Eaton® Intelligent Power Manager® (IPM)
Quick Start Installation Manual

Powering Business Worldwide

Microsoft Partner Network

CITRIX PARTNER Citrix Ready

vmware READY MANAGEMENT AND ORCHESTRATION

1. Downloading the software

From powerquality.eaton.com, please choose “Download software and drivers” from the right menu.

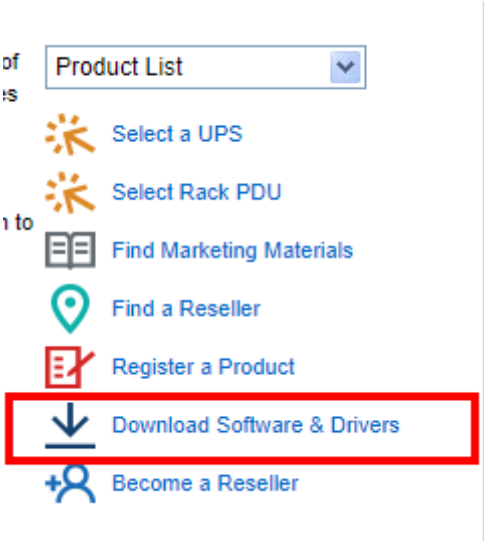

Figure 1: Select Intelligent Power Manager on the Download Software & Firmware page.

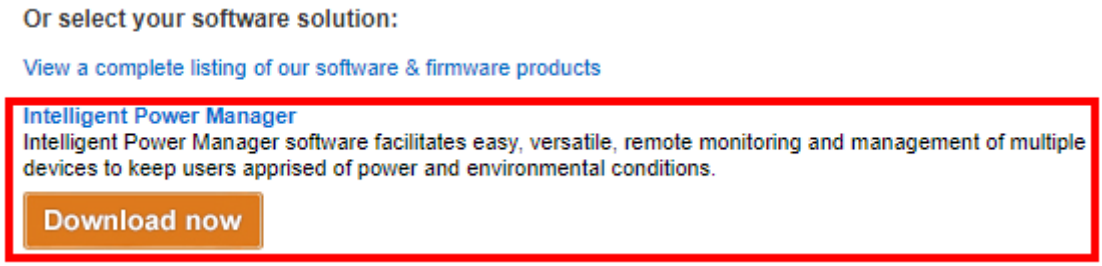

Figure 2: in the software download page.

Choose [Download now].

You may be prompted to register:

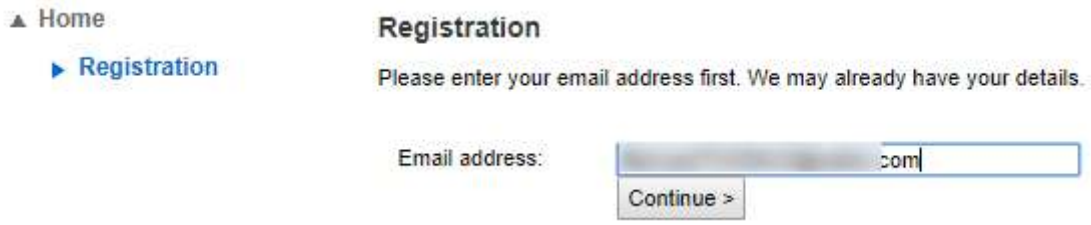

Figure 3: Registration before download (1st step)

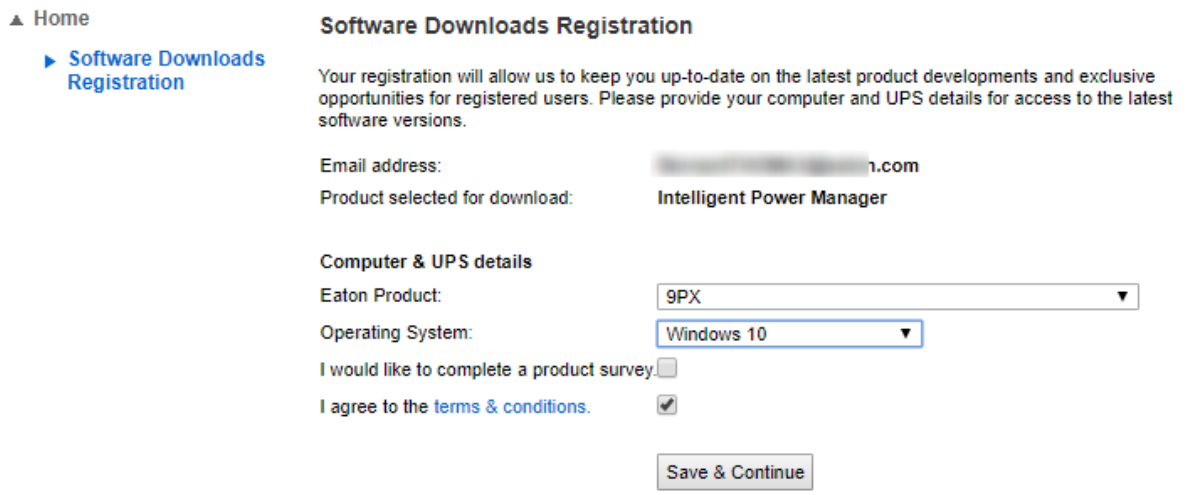

Figure 4: Registration before download (2nd step)

Once you've completed your registration details, you should have access to the download page:

Figure 5: list of the IPM downloadable packages

Choose the download package that corresponds to your need (according to the server operating system you will use for the installation of IPM).

