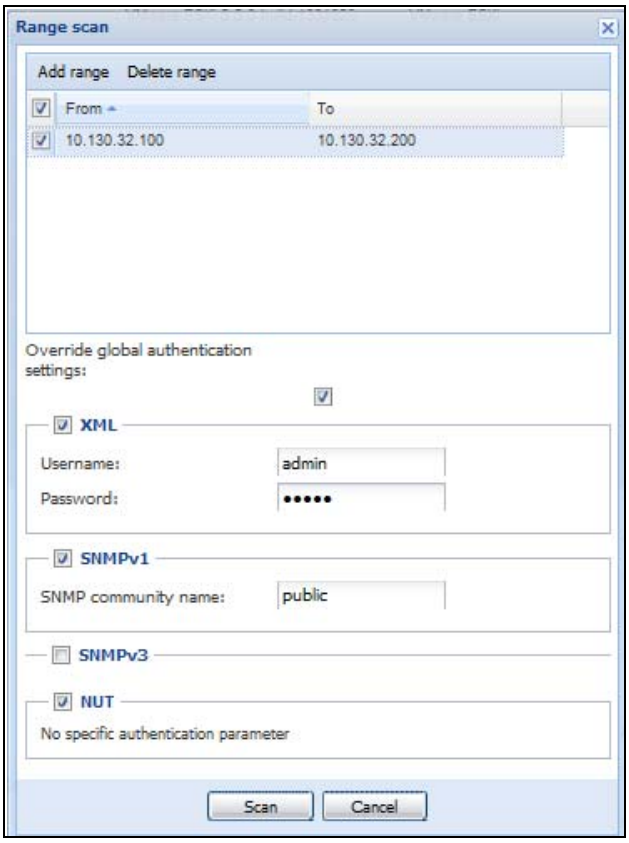


Figure 9. Range Scan Dialog Box

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 check (select) 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 check (select) 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).

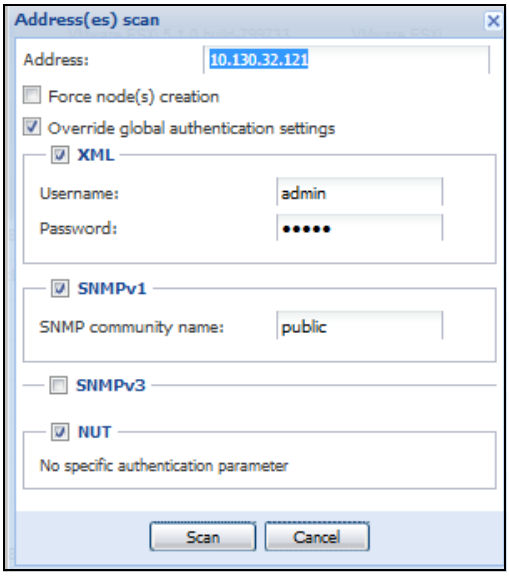


Figure 10. Address(es) Scan Dialog Box (Example 1)

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

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 8).
3. Set the scan settings by selecting or deselecting checkboxes, typing data, or make selections from the drop-down list.

Figure 12. 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).
3. By default, the driver of the node is selected. Choose another driver and click OK.

Then the node will use this new driver.

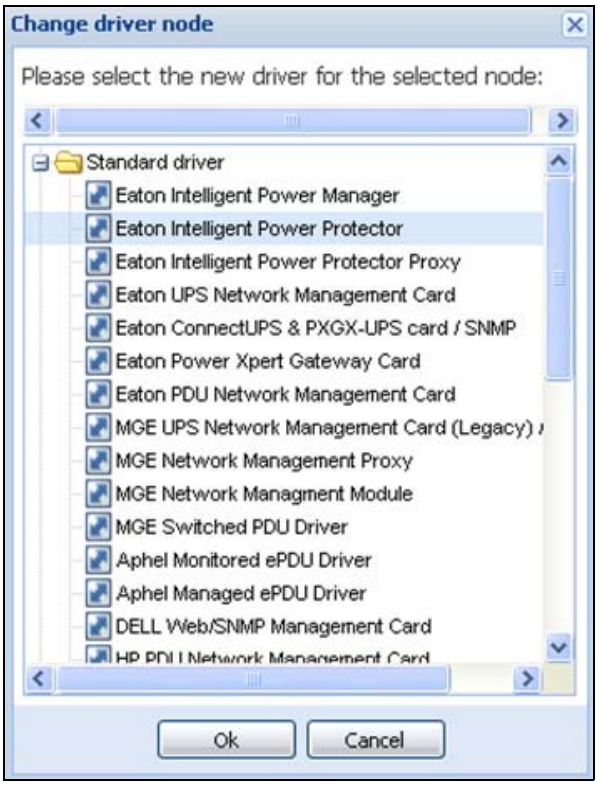


Figure 13. Change Driver Mode Dialog Box

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 14 and Figure 15):
   - **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 capabilities.

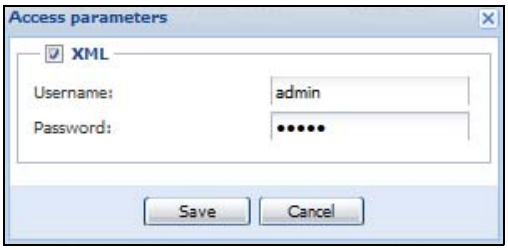


Figure 14. Node Access Parameters Dialog

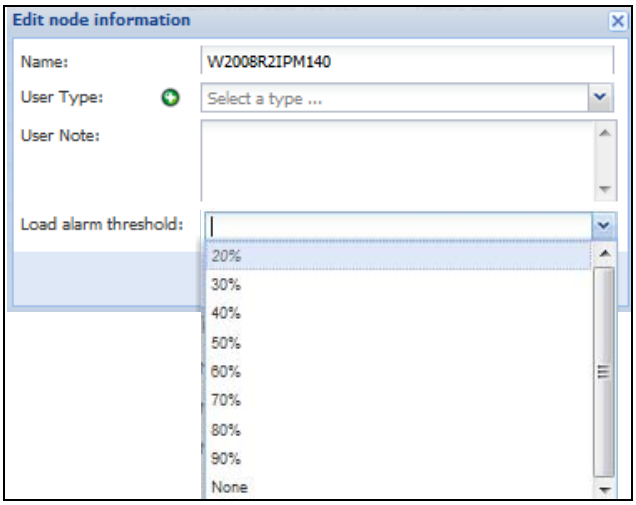


Figure 15. Edit Node InformationDialog

Configure Actions

From the ***Settings > Actions*** menu item, the following types of notifications or executable actions can be set to occur as the result of specific Eaton IPM actions (see Figure 16):

- E-mail
- Execute script/program
- Notification to the local alarm notification box, available from the System Tray icon

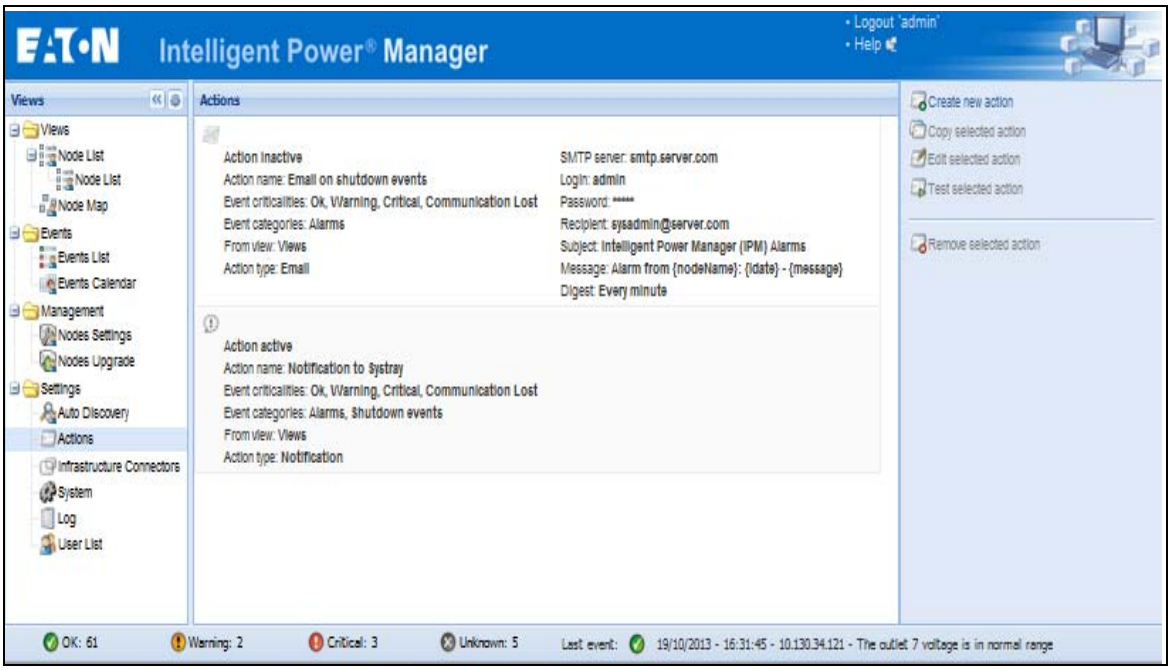


Figure 16. Actions Page

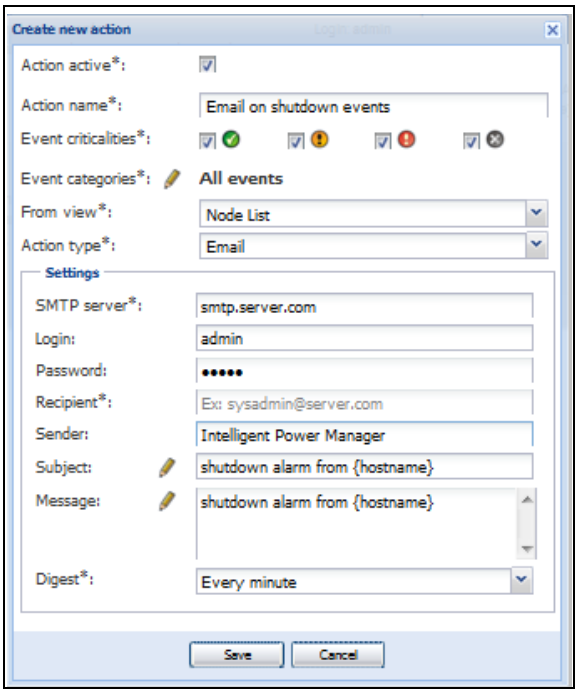


Figure 17. Create New Action Dialog

NOTE The "*" fields are required.

E-mail Notification Actions

You can set e-mail notifications for specific events in the Edit Action dialog box (see Figure 17). First, set the event filter to specify the event trigger. Then, set the e-mail notification criteria.

Events Filter

You can filter the action according to the following:

- **Event criticalities**: Critical, Warning, Normal, and Communication Lost

NOTE With this parameter, you can filter the notification according to the event level (see "Node Events List" on page 61). If you select "Critical" as the filter, you will not receive the associated "Normal" event informing that the device status changes from "Critical" to "Normal."

- **Event category**: All Events, Alarms, Shutdown events, Power events, and Measures

NOTE The pen icon allows you to select and edit the event category.

- **View**: The view that triggers the event

e-mail Criteria

To receive e-mail on UPS events:

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

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. 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

Execute Script/Program Actions

In order to execute a program on UPS events, the program path is required.

NOTE 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 be 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 "RunAs" 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.

Alarm Box Notification Actions

The alarms are displayed on the local computer in an alarm box (see Figure 18). The status part of the alarm box is optional. It only appears if a power source has been declared in the Shutdown configuration settings.

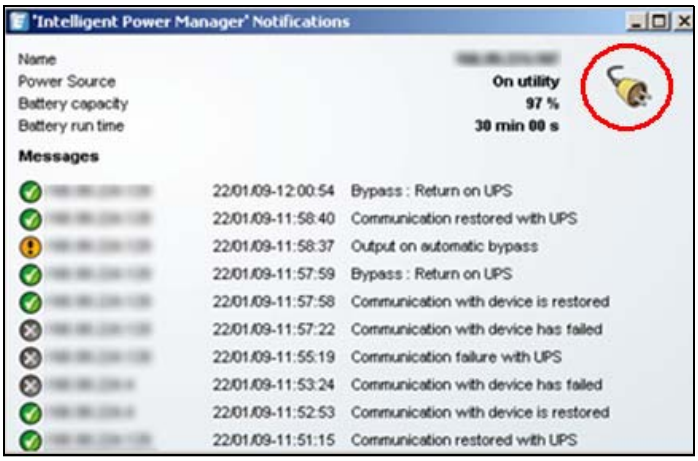


Figure 18. Alarm Notification Box with System Tray Icon

The Alarm notification box is accessible from the System Tray icon (see Table 6 and Table 7). 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 can have the states described in Table 6.

Table 6. System Tray State Icons (Power Source not Declared)

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 can have the states described in Table 7.

Table 7. 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.

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

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

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 19).
2. Click **Add user.** The Add user dialog box displays.
3. Type the user's login and the user's password (see Figure 20).

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**.

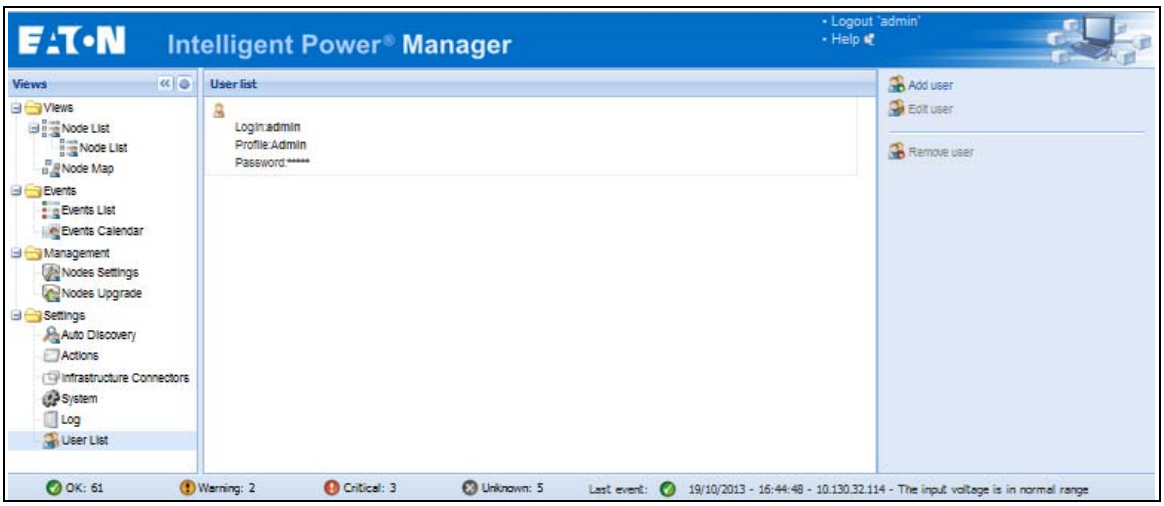


Figure 19. User List Page for User Account

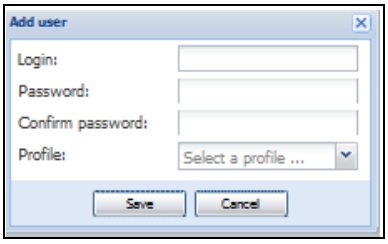


Figure 20. Add User Dialog Box

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

You can edit system settings. From the ***Settings > System*** menu item, you can edit system information and settings (see Figure 21).

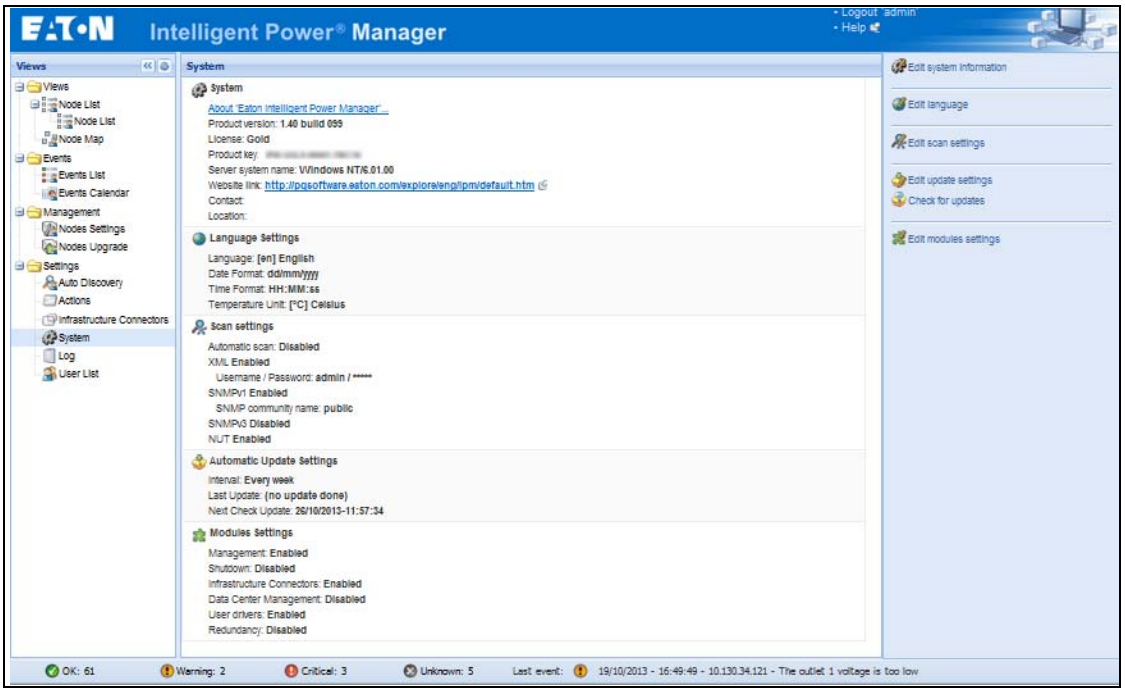


Figure 21. System Settings Page

Select one of the items on the System page, and then double-click the item, or single-click on 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 virtualized IT systems
  - **Redundancy** provides support for >1 UPS in N+1 redundant configurations
  - **User Drivers** integrates new devices in the IPM supervision application by using predefined common base objects and user-specific objects

NOTE This 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

Manage the Cisco UCS Manager Component

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 22).
3. Ensure that the **Infrastructure Connectors** checkbox is selected (checked).
4. Click **Save**.

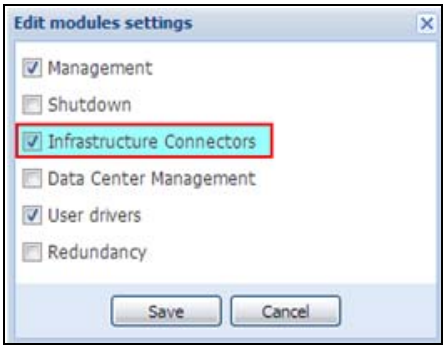


Figure 22. Edit Modules Settings - Infrastructure Connectors

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 Connectors page displays (see Figure 23).
2. Click **Add a connector** in the right panel. The Add a connector dialog box displays (see Figure 24).

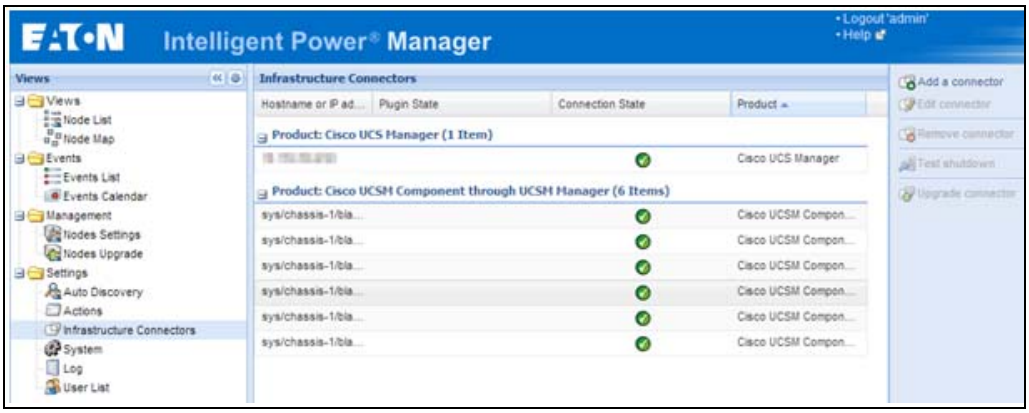


Figure 23. Select Add a Connector

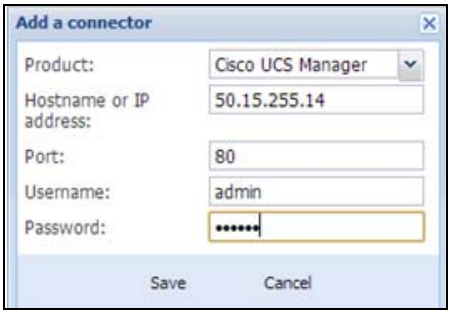


Figure 24. Add a Connector Dialog for Cisco UCS Manager

3. From the Add a Connector dialog, select Cisco UCS Manager from the Product drop-down list (see Figure 24).
4. Add identification information for the selected connector:
   - **Product:** Cisco UCS Manageris 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 25).
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 26).

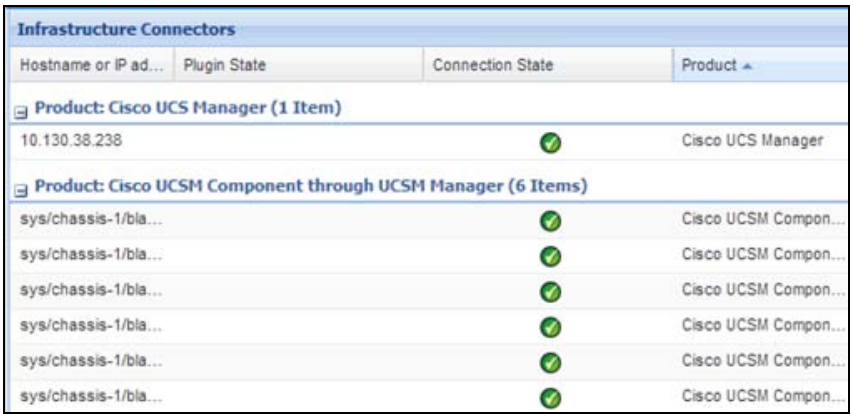


Figure 25. Cisco UCS Manager Component Added

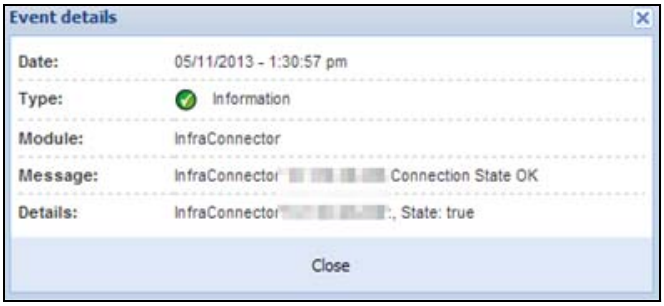


Figure 26. Event Details

Remove the Component

To remove a Component, right-click on the component in the list. From the action box, click Remove connector (see Figure 27).

