Eaton® Intelligent Power Manager ® (IPM) Editions

User guide

Rev 2.8.0 06/06/2024

Table of Contents

1 General information

1.1 The virtual appliance

All IPM Editions (version 2.0.0 and higher for IPM Monitor, IPM Manage and IPM Optimize) are available as a Virtual Appliance.

The VIrtual Appliance should be deployed on your virtualization platform and consists of a virtual machine hosting a Linux OS and all application dependencies required by your specific IPM Edition.

Eaton only validates the deployment in

- **VMware and Vitualbox** context (alternative configurations have not been validated) using IPM Editions virtual appliance packaged as an OVA file
- **Microsoft Hyper-V** environment (since version 2.1.0 and above) using IPM Editions packaged as an exe file.

1.1.1 Technical specifications

The Virtual Machine embedded in the OVA file is sized as described below:

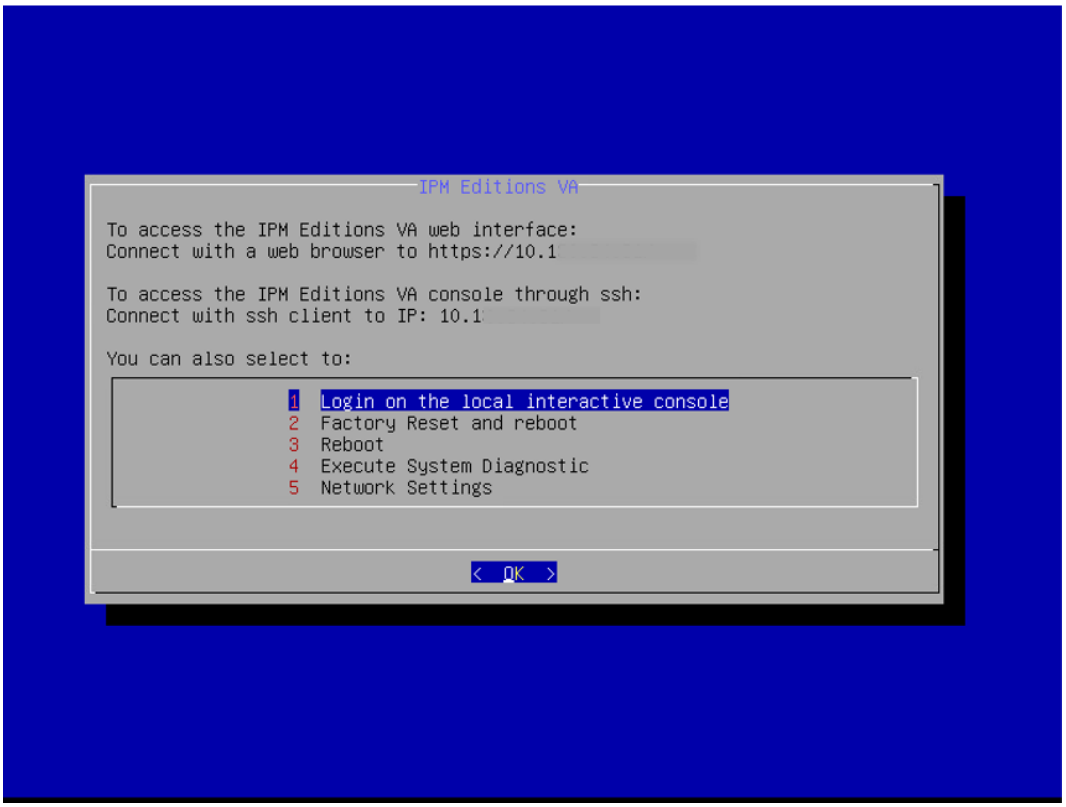
- 4 CPUs
- 8 GB of RAM
- 64 GB of disk storage (for user and system data)
- 4 GB + 300 MB for additionnal disk storages (system firmware and bootloader)

> Note that the above 64 GB value is a default setting that may be modified during the deployment of the Virtual Appliance.
> The disk storage may more specifically be set to Thin provisioning, to only consume the currently needed space, or to Thick provisioning to ensure that the needed storage space is reserved.

1.1.2 Virtual appliance console

Some administration functions are made available via the vCenter console.

This console is not needed for the normal usage of the product.



Console access allows administators to:

1. Log into a local shell for access to a limited command line interface
2. Do a full factory reset and reboot of the appliance (**WARNING**: this action will delete all configuration and comissionning data you may have entered previously)
3. Reboot the appliance
4. To execute the systems diagnostic tool
5. To set network settings

Note: Use of "System Diagnostic" should only happen on request of an Eaton support representative.

Note: To later access to the web interface, an IP address must be set to your SW instance.
If DHCP is enabled on your network at deployment time, you can start with the IP address automatically assigned and then use it to connect to the web interface to either stay in dynamic mode or change it for a static IP assignment.
In case, you have **no DHCP access available in your network at the deployment time**, you must configure the appropriate static IP address of your SW instance using "Network Settings" in this console.

1.1.3 How to Snapshot the IPM2 OVA?

For VMware / vCenter:

1. Log in to vCenter
2. Go to the summary page of the VM to take the snapshot from
3. In the "Actions" menu, select "Snapshots/Take Snapshot ..."
4. Give it a name and optionnaly a description
5. Validate the snapshot creation by clicking the "Create" button.
   The **snapshot** will be created.
   More details at https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.vm_admin.doc/GUID-9720B104-9875-4C2C-A878-F1C351A4F3D8.html

For Hyper-V:

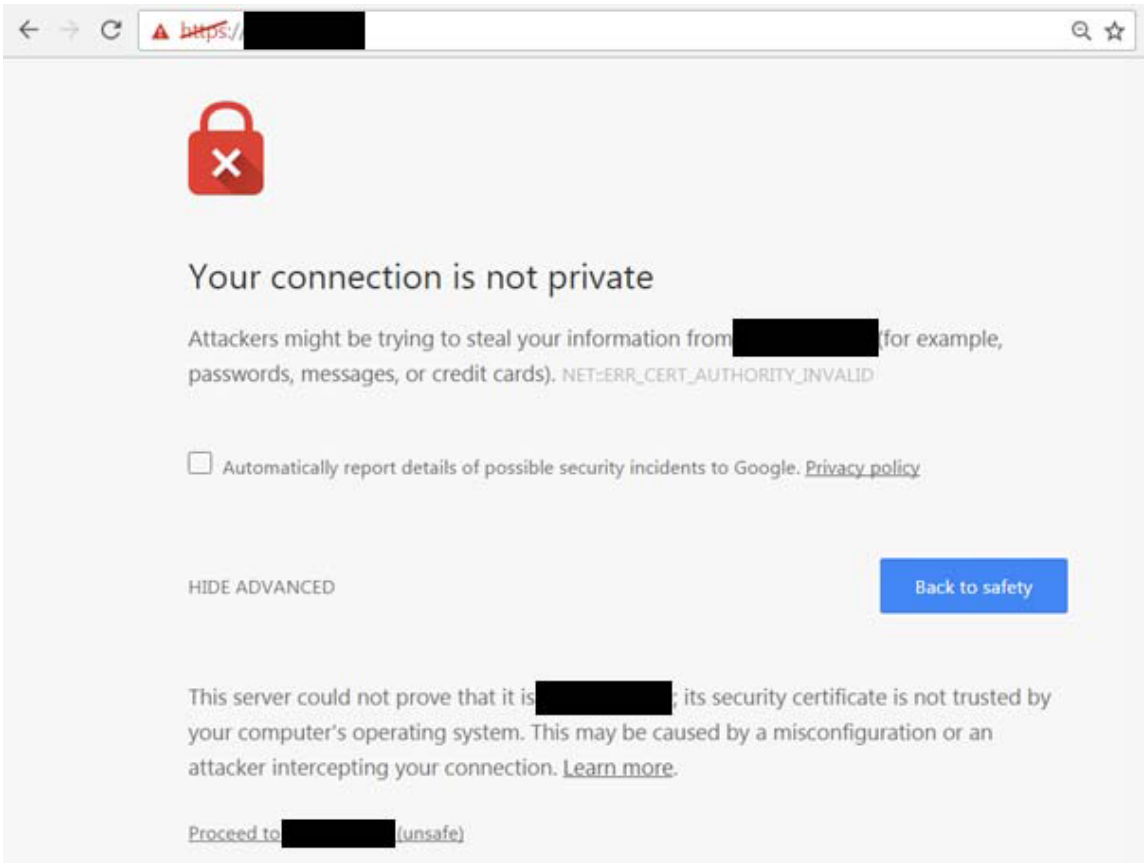
1. Open Hyper-V Manager
2. Select the VM you want to snapshot
3. In the action panel (or context menu), click on "Checkpoint"
   The **checkpoint** will be created.
   More details at : https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/user-guide/checkpoints

1.2 Initial setup & configuration

1.2.1 **Initial commissioning**

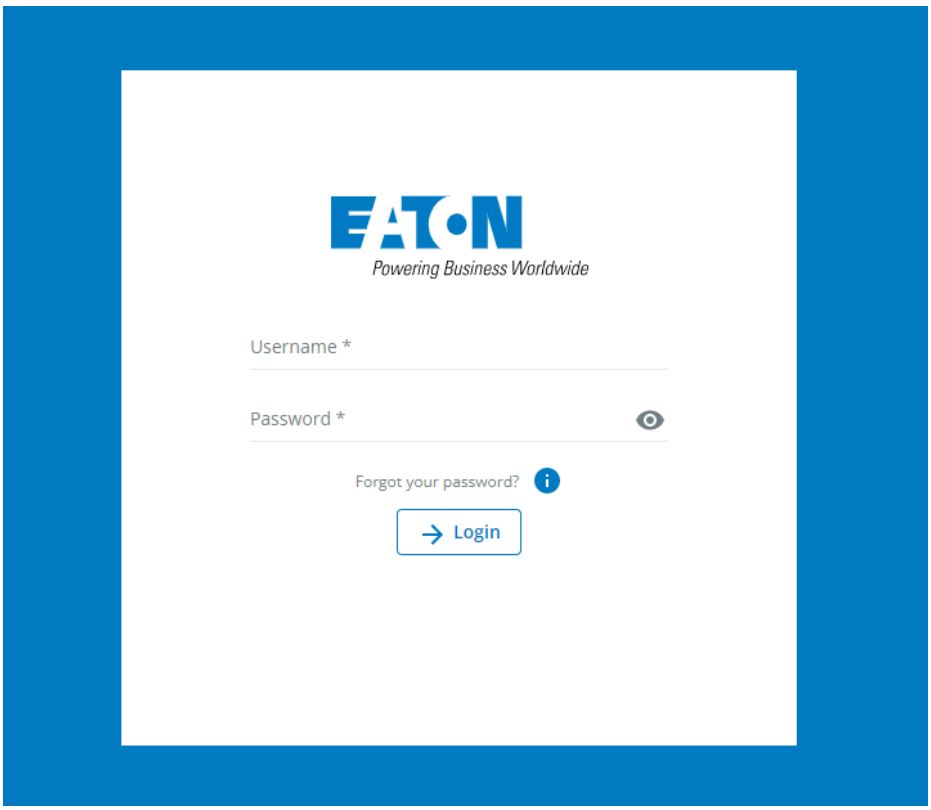
Login Wizard

In order to access the web UI after deploying the virtual appliance and navigating to its assigned IP address, you will first need to accept the untrusted certificate warning in your browser. This is due to application being factory provisioned with a self-signed certificate and is NOT due to a security issue.



Initial Login

After accepting the self-signed certificate, you are presented with the login page.



As you are logging into your IPM Editions application for the first time, you will be required to enter the factory default username and
password which are set to:

Username = admin
Password = admin

As you type in the password, the password details are obscured from view so please ensure that you enter the password carefully.

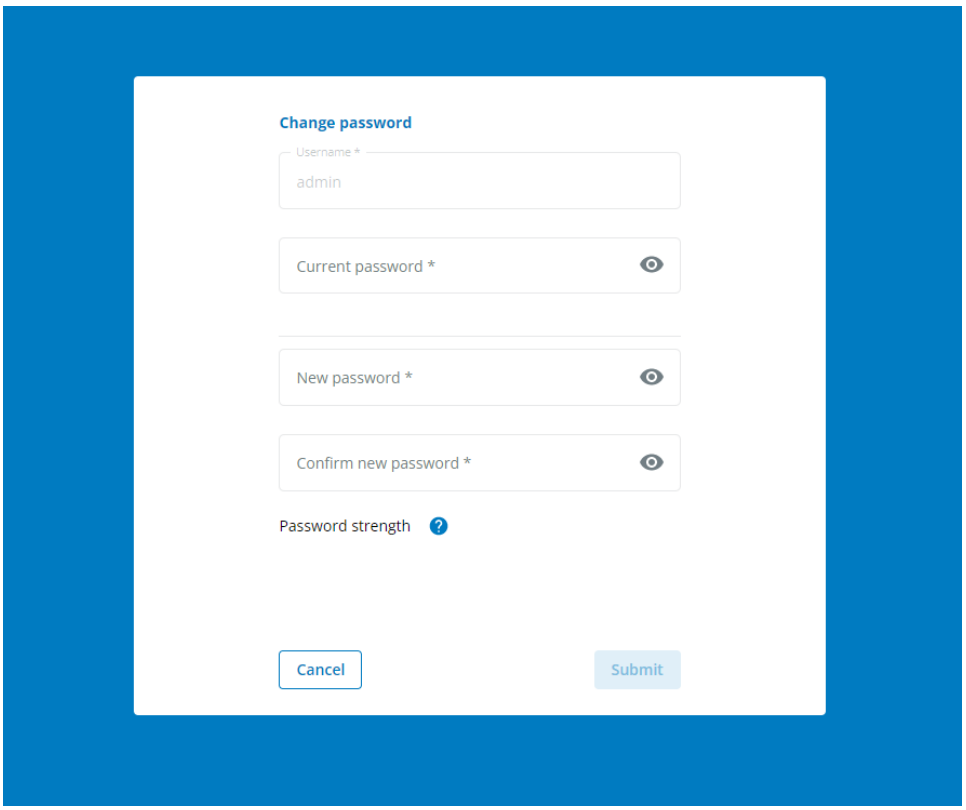
> Passwords are case sensitive!

During the initial login, the system requires that you change the default admin password for increased security.

- You are presented with a message requesting the current admin password ("**admin**") and a new password which you must also enter a second time to ensure you have entered it correctly.
- Follow the password format recommendations on the tooltip in order to define a secure password;
- A secure password is mandatory.

> The factory default password security policy requires that you enter a password with **at least *8 characters and that includes a minimum of 1 number, and 1 special character***.
> You may modify the password strength policy in the settings of the application. See User Management for more information.

- Click **Continue**

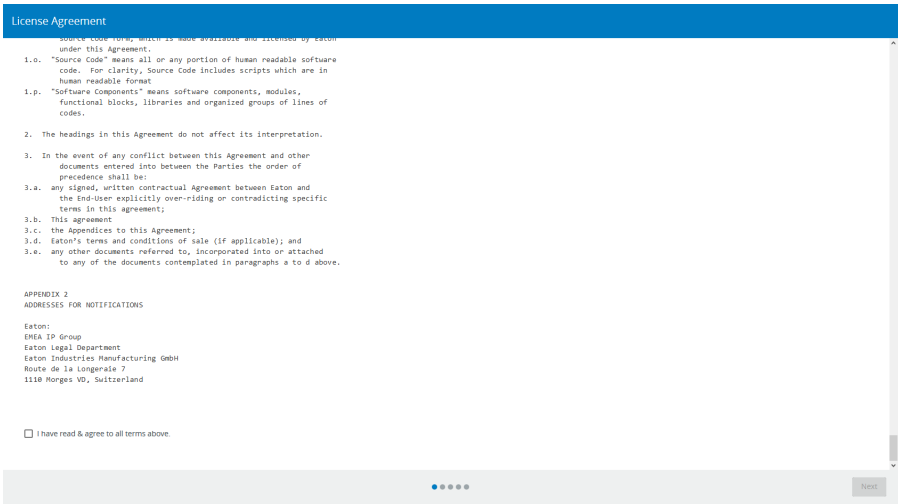


End User License Acceptance

After changing the password, you are presented with the License Agreement.

Please read it and accept the license terms in order to continue.

Please refer to the Legal Information below for more information.



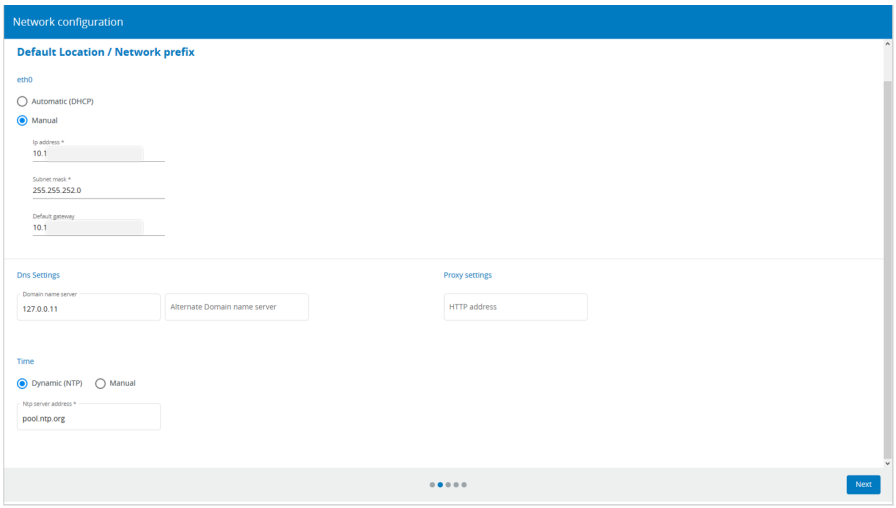
Network configuration

On the next page, you are presented with the network configuration settings.

Confirm that the network configuration settings are correct.

If no changes are necessary, proceed to the next step, simply by clicking on **Next**.

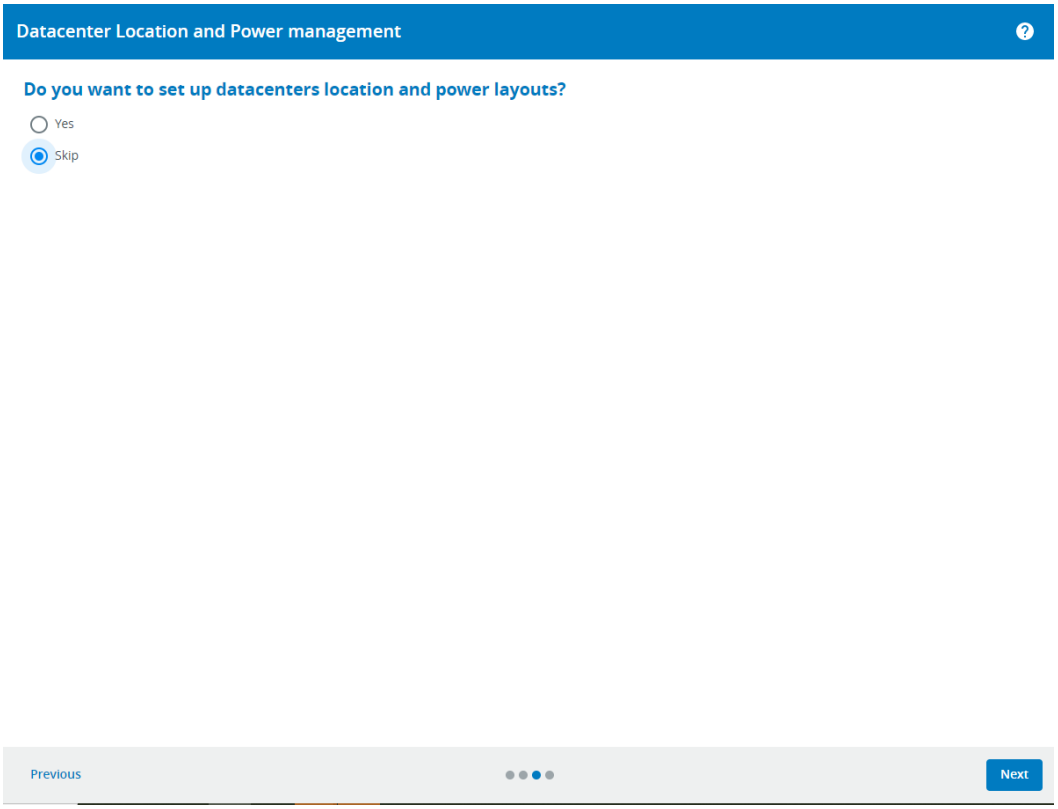
NOTE If you provide a Proxy URL, you will be able to activate your License online in the License activation step.