2. Installing the software

2.1. from a Windows package:

You MUST have administrator rights on this computer for the installation.

Double-Click on the .exe package and answer all the questions until the completion of the installation process. When the installation completes, you will be redirected to the application login page in order to start using IPM.

Go to the paragraph 3. Login into the IPM application

2.2. from a VMware OVA :

The setup of the OVA is the responsibility of the VMware cluster administrator.
Please contact your VMWare administrator to complete this installation.

At the end of the deployment of the OVA, you must edit the network settings if you want to have a static IP address ssigned to the server. DHCP is configured by default.

3. Login into the IPM application

This step assumes that you have successfully completed the initial installation in the previous step. You no longer have to be logged into the server hosting the IPM application.

A simple way to open the IPM monitoring application is is to Right-Click on the IPM Eaton icon in the Windows status bar (if you are connected to the computer hosting IPM).

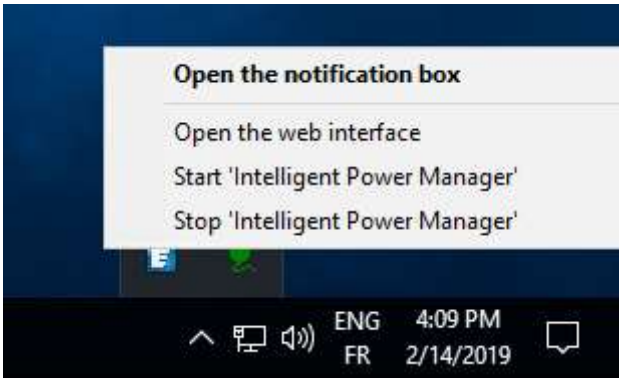

Figure 6: using the Eaton IPM command from the IPM icon in the Windows status bar.

You may also access the application from any web browser running in the same network as the IPM server (or a network segment with access to that network). You can access at the following URL:

http://ServerHostname_or_IPaddress:4679
https://ServerHostname_or_IPaddress:4680

Note: As the IPM security certificate is self-signed, you will have some security warnings before opening the web page. Please acknowledge all of the warnings in order to access the login page.

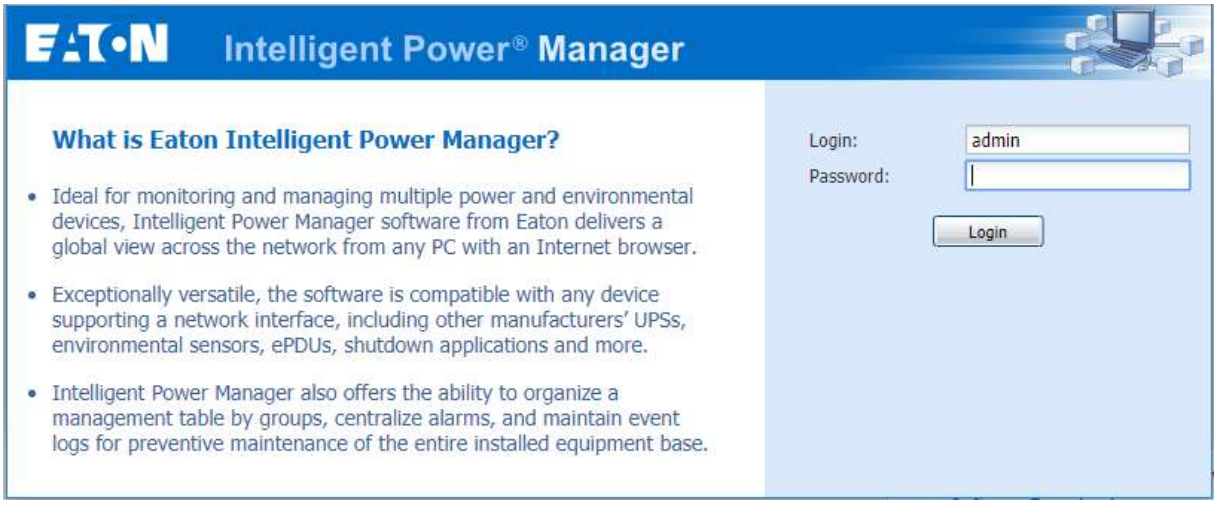

Figure 7: IPM login web page

Default credentials are admin / admin.

We recommend to change the default password and to save the new password in a secure place.

4. Entering a license in the IPM instance

You can use the basic software capabilities after installation; however, to unlock its advanced capabilities you will need to enter a license key. Your Eaton pre-sales contact can propose the best license for your needs. If you want to try the advanced features before buying, trial versions are available upon request.