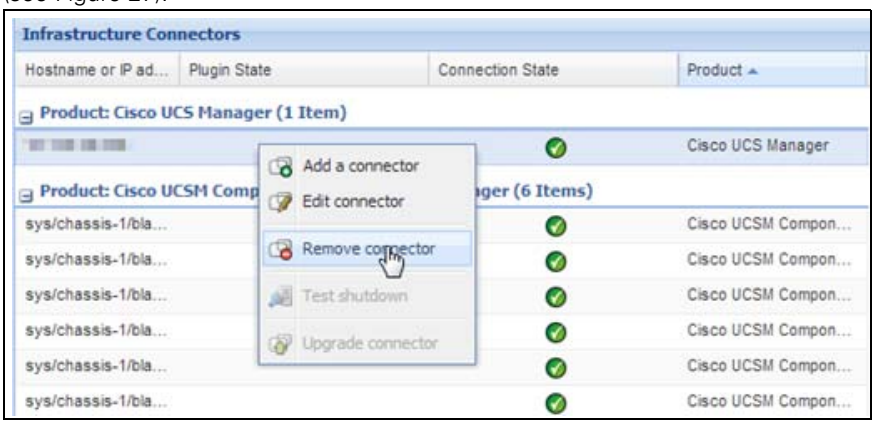


Figure 27. Remove a Connector

Edit a Component

To edit a Component, right-click on the component in the list. From the action box, click Edit connector (see) 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.

.

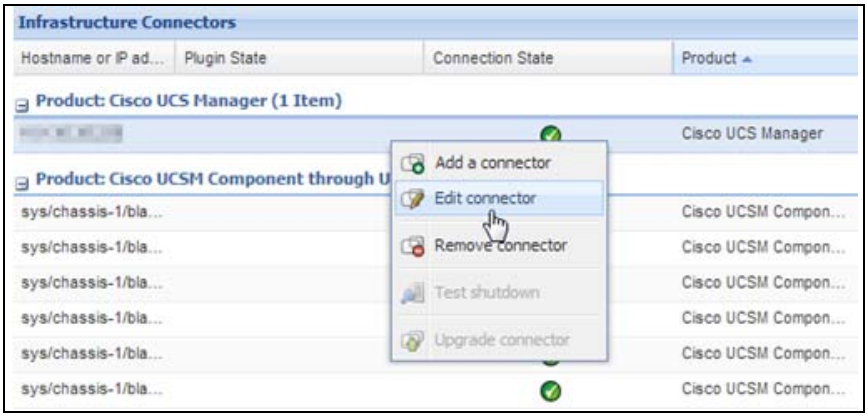


Figure 28. Edit a Connector

.

Figure 29. 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 30).

.

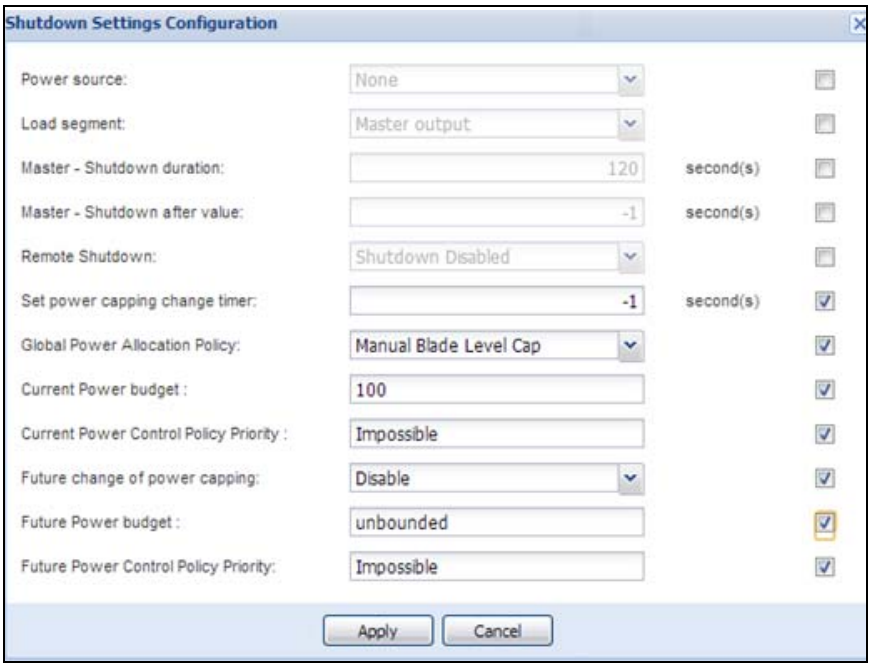


Figure 30. Shutdown Settings Configuration

Power source, Load Segment, Remote shutdown, Shutdown duration, 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, any change on those in IPM will set permanently the new values on UCS manager

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

Power Capping Timer

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

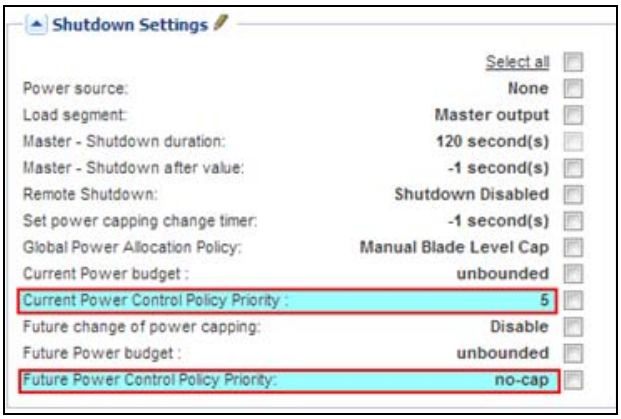


Figure 31. Shutdown Settings-Set Power Capping Change Timer

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.

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.

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

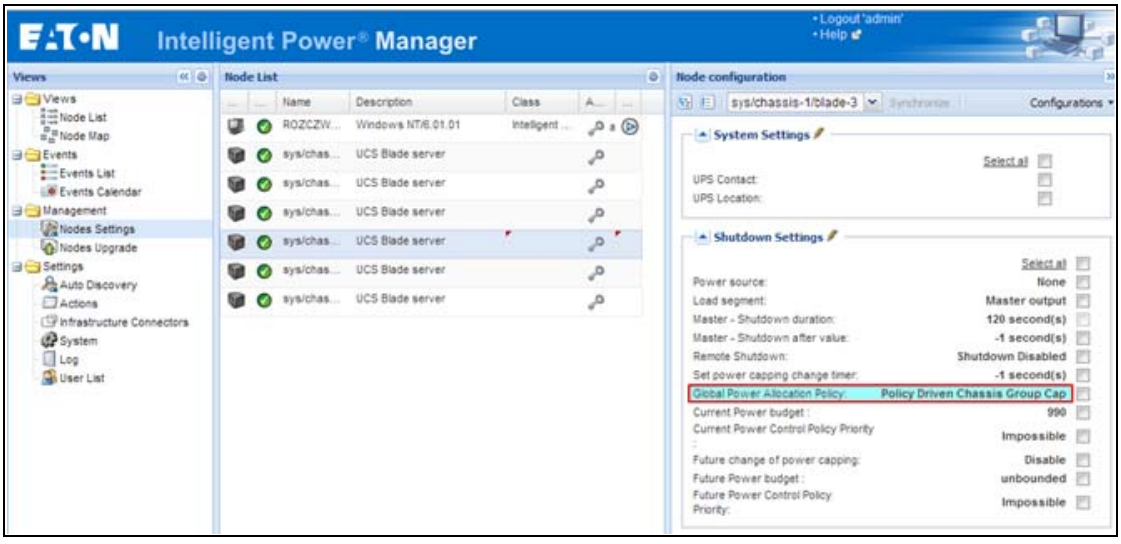


Figure 32. Policy-driven Power Chassis Group Power Capping

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.

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.

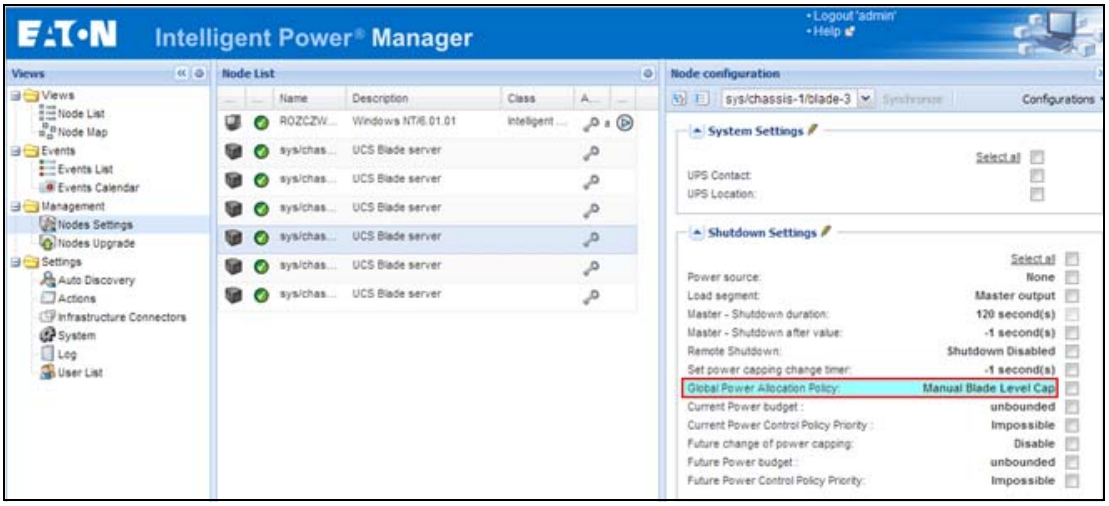


Figure 33. Manual Blade Power Capping

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.

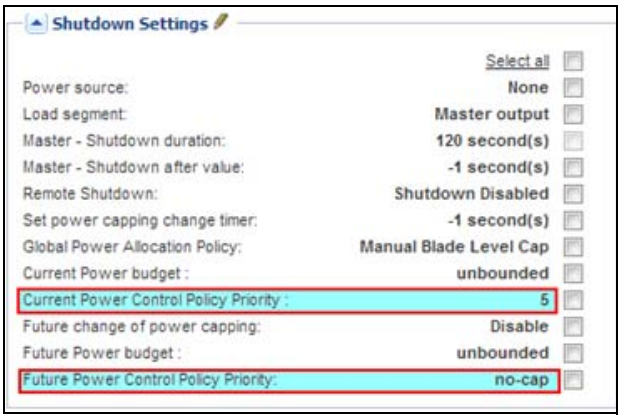


Figure 34. Shutdown Settings-Current Power Default Setting (Priority 5)

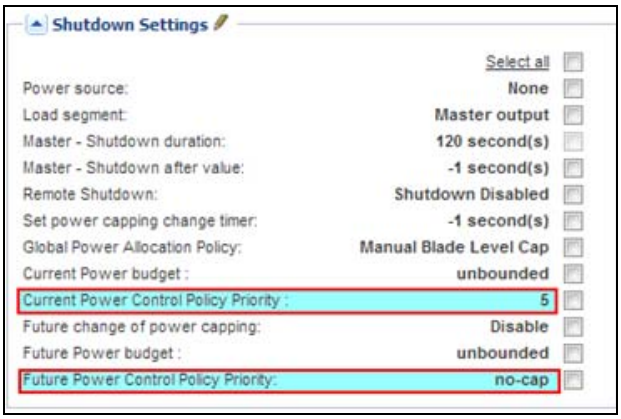


Figure 35. Shutdown Settings-Current Power Not Set Due to No Service Profile

Power Budget

Power budget allows you to specify the maximum amount of power (in watt) 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. The server can use as much power as it requires.

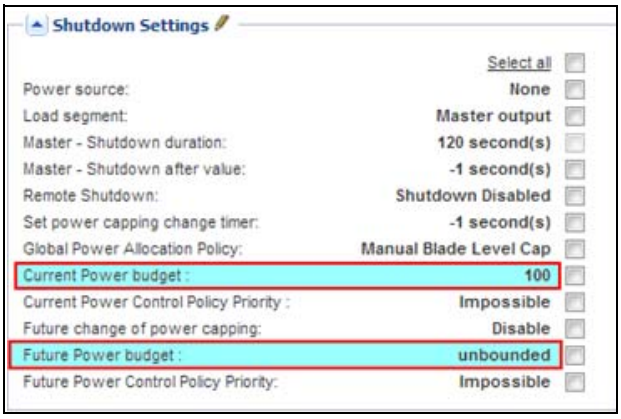


Figure 36. Shutdown Settings-Future Temporary Power Budget is Disabled

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.

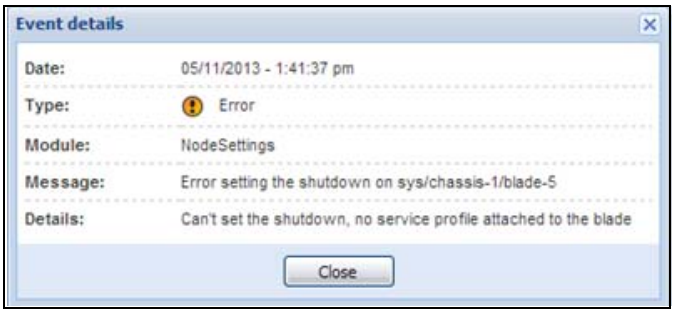


Figure 37. No Service Profile

2. You can't set a priority to a blade that doesn't have a service profile assigned.

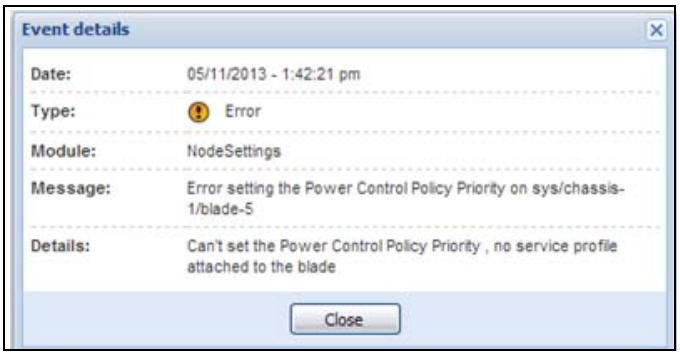


Figure 38. No Service Profile

3. IPM can't find a UCSM on the IP provided.

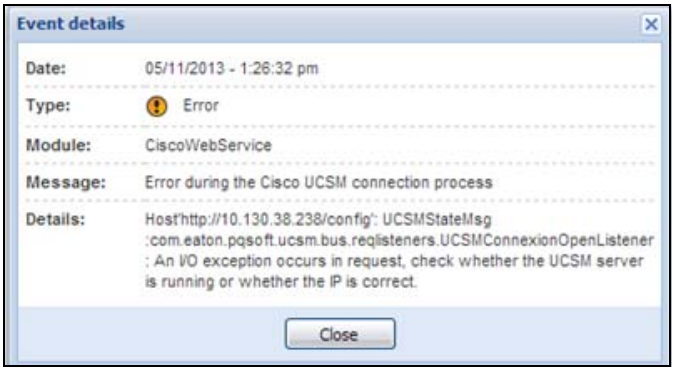


Figure 39. UCS Manager Not Found

4. A wrong value has been set for the power budget.

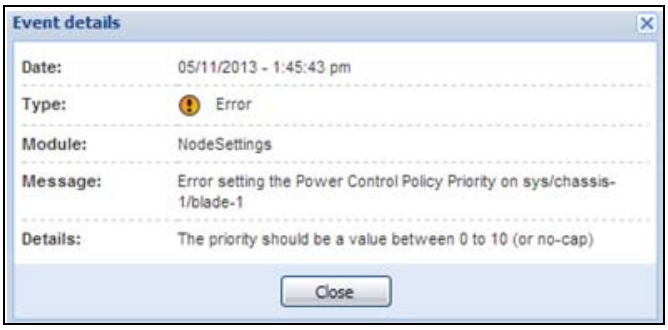


Figure 40. Wrong Power Budget Set

5. A new power budget has been requested by the client

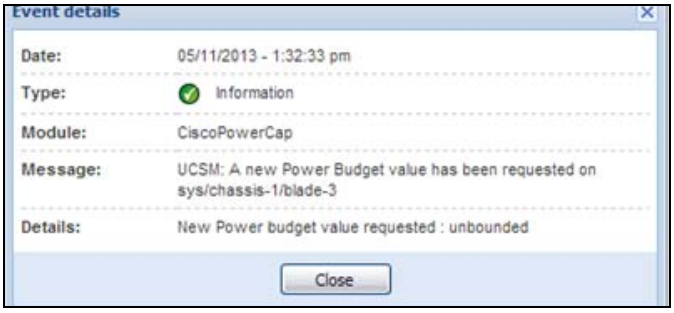


Figure 41. New Power Budget Requested

6. A new power budget has been successfully set by the server.

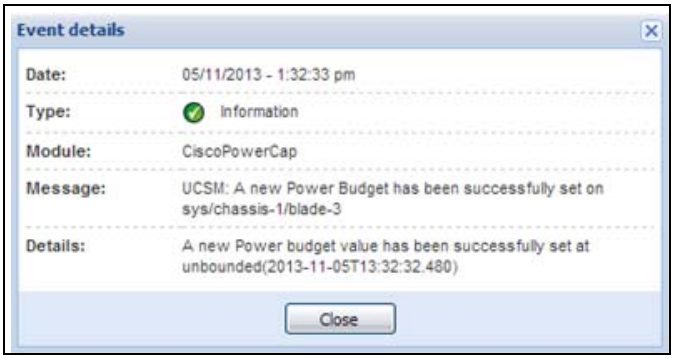


Figure 42. New Power Budget Successful

Chapter 4 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 Protector

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 in this page (see Figure 43):

- **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
- **Description:** Product name or description
- **Location:** Node location
- **Contact:** Node contact
- **Link:** Link to the device Web site (if available)

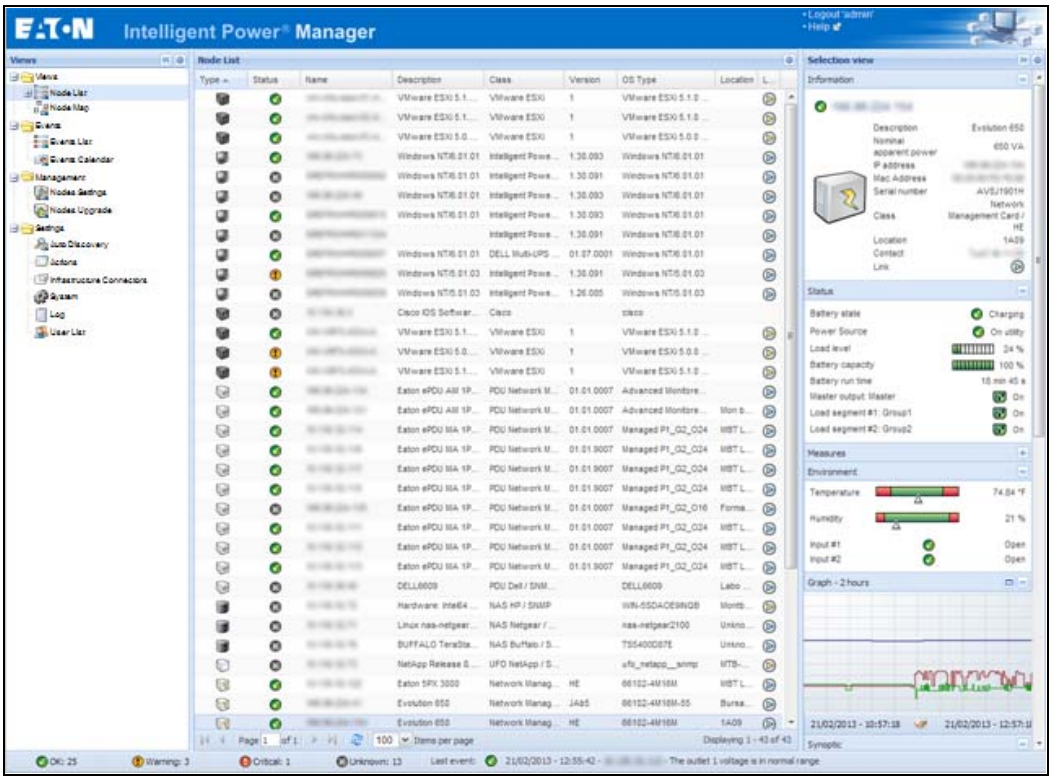


Figure 43. Node List View

You can sort (ascending or descending) your device list by clicking the column titles (Status / Name / Description/ Location / Load Level and so forth). You can also add columns, as illustrated in Figure 44.

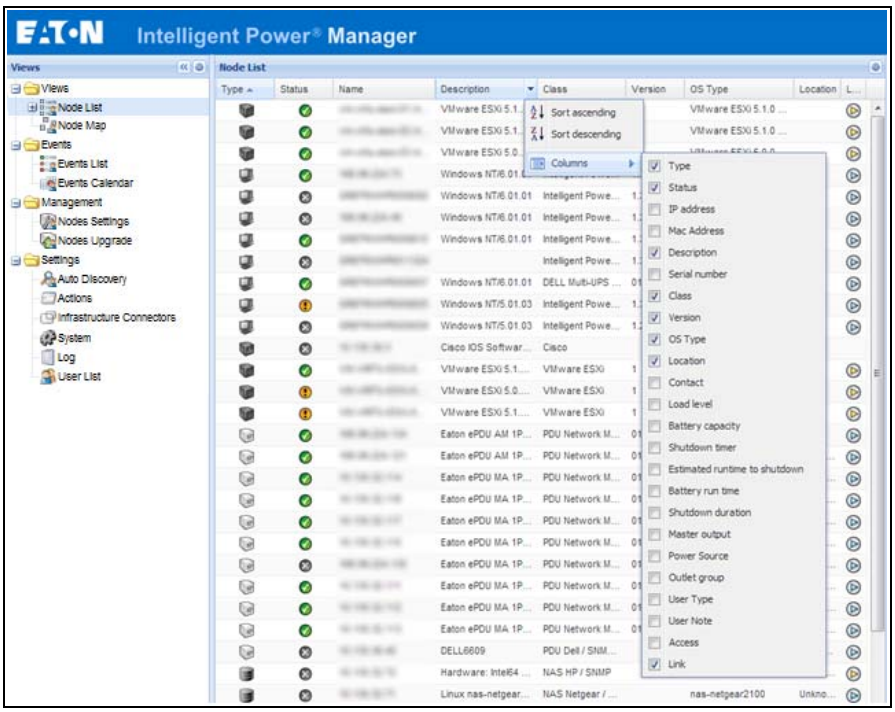


Figure 44. Adding Columns in Node List View

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. Click the selection button to select which panels you want to add in the selection view (see Figure 45).

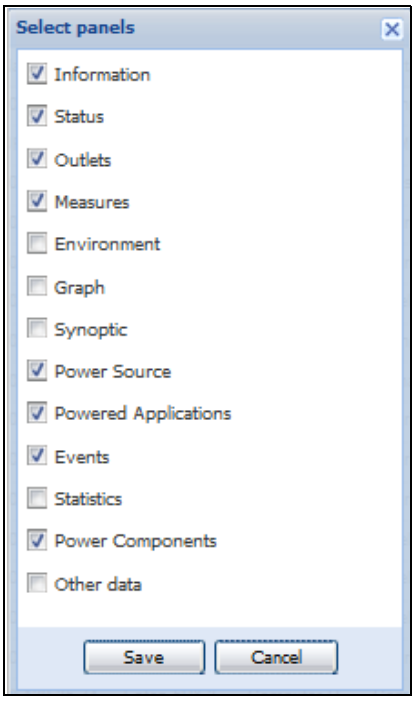


Figure 45. Panel Selection Dialog Box

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

Information Panel

The following node information displays in this panel (see Figure 46):

- **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.