Data center Location and Power Management configuration (Optional)

At this stage of the initial configuration, you have following choice:

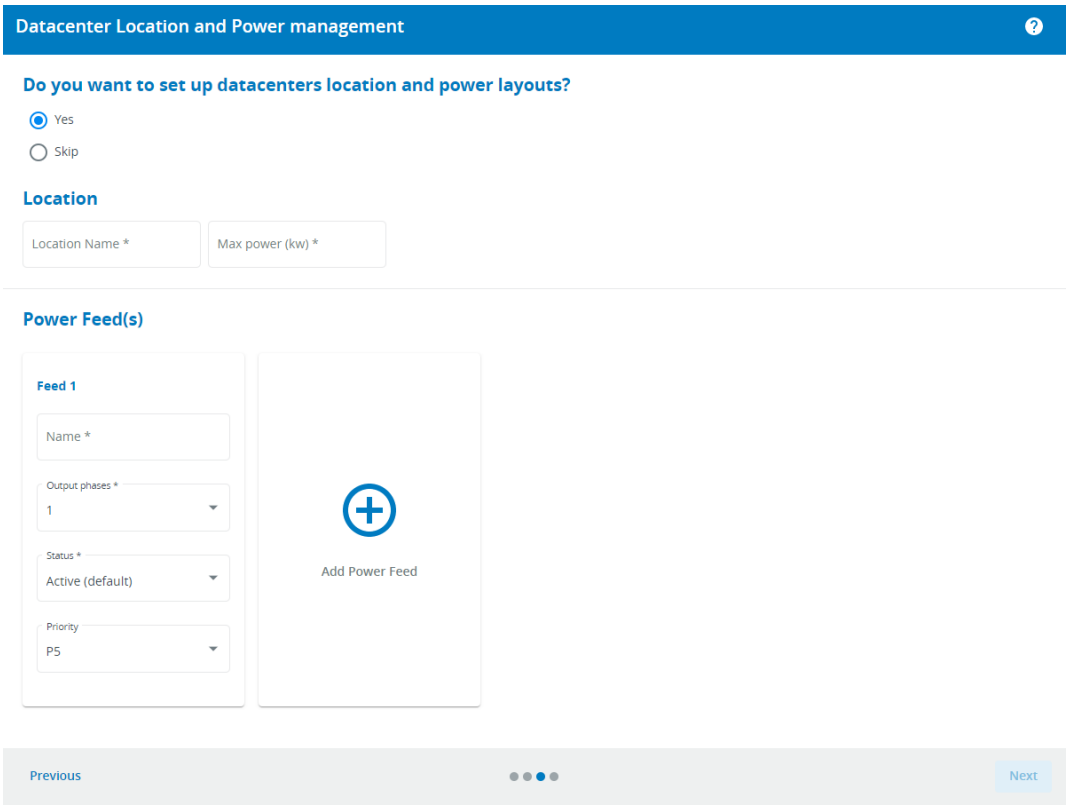
- **Yes** to configure Datacenter information such as Datacenter Name, Max power consumption, Power feeds, ... or
- **Skip (Default Option)** if Datacenter Power and Spatial topologies are not important for you. You will be directly re-directed to the **Licensing** page



Data center Location and Power Management configuration (Optional)

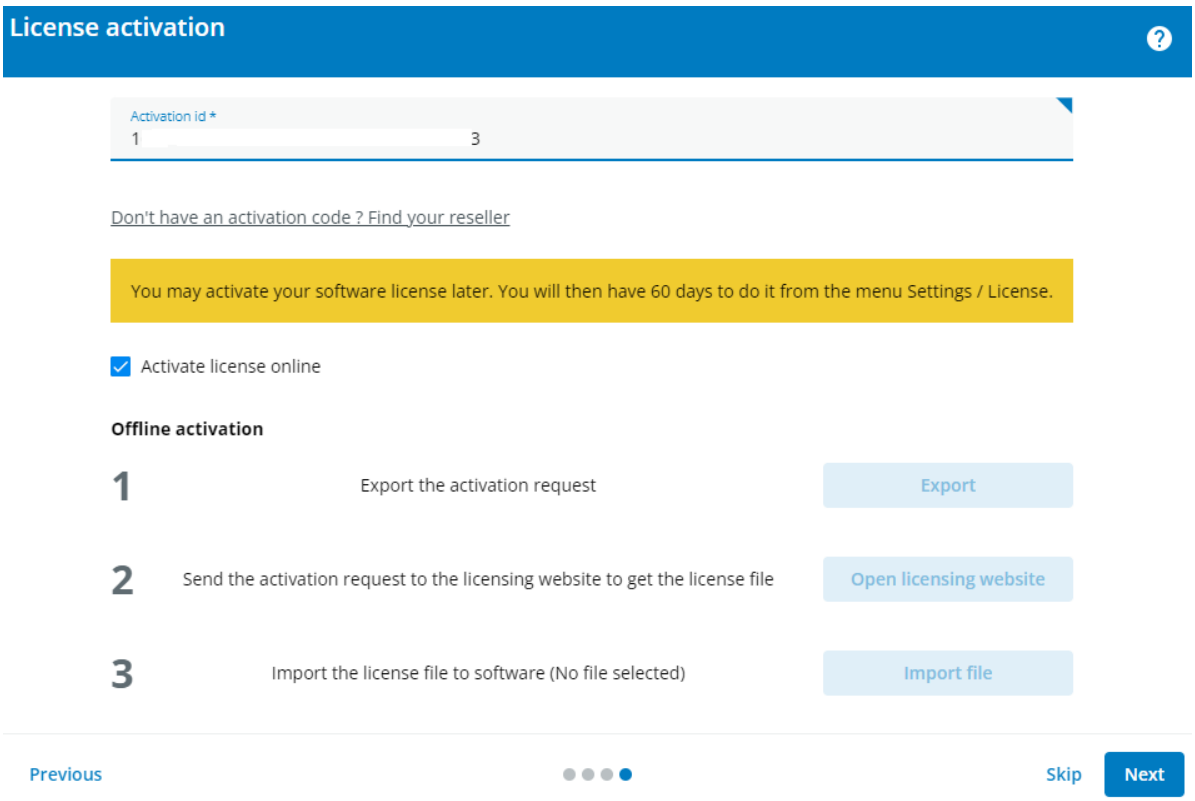
If you select **Yes,** you are able to configure Datacenter Name, Max power consumption, Power feeds, ...

> Please note that required fields marked with an asterisk "*" and are mandatory.
> At the end of this installation Wizard you will be able to configure asset location with following hierarchy (Data center -> Rooms -> Rows -> Racks -> devices).
> **NOTE** The data center layout can be updated later on from the Location Management page.



Software license or subscription configuration

At this stage, you are prompted for a license key. You have 60 days of full trial access to the application without a key so you may skip entering the license key now if you don't have the key at hand.



- To proceed without a license key, click the **Skip** button.
- To activate a license, enter a **valid activation ID,**
- **Recommended:** If you've already configured your **proxy settings,** you can **simply** proceed with **online License activation** by selecting the checkbox on the screen above
- Otherwise follow the 3 described steps
- And then click **Next**.

The details about the license activation process are described in the Licensing page.

Finalize data center asset configuration

When you exit the Setup Wizard, you arrive at the application's data center Asset Management page.

There are different ways available to help you finalize the setup and define your assets.

First click on **ADD ASSETS** then following options are offered to you:

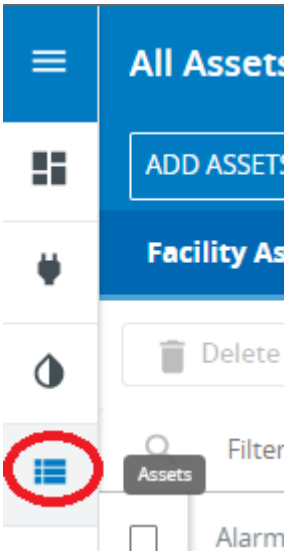
1. **AUTO DISVOVERY** for IP based devices. This feature will automatically import the power devices discoverable on the local network into the IPM Editions asset database
2. **UPLOAD CSV FILE (advanced)** This is an advanced configuration tool which will allow you to create your data center's topology with few restrictions. Note that this may create configuration issues if misused. It is not advised to use it without help from a qualified consultant.
   TIP: starting the csv file from an export of an existing configuration will help you understand the structure of the file. A detailed overview of the usage of the CSV import function is available in the Asset Management documentation.
3. **ADD ASSET** feature to manually define additional assets that are not auto-discoverable by the application
4. **ADD CONNECTOR** to automatically discover virtual assets

1.3 Asset Management

1.3.1 **Asset Management from the User Interface**

In addition to the possibility of managing assets through the CSV file, the user may manage his assets from the web user interface. The possible operations for assets are : Create, Edit and Delete.

To access to Asset management, click on the "Assets" button on the left hand Menu.



The Asset Management section offers 4 different pages :

- Facility Assets : To manage all assets related to facilities (Feeds, UPS, ATS, ePDU, sensors, ..)
- IT Assets : To Manage all assets related to IT (Servers, ...)
- Virtual Assets : To Manage all Virtual assets (Hypervisors, Virtual Machines, Clusters, Managers, ...)
- Dynamic Groups : To Manage Dynamic Groups

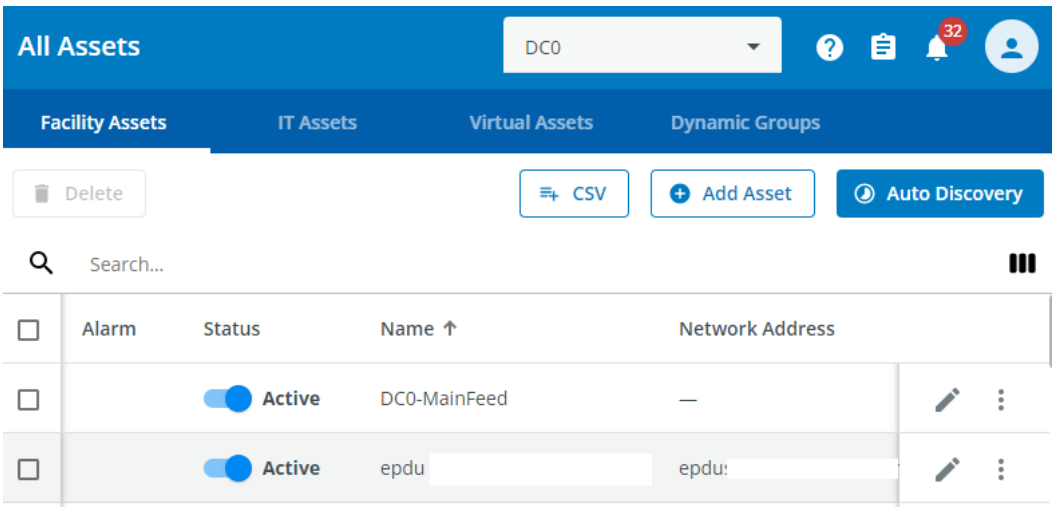
Each pages displays a table listing the existing assets. To display more or less information in the table, click the button in the up right hand corner.

> The "Network Address" column displays the IP address or the hostname given during the asset creation.
> The "Hostname" column displays the hostname communicated by the virtual assets or by the communication cards of the IT or Facility asset.

Asset creation

All asset management operations are available in the Asset Management page.

Each tab provides access to various operations on assets through top buttons:



Input Power Chain Configuration

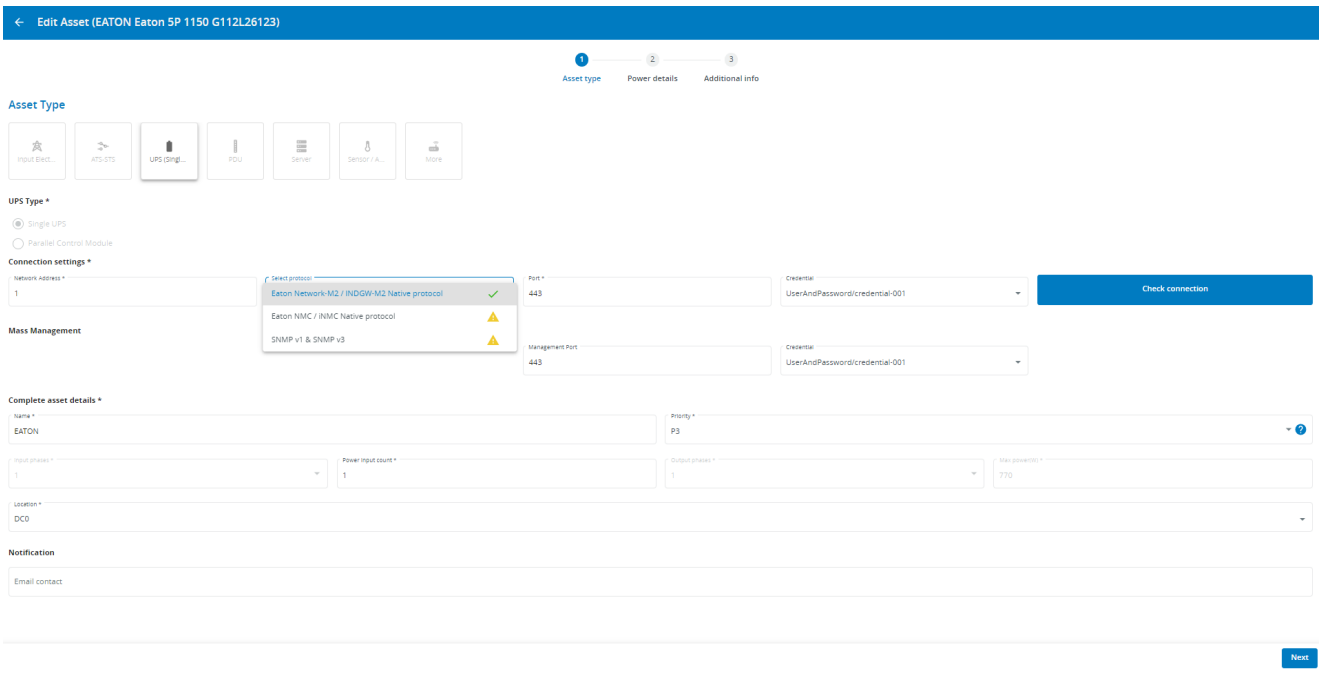
Before continuing with the addition of assets to your system, please consider the comments below:

1. Create the appropriate Input Power topology of your data center.
   There is a specific Power Chain object in IPM Editions called the **Input Power Chain**. These are the power devices including Feed(s), Genset(s), stand-alone UPS(s) which provide power to your Data center. All devices with a **location set to Data Center**, are included automatically in the Input Power Chain. See the different recommended topologies available in the Supported Power Chain Topologies section.
2. After defining the input power chain of the data center, we recommend to first proceed with the creation of all rack mounted power devices (i.e. rack mounted UPSs, rack PDUs) in order to complete the power chain down to the rack device level.
3. For information on adding sensors to the asset list, please refer to the dedicated **T&H Sensor and Actuator Management section** in this document.
4. For information on adding daisy chained rack PDUs to the asset list, please refer to the **ePDU G3/G3+ Daisy Chaining section** of this document.
5. For the Eaton power devices communication with the IPM Editions, the user has to enable SNMP v1 protocol from the Web interface of the ePDU. This is mandatory in order to get all data. Please don't forget to add SNMP v1 community in the dedicated credential in the Security Wallet (from the Settings section) if the ePDU community name is different than "public".

Manually add a new asset

In order to create a new asset, you simply use the **Add New Asset** button and a stepper will appear:

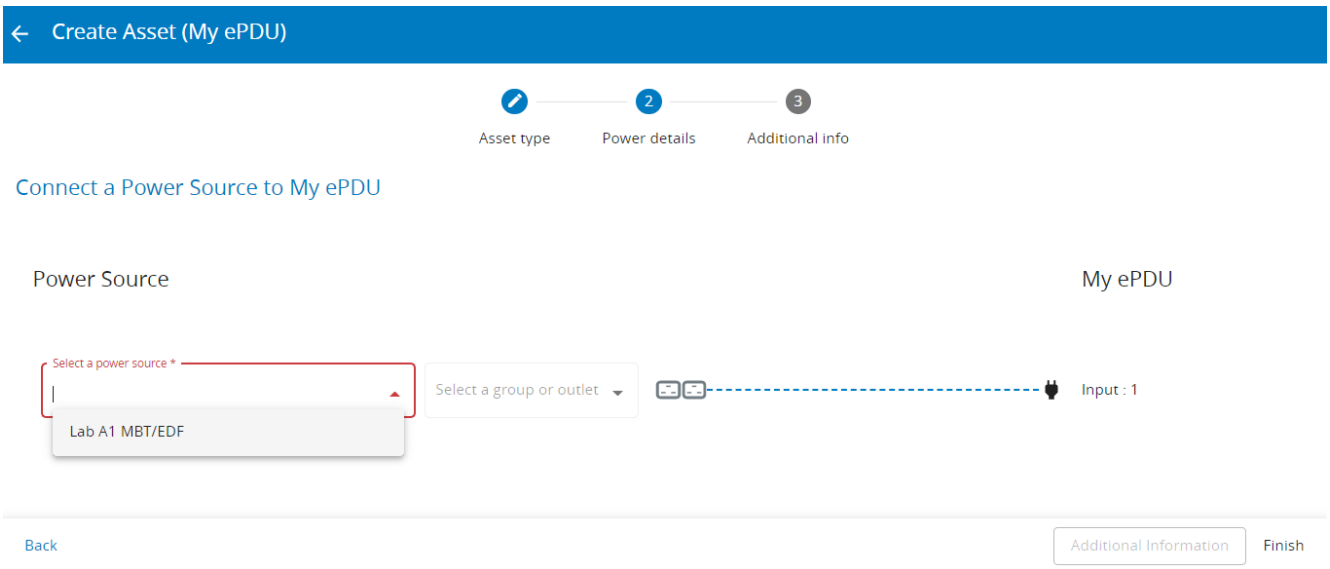
- **Step 1:** you select the asset type and configure the basic asset information.