The license string may be entered in the System view:

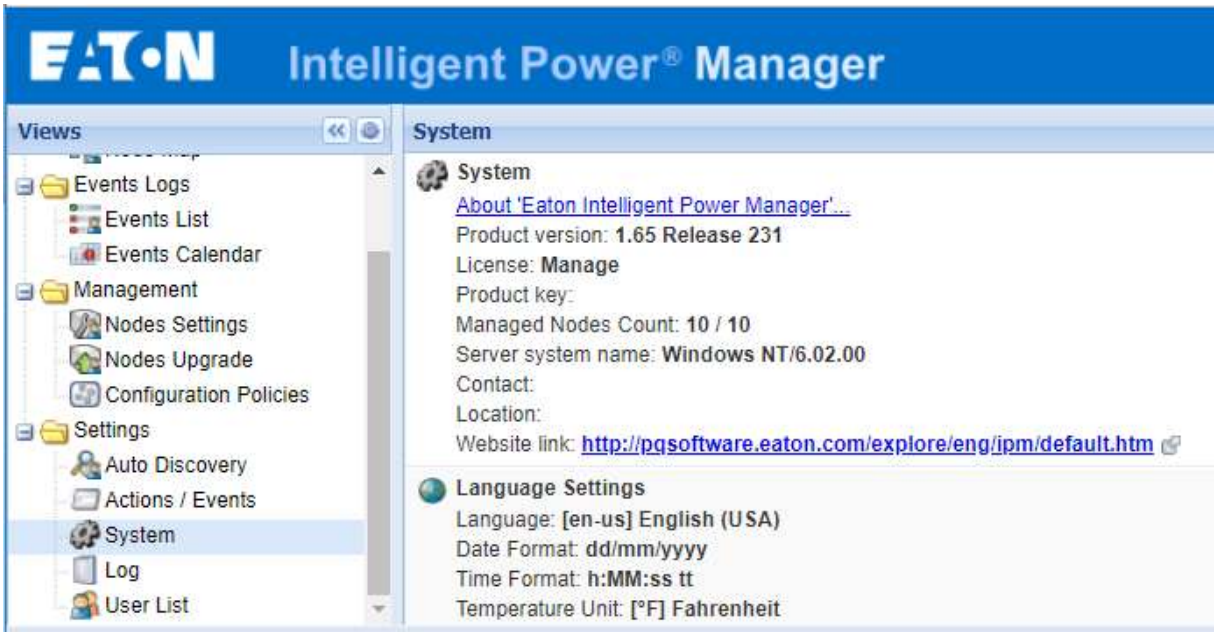

Figure 8: System view just after installation without any license string

You can use the “Edit system information” on the right or double-click on the information in the middle dashlet. Then, just paste the license string in the “Product key:” field and push the [Save] button.

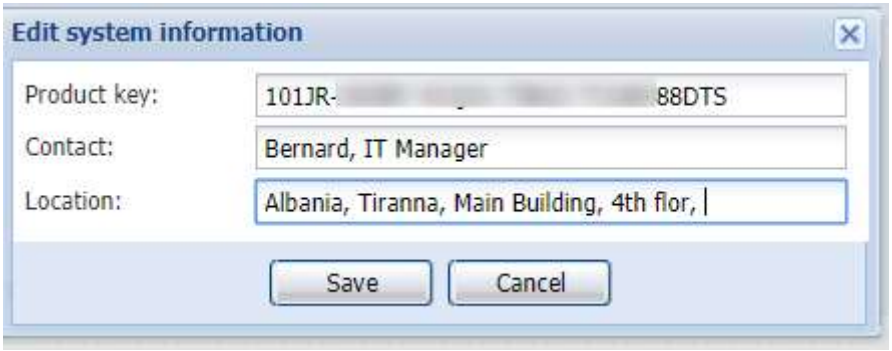

Figure 9: entering the system information (example of possible information).

The system information panel is updated according to license level:

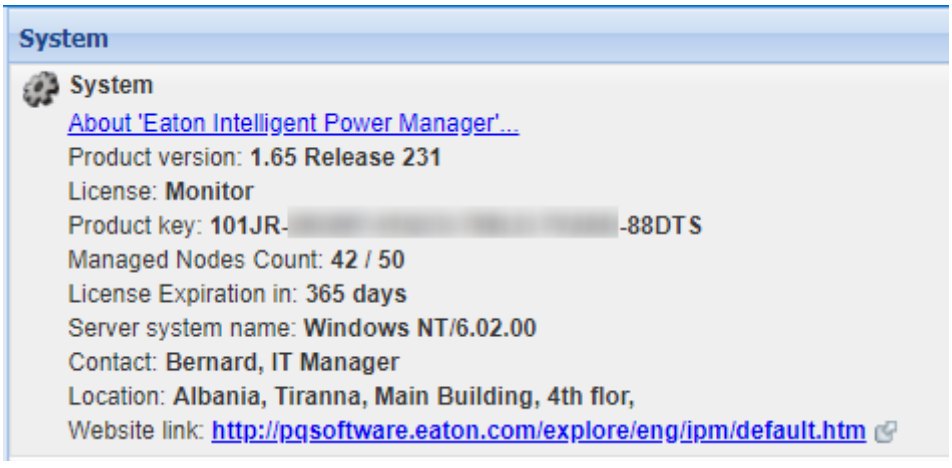

Figure 10: system information after insertion of a valid license string, and other information