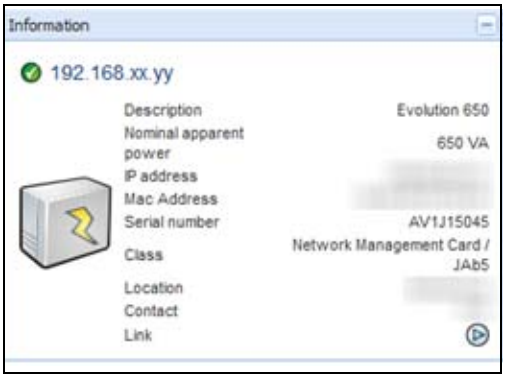


Figure 46. Information Panel

Status Panel

The following node status displays in this panel (see Figure 47):

- **Power source:** AC Power / Battery
- **Battery state:** Charging / Discharging / Default / Floating / Resting
- **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.

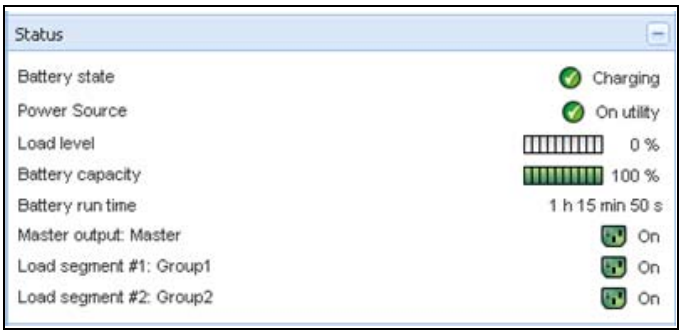


Figure 47. Status Panel

Outlets Panel

The following outlets status information displays for the selected ePDU in this panel (see Figure 48):

- 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)

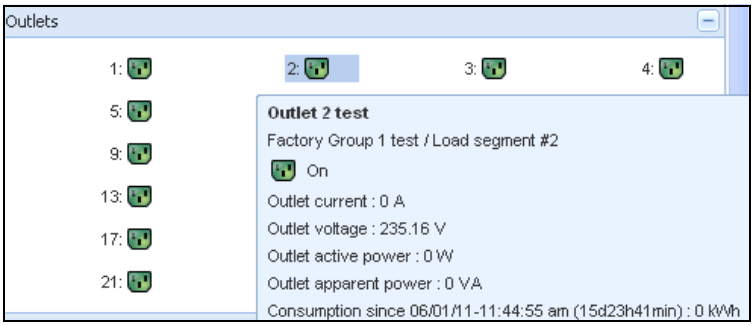


Figure 48. Outlet Panel

The outlet state is color-coded in the display (see Table 8).

Table 8. 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 49 and Figure 50).

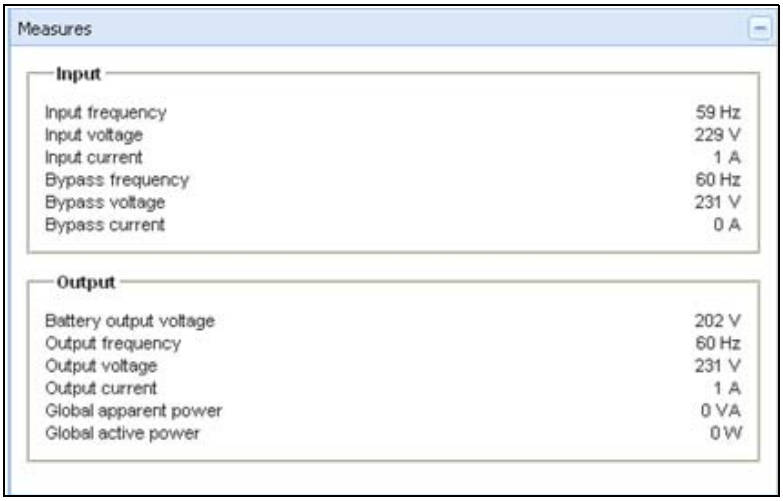


Figure 49. Measures Panel (Single-Phase)

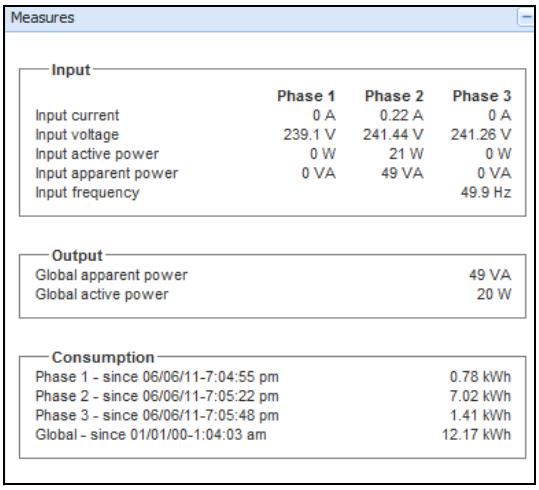


Figure 50. Measures Panel (Three-Phase)

Environment Panel

This panel displays the selected device sensor information if a device is attached (see Figure 51):

- **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) User Guide*.

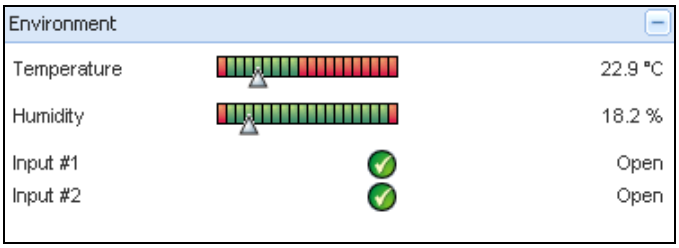


Figure 51. Environment Panel

Graph Panel

This panel displays the graph of the main measures of the selected device (see Figure 52):

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

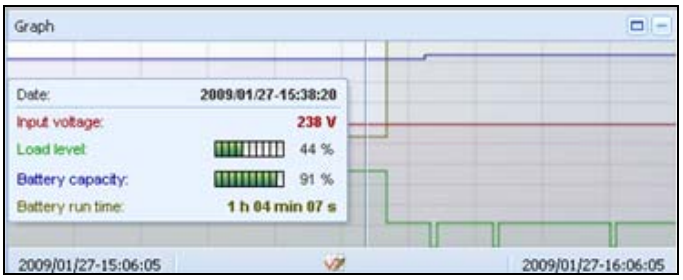


Figure 52. Graph Panel

Synoptic Panel

This panel displays the selected device synoptic (see Figure 53). A tool tip displays when you move the mouse over one of the functional block.

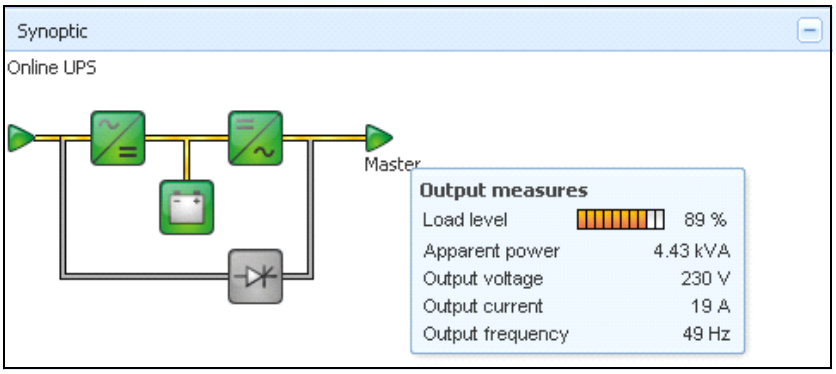


Figure 53. Synoptic Panel

The Synoptic color coded icons display for the following (see Table 9):

- 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 9. 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%
	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

Table 9. Synoptic Panel Icons (Continued)

Symbol	Color	Description
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 54).

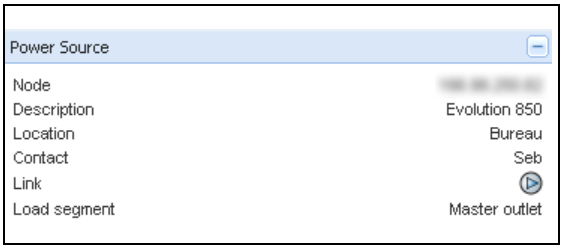


Figure 54. Power Source7

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 55)"

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

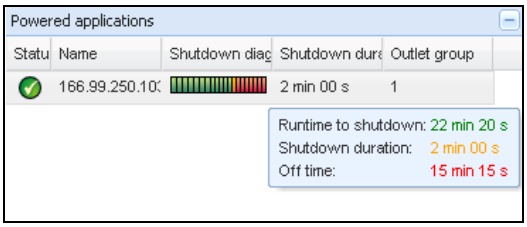


Figure 55. Powered Applications

Events Panel

This panel displays the events list of the selected node (see Figure 56). You can sort the events according to status, date, and message by clicking the column header.

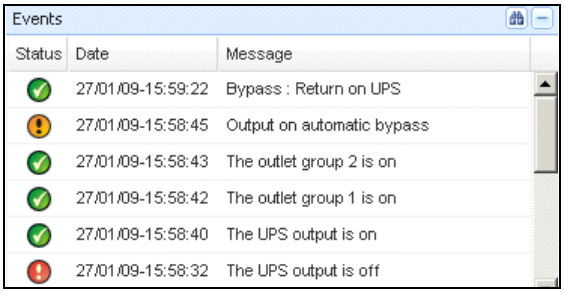


Figure 56. Events Panel

Statistics Panel

This panel displays the statistics of the selected node (see Figure 57). 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.

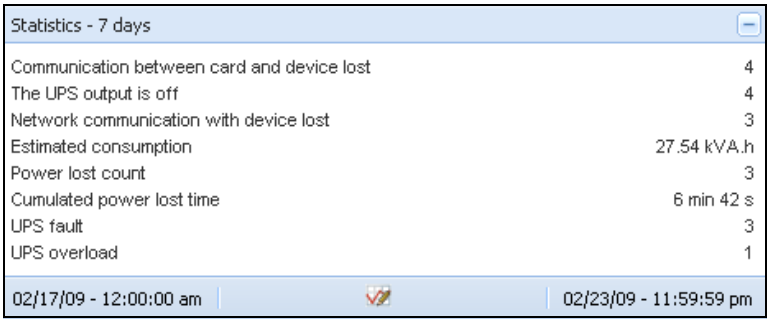


Figure 57. Statistics Panel

Power Components

Figure 58 illustrates the Power Components View. This panel displays the components of a redundant UPS system if the Redundancy feature is activated (see Chapter 8, "Redundancy" on page 97).

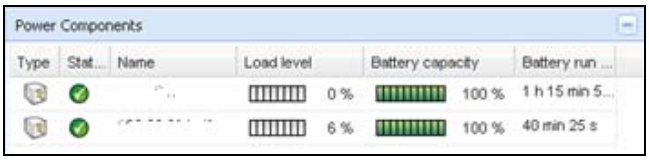


Figure 58. Power Component View (Sub-view of Power Source View)

Subviews

Defining Sub-views

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

To define a sub-view:

1. Select a view in the ***Views > Node List,*** such as Category: "Devices" or Location "HPO Finland" (see Figure 59).
2. Right-click this selection. The contextual sub-view menu displays (see Figure 60).
3. Click **Create a sub-view from ...** and follow the instructions.

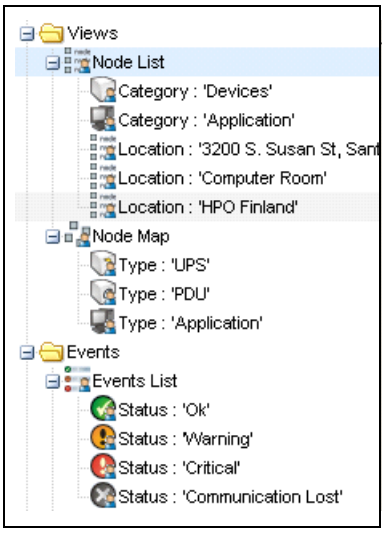


Figure 59. Views > Node List Example Hierarchy

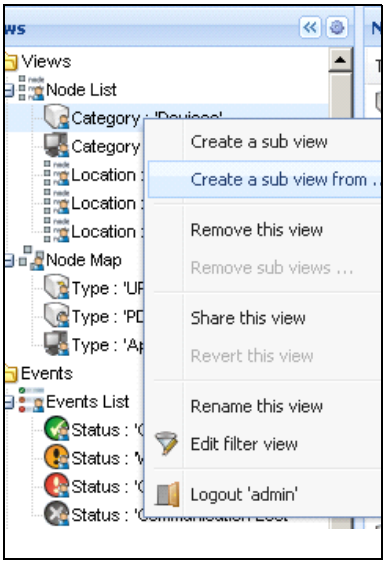


Figure 60. Contextual Sub-view Menu

To filter the nodes in this sub-view:

1. Select a view in the ***Views > Node List***, such as "Location: Computer Room" (see Figure 59).
2. Right-click this selection. The contextual menu sub-views displays (see Figure 60).
3. Click **Edit a Filter View**. The View Filter Rules dialog box displays (see Figure 61).
4. Click **Add rule**, then type the Object, Operation and Values.

NOTE With the setup shown in Figure 61, this filtered view allows you to view the devices whose location field contains the value "Computer Room."

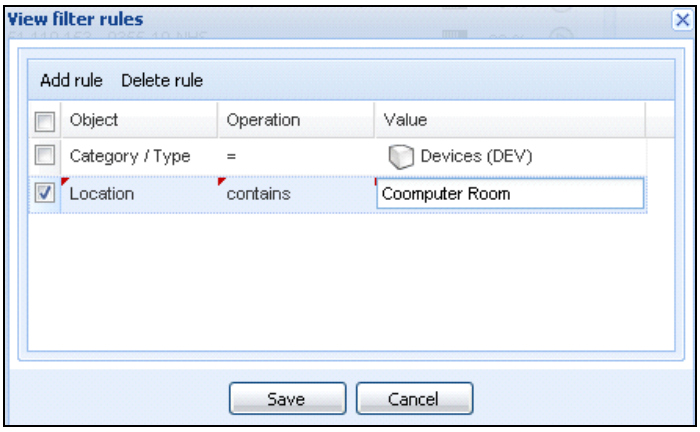


Figure 61. View Filter Rules Dialog Box

As the result of creating a subview, The following default information appears in the Applications List View page (see Figure 62).

- **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
- **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)
- **Power Source shutoff:** After the application is stopped, this information shows whether the power source is stopped or not
- **Outlet group:** UPS load segment
- **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.

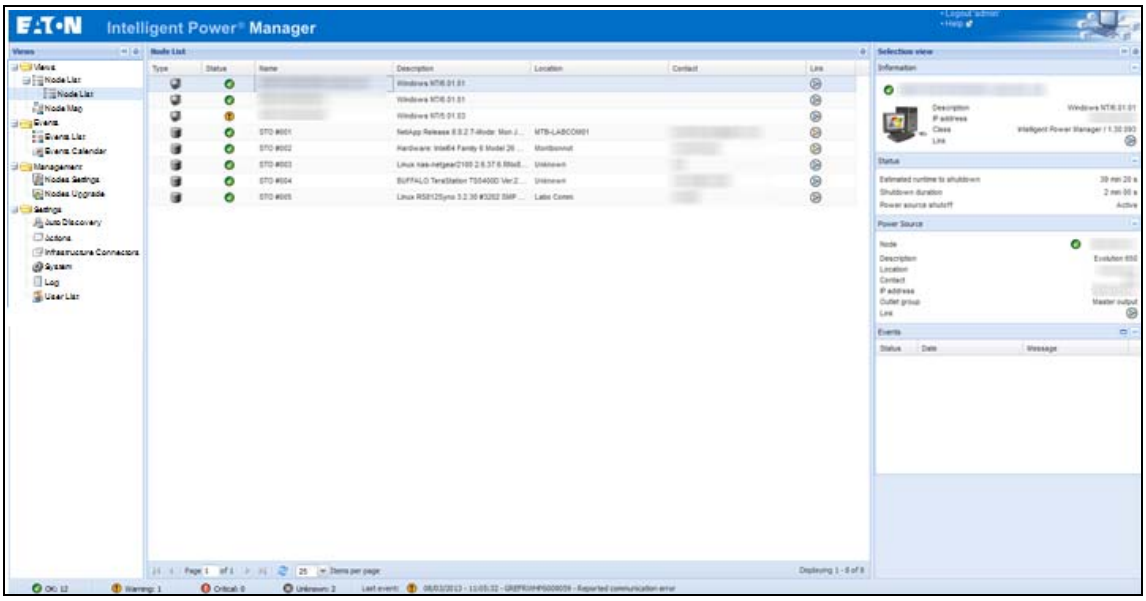


Figure 62. Applications List View Page

Sharing Sub-views

A customized sub-view is "attached" to the user that created it. It is private. The customized sub-view is marked with a small man next to the icon of the sub-view (see Figure 63).

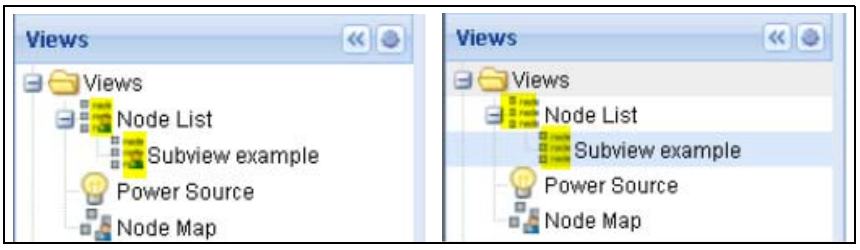


Figure 63. Shared View with Marker (left) and Public View without Marker (right)

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

To share the view:

1. Right-click the view to open the contextual menu (see Figure 64).

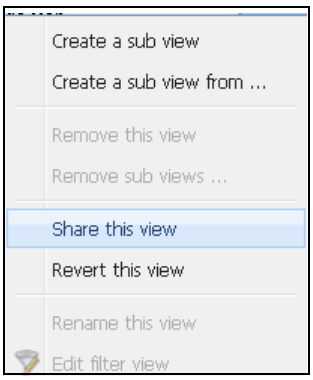


Figure 64. Contextual Sub-view Menu

2. Click **Share this View** (see Figure 65).

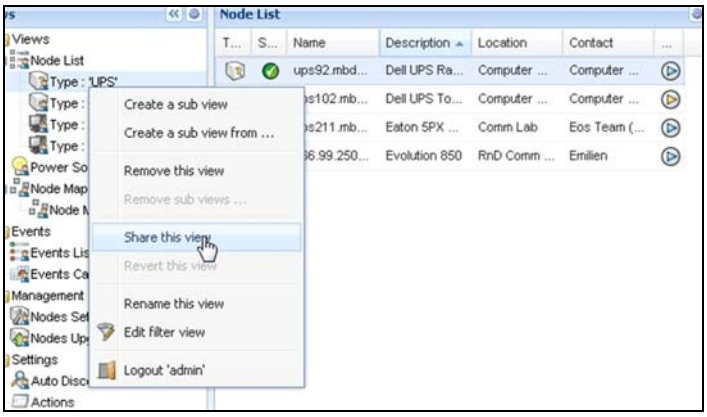


Figure 65. Share the View Selection

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 66:

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

Figure 66. 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 67):

- **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**.

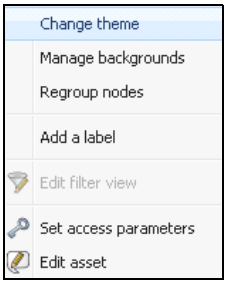


Figure 67. Contextual Tools Menu

Map Examples

This section provides examples of the following maps:

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

Figure 68. World Map View

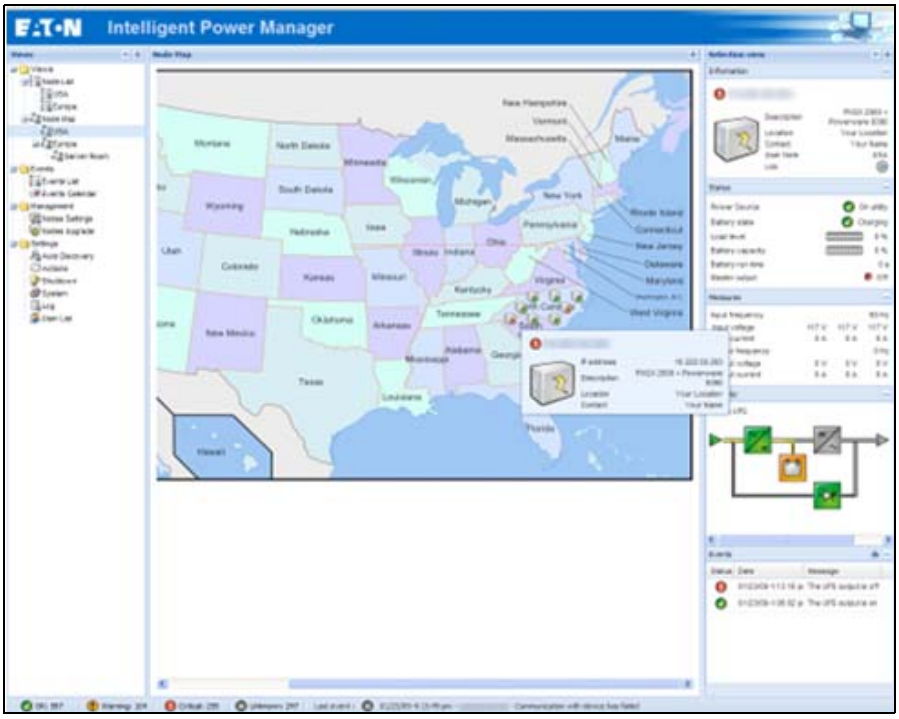


Figure 69. Country Map View

Figure 70. Server Room Map View

Events

List Representation

Select ***Events > Events List*** to display the Events List page (see Figure 71). All new alarms are stored in this log. You can sort the alarms according to the Status, Date, Name, and Acknowledge (ACK) fields.

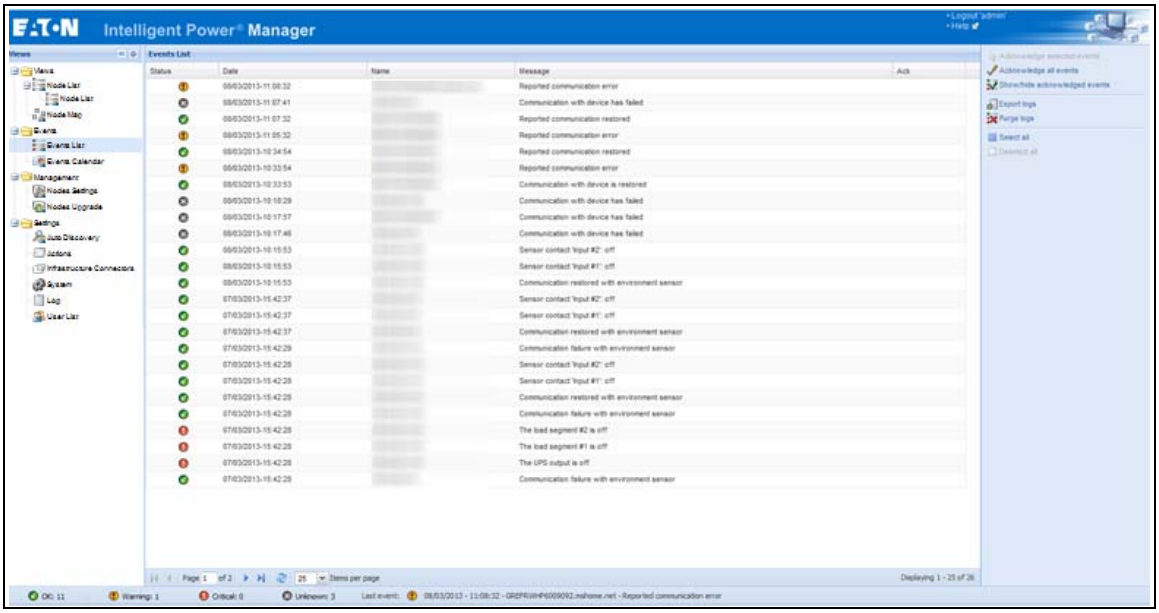


Figure 71. Events List Page

The following functions are available:

- **Acknowledge selected events**: Adds a check box in the Ack column for selected events
- **Acknowledge all events**: Adds a check box in the Ack column for all event.