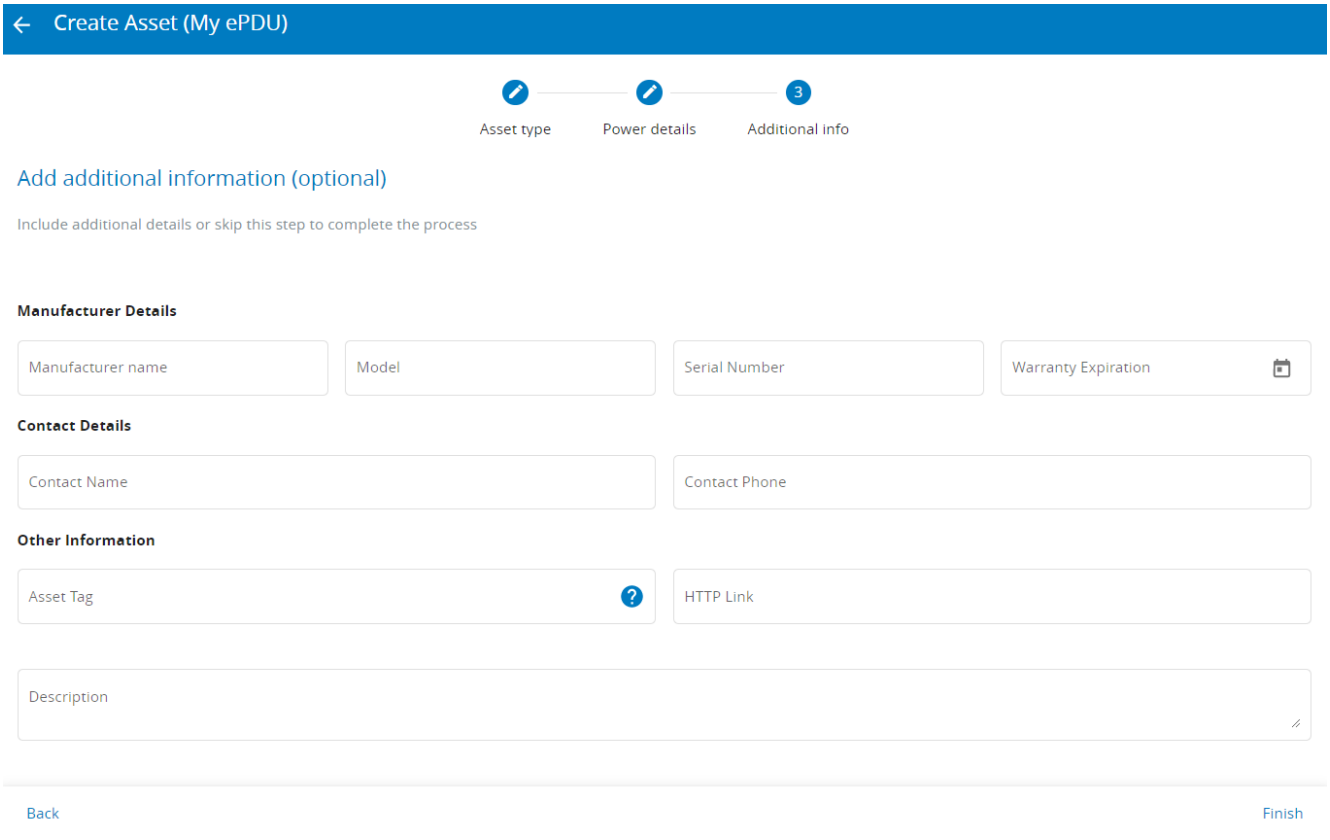
TIP

- All fields marked with an asterisk (*) are mandatory.
- Based on the selected asset type, the configuration screen will populate additional fields related to the specific device device type (e.g. for ePDU).
- Configuring **Network Address** + **Protocol +Port + Credential** allows you to discover automatically Asset capabilities
- In **Select protocol** a green check mark indicates that an asset is already discovered through this protocol
- If the asset is configured with custom port values, these custom port values can be configured for Monitoring and Mass Management features

- **Step 2:** From the select area, you configure the Asset Power Source



- **Step 3: (Optional)** Configure "Additional Information" that are used for contextual display purpose.



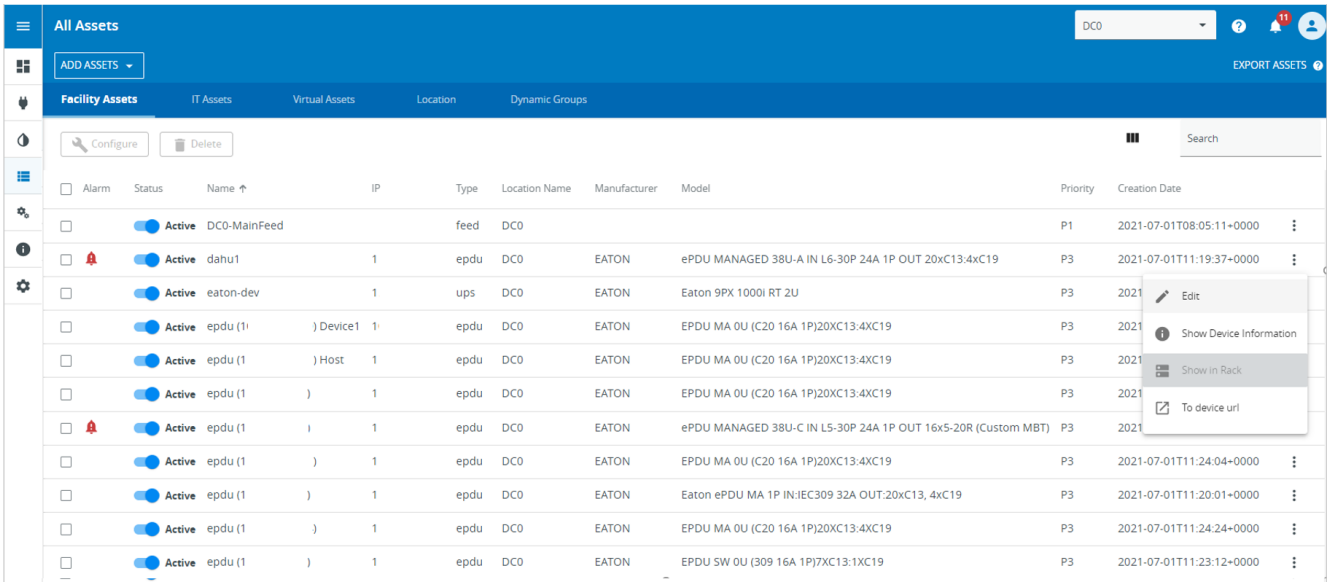
TIP

- Make sure you define the **location** of your assets and set them to **Active** in order to get telemetry data.
- If your Asset is configured with custom port values (e.g. with 444 instead of standard 443) then HTTP Link can be configured with following syntax https://xxx.xxx.xxx.xxx:444 so that you can access more easily **To device URL**

Once all the information has been input, simply click **Finish** and the device will appear in the Asset list.

Edit an existing asset

In order to edit an existing asset, the user must select the icon (3 vertical points) at the right hand of the Asset line, or directly right click on the Asset line and click on **Edit**.



The 3 steps wizard documented above will provide Asset edition feature.

All existing asset information will appear and the user will be able to edit the editable fields (there may be non-editable fields, shown in grey).

Delete an Existing Asset

You may delete any assets present in the Asset list except for the Data Center.

In order to delete an asset, it must not have any child devices from a power chain topology or from a location perspective.

All child assets must be deleted prior to deletion of a parent asset.

Asset Mass configuration

IPM Editions allows you to configure multiple assets at once by selecting:

1. a correctly configured source device first,
2. all or part of the settings of this source asset,
3. the set of all target assets last.

As a result, the selected data set from Step 2 will be bulk-applied to all of the selected target assets during Step 3.

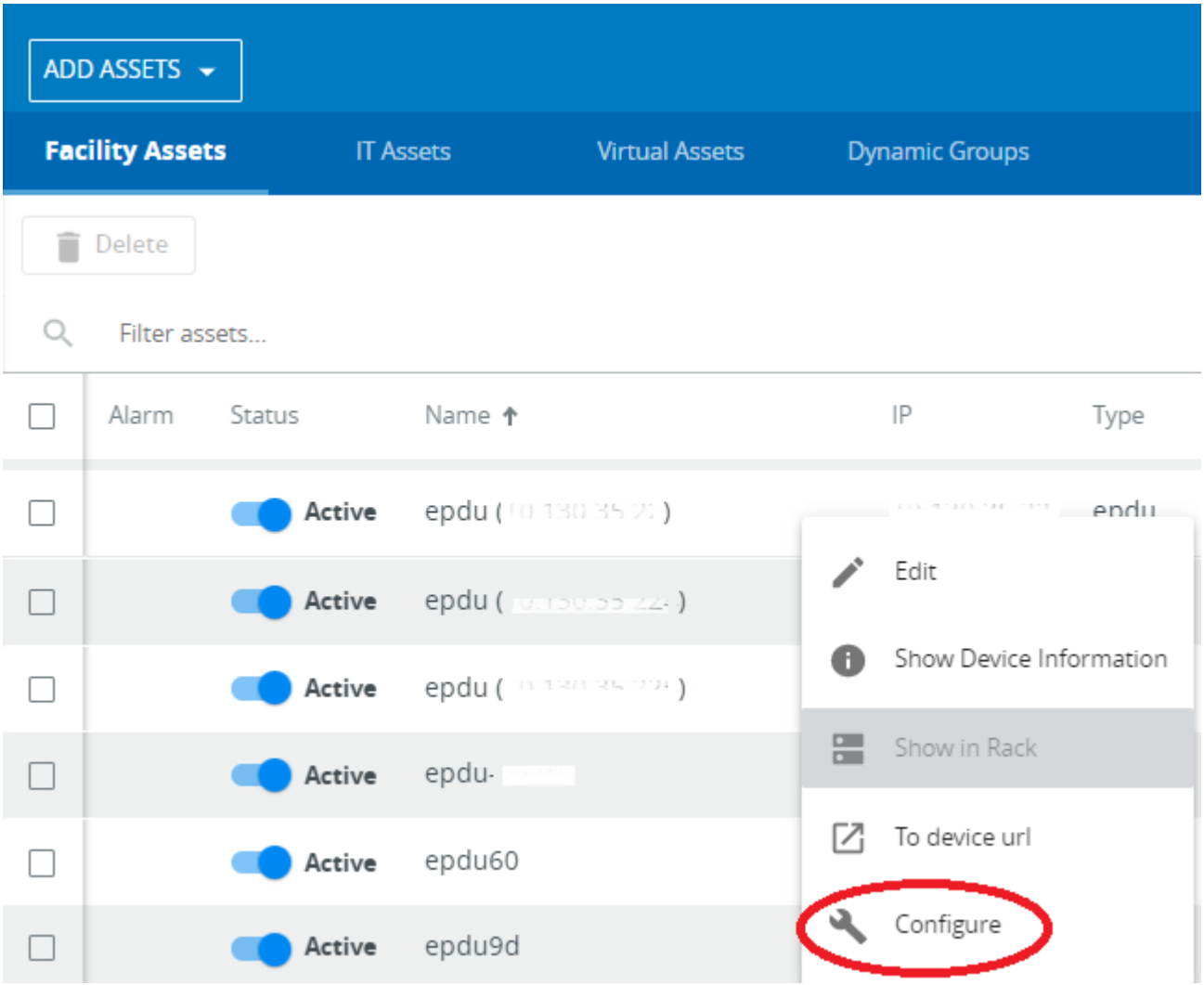
Note

Notice that a configuration can be copied only to the same type of device (card/product/vendor) running with the same firmware version.
List of eligible assets :

UPS/NMC	Network-MS / Modbus-MS cards
ePDU/G3	ePDU Network management card

Rack PDU/G4	Rack PDU Network management card (FW version 2.4.1 and upper)
UPS/NM2	Network-M2 / INDGW cards (FW version 1.7 and upper)
UPS/NM3	Network-M3 (FW version 1.0 and upper)
ATS/NMC	Network-MS / Modbus-MS cards
ATS/NM2	Network-M2 / INDGW cards (FW version 1.7 and upper)
ATS/NM3	Network-M3 (FW version 1.0 and upper)

To begin this process, go to the Asset management view, select the source asset from which you want to copy the configuration, then right-click on the selected item and select the **Configure** option in the drop down menu.



The mass configuration ease the way to apply a full configuration or a part of configuration from a device to other devices.

The detailed procedure is described in Asset mass configuration view page

Dynamic groups of assets

In Automation, some actions can apply either to a single device or to a group of devices.

In Asset Management, we provide the possibility to define a dynamic Asset Group by a dynamic rule.

Rules are covering the following fields:

- Asset Name : based on the column "Name" of the asset's table
- Asset Hostname : based on the column "Hostname" of the asset's table
- Asset Network Address : based on the column "Network Address" of the asset's table
- Asset Location : based on the column "Location Name" of the asset's table
- Asset Contact : based on the column "Contact Email" of the asset's table
- Hosted By : based on IPM Editions known hosts
- Tags : based on vSphere tags **(only for virtual assets managed by vSphere)**

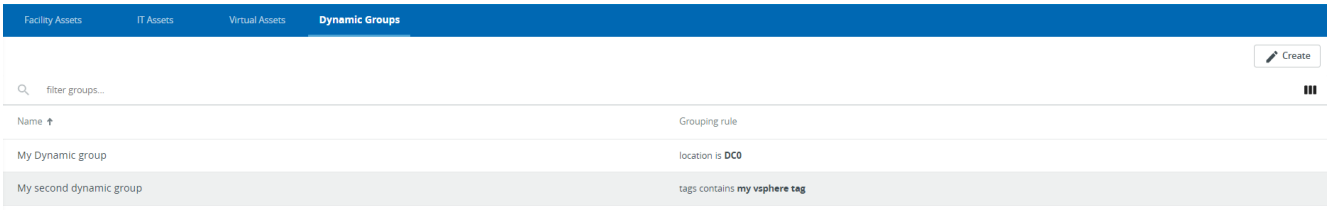
Group Table

The screenshot here after illustrates an example with several groups displayed in the table (one group on each line).

Create button allows to create a new Group. This feature is described on next paragraph.

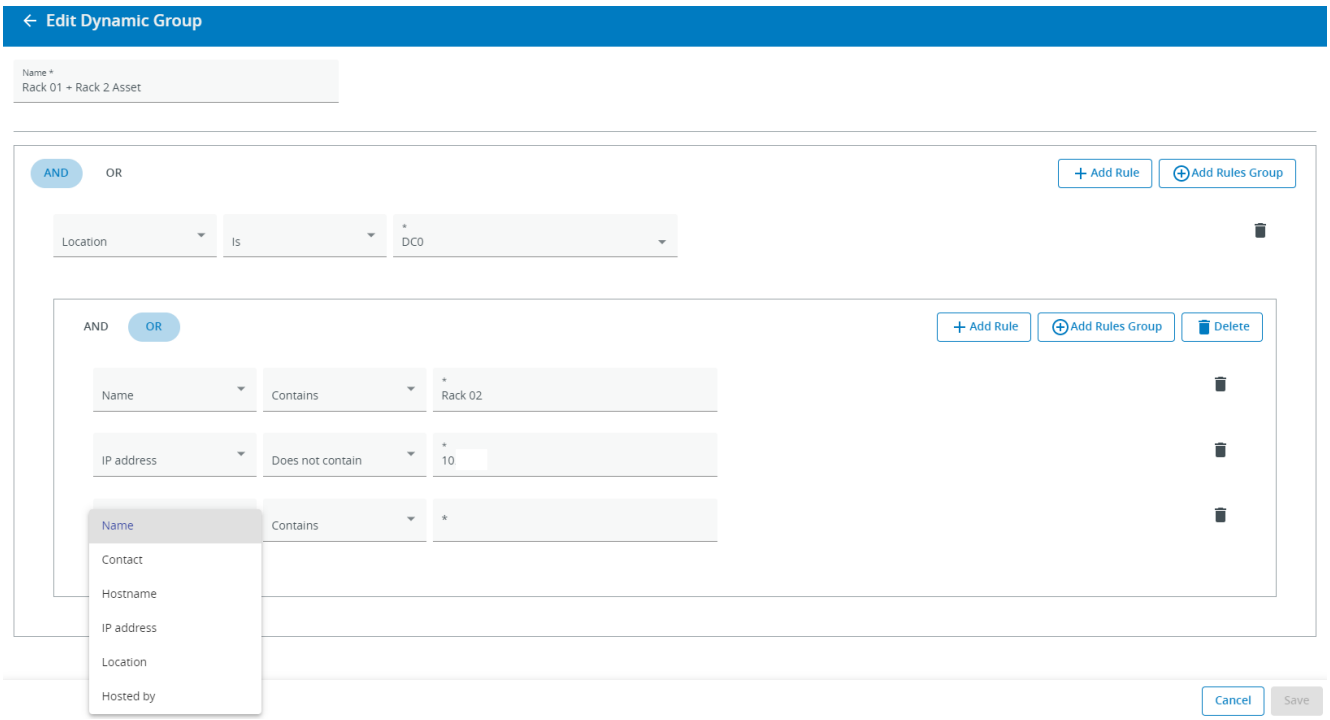
The table displays following information for each Group:

- Group **Name**
- **Grouping Rule** Summary is displayed in an intelligible manner
- Mouse over buttons allows to access to following features
  - **Edit** to edit the group
  - **Delete** to delete the group
  - **Info** to show the Group content



Create/Edit a Group

- In **Dynamic Groups** Tab click on **Create** button and following window will appear
- Enter following information :
  - Group **Name**
  - Enter a first criterion based on:
    - Asset **Name** : based on the column "Name" of the asset's table
    - Asset **Hostname** : based on the column "Hostname" of the asset's table
    - Asset **Network Address** : based on the column "Network Address" of the asset's table
    - Asset **Location** : based on the column "Location Name" of the asset's table
    - Asset **Contact** : based on the column "Contact Email" of the asset's table
    - **Hosted By** : based on IPM Editions known hosts
    - **Tags** : based on vSphere tags **(only for virtual assets managed by vSphere)**
  - Operator is automatically filled and you can choose (Contains / Does not Contain or Is / Is not)
  - Enter the filtering expression (Free text field or Location or Host list, ...)
  - Click on **Add Rule** if you want to add a second rule (the rules combine with the AND/OR logical operator)
  - Click on **Add Rules Group** if you want to add a second level rules group (the Rules Group combines with the AND/OR logical operator)



Groups usage

Once some groups are defined they can be used in Automation to feed the actions in a dynamic way.

Note that when one group is defined as the target of a action, the actual group content is evaluated at the time the action is executed.

To learn more about groups usage in Automation, please refer to the Automation section.