5. Auto Discovery view

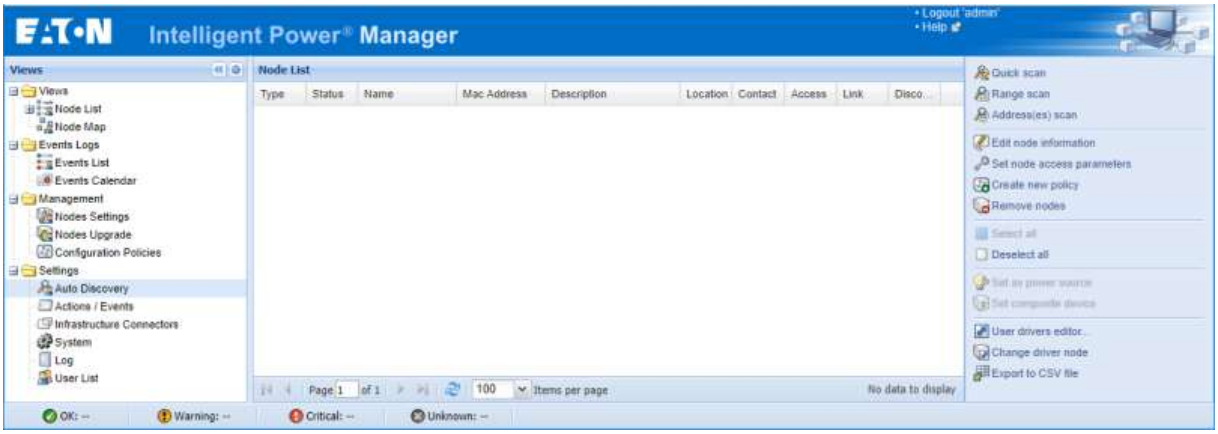

Figure 11: Auto Discovery view in the IPM graphic user interface.

Remember that the layout of this view may be tailored according to your needs. For example, you can display the IP addresses instead of the MAC addresses. In addition, this customization is local to the Auto Discovery view. Another layout could be defined in the Node List view because the available information are different in these 2 views.

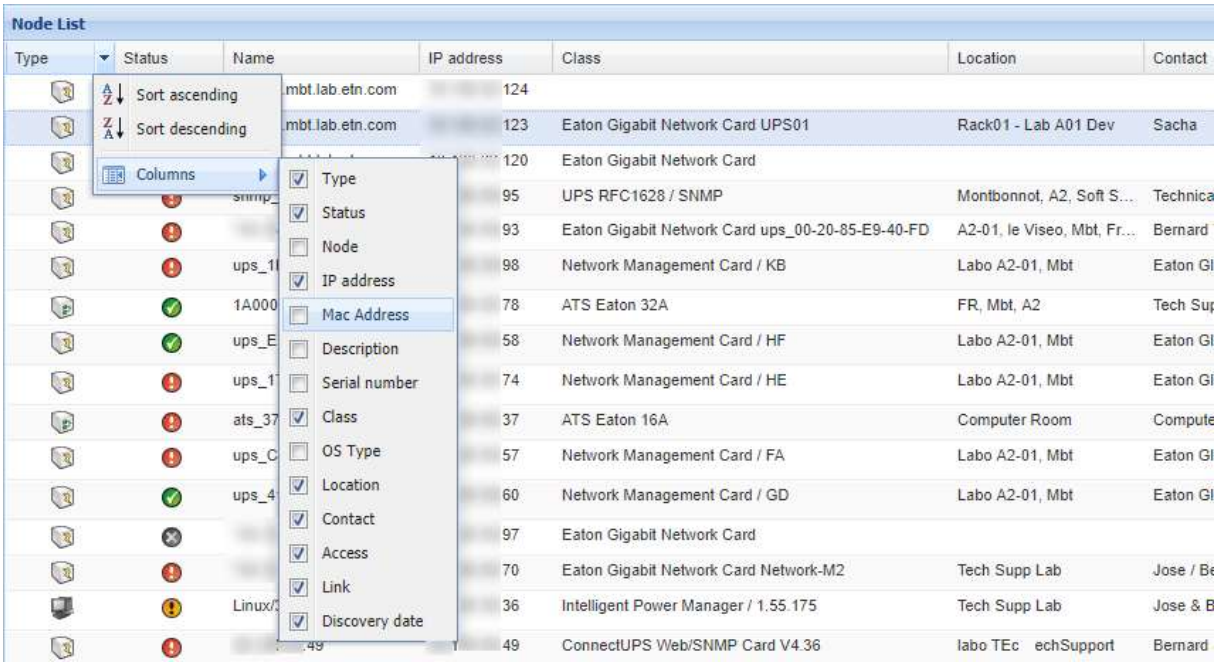

Figure 12: Customization of the layout of the Auto Discovery view. Just use the tile of the title bar!

At the end of the installation, the IPM software, automatically, performs a “quick scan” operation on the broadcast network. Some nodes may already be listed in this view, depending on your network architecture and other parameters.

If the UPSs, ePDUs, servers hosting Eaton applications (e.g. IPP or IPM) are not listed in the view, please use the command on the right: “Range scan” and “Address(es) scan” in order to discover the missing nodes.