NOTE When an alarm is acknowledged, it is marked with a check box 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**: Delete 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 72).

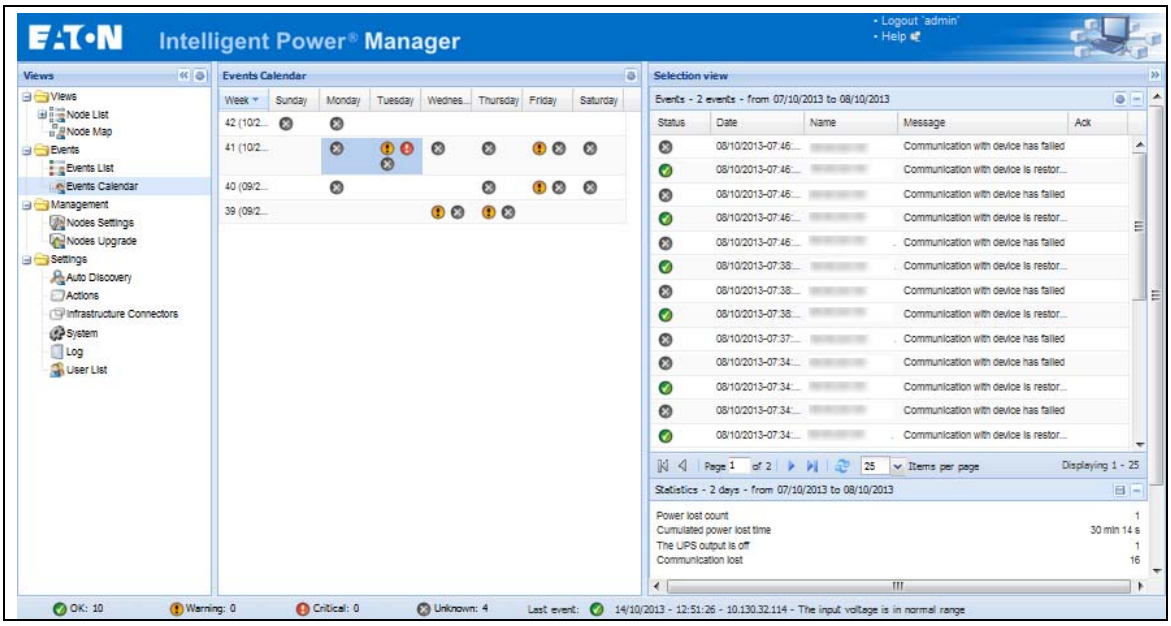


Figure 72. Event Calendar Page

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
- Communication restored with UPS
- The system is powered by the utility
- The UPS output is on
- Communication restored with UPS
- 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

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)
- The device is under its load alarm threshold
- The device is over its load alarm threshold
- Protection lost
- Redundancy lost
- Shutdown in <***time***>
- Remote Communication Error (remote communication or configuration issue is detected)

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

COMMUNICATION LOST Communication is lost.

Communication Lost Event List:

- Communication failure with Device or Application

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 73 provides examples of the opening view from different Web interfaces.

Figure 73. 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 74).

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.

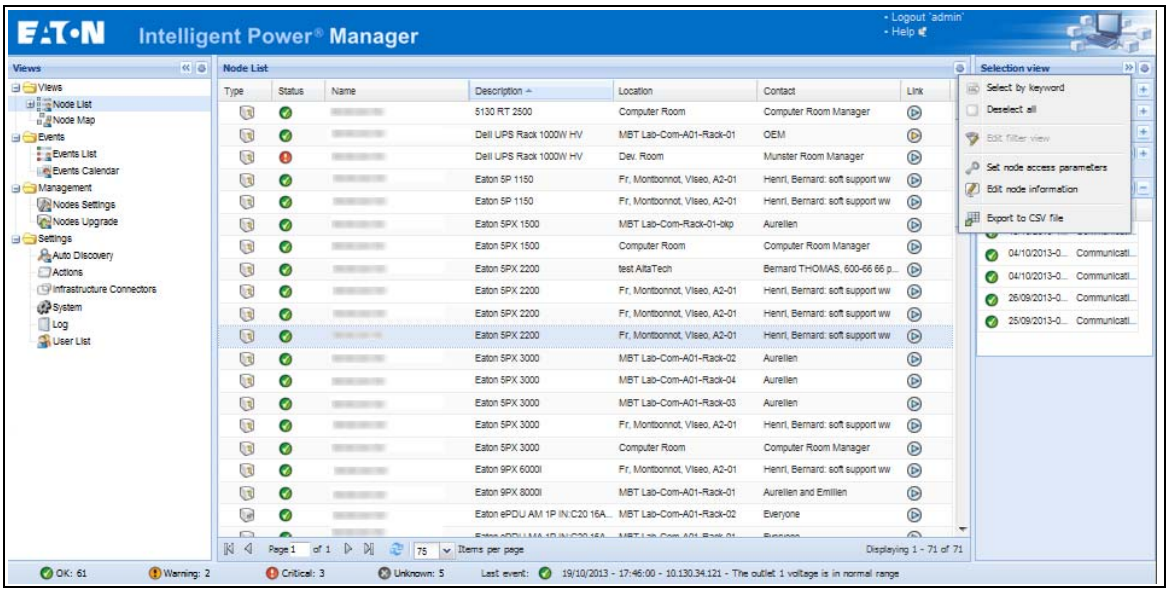


Figure 74. Export to CSV File

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

Chapter 5 Shutdown

The Eaton Intelligent Power Manager (IPM) provides local computer graceful shutdown when connected to a UPS through either a 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 Refer to the *Eaton Intelligent Power Protector (IPP) User's Guide* for a detailed description of the Shutdown feature.

NOTE When the Shutdown feature is enabled, the software displays a communication error until the Power Source is correctly configured as described in "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 75).

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

   - Edit power source
   - Edit shutdown configuration
   - Edit advanced shutdown criteria
   - Edit UPS configuration
   - Test access
   - Test shutdown

Figure 75. USB/Serial Power Source on 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 available with your operating system, there are a number of advantages to using the hibernation feature (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 76):

- 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.

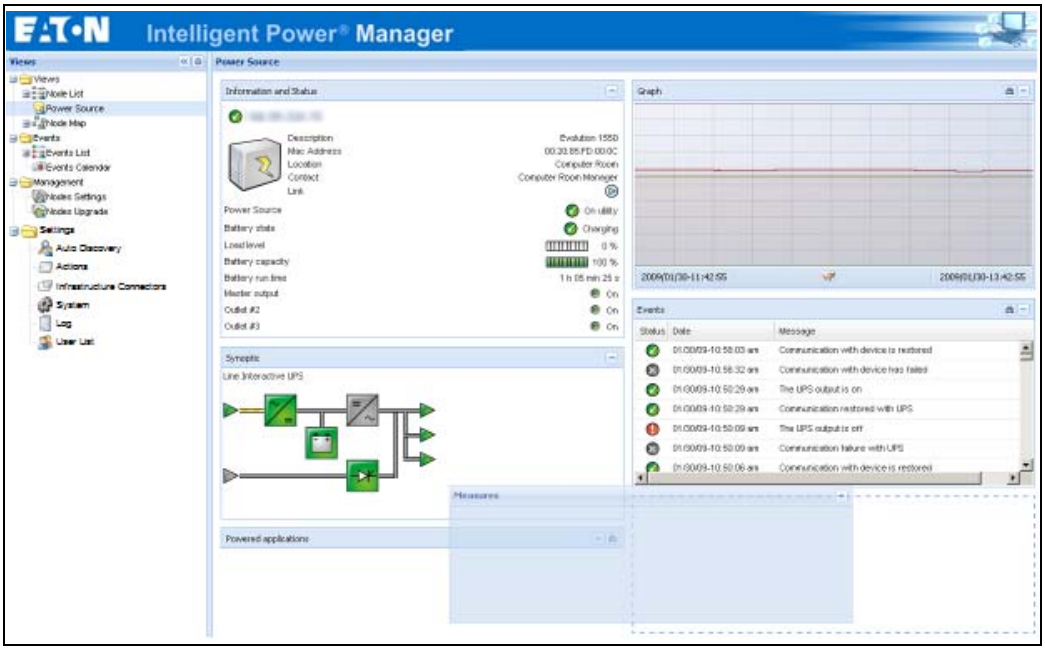


Figure 76. Power Source View

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 6 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 77).
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.

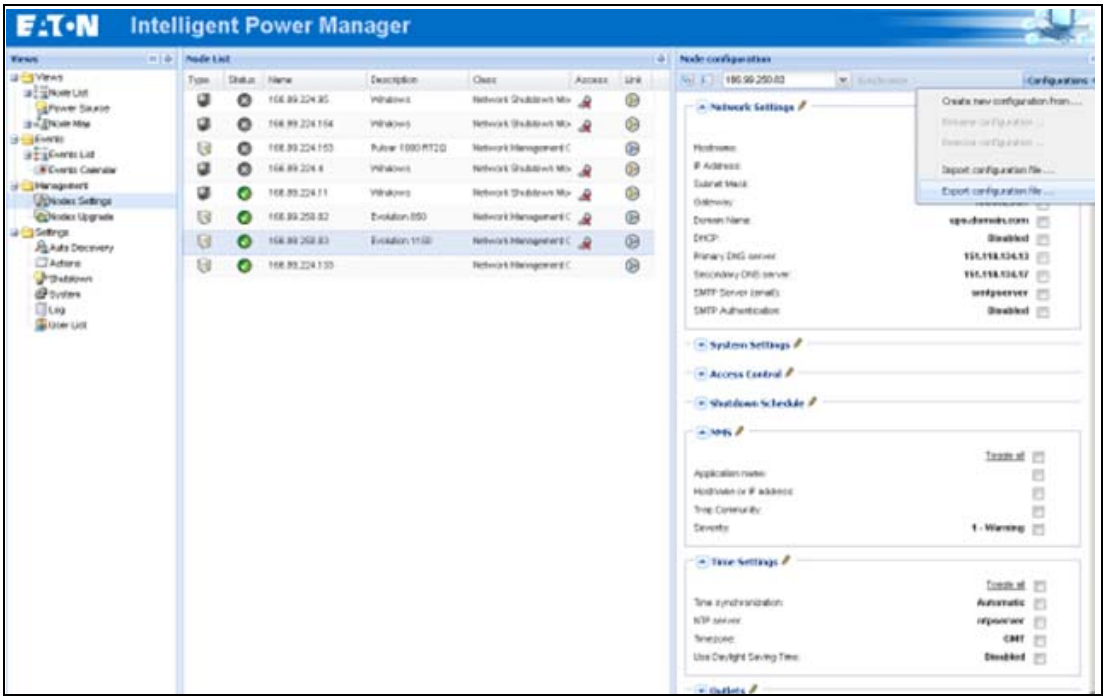


Figure 77. Nodes Settings View

Single Card Settings

Eaton IPM can configure a remote 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 77).

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 78).

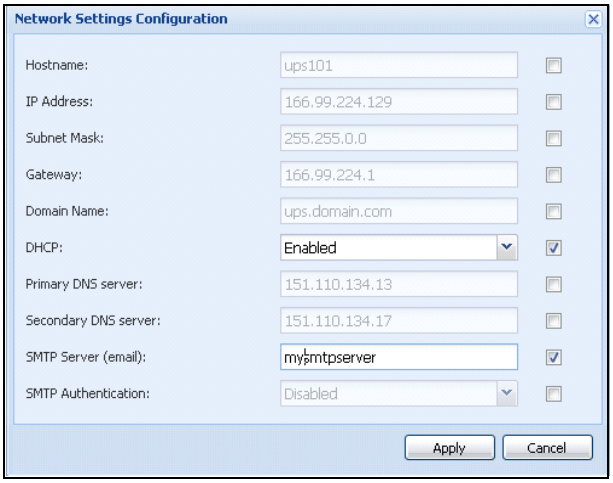


Figure 78. Network Section

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

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

7. Select the parameters you want to synchronize (with the check box).

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 79).

Figure 79 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 parameters details of the category.

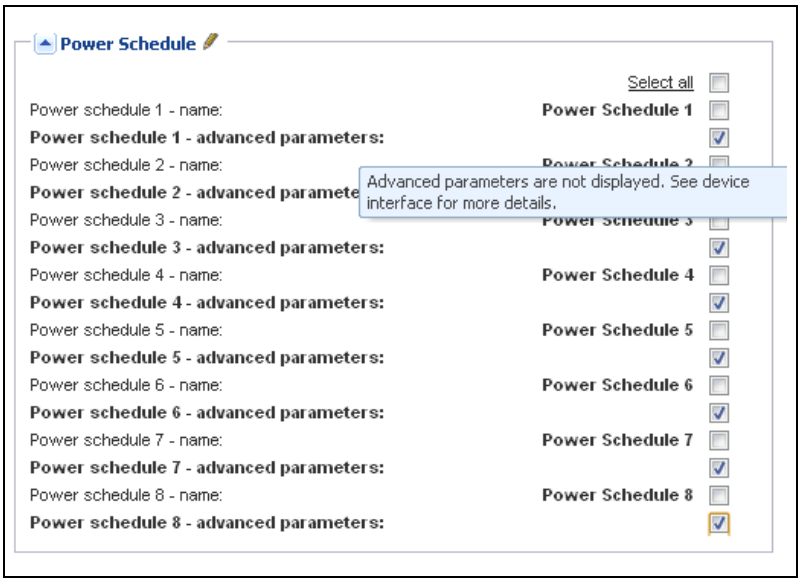


Figure 79. Advanced Parameters Not Displayed

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 (see Figure 80).
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 ≠ sign.
5. Select the check box associated with the parameters you want to synchronize.
6. Click **Synchronize**.

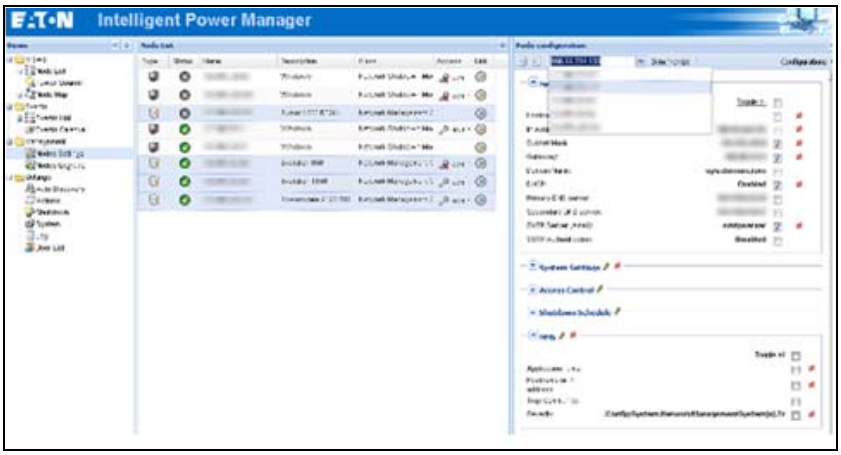


Figure 80. NMC Mass Configuration

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 (see Figure 81).
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.

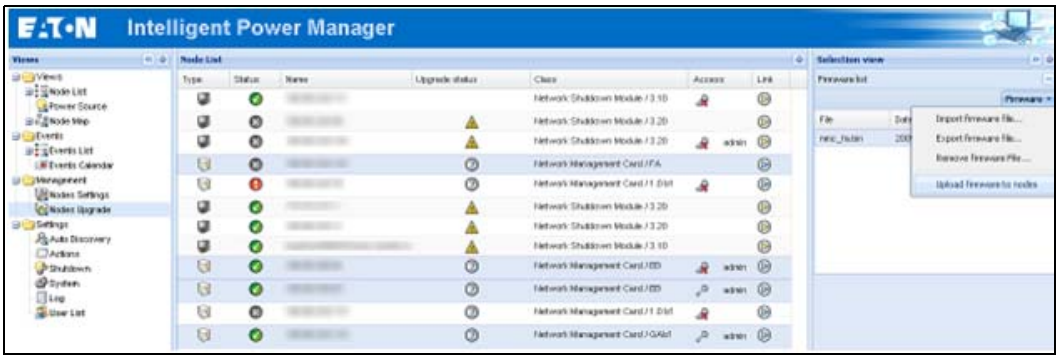


Figure 81. Management / Nodes Upgrade View 1

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 (see Figure 82).
3. From the Node List button , select **Set Login 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.

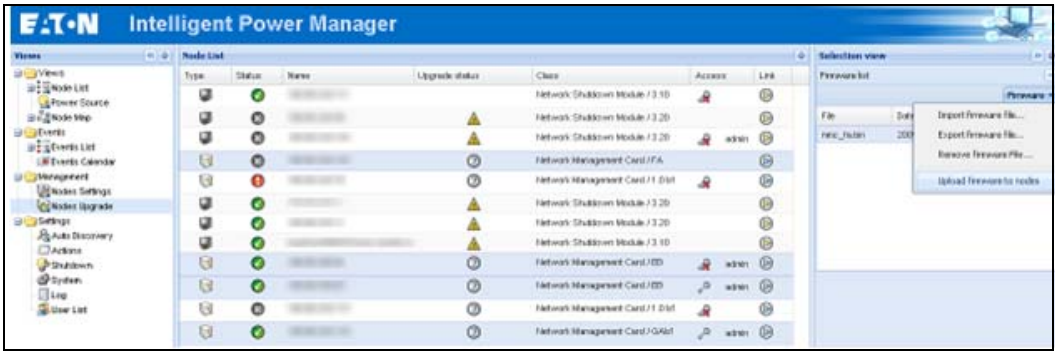


Figure 82. Management / Nodes Upgrade View 2

Chapter 7 Virtualization

The 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 virtualization products.

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.

Enabling the Infrastructure Connectors Module

To enable the Infrastructures 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 (see Figure 84).
2. Click **Edit modules settings** in the right panel. The Edit modules settings dialog box displays (see Figure 83).
3. Ensure that the **Infrastructure Connectors** checkbox is selected (checked).
4. Click **Save**.

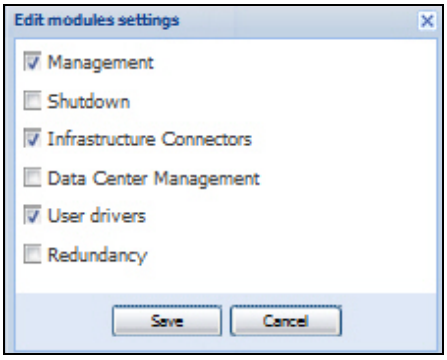


Figure 83. Enable Infrastructure Connectors Setting for Virtualization

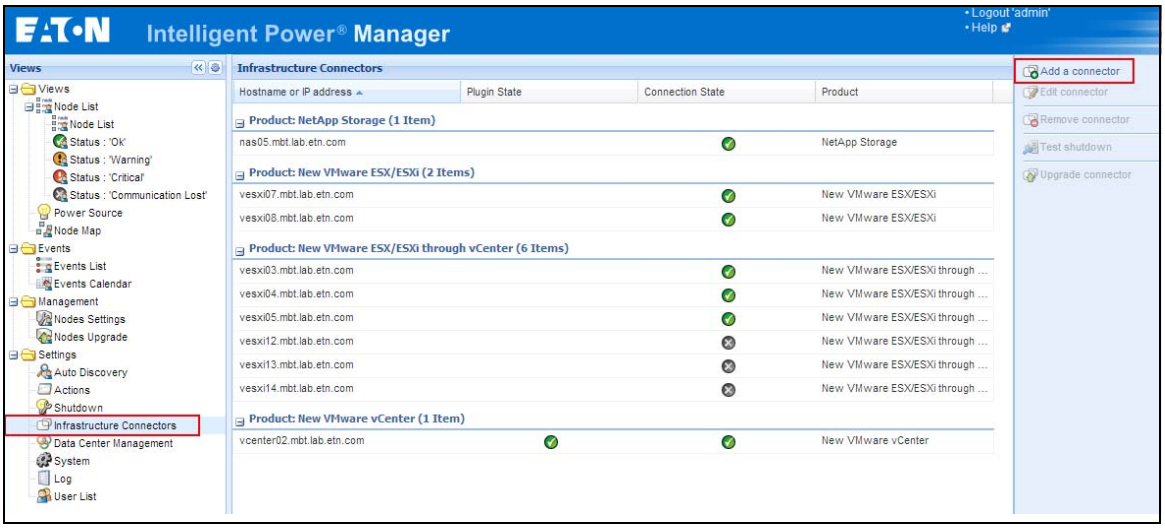


Figure 84. System Settings Page

When a user tries to add a connector by ***Settings->Infrastructure Connectors->Add a connector***, the sequence if screens show options available, depending of the JRE prerequisite (see Figure 85). The unselectable options are italic and grayed-out.

- If any JRE is not installed on the system hosting Eaton IPM, only legacy virtualization connectors can be selected (legacy for VMware), but new connectors cannot be selected (New VMware vCenter, New VMware ESX/ESXi, NetApp Storage, or Cisco UCS Manager).
- If a JRE is installed on the system hosting Eaton IPM, new infrastructure connectors are available (see "JRE Prerequisites" on page 10).

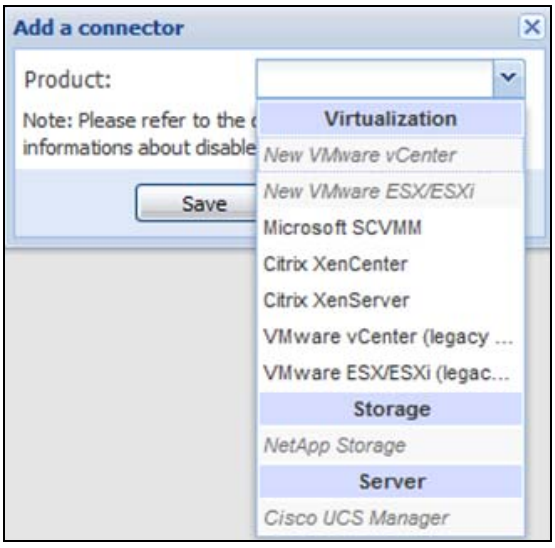


Figure 85. Selectable and Non-selectable Connectors

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 86.

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

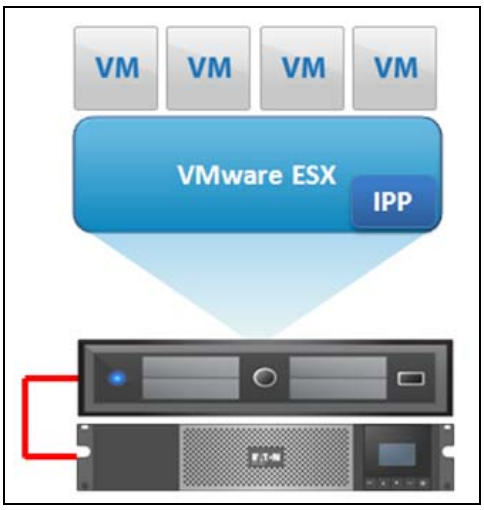


Figure 86. Eaton IPP Running on ESX Server

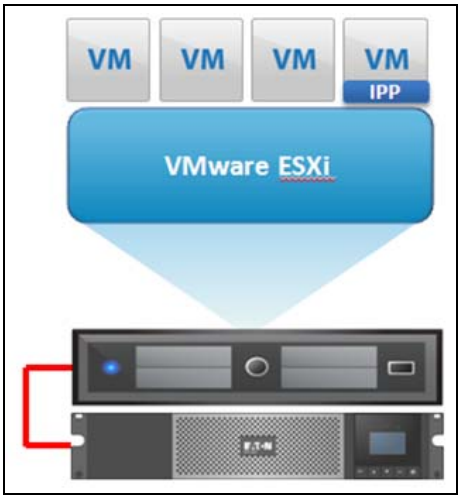


Figure 87. Eaton IPP Running on vMA

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 88and Figure 89.