1.3.2 T&H Sensors and Actuator Management

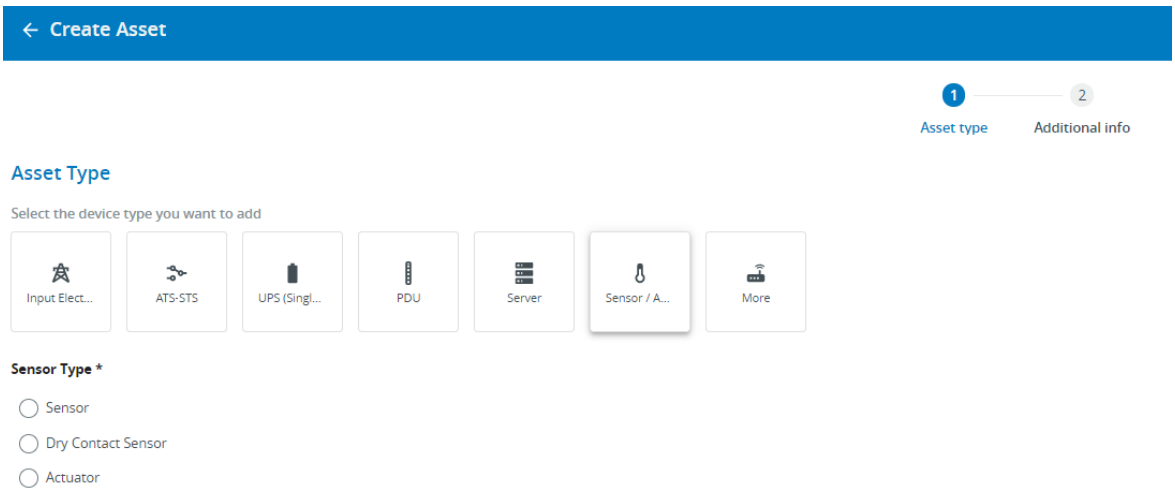
The T&H sensors and Actuators are managed as facility assets. Therefore, you may create and edit a sensor from the asset management page or via the CSV file. You may also delete any sensor from the asset management page.

IPM Editions can monitor :

- T&H sensors : sensors connected to Eaton power devices (i.e. UPSs, ePDUs)
- Actuators : Eaton EASYE4 PLC - 4GPOs (without extensions), with a Modbus TCP protocol.

In order to configure the sensor connection, you must specify the **Location port** and the **Location in DC** fields.

> **NOTE**
>
> For sensors, you will need to create the device to which the sensor is connected before creating the sensor itself.
> Rules for the location port numbering are provided in the asset management view documentation in "Add an Asset" section.



Temperature & Humidity sensors (T&H) are typically mounted physically in a rack. **The application requires that you specify a rack location for the sensor**. This is accomplished by selecting the **Logical asset**.
Once assigned to a rack, the values returned by the sensor will be used for computing the composite metrics of average temperature and humidity for that specific rack, as well as for the row, room and data center in which the rack is located.
The temperature and humidity values for rows are computed as averages of values of racks contained in the row. Row averages are then propagated to the data center level.

Rules for the sensors location port numbering
Eaton EMP001 sensors
If you are using first generation of Eaton T&H sensors (EMP001), no specific address is requested
Eaton Gen 2 T&H sensors (EMPDT1H1C2)
If you are using Eaton Gen 2 T&H sensors (EMPDH1T1C2), the sensor Modbus address is requested (refer to EMPDH1T1C2 specific User Manual to configure this Modbus address

NOTE

Make sure you define the power source for all of your assets in order to benefit from all contextual visibility and composite metric features in the application.

Some of the fields in the section **Additional Information** are used for enabling contextual visibility of metrics and/or in building the location and power chain topologies.

Once all the information has been input, you may simply press **Finish** and the device will appear in the asset list.

1.3.3 ePDU G3/G3+ Daisy Chaining

Eaton ePDU G3/G3+ offering can manage Daisy Chain configurations of up to 8 ePDUs connected in parallel requiring a single IP address and switch port to manage them all.

Depending on its topology, you must first configure the Daisy Chain on the ePDU device and define the host ePDU from the LCD (refer to Eaton G3/G3+ user manual for more information if required).

IMPORTANT NOTE

As for the ePDU in Single mode, you must enable the SNMP protocol from the Web interface of the daisy chained ePDUs. **This is mandatory to retrieve data from the ePDUs.**
You must also add a SNMP v1 community ("public" is the default SNMP v1 community name) or relevant SNMP v3 credentials accessible from the **Settings/Security Wallet** menu.
Refer to the Security Wallet documentation for more details on credentials management.

In the IPM application, you must create a new ePDU asset with the type "EPDU" and complete fill all mandatory fields.

This operation must be completed for all of the ePDUs in the daisy chain configuration (The host device plus all devices connected to the host).

NOTE

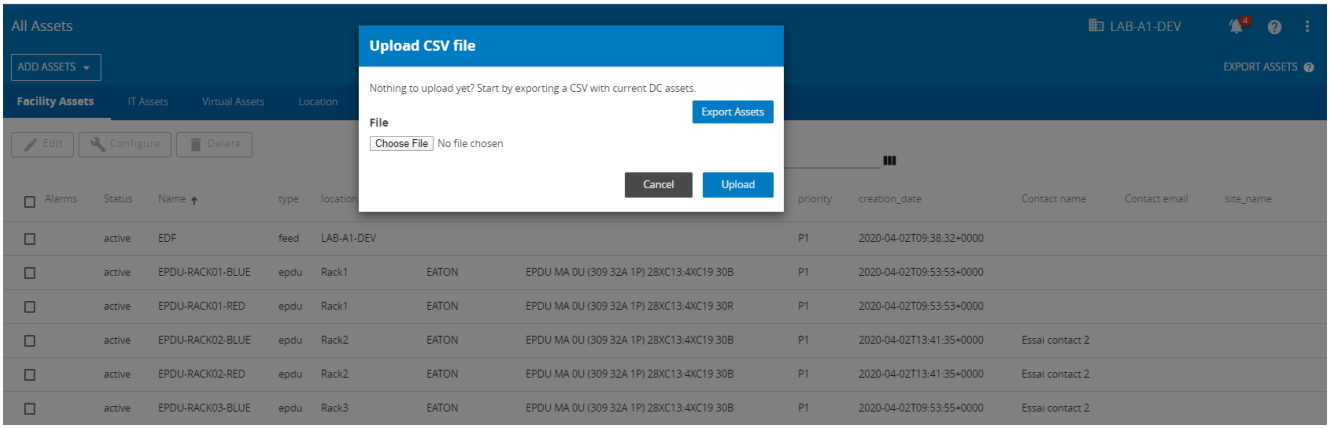
You must take care to ensure that the configuration defined in the application matches the configuration defined in the ePDU daisy chain topology, see table below:

ePDU LCD Configuration		Software Asset Daisy Chain Menu
0	(Host)	1 - Host
1	(Device)	2
2	(Device)	3
3	(Device)	4
4	(Device)	5
5	(Device)	6
6	(Device)	7
7	(Device)	8

How to use the CSV file for commissioning

It is possible to use a CSV file upload to add assets to the application.

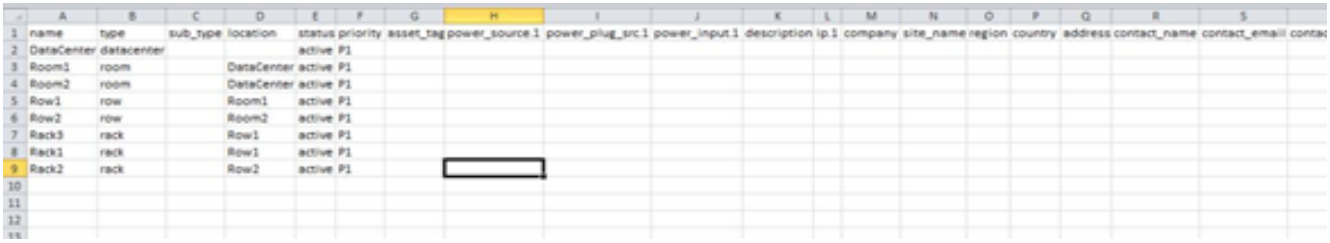
If you prefer to use the graphical tool, please click on **Cancel** and jump to the section **Asset Management from the User Interface**.



Initial CSV Creation

If you have not already completed your CSV file in advance of the IPM Editions installation and you want to continue with the asset configuration via CSV, you may simply start by exporting an initial copy of the CSV with all the information completed during the wizard steps.

To do this just click on **Export Assets**.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
1	name	type	sub_type	location	status	priority	asset_tag	power_source.1	power_plug_src.1	power_input.1	description	ip.1	company	site_name	region	country	address	contact_name	contact_email
2	DataCenter	datacenter			active	P1													
3	Room1	room		DataCenter	active	P1													
4	Room2	room		DataCenter	active	P1													
5	Row1	row		Room1	active	P1													
6	Row2	row		Room2	active	P1													
7	Rack3	rack		Row1	active	P1													
8	Rack1	rack		Row1	active	P1													
9	Rack2	rack		Row2	active	P1													
10																			
11																			
12																			

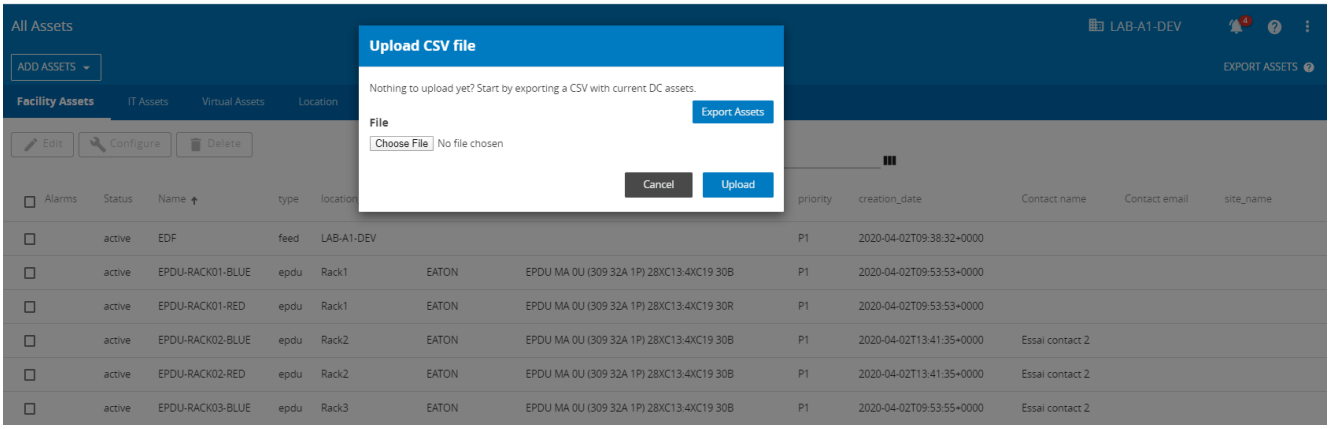
All the remaining details relating to the devices installed in the data center must be entered into the CSV file.

Once the CSV file is created, it will look like the populated sample displayed below.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	name	type	sub_type	location	status	priority	power_source.1	power_plug_src.1	power_inpu	power_source.2	power_plug_sr	manufacture	model	location_u_p	id
2	SRV31	device	server	Rack2	active	P3	EPDU-RACK02-RED	31		EPDU-RACK02-BL	31	HPE	G9	8	server-11
3	UPS04	device	ups	Rack4	active	P1	UPS01							1	ups-12
4	UPS01	device	ups	Rack1	active	P1	EDF							1	ups-17
5	UPS02	device	ups	Rack2	active	P1	UPS01							1	ups-18
6	UPS03	device	ups	Rack3	active	P1	UPS01							1	ups-19
7	SRV54 GENEPI	device	server	Rack1	active	P2	EPDU-RACK01-RED	11		EPDU-RACK01-BL	11	Dell	R6415	38	server-117
8	STS RACK01	device	sts	Rack1	active	P5	EPDU-RACK01-RED	1		EPDU-RACK01-BL	1			40	sts-118
9	HPE-PROD	device	ups	Rack1	active	P2	EPDU-RACK01-BLUE	5						33	ups-119
10	SRV32	device	server	Rack2	active	P3	EPDU-RACK02-RED	30		EPDU-RACK02-BL	30	HPE	G9	9	server-120
11	SRV33	device	server	Rack2	active	P3	EPDU-RACK02-RED	29		EPDU-RACK02-BL	29	HPE	G9	10	server-121
12	SRV34	device	server	Rack2	active	P3	EPDU-RACK02-RED	28		EPDU-RACK02-BL	28	HPE	G9	11	server-122
13	SRV35	device	server	Rack2	active	P3	EPDU-RACK02-RED	27		EPDU-RACK02-BL	27	HPE	G9	12	server-123
14	SRV36	device	server	Rack2	active	P3	EPDU-RACK02-RED	26		EPDU-RACK02-BL	26	HPE	G9	13	server-124
15	SRV38	device	server	Rack2	active	P3	EPDU-RACK02-RED	25		EPDU-RACK02-BL	25	HPE	G9	14	server-125
16	SRV45	device	server	Rack2	active	P3	EPDU-RACK02-RED	23		EPDU-RACK02-BL	23	HPE	G9	15	server-126
17	SRV20	device	server	Rack2	active	P3	EPDU-RACK02-RED	22		EPDU-RACK02-BL	22	HPE	DL385 G8	16	server-127
18	SRV16	device	server	Rack2	active	P3	EPDU-RACK02-RED	21		EPDU-RACK02-BL	21	FUJITSU	RX 300 S7	18	server-128
19	SRV42	device	server	Rack2	active	P3	EPDU-RACK02-RED	20		EPDU-RACK02-BL	20	DELL	PowerEdge R6	27	server-129
20	SRV43	device	server	Rack2	active	P3	EPDU-RACK02-RED	19		EPDU-RACK02-BL	19	DELL	PowerEdge R6	28	server-130
21	SRV44	device	server	Rack2	active	P3	EPDU-RACK02-RED	18		EPDU-RACK02-BL	18	DELL	PowerEdge R6	29	server-131
22	SRV41 (x3 - VXRAIL)	device	server	Rack2	active	P3	EPDU-RACK02-RED	7		EPDU-RACK02-BL	7	VXRAIL		30	server-132
23	SRV56	device	server	Rack2	active	P3	EPDU-RACK02-RED	4		EPDU-RACK02-BL	4	HPE	G10	32	server-133
24	SRV57	device	server	Rack2	active	P3	EPDU-RACK02-RED	3		EPDU-RACK02-BL	3	HPE	G10	33	server-134
25	SRV39	device	server	Rack2	active	P3	EPDU-RACK02-RED	10		EPDU-RACK02-BL	10	Lenovo	ThinkServer	25	server-135
26	SRV40	device	server	Rack2	active	P3	EPDU-RACK02-RED	9		EPDU-RACK02-BL	9	LENOVO	ThinkServer	26	server-136
27	EPDU-RACK04-RED	device	epdu	Rack4	active	P2	EDF								epdu-137
28	EPDU-RACK04-BLUE	device	epdu	Rack4	active	P2	UPS04								epdu-138
29	chassis test	device	chassis	Rack1	active	P1	UPS04			UPS01				2	chassis-139

CSV upload

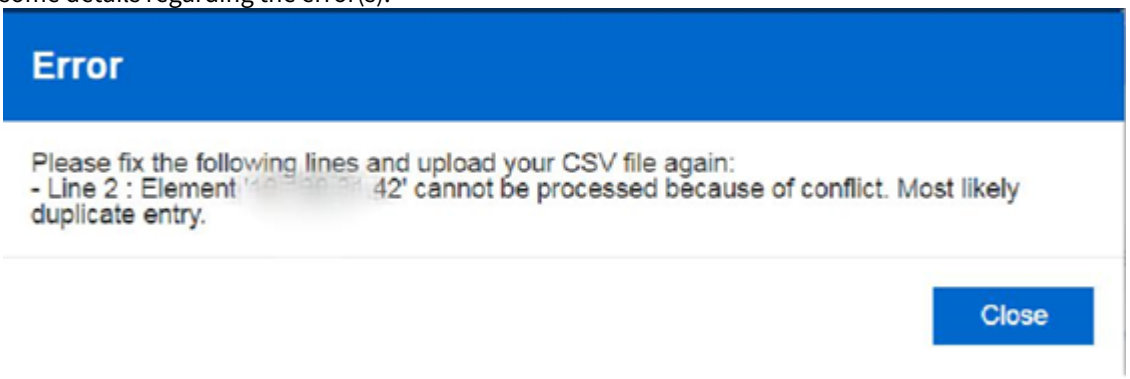
When you are done or if you already have a CSV file, you may upload it clicking on the **Choose File** button which will open a file browser in order to select your CSV file. Then click on **Upload** to import it in the system.



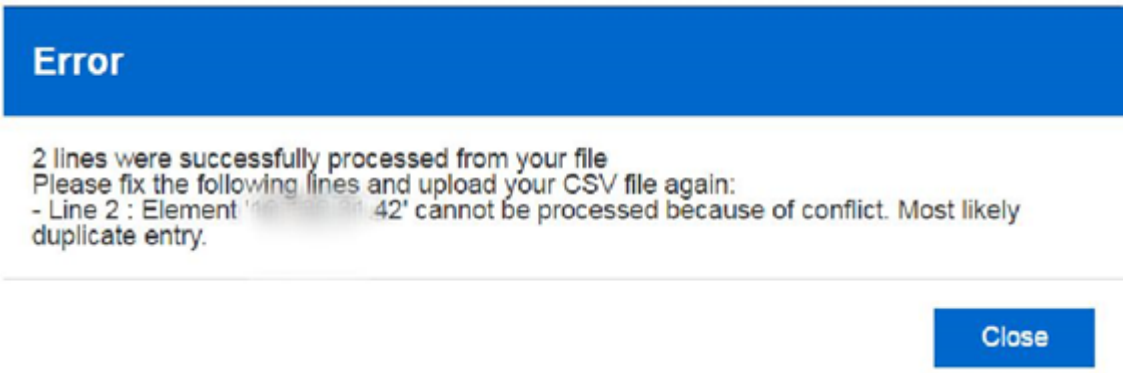
While the upload is being processed a progress indicator shows the progress of the activity.

Upload Errors

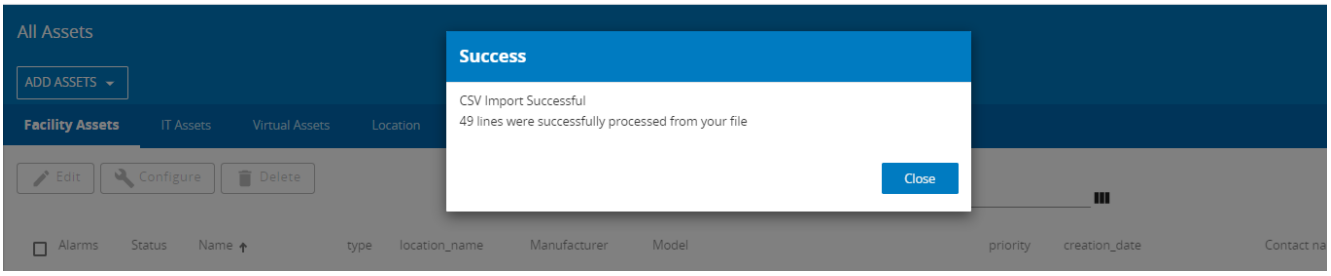
In the case an error occurs during upload, you will receive information about the line(s) that generated the error(s) and some details regarding the error(s).



In case the case where only some CSV lines are imported successfully, you will receive a after the import which will detail the import errors.



If the file upload is successful, you are given confirmation of the number of lines processed during the import.



Import Error Code Details

Error Condition	Code
Method is not allowed	45
Content size is too big	53

Error Condition	Code
File "assets" is missing	46
File "assets" has bad coding or bad format	47
Internal error (no connection to database, ...)	42
Mandatory columns are missing in the csv file	46
Load csv was success, but error occurred during configuration sending of asset change notification. Consult system log.	42
Request document has invalid syntax. Cannot detect the delimiter, use comma (,), semicolon (;) or tabulator.	48

To exit the CSV modal click on the **Close** button, this will bring you to the Asset Management page.