6. Enabling the right modules for operation

The possible modules are the following:

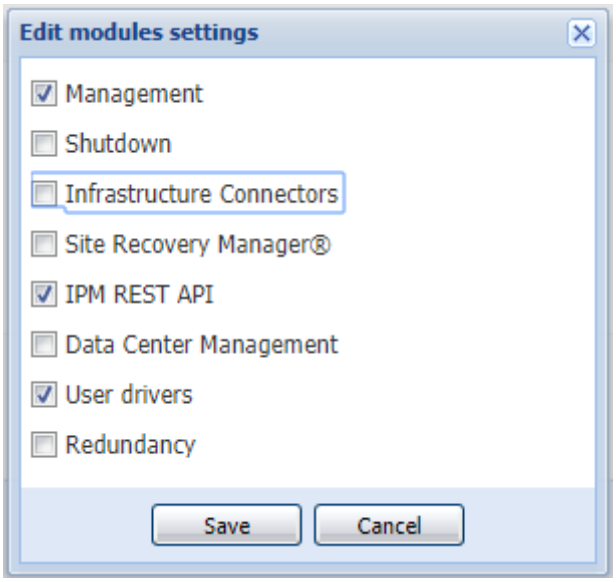

Figure 13: different possible modules

We recommend to enable the following modules :

Moduble label	Goal
Infrastructure connector	for the remote agentless protection of some hypervisors / VMs / etc…
Redundancy	for the protection of computers that are protected by several UPSs
Shutdown	is only useful when the graceful shutdown of the computer hosting IPM is required.

7. Discovering the UPSs

We recommend discovering the UPSs before configuring any setting regarding protection.

8. Adding the hyper visors

8.1. Most frequent case: VMware vCenter

In the Settings >> “Infrastructure connectors” view; use the “Add a connector” function:

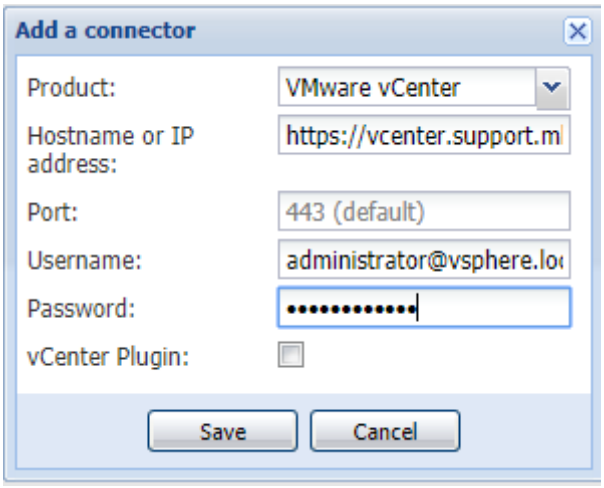

Figure 14: addition of a vCenter connector

The “vCenter Plugin” is not utilized in the protection features. So it is not mandatory to select it in this step. If you do enable it, it wil let you view the UPS(s) that protect(s) your ESXi(s) directly within the vCenter application.

Once the connector is configured, you should have the vCenter and all the managed ESXi displayed in IPM:

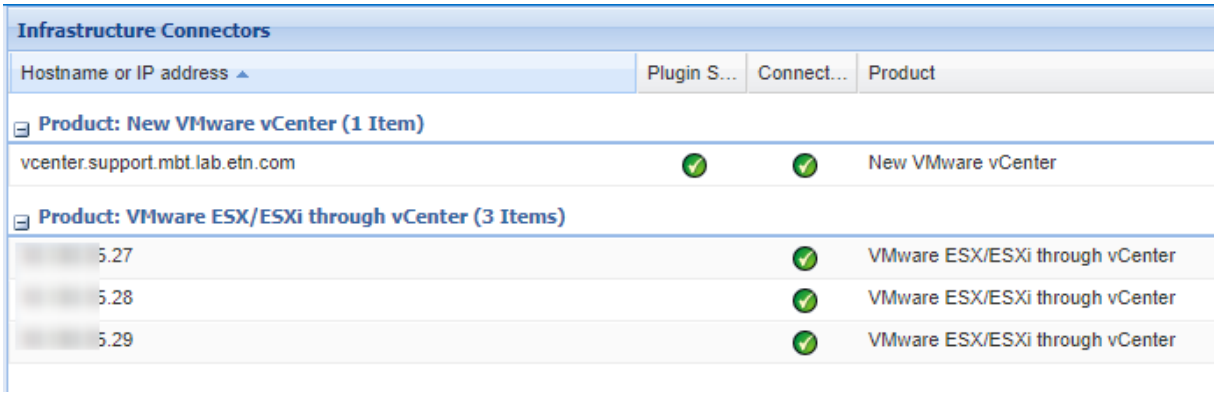

Figure 15: connectors displayed after the addition of a vCenter connector

8.2. Most frequent case: VMware ESXi direct connection

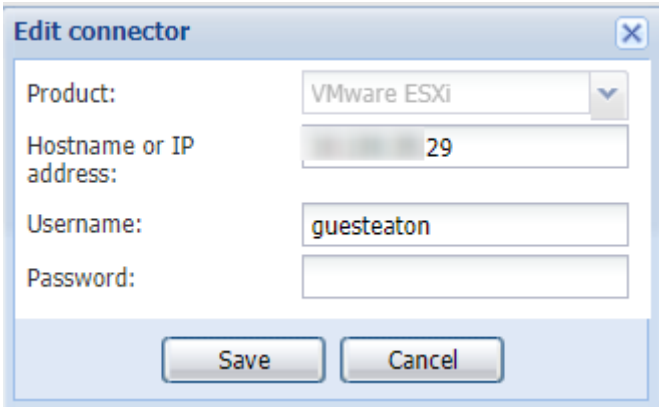

Figure 16: adding an ESXi as connector (without vCenter).