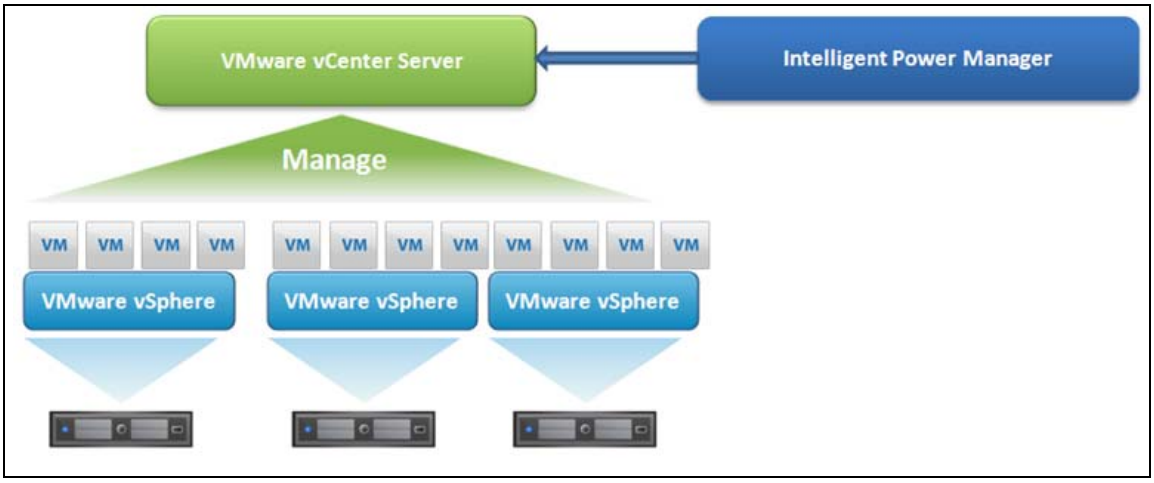


Figure 88. Eaton IPM Connected to vCenter to Protect VMware Infrastructure

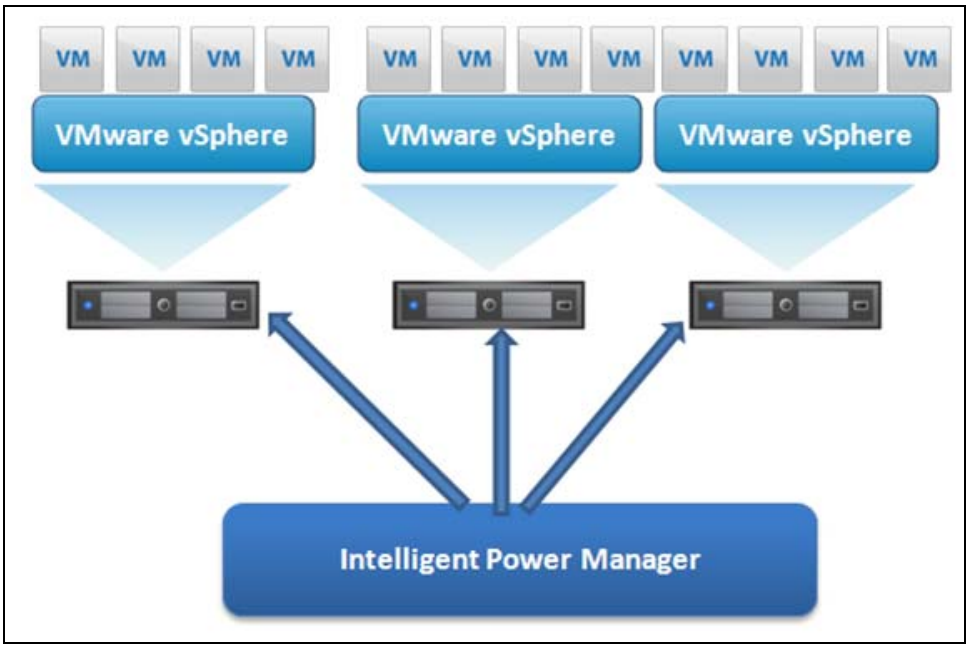


Figure 89. Eaton IPM Connected to ESX/ESXi to Protect VMware Infrastructure (Without vCenter)

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 network.

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

NOTE Since IPM version 1.25, vSphere SDK for Perl is no longer required.

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
- 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 90):

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.

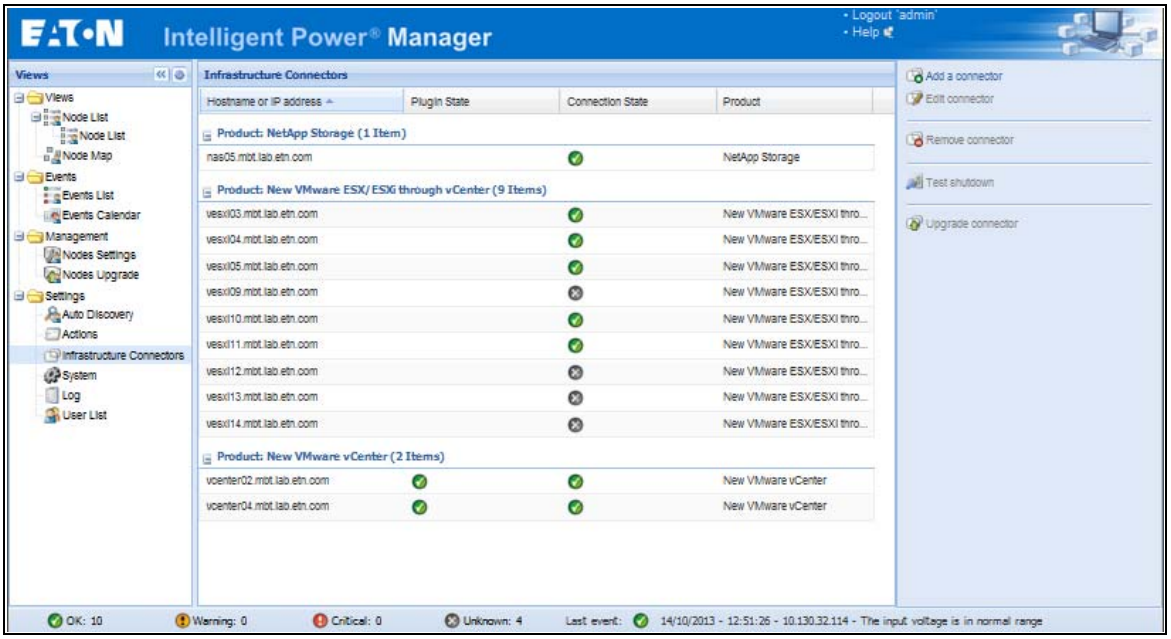


Figure 90. Infrastructure Connectors Page

Adding a vCenter Server Manager

To add a new VMware vCenter:

1. From the Add a Connector dialog, select New VMware vCenter from the Product drop-down list (see Figure 91). A second Add a connector dialog displays for your product connector selection.

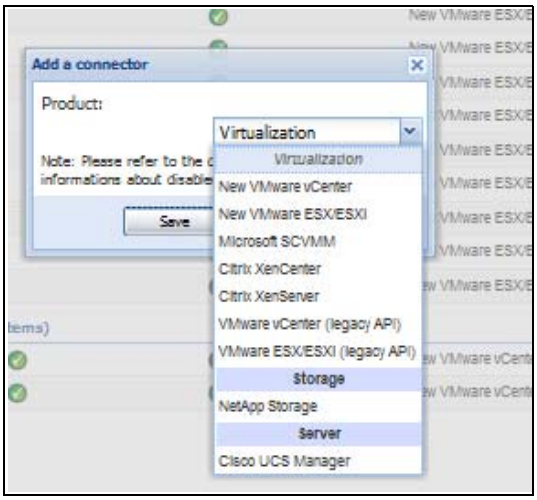


Figure 91. Add a Connector Product Selection Dialog

2. Add identification information for the selected connector (see Figure 92).
   - **Product:** Select New VMware vCenter from the drop-down list
   - **Hostname or IP address:** Type VMware vCenter Hostname 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 Plugin and WebPlugin" on page 125 when using this feature.

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

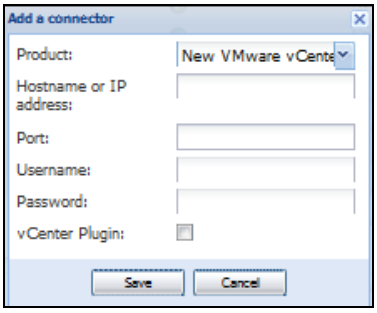


Figure 92. Add VMware vCenter

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. In both cases, the encrypted password is stored in Eaton IPM and never again sent on the Client side.

Adding a VMware ESX/ESXi Hypervisor List

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

To add a new 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 93)
   - **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.

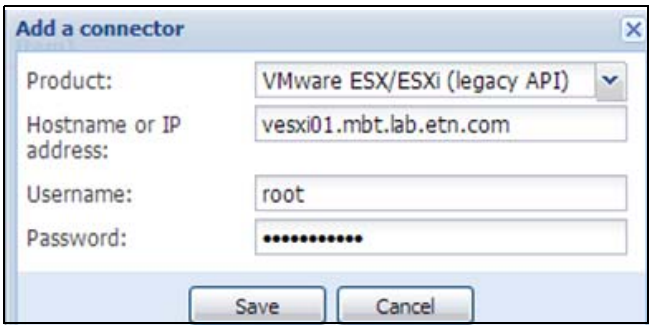


Figure 93. Add VMware ESX/ESX)

VMware Site Recovery Manager

Eaton developed a package to allow the connection between the Power and VMware Site Recovery Manager (SRM):
http:\\pqsoftware.eaton.com\\install\\win32\\ipm\\UserGuide_VMWareSiteRecoveryManagerIPM.pdf

This package 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.
- **Unattended execution of recovery plan before server crash:** SRM with IPM provide 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.

VMware LoadShedding Package

During utility failure, load shedding can reduce the effective runtime of highly critical devices because battery capacity is limited. Eaton has developed a package to allow you to perform load shedding in your VMware Data Center. The Eaton LoadShedding package provides a process of closing or shutting down less critical load so that remaining capacity can be used for highly critical loads. These modules have a simple GUI to set priority to the VMs and allow you to configure the time to shutdown /suspend the VMs of every priority.

Refer to the LoadShedding User Guide at the following location:
http://pqsoftware.eaton.com/install/win32/ipm/eaton_load_shedding_for_ipm_users_guide_en.pdf

Eaton Solutions for Microsoft

For Microsoft, Eaton IPM provides two solution architectures that are illustrated in Figure 94 and Figure 95. 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 94.

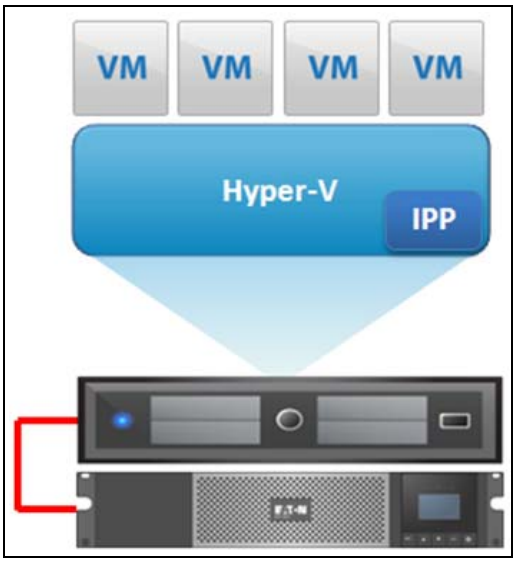


Figure 94. Eaton IPP Running on Hyper-V to Protect Hyper-V

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). This solution is ideal for large infrastructures working through an SCVMM server.

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*.

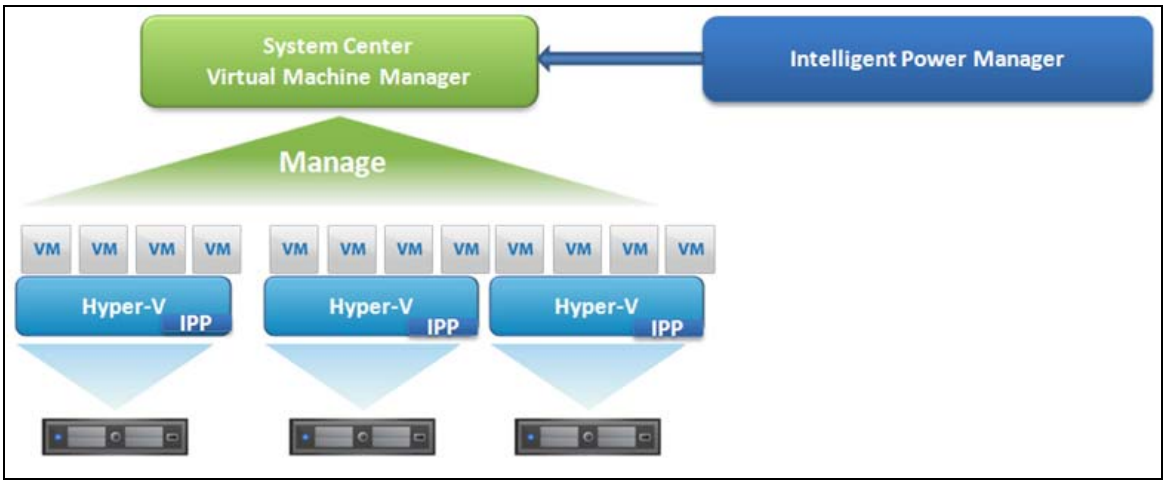


Figure 95. Eaton IPM Connected to SCVMM to Protect Microsoft Virtual Infrastructure

Prerequisites

The virtualization module requires following prerequisites:

- The Powershell Snapin 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 96 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.

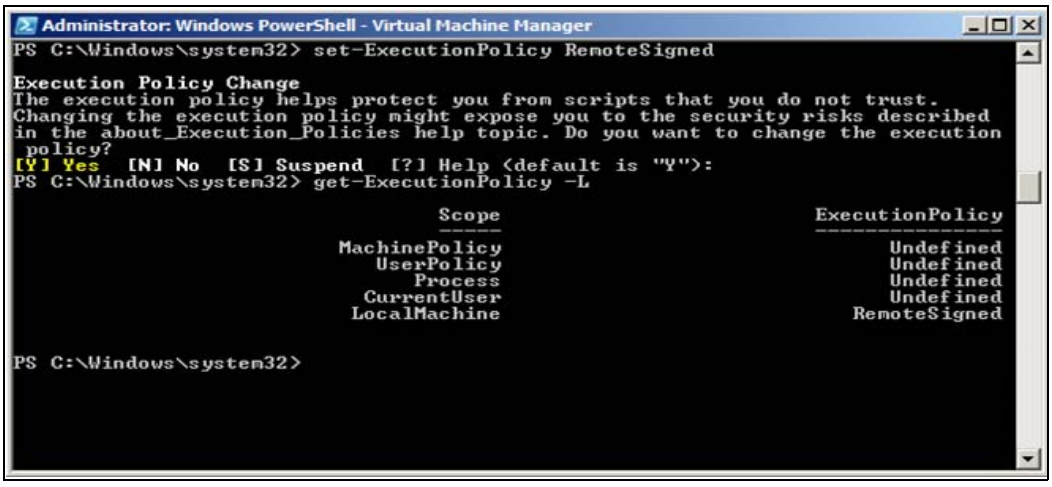


Figure 96. Windows PowerShell - Virtual Machine Manager

Adding an SCVMM Manager

To add a new Microsoft SCVMM (see Figure 97):

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 93)
   - **Product:** Microsoft SCVMM is 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.

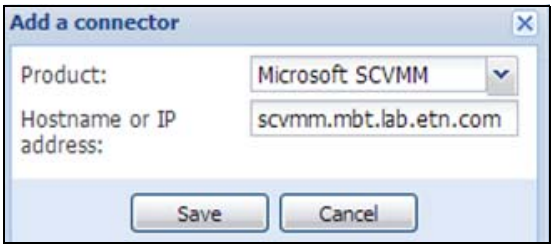


Figure 97. Add Microsoft SCVMM

Eaton Solutions for Citrix

For Citrix, Eaton IPM provides two solution architectures that are illustrated in Figure 98 and Figure 99. 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 98.

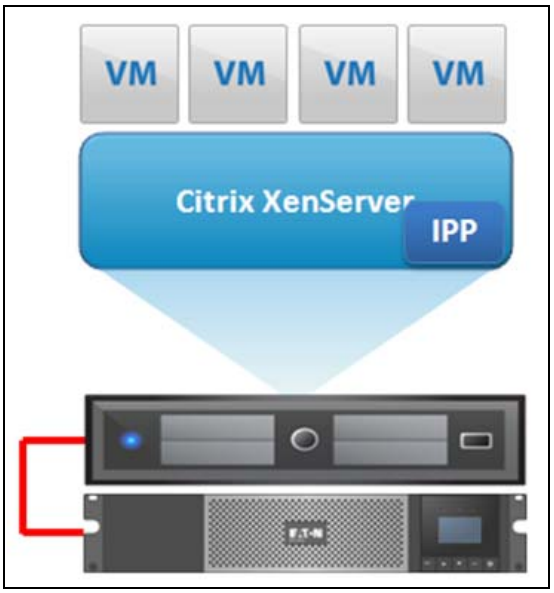


Figure 98. Eaton IPP Running on Citrix XenServer

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 Xen Center.

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

- Xen server remote maintenance to trigger VM Xen Motion
- Xen server remote shutdown

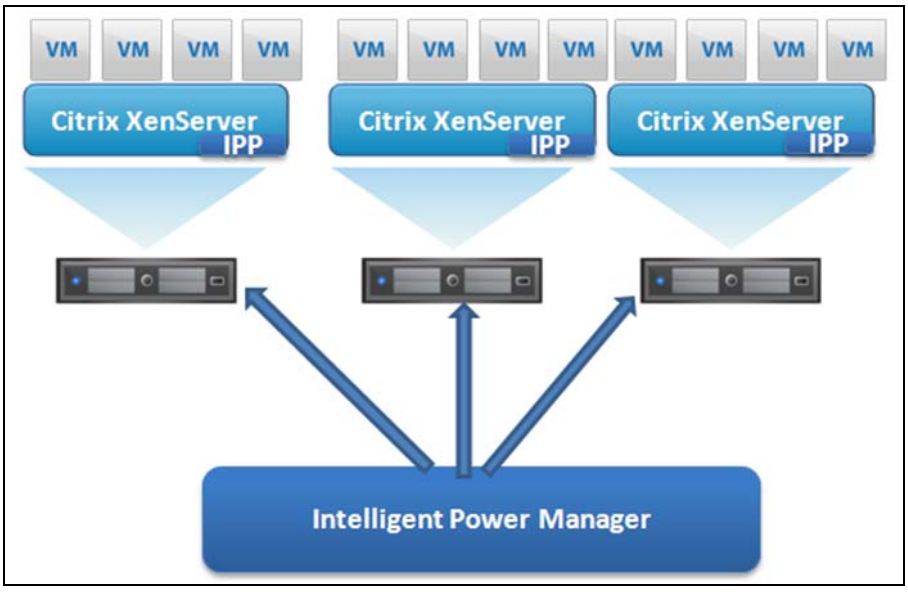


Figure 99. Eaton IPM Connected to XenServers (Triggers XenMotion and Eaton IPP Running on XenServer Infrastructure)

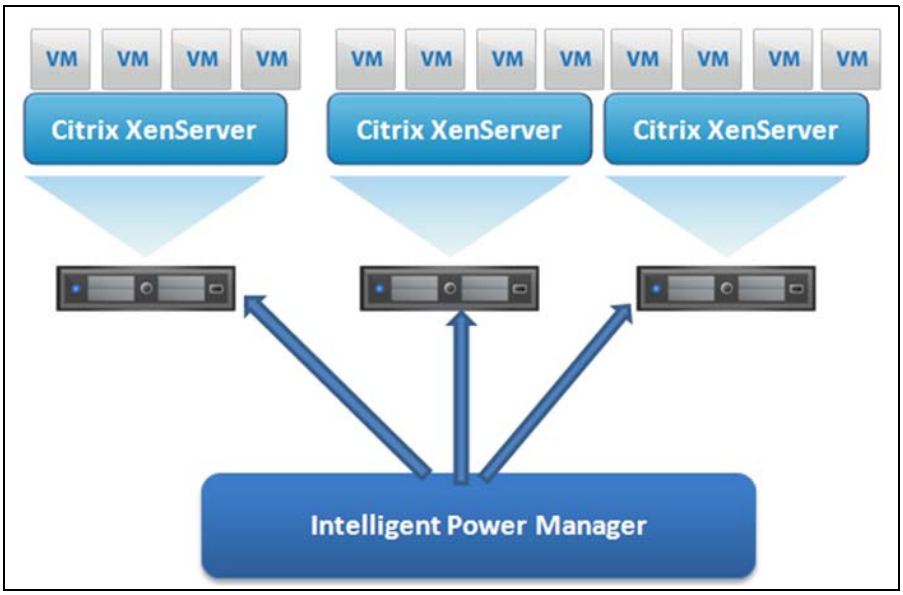


Figure 100. Eaton IPM Connected To XenServer to protect the XenServers

Prerequisites

The virtualization module requires 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 101):
   - **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 101. 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 102). 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 101):
   - **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.

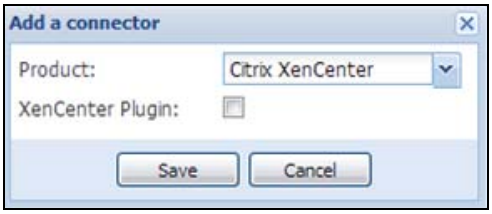


Figure 102. Add Citrix XenCenter

Eaton Solution for Red Hat

For Red Hat®, the Eaton IPM provides the solution architecture illustrated in Figure 103. 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*.

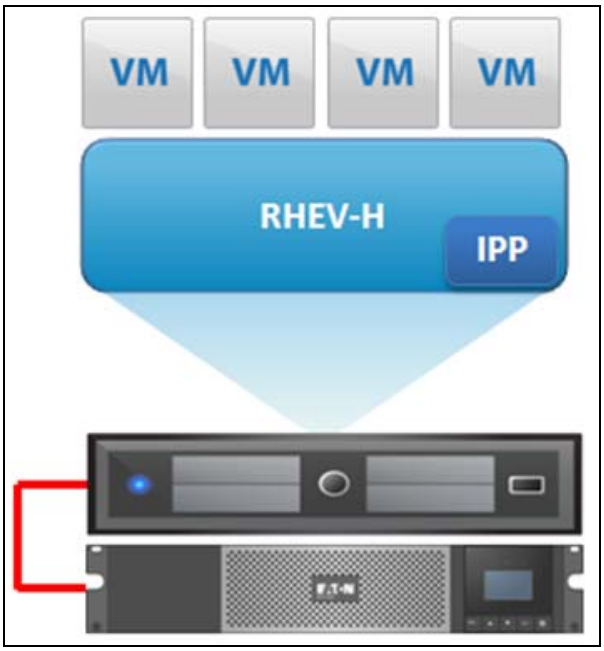


Figure 103. Standalone Hypervisor and Local Solution

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 104. 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 Xen Center.