The details submitted via CSV upload may now be viewed in the Asset Management page in a simplified spreadsheet format.

You may edit the data center assets using the CSV file as follows:

1. Press the "Export Assets" button
2. Update the downloaded CSV file
3. Re-upload the CSV file using the "Upload CSV File" button.

1.4 Alarms Management

1.4.1 **Introduction**

IPM Editions offer to the user the capability of managing alerts.

An event can be defined as any detectable or discernible occurrence that has significance for the management of the IT infrastructure or delivery of an IT service as well as the evaluation of the impact a deviation might have on the infrastructure or service. Any important event must be made visible to the user by triggering alarms.

There are two types of alarms that currently exist in the application:

- Alarms generated at the IPM Editions level, using user defined or automatically imported thresholds (see the alarm threshold setting section for additional information)
- Alarms acquired directly from the monitored power devices (E.g. ePDUs, UPS)

Independent of the alarm type, all alarms have a set of attributes and follow a specific lifecycle.

The severity types are predefined priority levels for alarms related to particular elements and systems within the data center. All alarms need to be well defined and categorized depending on the impact caused to the business. Incorrectly defining alarms, such as under-prescribing priority levels can have serious consequences, not setting the appropriate priority level may result in a business impacting issue that is costly to resolve at too late a stage.

Over-estimating the priority level, can also cost a company more in the long run, costs such as remote hands work, overtime and call-out charges for on-call engineers.

Below are examples of how data center priority levels may be set:

- **P1 (Priority 1): Absolute Highest Priority - Directly impacting business**

    - Any alarm related to the data center power chain that directly negatively impacts on redundancy should always fall into this category
    - Any alarm related to IT Network Connectivity that is directly negatively impacting business should fall into this category
    - Any alarm related to IT Systems that is directly negatively impacting business should also fall into this category
    - Any alarm related to main chillers, pumps, AHU (Air Handling Units) and CRAC (Computer Room Air Conditioning) units that are directly impacting on the cooling of the data center and will therefore directly impact the business
    - Any alarm related to smoke alarms, fire alarms, fire suppression systems.
    - Any alarm related to data center physical security systems.
- **P2 (Priority 2): High Priority - Not yet impacting business but has potential to escalate quickly**
    - Alarms related to the data center power chain that have potential to impact redundancy soon, but are not yet at the business critical level.
    - Alarms relating to IT Network Connectivity that has potential to become a business impacting issue, but are not yet at the business critical level.
    - Alarms related to IT Systems that has potential to become a business impacting issue soon, but are not yet at the business critical level.
    - Alarms related to main chillers, pumps, AHU (Air Handling Units) and CRAC (Computer Room Air Conditioning) units that have potential to impact on the cooling of the data center soon, but are not yet at the business critical level.
- **P3 (Priority 3): Medium Priority - Not impacting business but could become critical in the short term**
    - Alarms related to the Data Center power chain that will not impact redundancy immediately, but can negatively impact on performance, and have the potential to escalate into more serious issues.
    - Alarms relating to IT Network Connectivity that will not impact business immediately, but can negatively impact on performance, and have the potential to escalate into more serious issues
    - Alarms related to IT Systems that will not impact business immediately, but can negatively impact on performance, and have the potential to escalate into more serious issues.
    - Alarms related to main chillers, pumps, AHU (Air Handling Units) and CRAC (Computer Room Air Conditioning) units that will not impact the cooling of the data center immediately, but can negatively impact on performance, and have the potential to escalate into more serious issues.
- **P4 (Priority 4): Low Priority - Not impacting business but could become critical in the long term if left unaddressed.**
    - Alarms related to the Data Center power chain that will not impact redundancy immediately, but can negatively impact on performance, and have the potential to escalate into more serious issues if ignored long term.
    - Alarms relating to IT Network Connectivity that will not impact business immediately but can negatively impact on performance and have the potential to escalate into more serious issues if ignored long term.
    - Alarms related to IT Systems that will not impact business immediately but can negatively impact on performance and have the potential to escalate into more serious issues if ignored long term.
    - Alarms related to main chillers, pumps, AHU (Air Handling Units) and CRAC (Computer Room Air Conditioning) units that will not impact the cooling of the Data Center immediately, but can negatively impact on performance and have the potential to escalate into more serious issues if ignored long term.
- **P5 (Priority 5): Minimal Priority - Not impacting business but worth taking note of to be resolved in futures service/maintenance intervals**
    - Alarms related to the Data Center power chain that are not impacting performance in any way, but will need to be resolved during maintenance periods.
    - Alarms relating to IT Network Connectivity that will not impact business or performance, but will require resolution during prescribed downtime/maintenance periods
    - Alarms related to IT Systems that will not impact business or performance, but will require resolution during prescribed downtime/maintenance periods.
    - Alarms related to main chillers, pumps, AHU (Air Handling Units) and CRAC (Computer Room Air Conditioning) units that will not impact the cooling of the Data Center or its performance but will require resolution during prescribed downtime/maintenance periods.

In the IPM application, you may define priority levels for each asset existing in the application. All alarms related to any asset will inherit the priority level of the asset and they will be treated accordingly.

1.4.2 **Alarm Lifecycle**

Any alarm can go through several states, with state changes triggered by user actions or system behavior.

All of these states and the possible transitions between them are described below:

Active	**Acknowledged**				**Archived**
Active	Ignore	Silence	Pause	Work in Progress	Resolved

> **NOTE**
>
> Once the alarm is acknowledged and has moved into any of the acknowledged states listed, it cannot be unacknowledged. An Acknowledged alarm can only be changed to another state of acknowledgement or resolved.

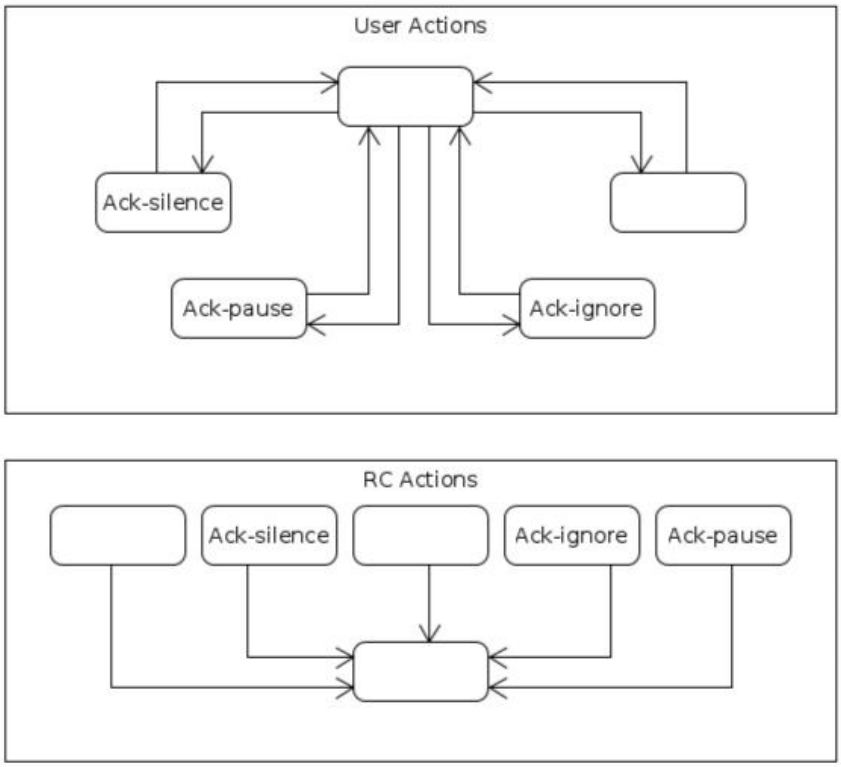
Ack State Changes	**Description**	**Visible on UI**	**Notification**	**Other**
ACK-IGNORE	Means that the user has acknowledged the alarm but has not taken action. The system should log the user's response & stop sending email/sms alarms for this alarm to this user, but continue sending the alarms to any of the other users in the group who have not acknowledged the alarm (group management post-alpha).	No	No	Can be un-ignored manually
ACK-SILENCE	Means that the user has acknowledged the alarm and is taking action to resolve it. The system should log the user's response & stop sending alarms to this person and any other person in the group. The alarms remains visible in the system.	Yes	No	Can be un-silences manually
ACK-PAUSE	Means that the user has acknowledged the alarm and is waiting for external input (user info, maintenance window, part delivery, ...) prior to resolving it. The system should log the user's response & stop sending alarms to this person and any other person in the group. The alarm remains visible in the system.	Yes	No	Can be manually un-paused or automatically after a specified amount of time
ACK-WIP	Means that the user has acknowledged the alarm and is currently classed as Work in Progress. The alarm remains visible in the	Yes	Email or SMS sent at regular intervals while the alarm is	

	system and continues to send out notifications at a specified time frequency depending on the priority/severity.		still present, interval determined by priority/severity	

If an alarm occurs in the system and is not acknowledged, the notification must be resent until the alarm is acknowledged and transitions into one of the states listed above.

Simplified Alarm Distribution Table

Critical	p1	5 min
	p2	15 min
	p3	
	p4	
	p5	
Warning	p1	1h
	p2	4h
	p3	
	p4	
	p5	
Info	p1	8h
	p2	24h



1.4.3 **Single Point of Failure detection**

IPM2 is able to detect "single point of failure" in the power chain. A single point of failure appear when all the input of a device are connected directly or indirectly to the same power source (see figure 1 for example). If a power outage happened your device may not be protected correctly. IPM2 is triggering an alarm to inform that it detect a single point of failure in the power chain.

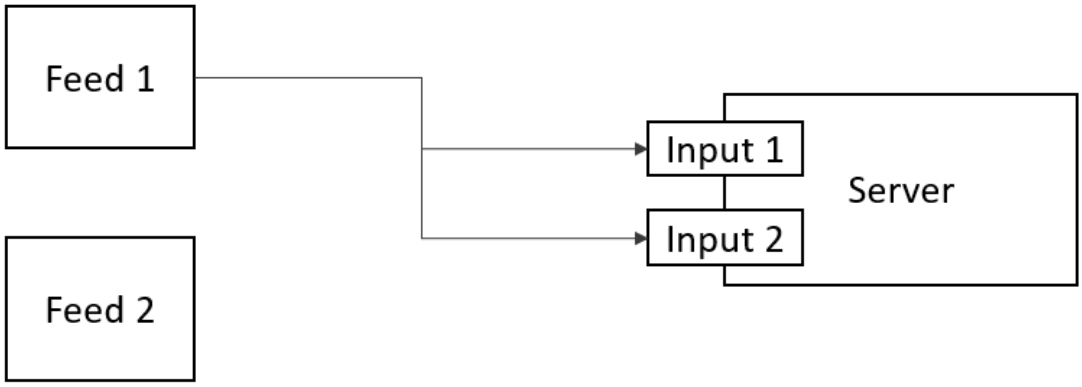


Figure 1

1.5 User Management

IPM Editions allows you to manage either:

- **Local User** (please go to the Local Users section of the documentation for more details)
  or

- **Remote Users** through LDAP (please go to the Remote Users section of the documentation for more details)

1.5.1 Local Users

IPM Editions allows you to manage up to 40 local user accounts split on two predefined profiles:

- **Administrator profile**: may access all features (monitor, commissioning, settings, user administration)
- **Viewer profile**: may access only the Dashboard and its own user preferences

> **Primary administrator**
>
> By default on the first install of IPM Editions, two user accounts are created : **admin** and **monitor**. (see default password below).
> Please note, that the built-in monitor user is deactivated by default.
> This initial **admin** account will be automatically defined as the **Primary administrator account**. This means that this account may not be edited by other user accounts with an administrator profile.
> The first connection is only possible with the "admin" account created by default. The password change will be requested on first connection.

Default passwords:

Login	Password
admin	admin
monitor	monitor

You may change the password for both user accounts from the Settings page, in the Preferences section.

> **WARNING**
>
> You should be forced by the application to choose a new password at first connection.
> In any case, it is strongly recommended to not keep the default passwords.

> **NOTE**
>
> The default password strength policy includes:
> - Minimum of 8 characters
> - At least 1 special character
> - At least 1 digit

Please go to the **Local Users** section of the documentation for more details

1.5.2 Remote Users

Please go to the **Remote Users** section of the documentation for more details

1.6 Automation

IPM Automation features allow you to create business continuity policies based on trigger events which define appropriate action(s) to protect your IT environment : both physical and virtualized.

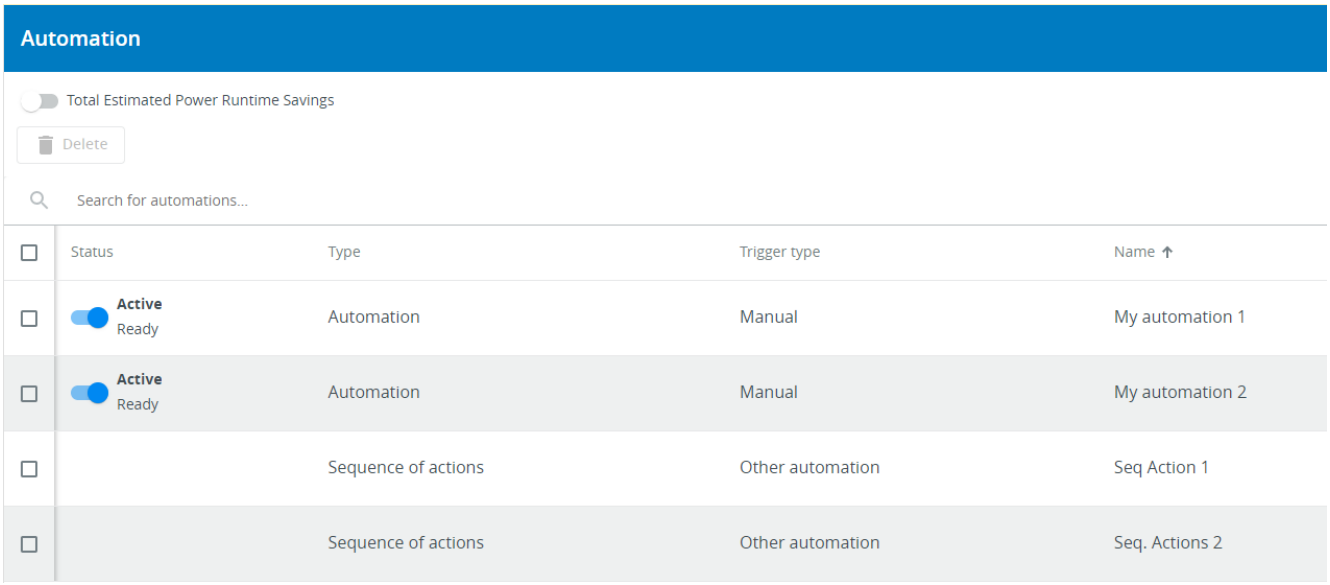
A wizard will assist you step by step to configure the automation policy.

You may create basic policies with simple actions like :***Send an e-mail in case an alarm is generated on my device***; but automation can also trigger **power actions** or **IT actions** to protect an environment like : **When a power outage is detected on *this* UPS then Shutdown my hypervisor and switch off the powering ePDU outlets**.

The automation panel enables you to configure 2 types of object:

- An "Automation" that will be executed when triggered. An automation is composed by a Trigger and a list of actions. An automation can be activated.
- A "Sequence of actions" that can only be executed in an "If/Else Action" of an Automation. A "Sequence of actions" cannot be activated. Its 'Trigger type" is "Other automation".

This chapter introduces how to automate actions and notifications in the Eaton Intelligent Power Manager (IPM) Editions application.



> **Note**
>
> Some feature restrictions may apply with respect to your software licence and kind of devices you are managing.
> Please check the license for more details.

1.6.1 Creating an automation :

1.6.2 Trigger events

To create an automation policy, the trigger event is the starting point of the configuration : **What event do I want to protect my IT environment from?**

The **Automation Wizard** is able to detect your configuration's capabilities. This means that the wizard will **only display the triggers provided by the assets that IPM has discovered and is actively monitoring.**

Once trigger event is selected, you must select the device to which it applies.

> **Note**
>
> An automation policy can based on a single trigger event.

A trigger can be derived from one or several assets :

- in the case of a trigger event derived from a **single asset** : the automation policy is started when the **trigger is generated by the asset**
- in the case of a trigger event derived from **multiple assets** : the automation policy is started when **trigger is generated by either all of the assets / or by any asset** (both configuration options are available)

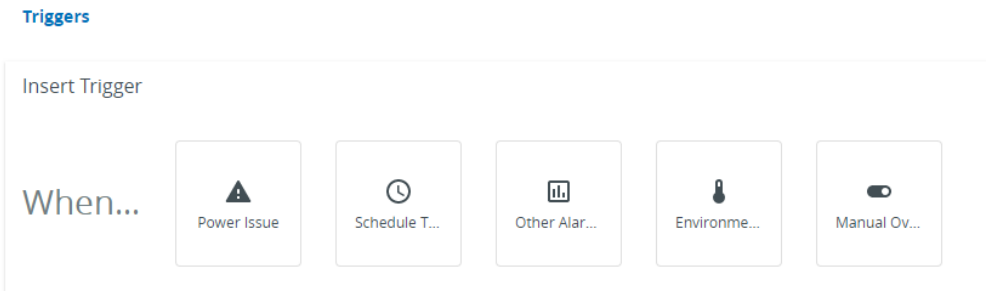
An automation can also combine multiple types of trigger events. (e.g. You can trigger an automation when a given UPS lose the power OR when a given rack temperature is critically high)

You just have to perform following steps:

- Configure a first Trigger
- Select **AND** or **OR** as logical operator to combine the triggers
- Click on **+ ADD Another** to configure a second trigger

An automation can also be triggered by composite devices (e.g. UPSs in parallel, ...)