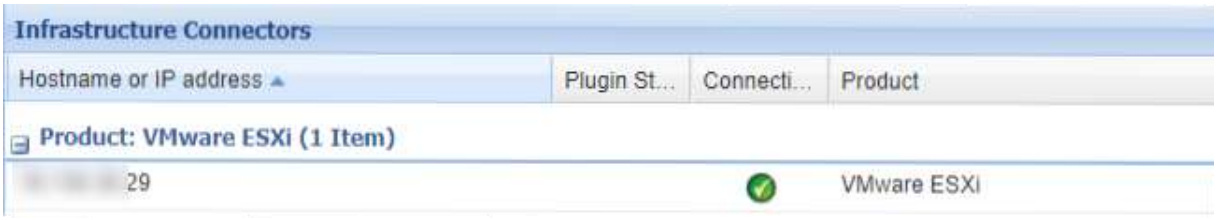

Figure 17: ESXi listed when creating a direct connection with an ESXi

After this step, go to the paragraph “10. Protecting the hypervisors

9. Viewing the hypervisors

In the latest release of IPM software, the hypervisors may only be listed in the “Nodes List” view, instead of the “Infrastructure connectors” view. As this view could list a very large number of nodes, we recommend to create sub views based on node types: To create a sub view, right-click on “Nodes list” in the left part, and then choose the “Create a sub view from ….” sub-function:

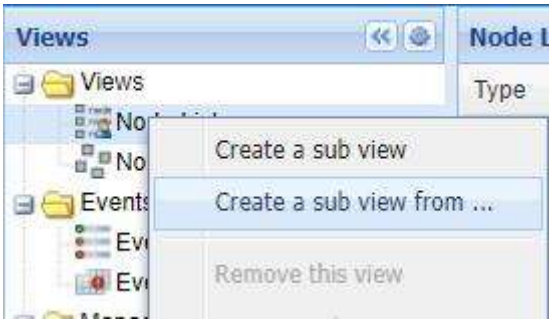

Figure 18: sub-function for creation of sub views.

And select “Type”:

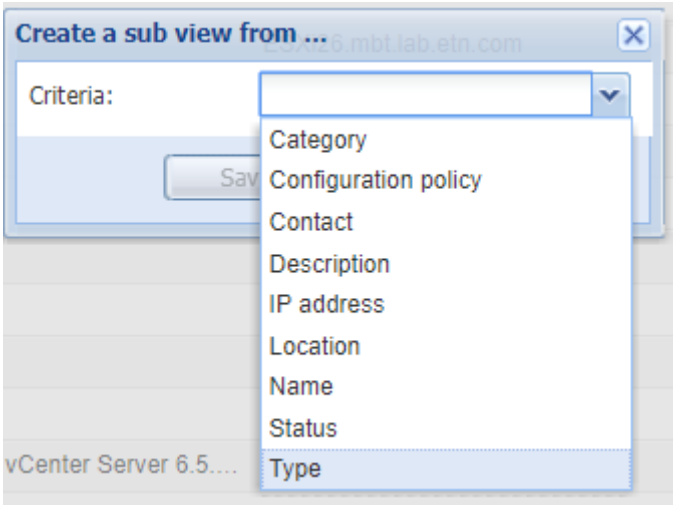

Figure 19: creating a sub view according to “Type”.

Figure 20: prompt for confirmation of the sub views creation

The result is the creation of a sub view for hypervisors :

Figure 21: Hypervisor subview with several hypervisors present in the node list

10. Protecting the hypervisors

Before you configure any settings, you should define the following for each node you want to protect:

- the trigger event that will start the graceful shutdown of the node(s),
- the time required for the completion of this graceful shutdown.

10.1. Using the wizard for graceful shutdown protection

First, select the hypervisors you want to protect with a given set of shutdown parameters (in this example we have selected 2 ESXi from the list of 4) and Right-Click on the selection:

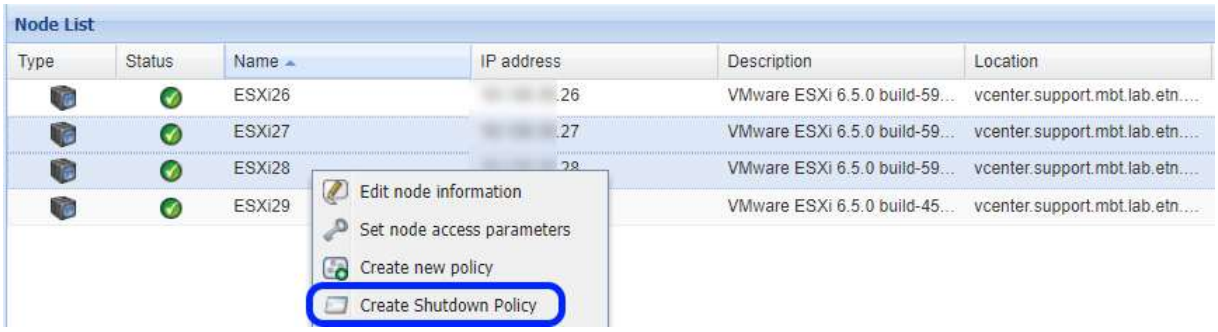

Figure 22: contextual sub command “Create Shutdown Policy” feature in order to start the wizard

Use the “Create Shutdown Policy” and then define the trigger (event) and the action required for the protection scenario: (for example for a group of servers that require 10 minutes for the complete shutdown, the settings could be the following).