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*.

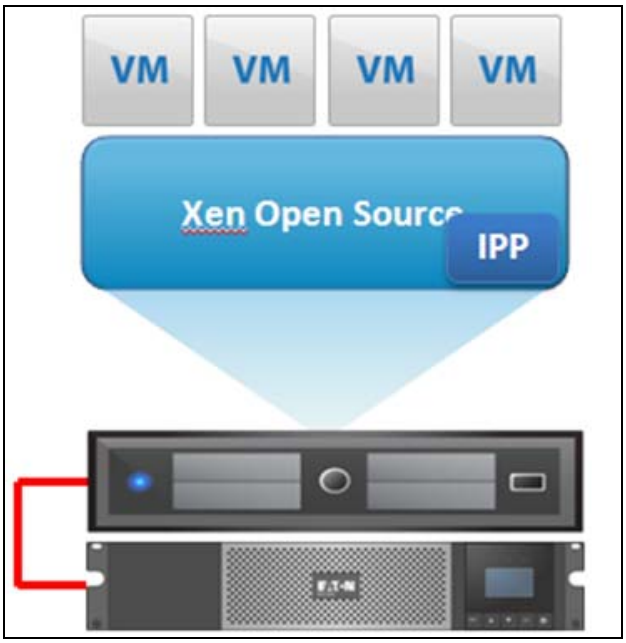


Figure 104. Need Title

Configuring Hypervisors

Descriptions of two methods for configuring Hypervisors follow (see "Adding Infrastructure Connectors" on page 82).

- 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 SCVMM).
  - 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" on page 93).
- 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 creates two different types of nodes (you can see the new node in the Node List).
  - 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" on page 93).

Configuring Maintenance and Shutdown

After you enter the correct credential information for your Managers and Hypervisors, you need to 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

No Eaton IPP on VM Host

If no Eaton IPP is installed on the server that is hosting the Hypervisor (VMHost), the Shutdown is performed remotely by IPM. This shutdown configuration is used only with VMware Hypervisors and Citrix XenServer.

To configure the node and add a Power Source in the Shutdown Settings dialog:

1. From the ***Management > Nodes Settings*** menu item, click the host in the Nodes list (see "Nodes Settings" on page 71).

2. In the Shutdown Settings panel on the right side of the page, select the applicable checkboxes to configure the required parameters (see Figure 105 and Table 10).

NOTE The shutdown settings that display vary depending on the node you select. In this example, the node functionalities include remote maintenance mode and remote shutdown.

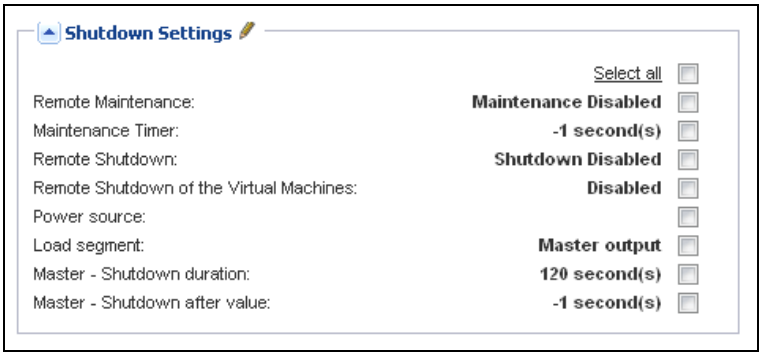


Figure 105. Example Shutdown Settings - Before Configuration

Table 10. Shutdown Settings for VMhost without Eaton IPP

Parameters	Values	Description
Remote Maintenance	Enabled or Disabled	When enabled, the Eaton IPM client sets the host to "Maintenance Mode." Depending on your host/cluster configuration, this can trigger vMotion/live migration to another host. This event is triggered at the time set in the "Maintenance Timer" parameter.
Maintenance Timer	User to 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 timer is disabled.
Remote Shutdown	Enabled or Disabled	When enabled, this setting allows Eaton IPM to gracefully shutdown this server in case of "UPS on battery state" and Shutdown criteria reached.
Remote Shutdown of the Virtual Machines	Enabled or Disabled	When enabled, this allows the Eaton IPM to shut down the VMs.
Power Source	IP address of UPS	This parameter identifies the UPS powering this server. This node must already exist in Eaton IPM.

Table 10. Shutdown Settings for VMhost without Eaton IPP(Continued)

Parameters	Values	Description
Load Segment	Master Load Segment 1 Load Segment 2	This parameter identifies the UPS load segment powering the server.
Master - Shutdown Duration	User to type a value	This server shutdown criteria defines the time needed for graceful host shutdown.
Master - Shutdown After Value	User to type a value	This server shutdown criteria defines the time elapsed "on battery state" before graceful Shutdown. This timer must be greater than the maintenance timer.
NOTE	Shutdown settings that display vary depending on the node you select.	

Figure 106 illustrates an example of the Shutdown Settings Dialog after configuration.

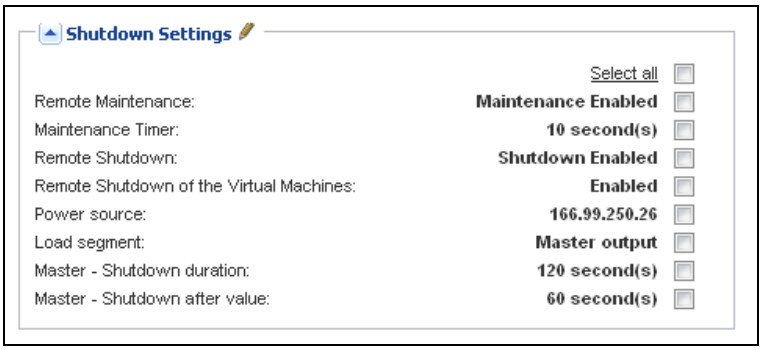


Figure 106. Example Shutdown Settings - After Configuration

NOTE Maintenance and shutdown information:

- See "Nodes Settings" on page 71 to use the configuration interface.
- The Remote Shutdown functionality is reserved for VMware ESX/ESXi and Citrix XenServer nodes. (Microsoft HyperV benefits from local IPP shutdown).
- The Remote Shutdown of VMs is supported on VMware ESX/ESXi.
- The Maintenance Timer must be less than the Shutdown after value.

Eaton IPP Running on the VMHost

If Eaton IPP is installed on the server that is hosting the Hypervisor (VMHost), 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" on page 71 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" on page 71).

2. In the Shutdown Settings panel on the right side of the page, select the applicable checkboxes to configure the required parameters (see Figure 105 and Table 10).

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.

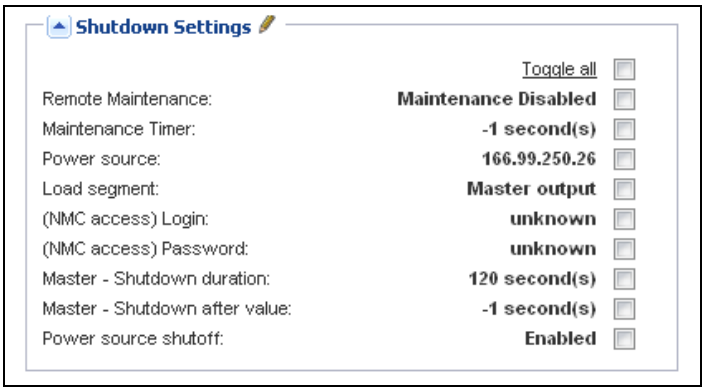


Figure 107. Shutdown Settings for VM Host with

Table 11. 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 timer is disabled. See "Configuring Maintenance Mode and vMotion with vCenter" on page 130 and "Configuring Maintenance Mode and Live Migration with SCVMM" on page 133 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 server shutdown criteria defines the time needed for graceful host shutdown.
Master - Shutdown After Value	Type a value	This server shutdown criteria 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 right node type and retrieves both the VM Host information and the Eaton IPP information.

Chapter 8 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 108). 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 shutdown a remote server linked to the composite device through the infrastructure connector feature.

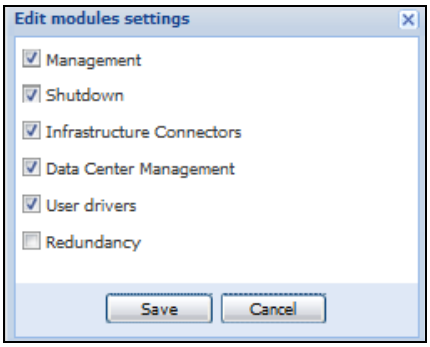


Figure 108. Edit Modules Settings Dialog Box

Electrical Redundancy Schemas

Figure 109 to Figure 112 illustrate the electrical redundancy topologies.

- **Redundant supplies (such as dual feeds or triple feeds):** Figure 109 illustrates a scenario when two UPSs provide power on one or several multiple-feed servers.

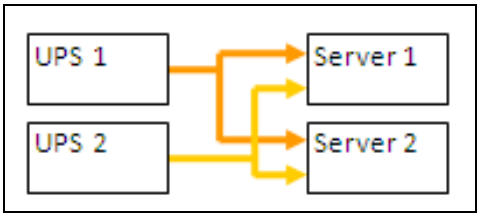


Figure 109. Redundant Supplies

- **Hot standby mode:** When the upstream UPS powers the load, the downstream UPS is on bypass.

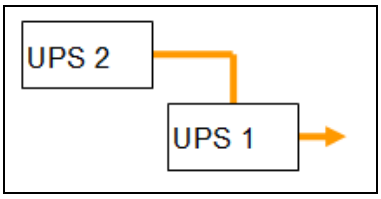


Figure 110. Hot Standby

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

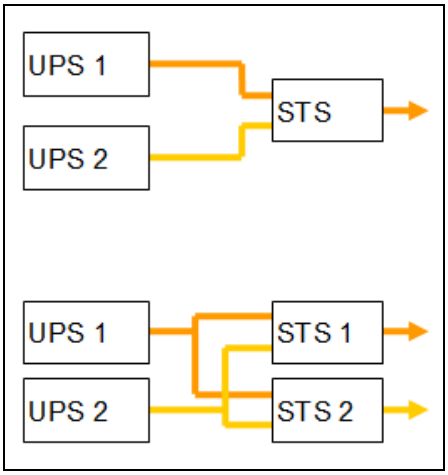


Figure 111. Static Transfer Switch

- **Parallel for two or more components:** All the UPSs power the load at the same time.

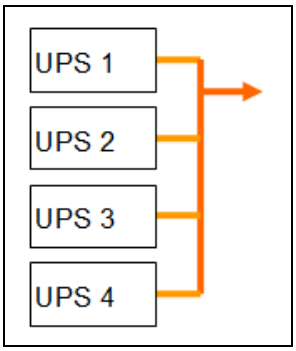


Figure 112. Parallel Redundancy Schema

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 113).

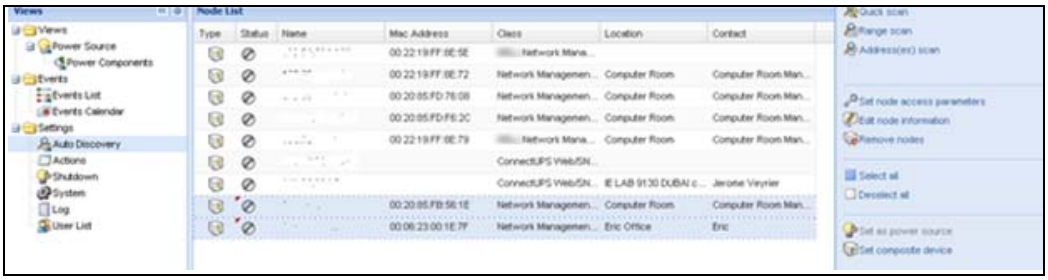


Figure 113. Selecting Set Composite Device for Nodes

5. In the dialog box, specify a device name, redundancy mode, and level (see Figure 114):
   - **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.

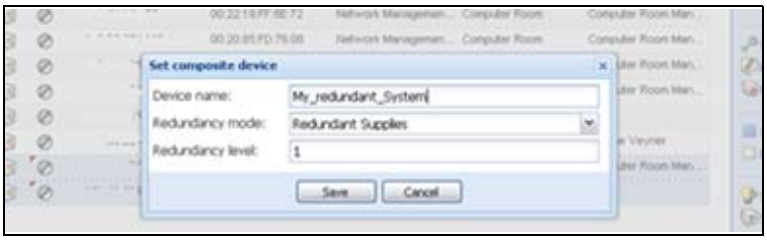


Figure 114. Set Composite Device Dialog Box

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

Actions you can perform on the new node are as follows (see Figure 113):

To select the new node as the power source:

1. Select the new node in the discovery view.
2. Click the **Set as power source** button in the right panel.

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

To Edit composite device properties.

1. Select the new node in the discovery view
2. Click the **Set composite device** button in the right panel.

To retrieve properties of an existing composite device:

1. Select components of a composite device.
2. 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 following information (see Figure 115):

- **Information panel and Status panel**: Displays composite device settings
- **Events panel**: Displays events from the composite devices and all related child components
- **Power components panel**: Displays component states, including load level and battery run time

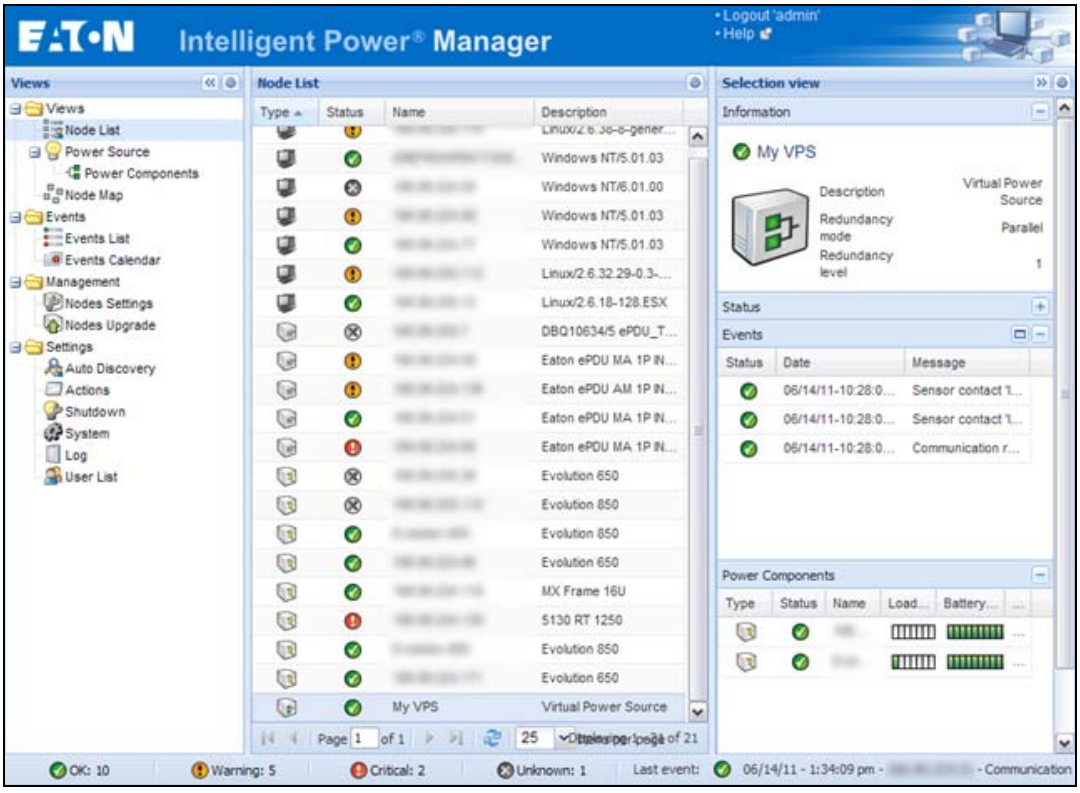


Figure 115. Virtual Power Source Selection View

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 116).

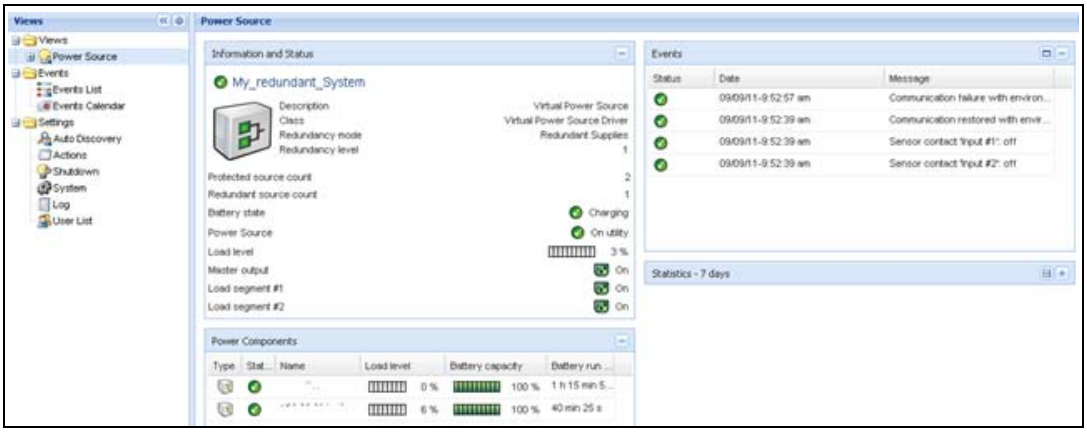


Figure 116. Composite Device Power Source View

Power Components Sub-view

When redundancy and shutdown modules are activated, a new power component view is also available as a sub-view 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 display properties of the power component selected in the Node List (see Figure 117).

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

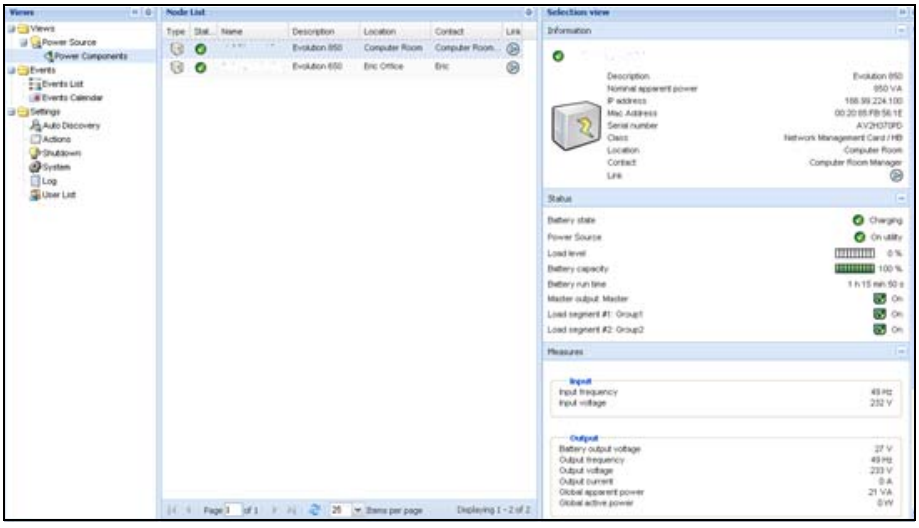


Figure 117. Power Components Sub-view

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 118).
- For Network-MS (example, 66102/103006826) and Modbus-MS (example, 66103), the default configuration for the Network Management Card shutdown configuration is available from ***UPS > Shutdown Parameters*** (see Figure 119).
- For ConnectUPS-X Slot or ConnectUPS-BD network cards, the Network Management Card default shutdown configuration is available from ***Configuration > UPS Shutdown and Restart Settings*** (see Figure 120).

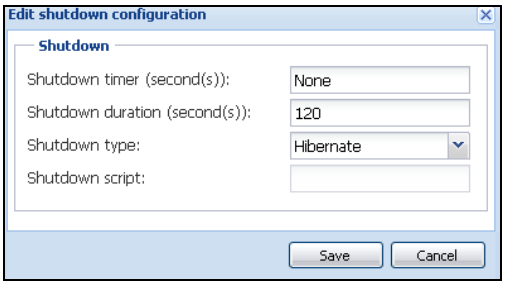


Figure 118. Edit Shutdown Configuration Dialog Box

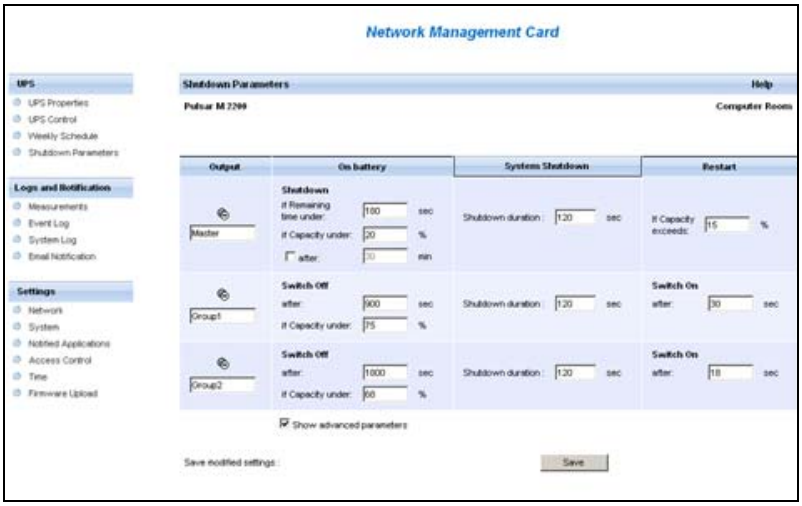


Figure 119. Network Management Card Web Interface

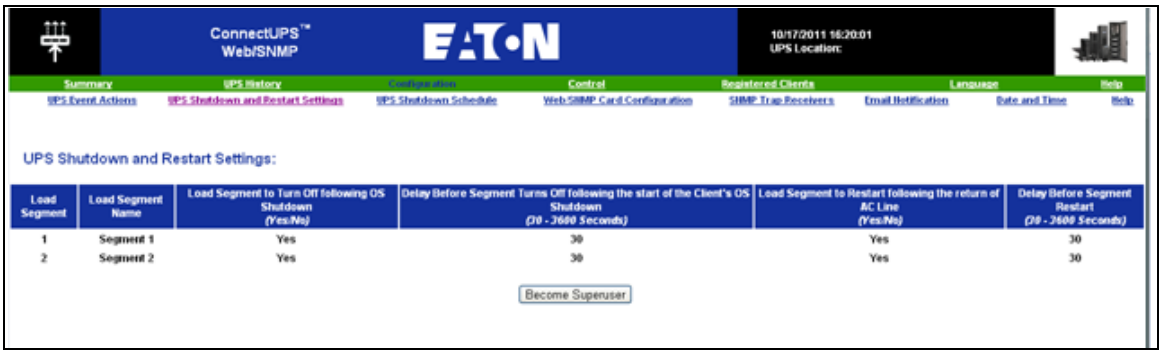


Figure 120. UPS Shutdown and Restart Settings

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 121).
- In this case, each server can have its own shutdown timer (10 min, 8 min, 6 min…). 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 102).

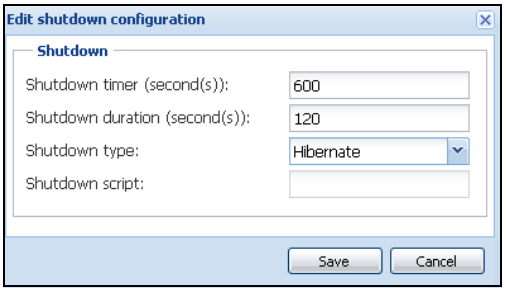


Figure 121. Edit Shutdown Configuration Dialog Box

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 122).
- For ConnectUPS-X Slot or ConnectUPS-BD network cards, the NMC default shutdown configuration is available from ***Configuration > UPS Shutdown and Restart Settings*** (see Figure 120)
- 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.