Trigger events are categorized into 5 groups :



For more details, here's the list of main alarms templates currently managed by the IPM Editions application to trigger an automation policy :

	Datacenter	Rack	Row	Sensor	UPS	ePDU	STS
Average Humidity	✓	✓	✓	N/a	N/a	N/a	N/a
Average Temperature	✓	✓	✓	N/a	N/a	N/a	N/a
Charge battery	N/a	N/a	N/a	N/a	✓	N/a	N/a
Door Contact State Change	N/a	N/a	N/a	✓	N/a	N/a	N/a
Load default	N/a	N/a	N/a	N/a	✓	N/a	N/a
Input Load (1 phase)	N/a	N/a	N/a	N/a	N/a	✓	N/a
Input Load (3 phase)	N/a	N/a	N/a	N/a	N/a	✓	N/a
Low battery	N/a	N/a	N/a	N/a	✓	N/a	N/a

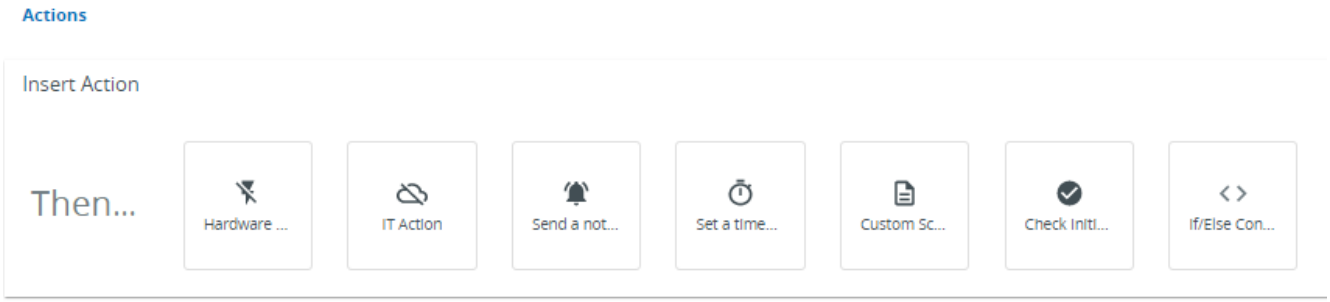
UPS running on battery	N/a	N/a	N/a	N/a	✓	N/a	N/a
On bypass	N/a	N/a	N/a	N/a	✓	N/a	N/a
Phase imbalance	✓	✓	N/a	N/a	✓	✓	N/a
Motion detected	N/a	N/a	N/a	✓	N/a	N/a	N/a
Total Power	✓	N/a	N/a	N/a	N/a	N/a	N/a
Section Load	N/a	N/a	N/a	N/a	N/a	✓	N/a
Smoke detected	N/a	N/a	N/a	✓	N/a	N/a	N/a
STS Frequency	N/a	N/a	N/a	N/a	N/a	N/a	✓
STS Preferred Source	N/a	N/a	N/a	N/a	N/a	N/a	✓
STS Voltage	N/a	N/a	N/a	N/a	N/a	N/a	✓
UPS internal temperature	N/a	N/a	N/a	N/a	✓	N/a	N/a
Vibration detected	N/a	N/a	N/a	✓		N/a	N/a
Input voltage (1 phase)	N/a	N/a	N/a	N/a	✓	✓	N/a
Input voltage (3 phase)	N/a	N/a	N/a	N/a	✓	✓	N/a
Water Leakage	N/a	N/a	N/a	✓	N/a	N/a	N/a
AC present	N/a	N/a	N/a	N/a	✓	N/a	N/a
Runtime	N/a	N/a	N/a	N/a	✓	N/a	N/a
Utility Restored	N/a	N/a	N/a	N/a	✓	N/a	N/a
Internal failure	N/a	N/a	N/a	N/a	✓	N/a	N/a
License is going to expire	NOK	NOK	NOK	NOK	NOK	NOK	NOK

1.6.3 Actions

Once the trigger event is configured and the asset, or the group of assets generating the trigger defined, you may define actions or a sequence of actions that you want to have applied when the automation is started.

As it is the case for the trigger events, the **Automation Wizard** is able to detect your configuration's capabilities and **filters the available actions** with respect to your assets and licensed capabilities so you are sure to only use authorized actions in your business continuity policy.

Actions are split into categories in the wizard to simplify the configuration :



- **Hardware - Turn on/off devices : you may control individual ePDU outlets**
  - Switch on/off ePDU individual outlets
    - Select individual outlets
    - Individual and daisy chained ePDU configurations are supported
  - Power on or Power Off a physical server
  - Power on or power Off one or more outputs of an actuator. Please see the Appendix IV - Configuring EasyE4 PLC with IPM for more information.
- **IT actions - you may configure actions to target your IT infrastructure including physical servers and virtualized assets when virtualization connectors are configured :**
  - vApp Power Action: this action executes a power command on a virtual application.
  - VM Action:
    - this action executes a command (migrate, power on/off, resume, shutdown, suspend, ...), on one or more virtual machines, or on one or more dynamic groups.
    - Savings Estimations : IPM is able to show an estimation of savings. For more details, please see the **Saving estimations** section of this document.
  - Host Power Action: this action executes a command on the targeted hypervisors, or on dynamic groups.
  - Cluster Power Actions : this action will initiate a cluster shutdown. Cluster Configuration supported :
    - VMware
    - VxRail
    - Nutanix
  - Storage : execute the shutdown on a storage node
  - HPOV Server Action : execute a command on HPOV server
  - Recovery Plan (SRM) : this starts a predefined recovery plan in fail-over mode. (only for VMware connectors)
  - Server action : execute a command on a physical server via ssh command, like Power on or Power Off
  - Fault Domain Action (VMware only)

- **Send a notification (email message) :**
  - possibility to edit the recipient list
  - possibility to customize the content of the email
- **Set a time delay - a configured interval (time or threshold) before a new action is run :**
  - wait for a duration (in seconds)
  - wait for a battery threshold (in %)
  - wait for a battery runtime threshold (in minutes)

- **Custom Script - you may configure an automation with predefined action based on a user defined script :**

> **Note**
>
> If the available automations actions within IPM application do not cover your use case, IPM allows you to launch your own custom script as an automation activity.
> We recommend you first manually develop your script and validate it and only after upload the custom script to the IPM application instance.

To configure custom script execution, you will have to:

- Upload the script to be executed:
  - A dedicated page in **Automation settings** is available for script management : Import/ Execute for test purpose /Download/Delete
  - Into **Custom Script** action definition you have a stepper with 3 steps:
    - First you can select or import a local script to configure an action
    - Then you have the option to specify:
      - the execution parameters (if any) to pass to it (command-line arguments to be concatenated to build the full calling syntax)
      - the appropriate values of the environment variables that the script uses (Environment variables) providing a <name,value> pair for each involved variable (if any)
      - test the script execution with a maximum execution time allocated (timeout)
    - Finally you define the how to proceed in case of action Timeout or Error

> **Note**
>
> - Script formats supported include : **BASH, Python, Perl**
> - Free IPMI library included in the IPM OVA for use in scripts
> - Redfish Tools library included in the IPM OVA for use in scripts
> - Wake on Lan libraries included in the IPM OVA for use in scripts
> - Expect command included in the IPM OVA for use in scripts

When using Python in User Scripts, beware that there is a vulnerability when the ipaddress library is used.
For more information, refer to [CVE-2021-29921|https://nvd.nist.gov/vuln/detail/CVE-2021-29921].

Note that the script must be written and saved in Unix format.
Other script formats are not supported.

Wake On Lan
etherwake package is used for the Wake on Lan feature.
To use this one, the following content must be added into your script:
sudo /usr/sbin/etherwake 00:00:00:00:00:00

(where 00:00:00:00:00:00 has to be replaced by the MAC address of your target system)

- **Check Initial Trigger Validity**
  - If initial trigger is no more valid you can configure several possibilities:
    - Continue the automation
    - Stop the automation
    - Start a rollback automation

- **If/Else action in the automation**
  - Possibility to execute a predefined "Sequence of actions" depending on the following conditions:
    - PowerSource status
    - PowerSource capacity %

- PowerSource runtime
- PowerSource load
- Temperature
- Humidity
- Day of the week (1st day is Monday)
- Time of the day (expressed in UTC time)

- Possibility to end the automation or to continue it in each "if" or "else" bloc

> **Note**
>
> If one of the actions performed in the "If/Else action" turn into error, then the "If/Else action turn into error, and the full automation will stop, and its ending status will be in error.
> An "if/else" action cannot run another inner "if/else" action.

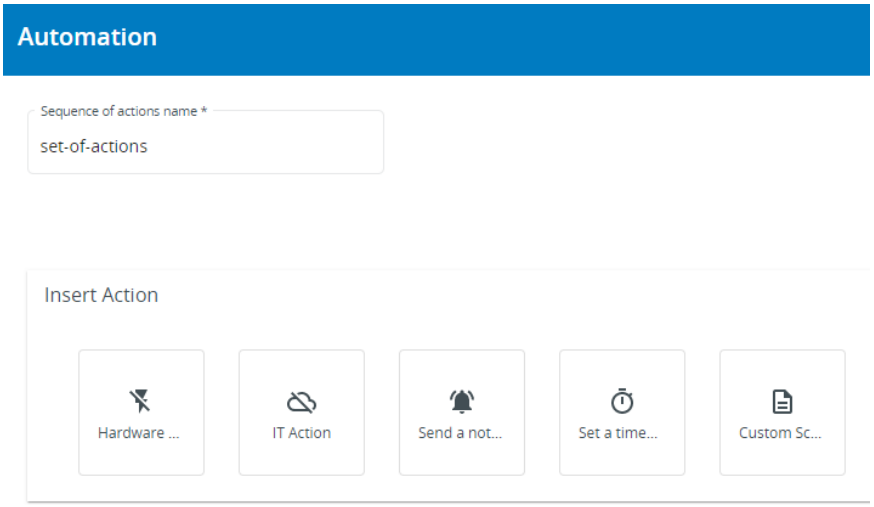
> **Note**
>
> For the IT actions, please note that some restrictions may apply with respect to your software licence and the virtualization connector configured. A given action may not be valid for all connectors.
> Please check the **IT actions supported** section below for more details.

Sequence of Actions:

A "Sequence of actions" is sorted list of actions that can be executed only in a "If/Else Action".

It can be created through the Automation panel : "Create new">"Sequence of actions" :

The "Sequence of Actions" Wizard will then guide you through the steps to create one "Sequence of actions":



An action is created within the Automation action wizard that guides you to setup one action.

Note

The "Check initial trigger" and "If/Else" actions are not available in a "Sequence of actions".
An executed action in a "Sequence of actions" ending in an error mode cannot run another automation before ending the "Sequence of actions".

If you edit a "Sequence of actions", all automations depending on this "Sequence of actions" are disabled until you review it, and saved it.

1.6.4 IT Actions supported

	Operating systems (Windows / Linux / ...)	vmware	Microsoft	NUTANIX
Host Power Actions				
Shutdown Host	n/a	✓	✓	✗
Shutdown VMs Then Host		✓	✓	✗
Enter Maintenance Mode		✓	✓	✓
Enter Maintenance Mode Then Shutdown		✓	✓	✗
Exit From Maintenance Mode		✓	✓	✓
Power Down To Standby Mode		✓	n/a	n/a
Power Up From Standby Mode		✓	n/a	n/a
Shutdown commands				
Windows Shutdown	✓	n/a	n/a	n/a
SSH	✓			
VM Actions				
Power On	n/a	✓	✓	✓
Power Off		✓	✓	✓
Shutdown Guest		✓	✓	✓

Shutdown Guest With Timeout		✓	n/a	n/a
Suspend		✓	✓	✓
Resume		✗	✓	✗
Migrate		✓	✓	✗
Fault Domain Actions				
Enter Maintenance mode then shutdown	n/a	✓	n/a	n/a
Enter Maintenance Mode		✓		
Exit Maintenance Mode		✓		
Recovery Plan (SRM) Action				
Recovery plan activation	n/a	✓	n/a	n/a
vApp Power Actions				
Power On	n/a	✓	n/a	n/a
Shutdown		✓		
Suspend		✓		
Cluster Power Actions ***(check info note below for cluster configurations supported by IPM)***				
Cluster shutdown	n/a	✓ (including VxRail cluster shutdown)	✓	✓
Servers Actions				
Power capping	n/a	n/a	n/a	n/a
Power On				
Power Off				

Storage Action				
Shutdown	n/a	n/a	n/a	n/a

Blue cell = connectors/actions available with "Optimize" license

Green Cells = connectors/actions available with "Manage" license

VMware Cluster configurations supported by IPM for cluster shutdown action :

- VMware,
- VMware HA + DRS
- VMware vSAN
- VxRail

Configurations with Critical and management VM embedded in the cluster are supported (IPM or vCenter within the cluster)

Nutanix Cluster configuration supported by IPM for cluster shutdown action :

- Nutanix AHV only

CLuster shutdown action is possible if IPM is outside the cluster : Critical and management VM embedded in the cluster are not yet supported

1.6.5 Saving Estimations:

IPM Edition is able to display an estimation of savings.

This feature is for information only. It is available for Virtual Systems plugged on a Eaton UPS. Supported models are 9PX and 5PX, all models.

Shown estimations are not contractual, **in no event nor circumstances shall Eaton or IPM Editions be held liable for any special** or consequential damages, loss or injury.

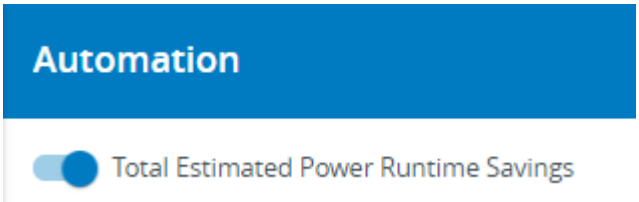
This feature is available from an "Optimize" License level.

Savings are estimated in terms of saved Runtime and saved Power.

It is based on an Artificial Intelligence algorithm and needs at least 120 minutes to train.

To have this feature activated, the user must first pair and power-chain is compulsory to link VMs with supported UPS.

Then, the toggle available from the Automation section, named "Total Estimated Power runtime Savings" must be powered on:



After this toggle activated, the system needs at least 120 minutes to learn before being able to display data.

When a Virtual Machine or an Hypervisor action is created or edited in Automation and saved in the list, the savings in terms of both power and runtime are displayed to the user:

Savings information are present for the following VM actions in automation, on Virtual Machines or on Hypervisors (pairing and power-chain is compulsory to link VMs with supported UPS) :

- shutdown
- shutdownGuest
- poweroff
- suspend

Only apply to static targeted assets (dynamic groups are not supported)
Savings always displayed even when accuracy is weak for all simple power chain without COPS

1.7 Xtreme Support Process

IPM Editions is intended to grow to support many third party devices, and especially Simple Network Management Protocol (SNMP) enabled ones.

If you would like to request support for a specific SNMP device that is not yet supported, please follow the support process defined in this section.

NOTE

The product embeds a tool that can be used to extract SNMP information from devices that are not yet supported.This tool can be used through a Secure Shell (SSH) connection.

Procedure to run the tool:

1. Connect to your IPM Editions instance via SSH, using the "admin" account
2. Run " fty-device-scan <IP address of the device> <your email address>"
   Example: fty-device-scan 192.168.0.10 john.doe@organization.com
3. Send the archive received by mail to EatonProductFeedback@eaton.com.

If possible, provide as much information on the device as possible in your mail, such as:

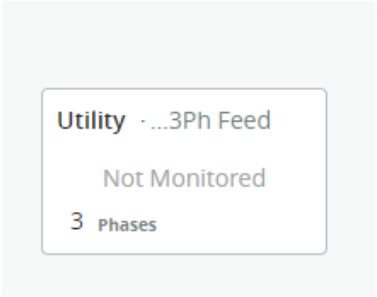
- the type of device, exact manufacturer and model names
- MIBs related to the device (or pointers to online versions, if available)
- any other information that you may find suitable.

Information and directions will be provided back to you shortly by mail to add support for your device.

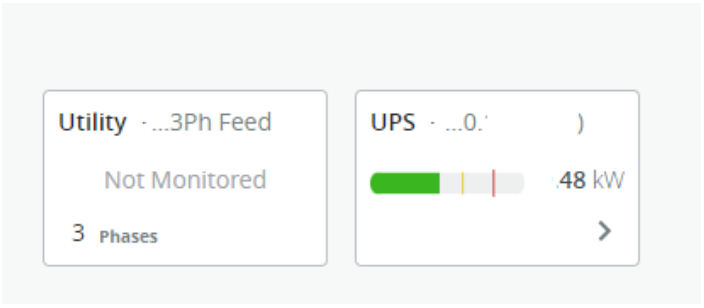
1.8 Typical Power Chain Topologies

1.8.1 Typical configurations for the input power infrastructure

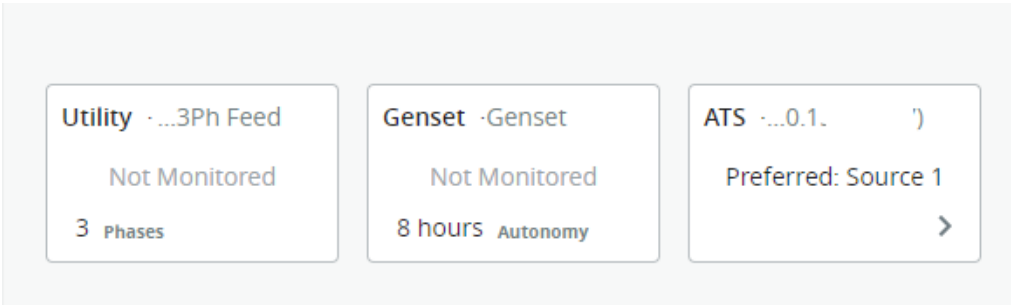
1. **Zero resilience configuration** with 1 main feed powering the infrastructure directly.



2. **Minimal resilience configuration with 1 utility feed and 1 UPS** protecting the critical infrastructure.

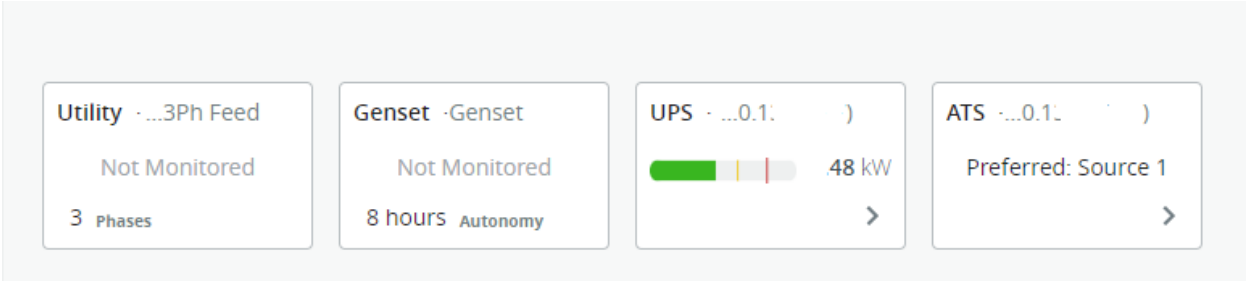


3. **Minimal resilience configuration with 1 utility feed, 1 GenSet, 1 ATS and a rack mounted UPS** (instead of a standalone UPS) installed in the white space with the IT devices

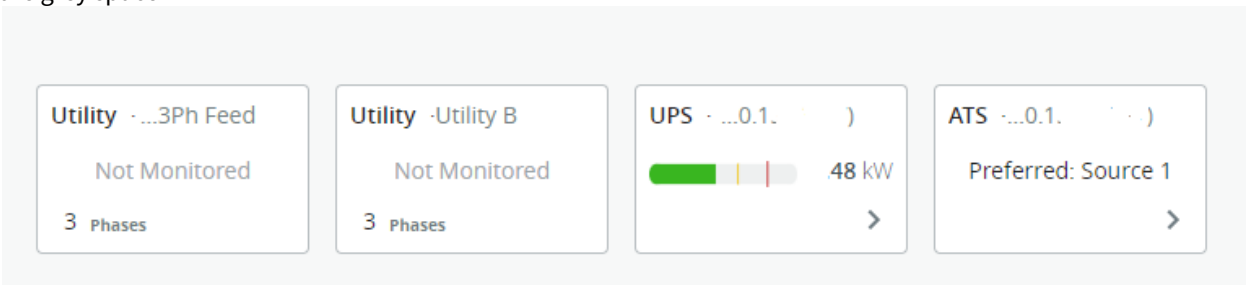


4. **Minimal resilience configuration with 2 utility feeds (Utility A & Utility B), an ATS and a rack mounted UPS** (instead of
a standalone UPS) installed in the white space with the IT devices