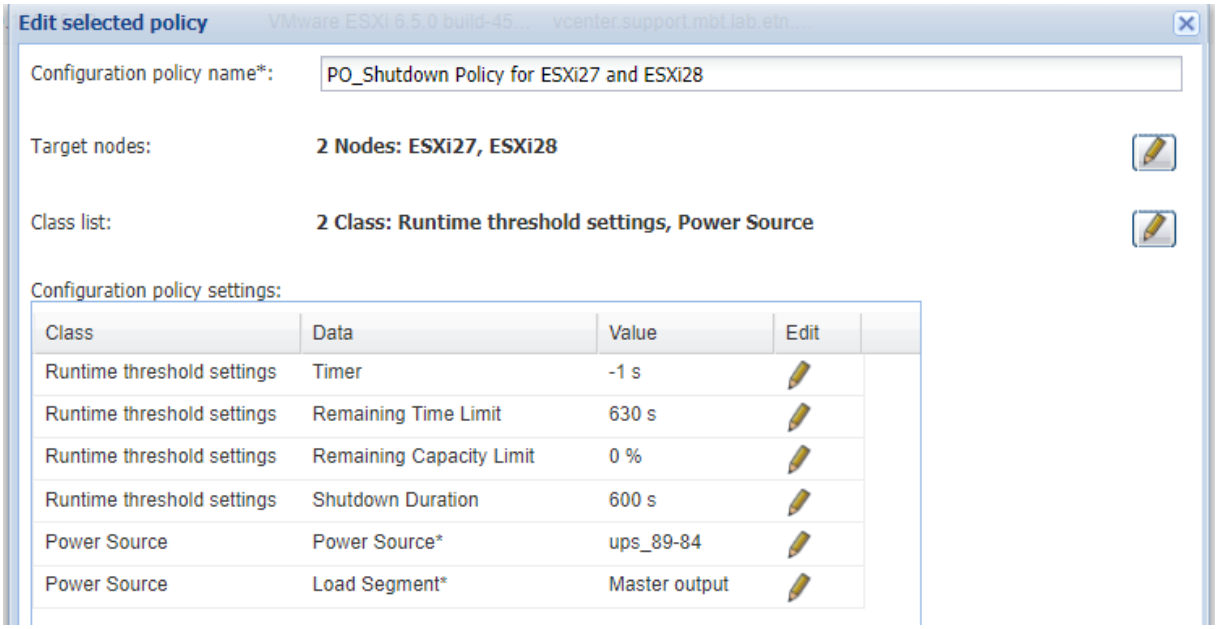

Figure 23: Shutown policy example

When you click the [Save] button, the wizard proposes the following operations :

Figure 24: wizard prompt after policy save operation

Click [Yes] and configure the suitable action for the protection (for example) :

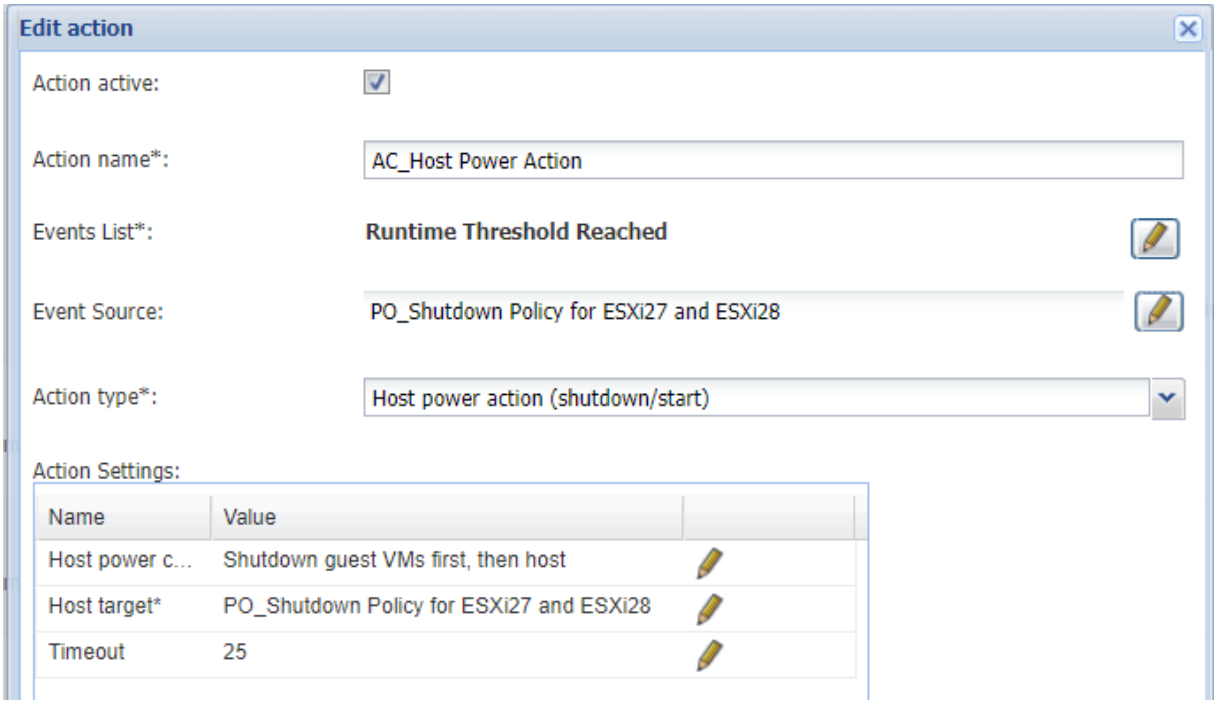

Figure 25: example of possible action configuration

During this definition, if you are unable to select Policy in the host target field, just configure the other settings, then save and re-open the action again. Sometimes a refresh is required to enable the selection of the policy for the host target.