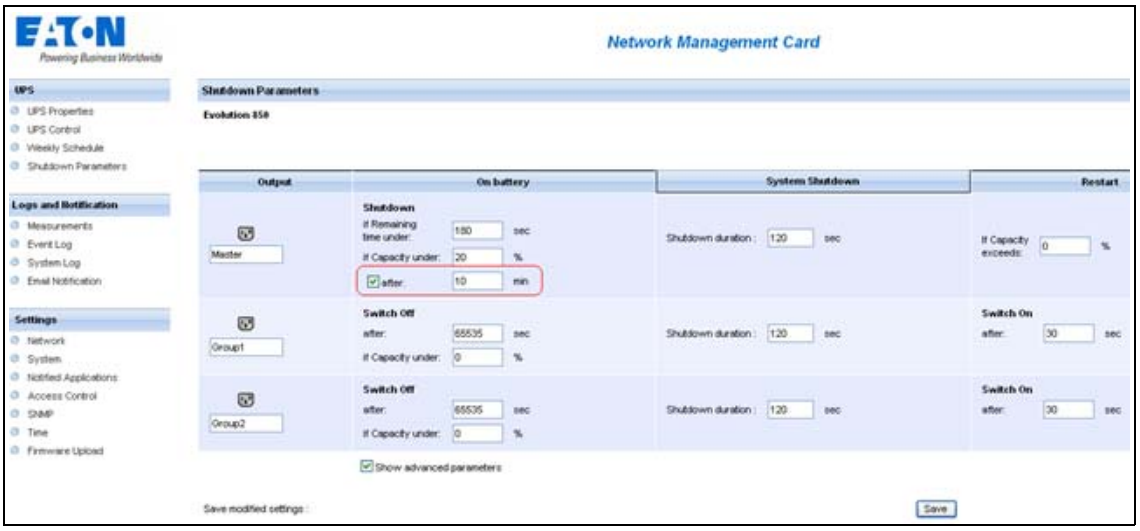


Figure 122. Network Management Card Shutdown Parameters

Figure 123. 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 124).
- 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").

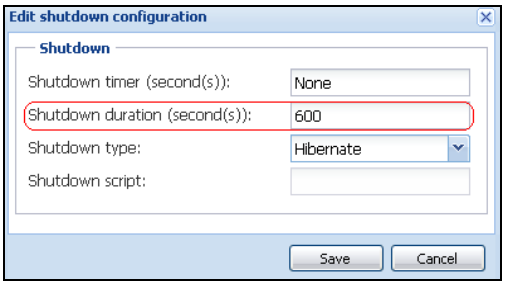


Figure 124. Edit Shutdown Configuration Dialog Box

- You must use the default Network Card Configuration. See "Use Case #1" on page 102 for more details.

Redundancy Advanced Behavior Example

For 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.

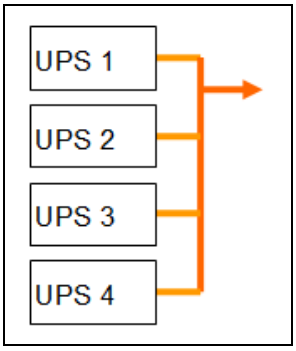


Figure 125. Example Topology

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 12 provides redundancy alarm management details.

Table 12. 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 13 provides protection alarm management details.

Table 13. 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 14 provides a compatibility list for single-phase UPSs and Table 15 provides a compatibility list for three-phase UPSs.

Table 14. 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

NOTE 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 15. 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

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

Chapter 9 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, nodes already discovered 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$^{t®}$ / SNMP: Manages the SNMP Buffalo Network Attached Storage (NAS)
- NAS HP / SNMP: Manages the SNMP HP 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

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 126).

The User drivers editor page displays.

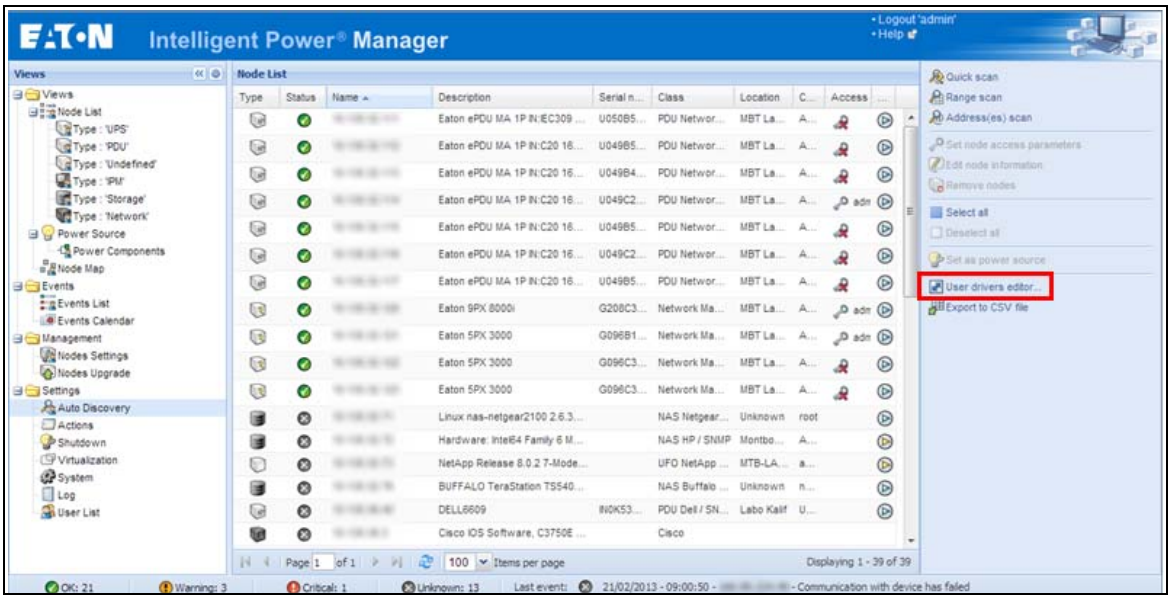


Figure 126. User Drivers Editor Selection

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 127).

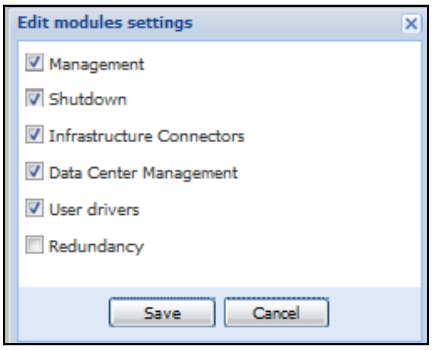


Figure 127. Enable or Disable User Drivers

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 128 illustrates the User drivers editor dialog.

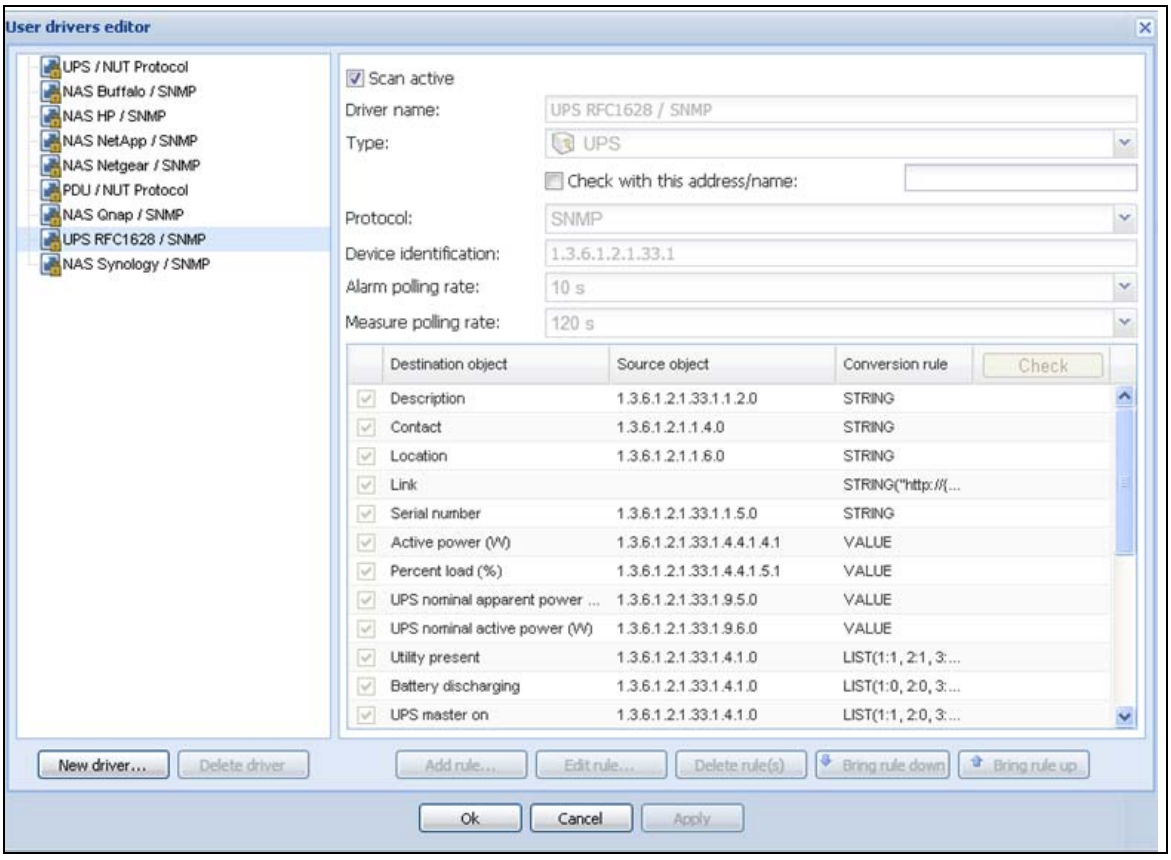


Figure 128. User Drivers Editor Dialog

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 check box 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 113 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 129 illustrates the Rule editor dialog.

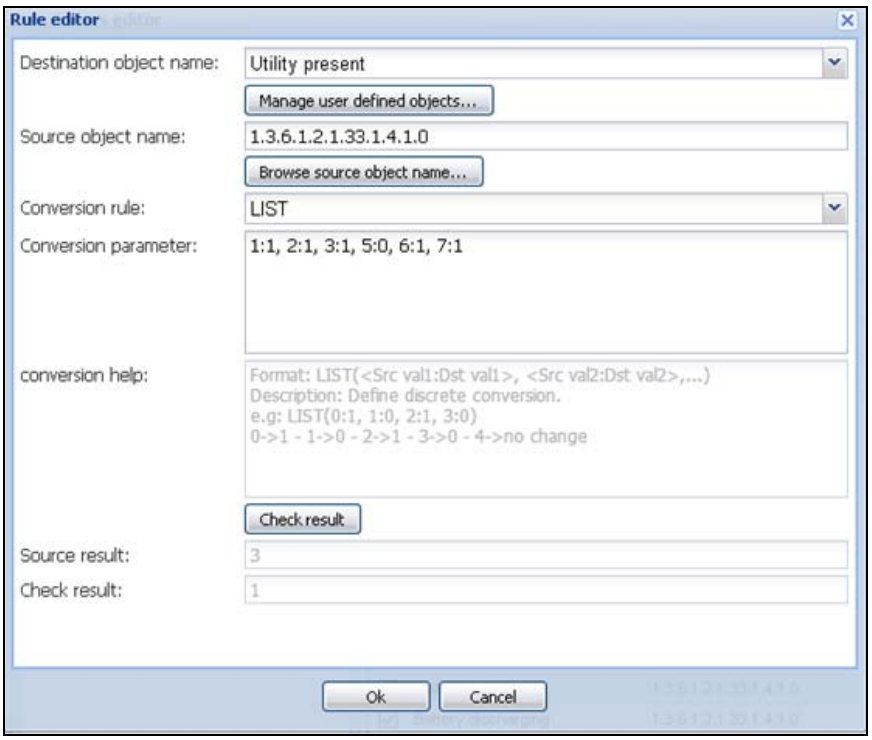


Figure 129. Rule Editor Dialog

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 address or the 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 16.
- Select a specific user-defined object when the needed object is not defined in the standard object list.

Table 16 lists the standard objects used by the Eaton IPM.

Table 16. 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	Environment humidity alarm
Contact	UPS overload	UPS input frequency (Hz)	UPS outlet #1 on	Battery low	Environment temperature alarm
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)	Environment temperature (°C)
Platform	Automatic bypass in tolerance		UPS output voltage (V)		Environment humidity (%)
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		
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)		

Table 16. Standard Objects (Continued)

Information	Status	Input	Output	Battery	Environment
	Communication error		PDU outlet [x] power factor		
	Overload warning				
	Percent load (%)				

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 130 illustrates the User defined object editor dialog.

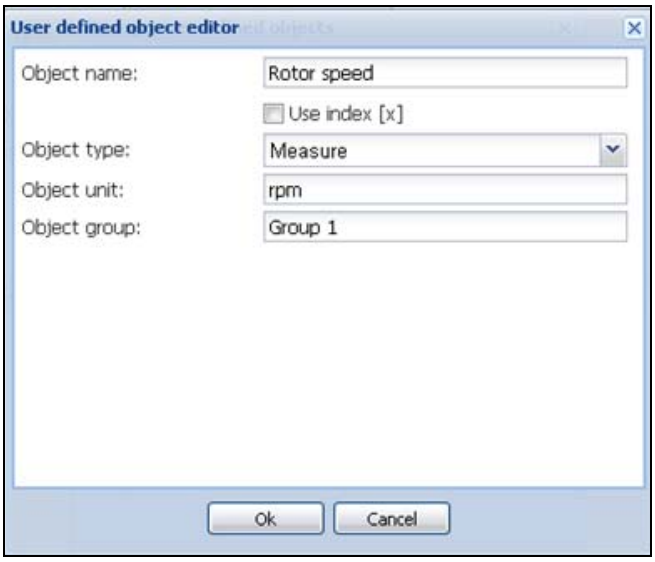


Figure 130. User Defined Object Editor

IMPORTANT

- The user-defined objects only display in a specific Node view panel named Other data (see Figure 131). 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 16).
- 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 131. 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 17 provides a list of conversion rules.

Table 17. 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 17. 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 10 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 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 111). After performing a Range scan, you will have a list of storage managed by Eaton IPM.

Enabling the Infrastructure Connectors Module

To enable the Infrastructures 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 (see Figure 133).
2. Click **Edit modules settings** in the right panel. The Edit modules settings dialog box displays (see Figure 132).
3. Ensure that the **Infrastructure Connectors** checkbox is selected (checked).
4. Click **Save**.

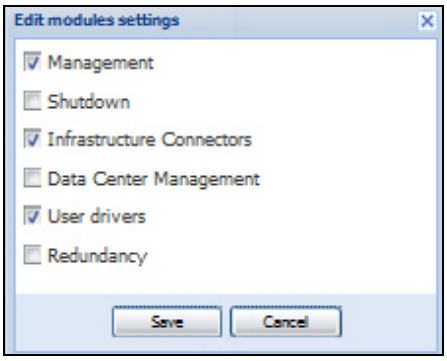


Figure 132. Enable Infrastructure Connectors Setting for Virtualization

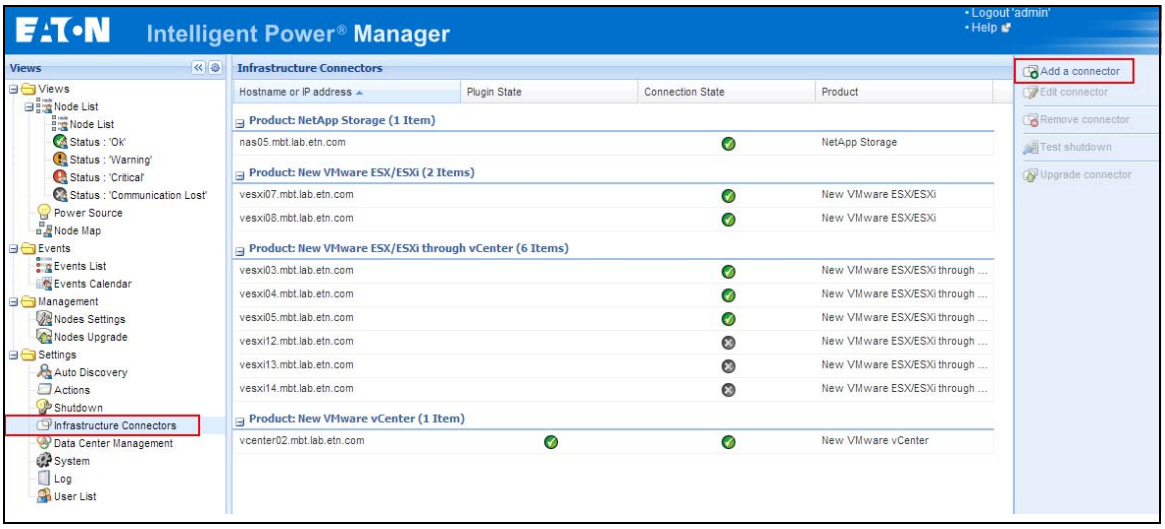


Figure 133. System Settings Page

5. Add identification information for the selected connector (see Figure 134).
   - **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
6. Click **Save** after the fields are updated.

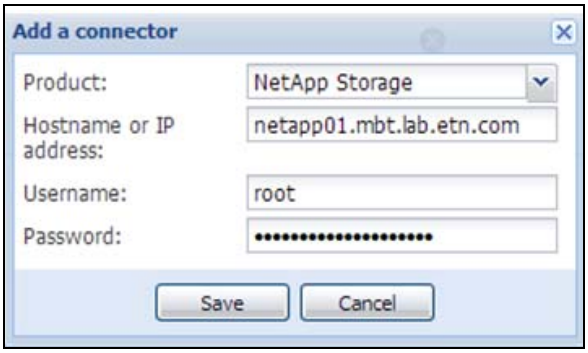


Figure 134. Add NetApp

Configuration

You can configure the node and add a Power Source in the Node Configuration Panel (see).

Figure 135. Node Configuration Panel

1. Check (select) a checkbox to identify this settings you would like change.
2. Add identification information for the selected settings.
   - **Power Source:** The UPS powering this server. This node should exist in IPM. Type the IP address of the UPS.
   - **Load Segment:** UPS load segment powering the server. The the Master Load Segment 1 and 2.
   - **Master Shutdown Duration**: This is a Server Shutdown criteria is the time needed for the server to shutdown gracefully. Type a value.
   - **Master Shutdown After Value:** This is a Server Shutdown criteria is the time elapsed "on battery state" before graceful Shutdown. This timer must be greater than the maintenance timer. "-1" value means that timer is disabled. Type a value.
3. Click **Save** after the fields are updated.

Shutdown

IPM can manage the remote shutdown for NETAPP devices. To enable this feature, you must apply a specific configuration. Refer to the following document:
http://pqsoftware.eaton.com/install/common/nas_ups_user_doc_aa.pdf

In addition, put the netapp_shutdown.ppk file in the following folder:
<Eaton install directory>\configs\scripts

After this configuration is completed, you can configure the power source of your storage and perform the following steps:

1. From ***Start > Programs > Eaton > Intelligent Power Manager***, select Open Eaton Intelligent Power Manager to start the main Eaton IPM graphical interface.
2. Select the ***Settings > Auto Discovery*** menu item.
3. In the Node List, double-click the storage device name (node). The Edit node information dialog displays
4. In the User note field, type the following:
   `<upsHostName>;<shutdownTimer>;<shutdownDuration>`

   where:
   - **<upsHostName>**: UPS hostname attached to the storage
   - **<shutdownTimer>**: Only used when the UPS is on battery (utility lost). Storage device shutdown will complete in this amount of time after the UPS is on battery
   - **<shutdownDuration>**: Time needed for the storage device to stop gracefully

   Example:

   `ups_1;300;120`

When the ups_1 in on battery, the storage (netApp_1) will be shut off 300 seconds after the UPS loses utility power.

5. Activate your user script (<Eaton install directory>configs\scripts\ netapp_shutdown.js) by the entering the following:

   `UserScript. enabled: false, to UserScript. enabled: true`

6. To activate the user trace (print information in the debug console and in the NetAppShutdown.log file), set `UserData.print = false`
   - to -
   `UserData.print = true`.

7. Restart the service to apply the NetApp shutdown feature.

IMPORTANT

- The access settings for <upsHostName> should be correctly set to enable communication with the storage.
- Because the Eaton IPM manages the shutdown of the NETAPP storage, it must be the last to shut down. Therefore, the Eaton IPM shutdown timer setting must be greater than the shutdown timer setting for the storage. (The IPM shutdown timer is configured from ***Settings > Shutdown > Edit Shutdown Configuration***.)
- The first time the Secure Shell (SSH) function is called to shut down the NETAPP server, the Eaton IPM automatically accepts the public key.

Chapter 11 Extended Functionality

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

- Configuring the Eaton IPM vCenter Plugin
- 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 Plugin and WebPlugin

The VMware® vCenter Server platform forms the foundation for virtualization management. It provides management of hosts and virtual machines (VM) 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 (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 136).
2. Locate the Eaton IPM Plug-in for vCenter in the Plug-in Manager (see Figure 137).

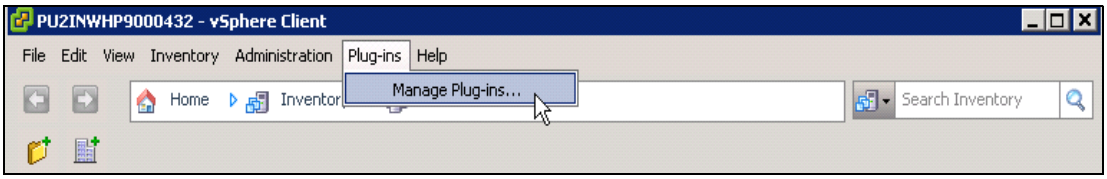


Figure 136. vSphere Client - Manage Plug-in Menu

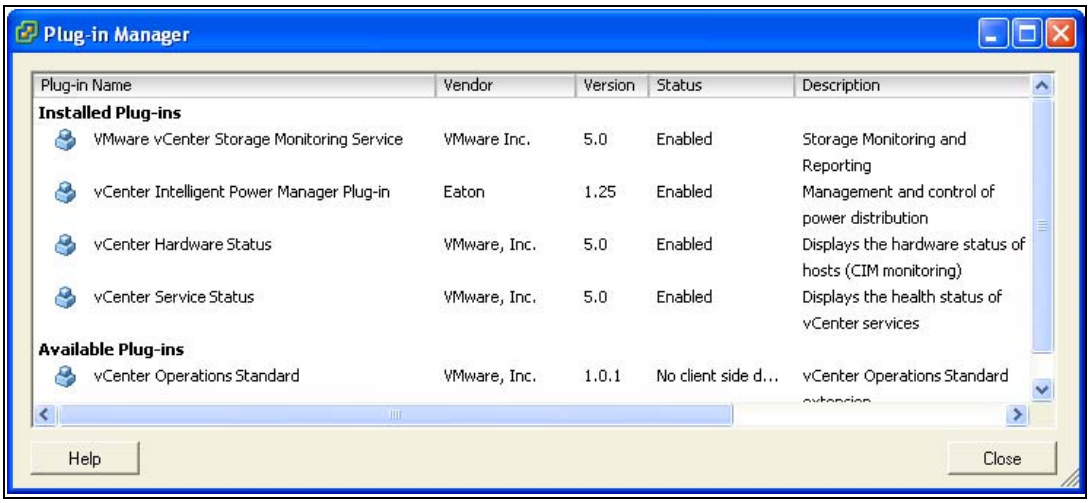


Figure 137. vCenter Plug-in Manager

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 138).