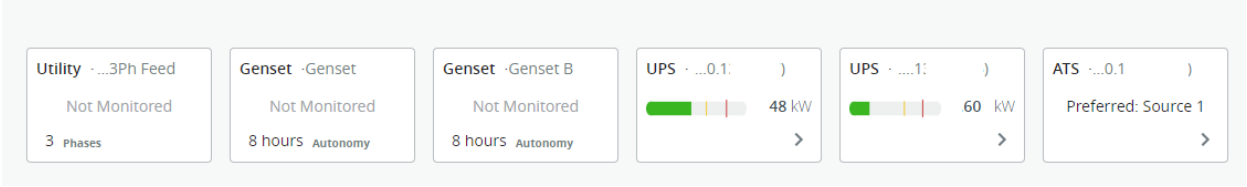
5. **N configuration (Tier I) with 1 utility feed, 1 GenSet, 1 standalone UPS** installed in the grey space



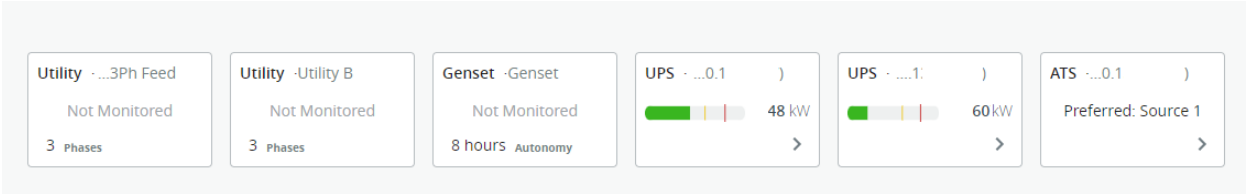
6. **N configuration (Tier I) with 2 utility feeds (Utility A & Utility B), 1 ATS and 1 standalone UPS** installed in the grey space



7. **N+1 (Tier II) Smart grid Configuration: 1 utility feed, 2 Gen Sets for additional redundancy, and 2 UPS**



8. **N+1 (Tier II) Smart grid Configuration: 2 utility feeds (Utility A & Utility B), 1 Gen Set for additional redundancy, and 2 UPS**

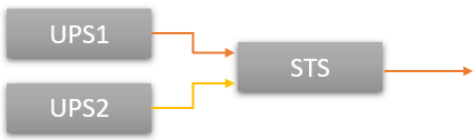


1.8.2 Local power redundancy schemes supported

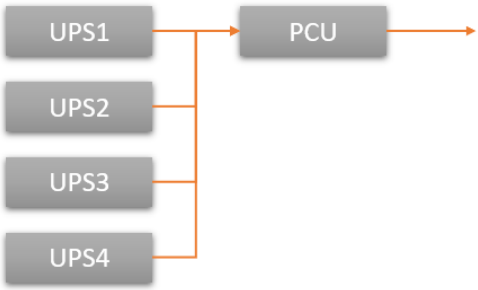
The following patterns are handled as composite power sources:

- UPS in serial:

- UPS connected to ATS



- UPS in parallel connected to a Power Control Unit (PCU)



> Connected UPS must be configured as exclusive feeds (but sensors) of the ending device of each pattern (UPS or STS or PCU)

Power chain analysis algorithms implemented in IPM Editions (starting at the Manage level) are able to automatically detect in the power chain the 3 patterns above and compute the composite power model providing two events:

- status change from "on line" to "on battery"
- low battery (based on capacity % less than a given threshold)

Those two events are usable in Automation as power events triggers as soon as the power chain configuration is completed.

1.9 Cybersecurity

At Eaton we are focused on analyzing emerging threats and ensuring that we are developing secure products and assisting our customers deploy and maintain our solutions in a secure environment.

We continously evaluate the cybersecurity landscape for emerging threats and provide the necessary communication on our website as soon as possible.

Eaton strongly recommends our customers to apply the deployment practices that are outlined on our Eaton Cybersecurity white paper *Cybersecurity considerations for electrical distribution systems* accessible on the Eaton website :

Cybersecurity considerations for electrical distribution systems *

* https://www.eaton.com/us/en-us/company/news-insights/cybersecurity/white-paper-cybersecurity-considerations-electrical-distribution-systems.html

1.9.1 Eaton cyber security notifications

You may view and register to receive notifications on current cyber security product vulnerabilities and recommended remediation actions at : Cyber security notifications **

** https://www.eaton.com/us/en-us/company/news-insights/cybersecurity/security-notifications.html

1.9.2 Cyber security known Issues

> When using Python in User Scripts, beware that there is a vulnerability when the ipaddress library is used. For more information, refer to [CVE-2021-29921|https://nvd.nist.gov/vuln/detail/CVE-2021-29921].

1.10 Licensing

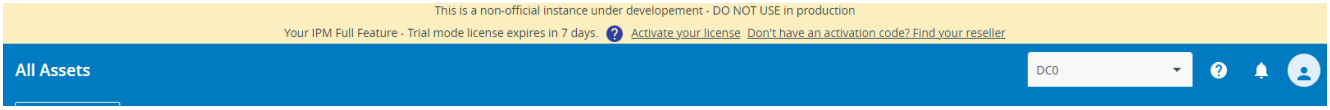
1.10.1 Initial trial period

All IPM Editions come with 60 days of trial embedded.

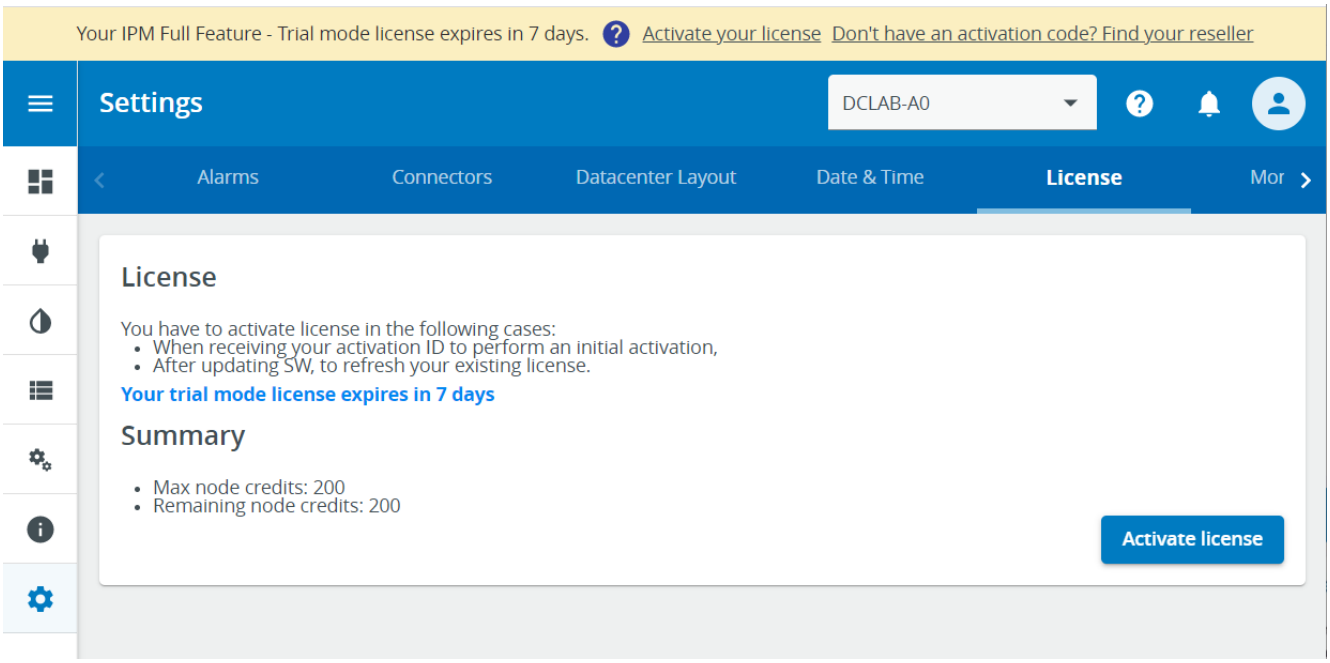
If you skip the license activation during the setup wizard, you may begin to configure your software and commission your assets prior to the activation of any additional license.

> **Note**
>
> Please note that after one week, the access to the software will be blocked and that an activation ID will be required to connect to the software again.

During these first days a yellow notification bar will appear on top of the application to tell you how many days are left in this initial trial mode.



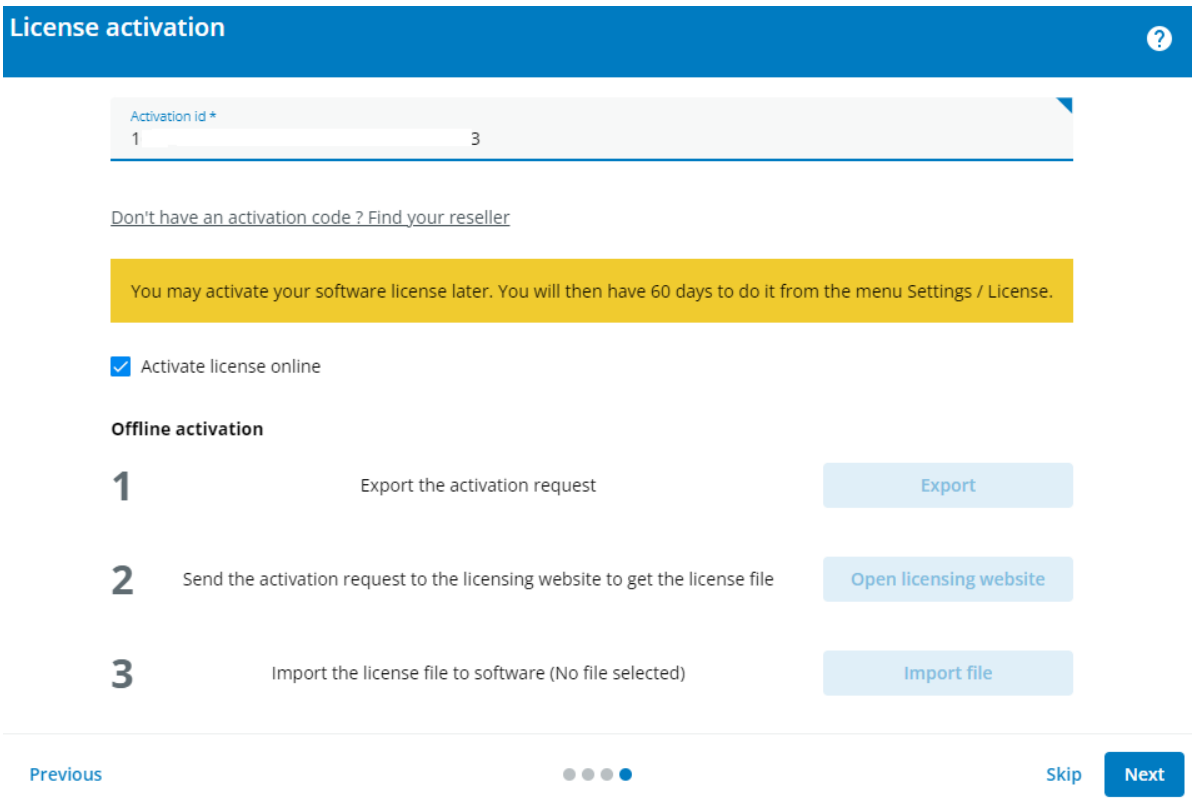
At any point, you can submit a license or subscription key to activate the software for a longer duration.
To do so, click on the **Activate your license** link in the notification bar or navigate to **Settings > License**



The current status of the License is always visible here.
In the above screen, you can see that the trial period is about expire and the high level features that we are entitled to at the moment.

At the bottom of this licensing information panel, you may click on the **Activate License** button to access the license activation wizard.

1.10.2 Online license or subscription activation



The IPM application supports both online and offline activation.

The screen shown above illustrates the situation where an IPM Edition is connected to the internet and can perform an online activation.

If the application is not able to reach the internet, a notification is displayed to tell you that Online activation is not available.

Type (or paste) your Activation ID into the corresponding input field and click **Activate** to start the activation process.

If you are in online activation mode, after you have clicked **Activate** you should simply wait a few seconds for the system to display a feedback in the current page.

> **Note**
>
> To get access to online activation, the configuration of the proxy address to be used to access the internet from your local network may be required. Refer to the network settings tab described in the contextual help chapter of this document for more details on configuring the proxy.

> **TIP**
>
> Make sure to use the Activation ID and not the Entitlement ID from the entitlement email you received.
> If you copy/paste the Activation ID into an input field, make sure to delete any preceeding or trailing spaces that may be inadvertently copied.

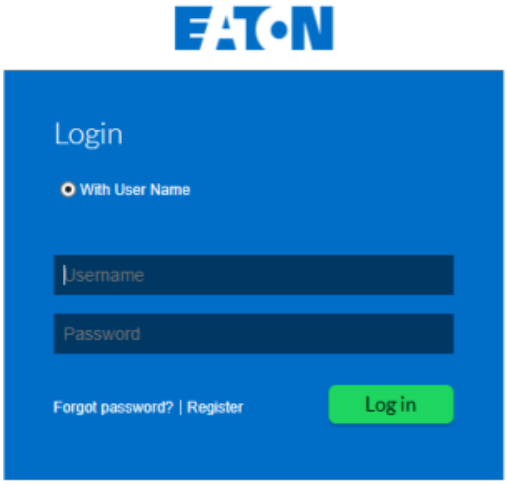
1.10.3 Offline license or subscription activation

If online activation mode is unavailable or unchecked, the below offline activation wizard screen should appear:

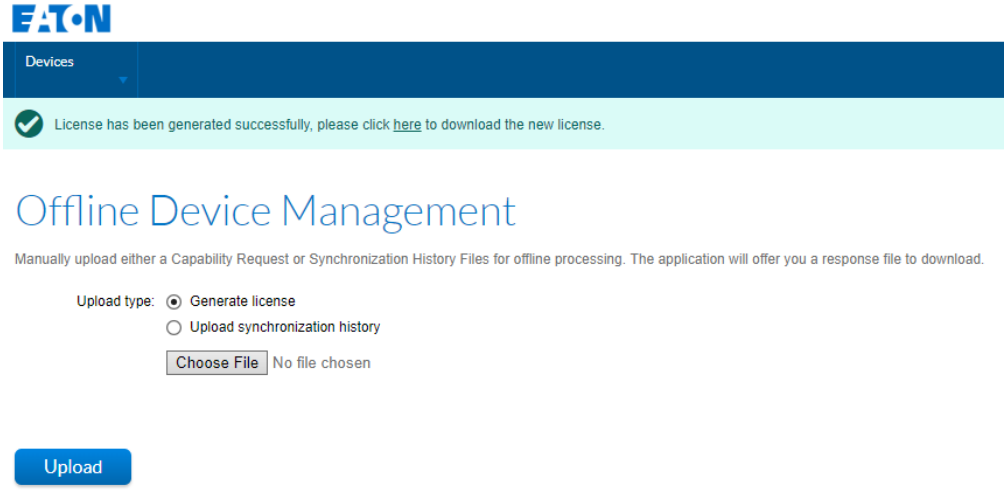
The manual (offline) activation process is comprised of 3 steps:

1. Click on "Export" button to generate a file called **capability_request.bin**

2. Click on the **Open Eaton website** button (or open following URL https://eaton.flexnetoperations.com/flexnet/operationsportal)
    a. This should open a new tab in your browser
    b. Select to authenticate **With User Name** and enter your username and password (if you didn't have a username yet, please proceed to a self-registration with your activation ID**)**



    c. Once connected, make sure you claimed all your Activation IDs, by using the menu *Activations and Entitlements → Claim Activation IDs* , and entering your Activation ID
    d. Then click on **Devices** from the top menu and then on **Offline Device Management**



    e. Click on **Choose File** and select the capability_request.bin file you generated in Step 1
    f. Click on **Upload**. You should be notified of the license generation success.
    g. Click on the "**click here**" link in the notification ribbon to download the generated license. This will download a file named **capabilityResponse.bin** . You may now close this tab and return to the IPM application tab in your browser.
3. The third step consists of importing the capability response file (generated at step 2.f above) into your software.
    a. Click on **Choose File** button in the Activation Wizard.
    b. Select the capability response generated during Step 2.
    c. Click on **Import**

You should be notified about the success of the software activation process. Congratulations!

1.10.4 Other license activations

The above process applies to the first activation of your SW instance. There are other situations when you need to activate again.

Here is the list of the other situations requiring a license activation to take advantage of your latest purchases:

- If you have already activated a perpetual SW license, activate your Subscribed maintenance to benefit of feature updates for free when available.
- If you have updated your SW version (2.2.0-1 → 2.3.0 ; 2.3.0 → 2.4.0 ; ...), refresh your license to take advantage of the new features of the newer version.
- If you have upgraded your Edition from Monitor to Manage or Monitor to Optimize or Manage to Optimize, refresh your license to take advantage of the new features of your instance.
- If you have purchased an increase of licensing credits, refresh your license to take advantage of those additional credits (and hence of additional assets).
- If you have purchased a renewal, refresh your license to take advantage of the extended duration of your entitlement
- If you have purchased a Plugin license, activate it to benefit from its pecific features.

Whenever an initial activation has already been done (after a self registration), and online connectivity is available, you will be able to use the Online Activation for all the above!

1.10.5 What does licensing do?

The licensing model allows to define which features you are entitled to and the duration of this entitlement.

In particular, your license or subscription allows you:

- to manage an infrastructure made of active assets which number is governed by the purchased of node credits
- to benefit from free updates of the software with a valid subscription or maintenance entitlement

Once a license has expired, configuration changes and asset management functions are deactivated.

Make sure to purchase a renewal of your license early enough to avoid any disruption in your usage of IPM Editions product.

For that matter, the application will warn you in advance about the expiration of your time delimited maintenance or subscription products.

1.10.6 How node credits are counted?

Each IPM instance is having a node credits count.
The initial trial period comes with a default count.

After this period, a license must be acitvated in order to unlock the SW and get a longer term node credits count.

This count controls whether the end user can or cannot activate a new asset.

Activating an asset is mandatory to monitor it and to take an action on it.

In order to activate successfully an asset, there must be enough credits in the IPM instance count at the time of activation.

The required count depends on the asset type:

- Power device (UPS, ePDU, ATS,...), always require one (1) credit
- Locations, IT assets (except servers) and Virtual assets (except hypervisors) always require 0 node credit
- Independant Hypervisors and Servers require one (1) credit
- Hypervisor/Server pairs require only one (1) node credit for both elements as they are seen as 2 facets of the same server.

Credit count evolution through a simple example

Operation	Node credits count	Rule that applies
Initial order of 40 node credits	40	Result of initial purchase
Activate a data center	40	Locations are not counted in the node credits

Operation	Node credits count	Rule that applies
Activate a room	40	Locations are not counted in the node credits
Activate a row	40	Locations are not counted in the node credits
Activate 2 racks	40	Locations are not counted in the node credits
Activate 2 UPS	38	Each power device count for 1
Activate 4 ePDUs	34	Each power device count for 1
Activate 10 servers	24	Each independent server count for 1
Activate 8 hypervisors	16	Each independent hypervisor count for 1
Pair a server to an hypervisor	17	A server/hypervisor pair count just for one
Pair 7 other servers to the 7 remaining hypervisors	24	A server/hypervisor pair count just for one

All impacts of assets activation status

As mentioned before, inactivated assets can't be monitored and won't be managed.

Here are the additional rules based on activation status:

- Clusters and vApps are manageable if all their embedded hypervisors are activated
- A VM is manageable if its embedding hypervisor is activated

1.11 Graphite / Grafana deployment

IPM provides a connector to a Graphite server. This connector maybe available or not depending on your license.