10.2. Manually or modifying an existing installation

If you need to modify some shutdown settings or prefer to manually create a policy, you may create/modify a policy in the Management >> Configuration policy view and create/modify an action in the Settings >> “Event / Actions” view.

11. Testing the protection

11.1. Testing the action

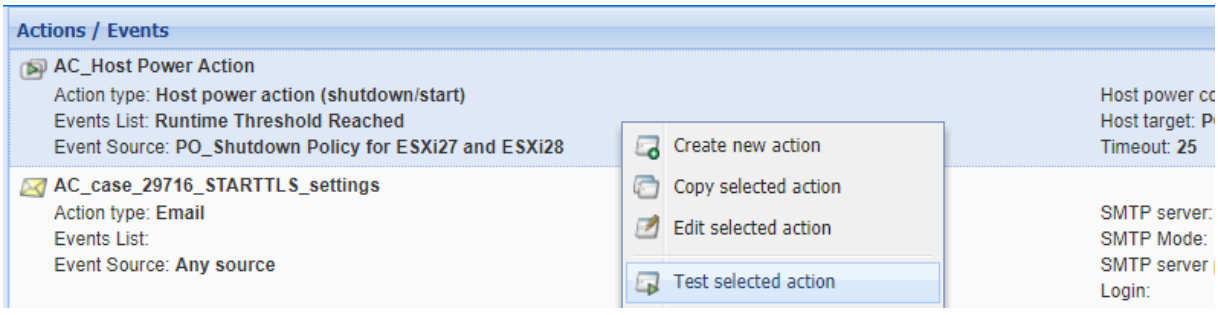

Figure 26: Right-Click on the action you need to test.

Then, confirm your request by clicking the [Yes] button.

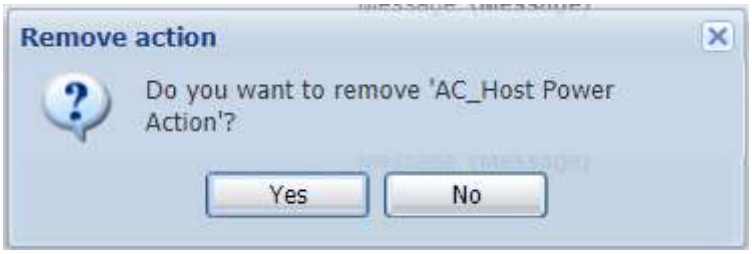

Figure 27: confirmation for test of the action.

11.2. Testing the triggers

You may modify the shutdown policy for a quick test without draining all the power out of the battery. To do so, just use the Runtime threshold settings >> Timer:

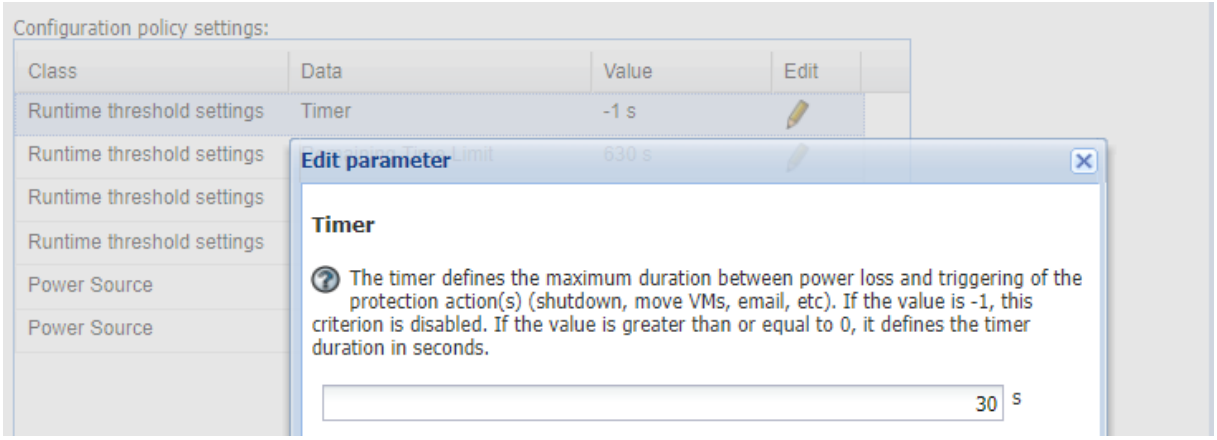

Figure 28: shutdown timer for test conditions.

This will reduce the delay between the power failure and the occurrence of the trigger to the specified delay.

Caution: this modification needs to the cleared for use in a production environment.

ꕥ