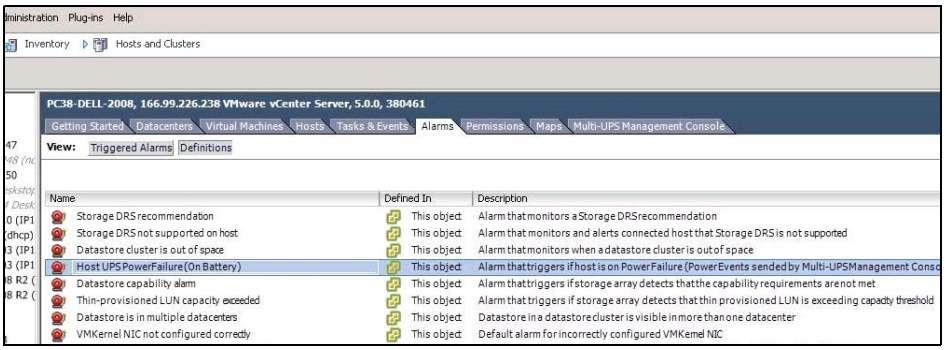


Figure 138. vCenter New Alarm from Eaton IPM

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 139).

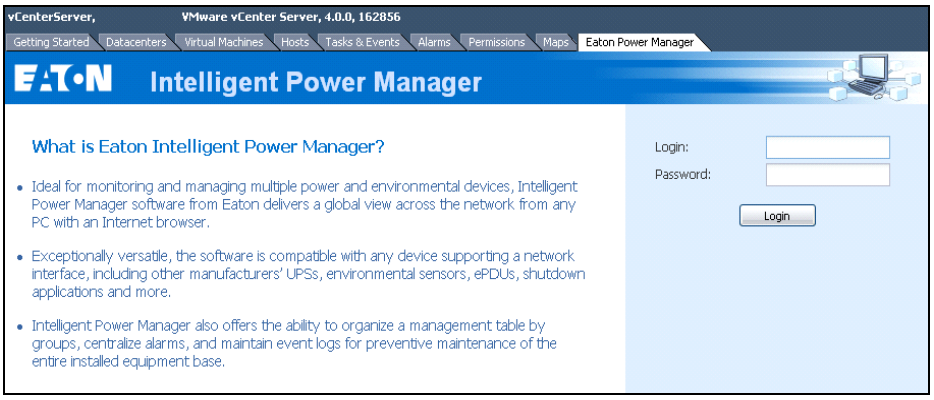


Figure 139. vCenter Server Console

Using the WebPlugin 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 140).

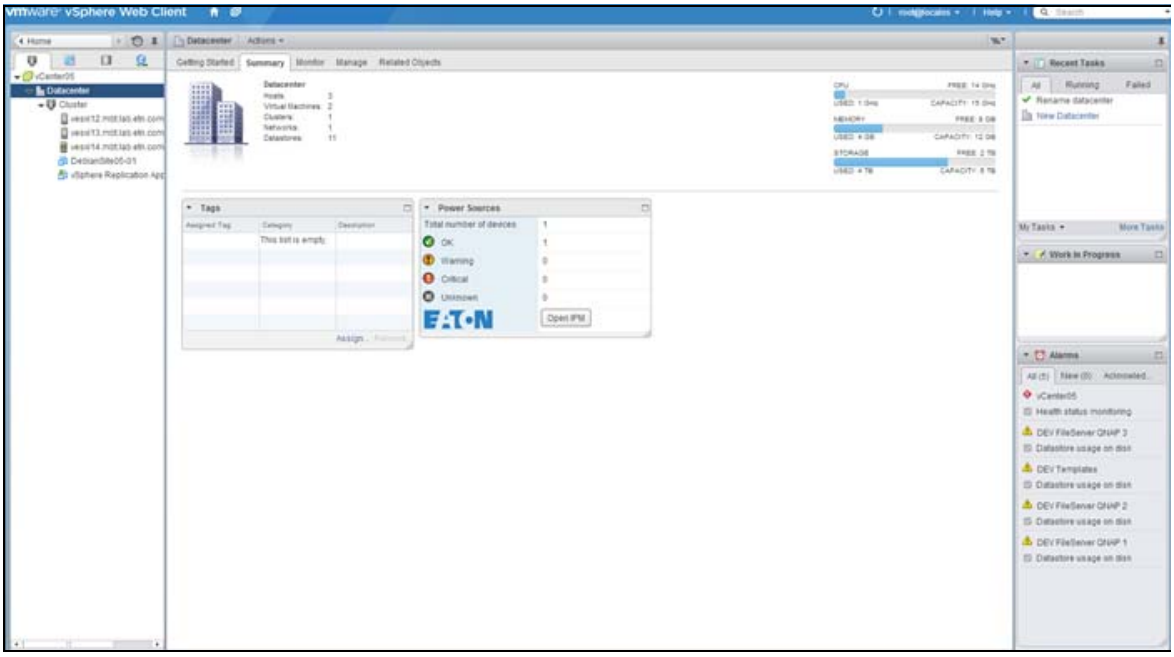


Figure 140. WebPlugin DateCenter Level

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.

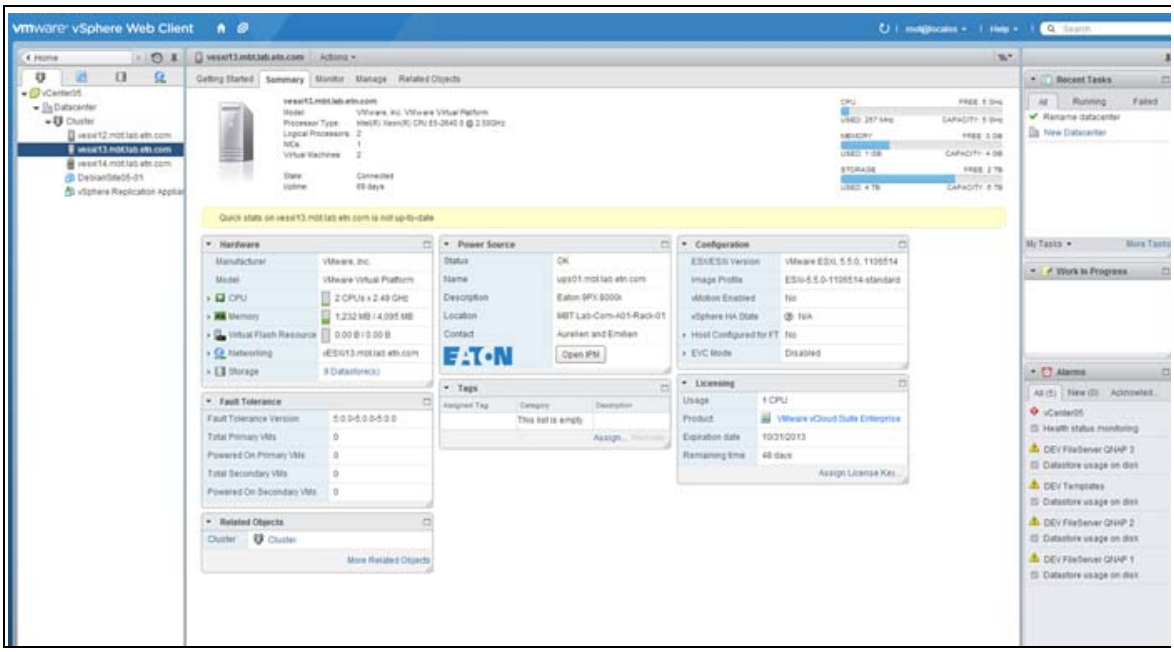


Figure 141. WebPlugin Host Level

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 142).
- You see the ***Plugin in XenCenter > Tools > Plugins***.
- If not, click **Re-scan Plug-in Directory** (see Figure 143).
- Ensure that the Eaton IPM checkbox is selected.

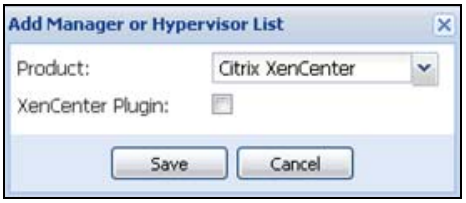


Figure 142. Add Manager or Hyperviusor List Dialog

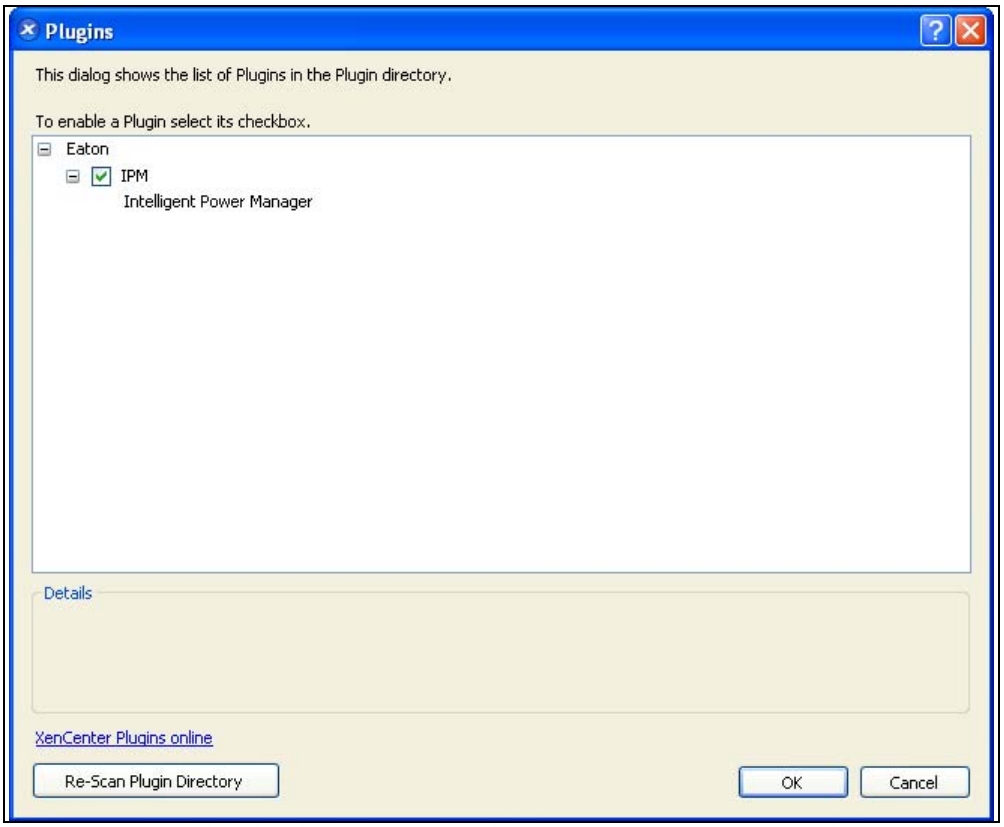


Figure 143. Plugin Directory (Rescan)

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 144).

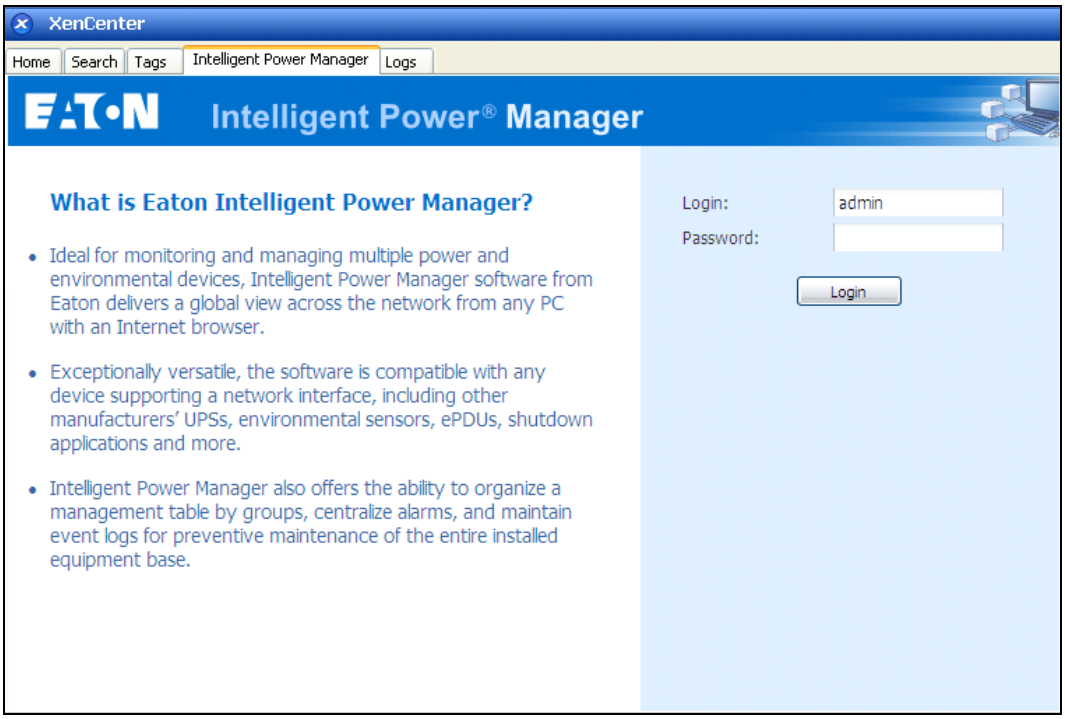


Figure 144. XenCenter Eaton IPM Tab

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 133.

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 145).

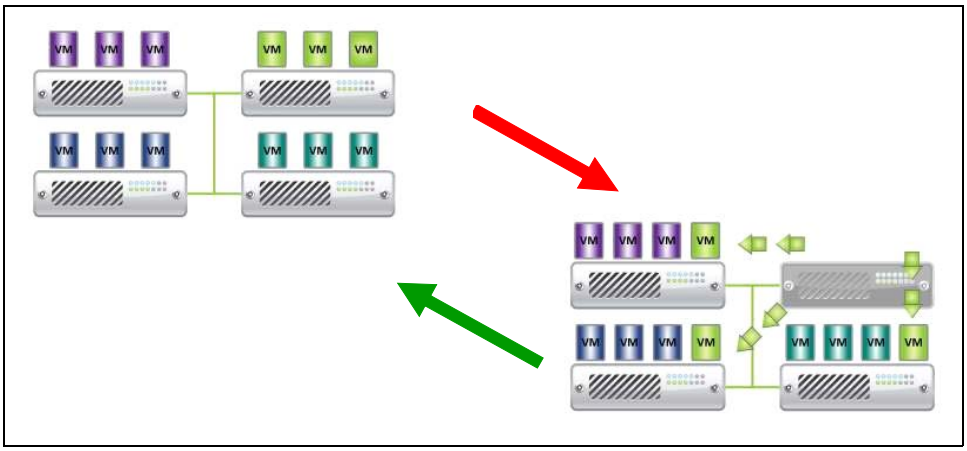


Figure 145. HA Mode with Eaton IPM

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

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

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 a 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 18. 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 134.

Configuring Maintenance Mode and Live Migration with SCVMM

Maintenance Mode

In Virtual Machine Manager (VMM) 2008 R2, you can start maintenance mode for a VM host anytime that you need to perform maintenance tasks on the physical host computer, such as applying security updates or replacing hardware.

When you start maintenance mode on a Windows-based host, VMM automatically does the following:

- On a stand-alone host, VMM places all operating VMs into a saved state.
- On a Windows-based host cluster that is capable of live migration, VMM provides the following options:
  - Live migration of all running, highly available VMs to other hosts in the cluster, and place any operating VMs that are not highly available in a saved state.
  - Place all operating VMs into a saved state.

NOTE Refer to Microsoft® Hyper-V™ reference on 134.

Understanding Live Migration

Live migration is a Hyper-V feature in Windows Server 2008 R2. The failover clustering feature must be added and configured on the servers running Hyper-V. Live migration allows you to transparently move operating VMs from one node of the failover cluster to another node in the same cluster without a dropped network connection or perceived downtime.

In addition, failover clustering requires shared storage for the cluster nodes. This can include an iSCSI or Fiber-Channel Storage Area Network (SAN). All VMs are stored in the shared storage area, and the running VM state is managed by one of the nodes.

NOTE Refer to "Microsoft Hyper-V References" on page 134.

Configuration Test

To test the installation, perform a power failure on the UPS. On the Microsoft System Center Virtual Machine Manager (SCVMM) console, verify that the corresponding Hyper-V host enters in Maintenance mode after the "Maintenance mode timer." Hyper-V machines must be started before the machine that is hosting the SCVMM. The SCVMM service needs some time to refresh its status. If the starting sequence is not correct, the Hyper-V stays in Maintenance mode.

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/ for more information about download and installation of vCenter Server.
- Visit also http://www.vmware.com/products/drs/ 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/default.aspx

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.

Chapter 12 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 hypervisor than support OVF/OVA templates.

- 14 GB data store
- 1GB free memory

Virtualization Platform Supported

The virtualization features are supported on:

- VMware ESX 4.1, ESXi 4.1 and ESXi 5.0/5.5

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

Free Version Limitation

IPM as a virtual appliance is delivered as a "Free" version with the limitation of 10 nodes (UPS/PDU devices).

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

- 10 to 100 nodes need an upgrade with the Silver License (Ref:66925)
- Unlimited License need an upgrade with the Gold License (Ref:66926)

Deploying a Virtual Appliance in VMware vSphere

To deploy the IPM virtual appliance:

1. Download the virtual appliance from **http://pqsoftware.eaton.com**.
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 146).
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 146).

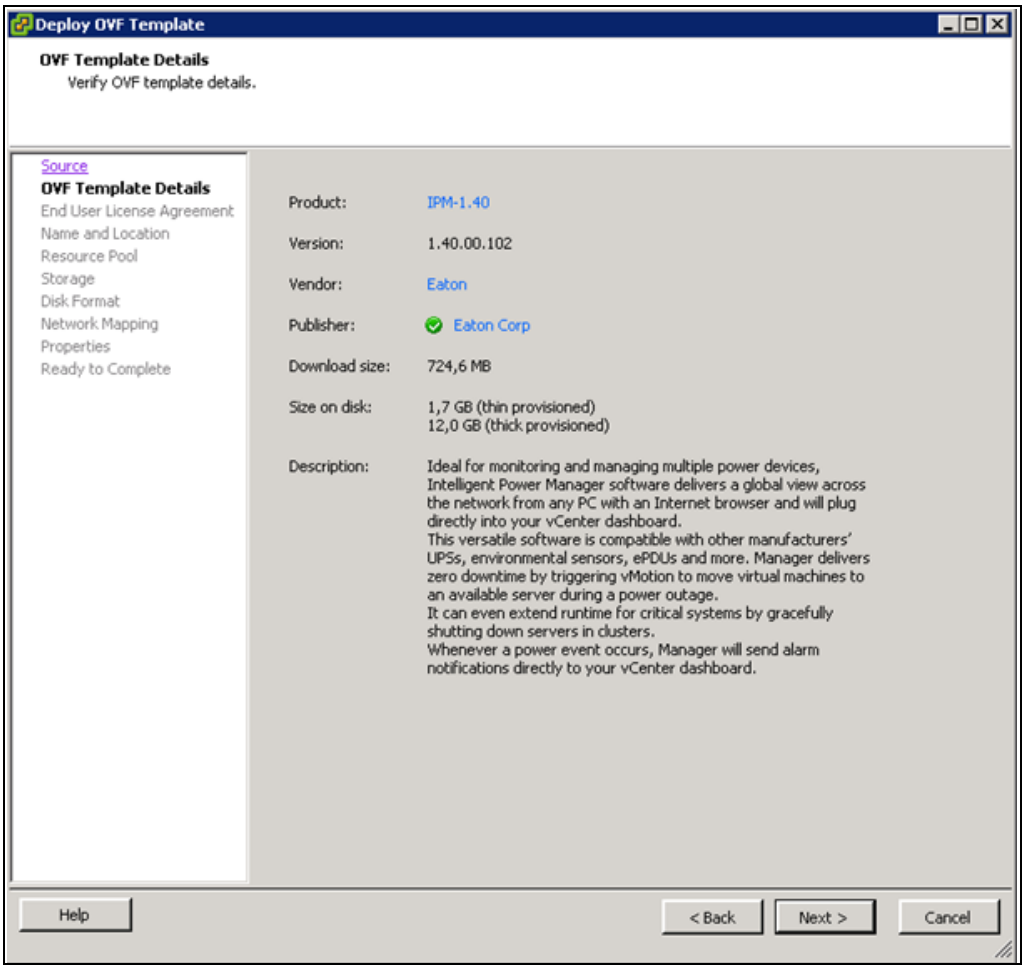


Figure 146. Deploy OVF Template

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 147).

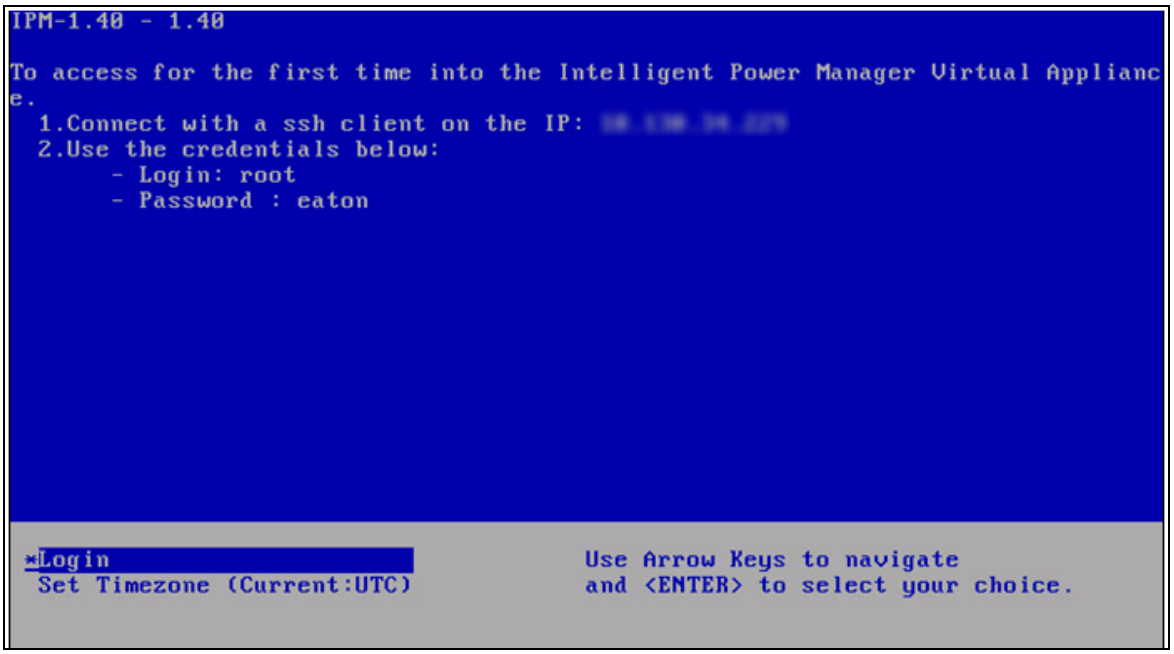


Figure 147. Standard Console

With SSH Client use the following credentials:

- Login: root
- Password: eaton

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 connection.

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 on 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 148. 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 149.

```
[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 149. 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 2 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" on page 139.

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 NetFiolter website
- Project - http://www.netfilter.org/projects/iptables/index.html
- Documentation - http://www.netfilter.org/documentation/index.html

Chapter 13 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.