You can find additional information on the Graphite server and Grafana documentation at the links below:

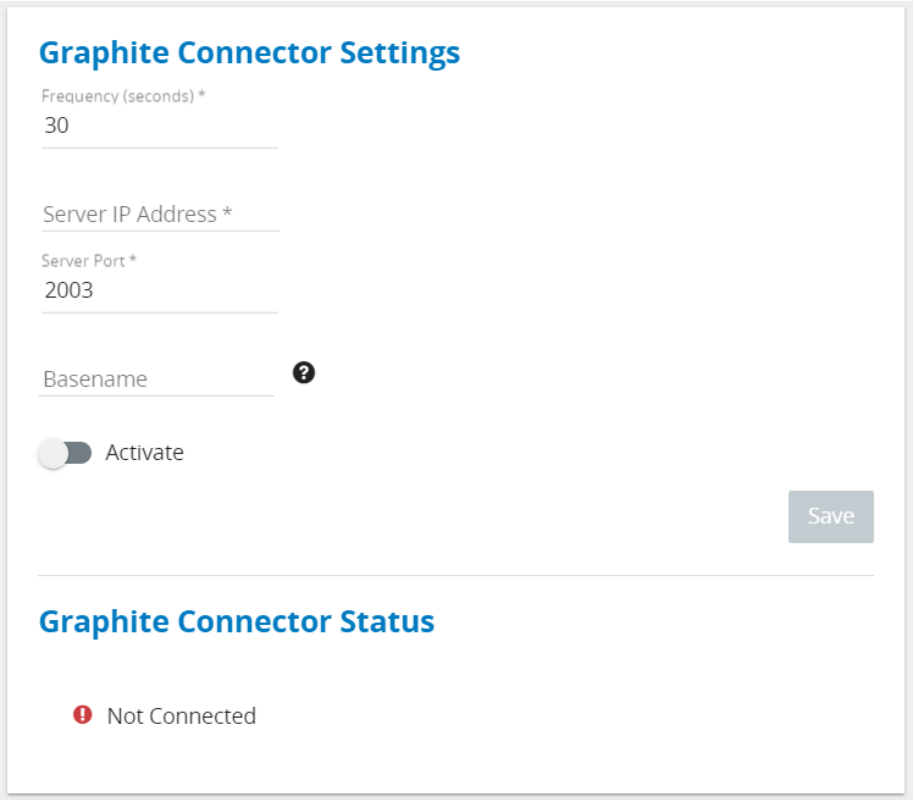
Graphite documentation : https://graphite.readthedocs.io/en/latest/

Grafana documentation : https://grafana.com/docs/

Eaton does not provide a validated, preconfigured Graphite & Graphana environment.
To setup such an environment, one good approach may be to create a Docker Compose in order to create a correctly configured docker container via a yaml (.yml) descriptor file.
There are a- number of good tutorials available on the web if you search for "***deploy graphite with grafana***", for example.

1.11.1 IPM Editions graphite connector configuration

The **Graphite Connector Settings** panel may be accessed from the **Monitoring tab** in the **Settings** menu item from the left navigation menu.



Frequency (seconds) defines the Graphite data push frequency. **Default value is 30**.

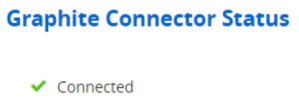
Server IP address should be configured with the IP address of your Graphite server

Server Port is the port number to be used for your Graphite server. **Default value is 2003**.

Basename is the name which will be display on the Graphite server for the IPM Edition connection. If none is set, your IPM Edition will send its hostname as the Basename.

Activate is a toggle to turn on / off the Graphite server connection. Please keep in mind that you must click **Save** to start the connection between the applications.

If everything is configured correctly, the **Graphite Connector Status** should turn to a green **Connected** state



Example Grafana dashboard

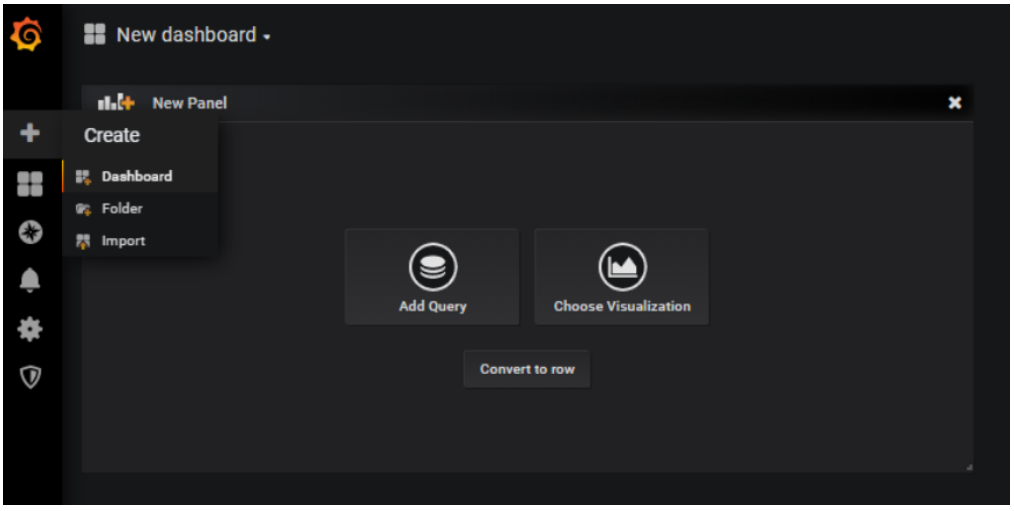
Below you can see an example of Grafana being used to aggregate top level dashboard metrics from IPM Understand Edition sites.

This enables you to have a global overview in multi-site deployments and is a typical use case for the IPM Graphite connector.

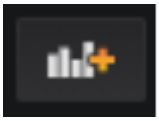
Grafana - Dashboard creation

Once your Grafana server is setup and configured with your Graphite server, you may use it to create custom dashboards with information from one or multiple IPM Edition instances.

From the Grafana home page, click on the **plus (+)** icon and select **dashboard**

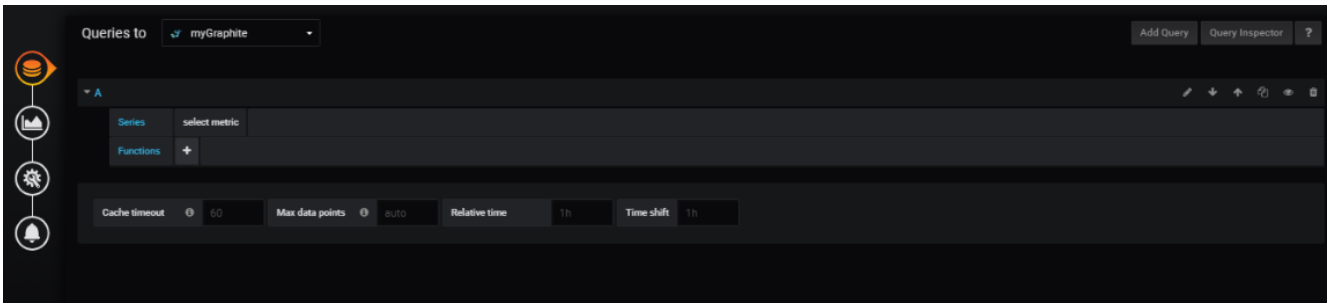


By default, Grafana will add a new panel to your dashboard. You can add additional panels using the **Add panel** icon :

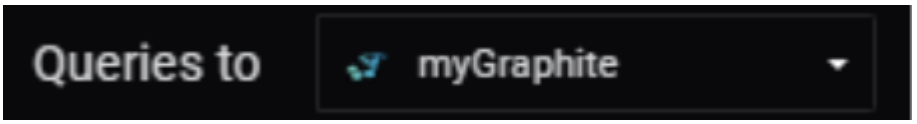


On a new panel you may begin by either selecting the **query** (the data you want to see) or the **visualization** (the type of graphical item you want to display).

Query



When creating a query, you must fselect the database you want to use. In this example, we select the Graphite instance linked to the Graphana instance during the deployment of your environment.



Once you've selected the database, you then select the **Series** you want to display. The Series are divided into several layers which go progressively deeper into the data center assets. You continue drilling down until you locate the data you want to visualize.

The first part of the Series is the IPM Edition containing the asset. This is where you will find the basename that you configured for the IPM Edition Graphite connector configuration or IPM Edition instance's hostname if you didn't configure the basename.

Next you select the asset you want to monitor.

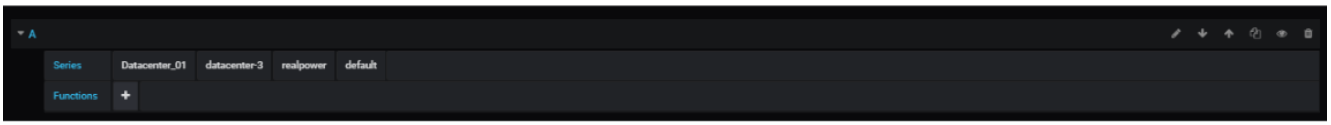
Due to technical limitations on the length of metric names in Graphite, your IPM Edition sends the internal identifier of the asset instead of the name. This means that you will need to be able to find the mapping between the two in order to configure the correct asset ID.

You may find the name of an asset ID either from performaning an export to CSV of the asset database or, alternatively by using a REST API call to display it in a browser.

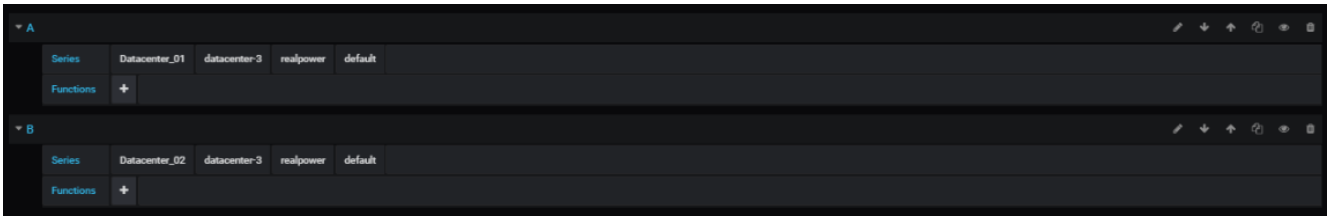
Using the REST API to display the Asset ID - Asset name mapping

From your favorite web browser, log into your IPM Editions web interface. Then, on a new tab, type https://[*your_**IPM Edition_IP address_or_hostname***]/**api/v1/assets**. You will find the list of all the assets provided by the instance of IPM Editions including their ID, name, type and subtype.

For example, here is an example of how to get the default **realpower** metric for the Datacenter with the ID **datacenter-3** which is present in the IPM Edition with the basename **Datacenter_01**

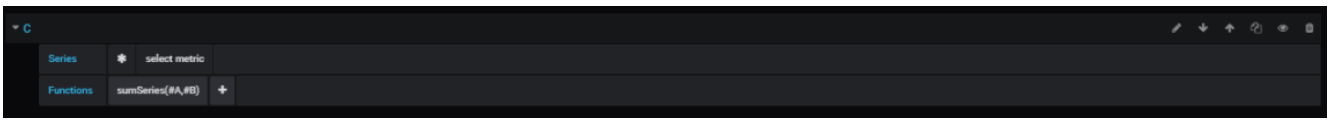


Then you can add a second query by using the **Add query** button at the top right of the Query panel in order to get the same data from another IPM Editions instance with the basename of **Datacenter_02**.



Now that you have your two queries, you may use them in other queries.

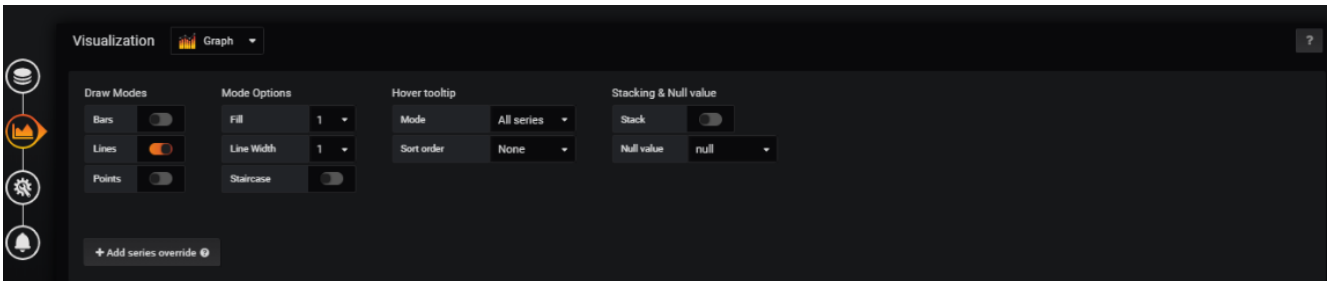
For instance, I can use the **sumSeries** function to create a sum of the power consumption from my two data centers.



Using the **Text mode** icon  you can use the Graphite syntax istead of the Grafana UI in order to create your query

Visualization

When your queries are complete, you may change the visualization by clicking on the left vertical menu



The default visualization is **Graph** but you can easily change it to another type of visualization.

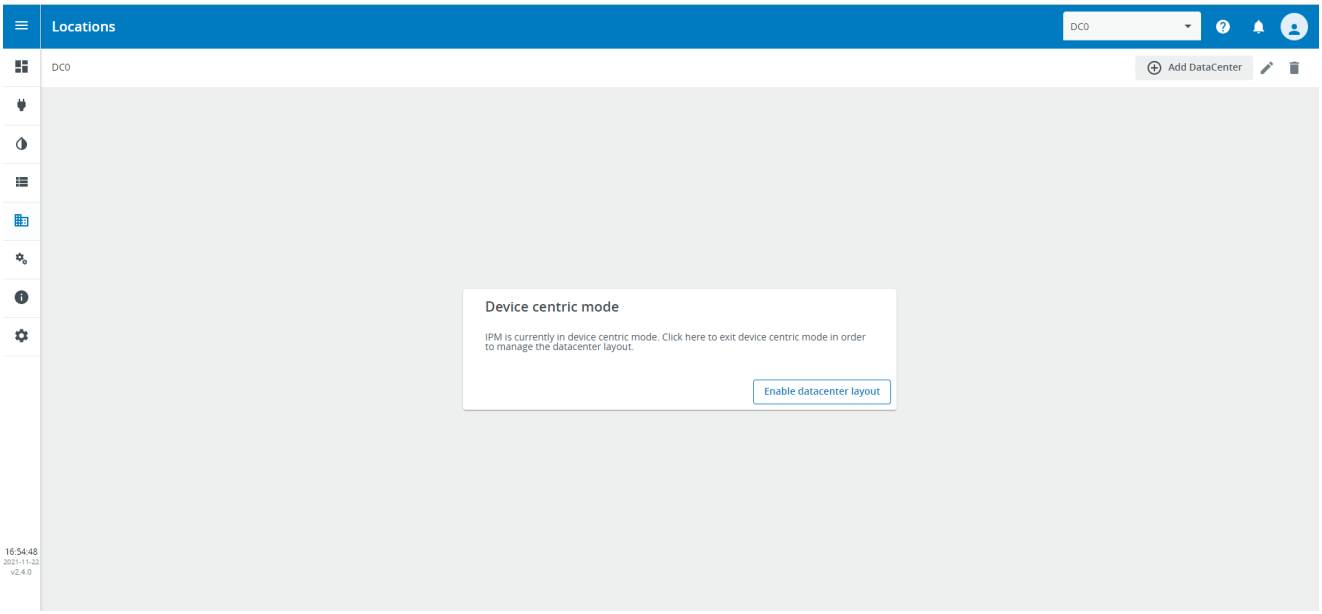
Each visualization has its own configuration panels.

1.12 Location Management

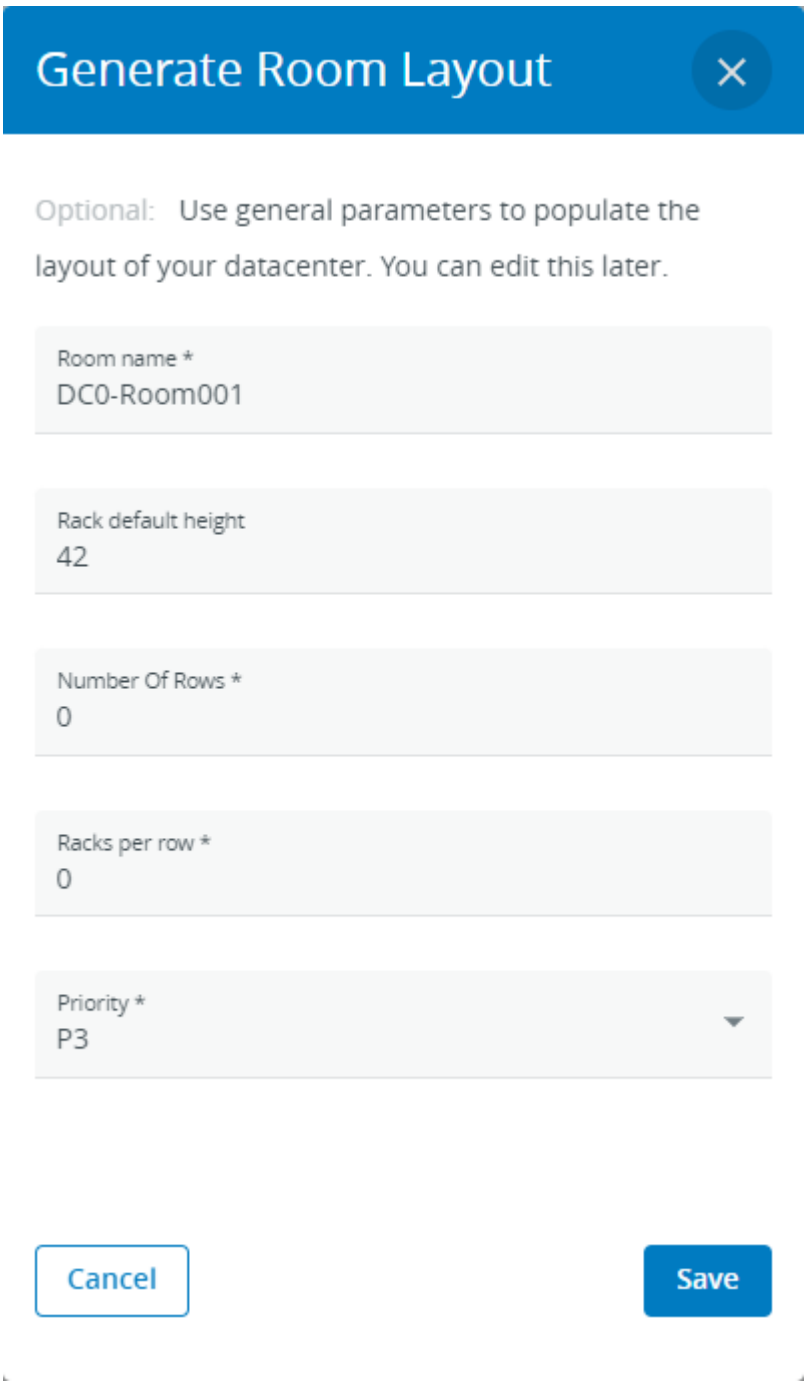
The Data center layout settings page is accessible from the **Locations** menu item in the left navigation menu.

If you did not configure Datacenter Layout during initial installation wizard, the button **Enable Datacenter layout** allows to unlock Datacenter Layout configuration for advanced Power and Spatial views.

If you click on the **Enable Datacenter layout** button it will not be possible to come back later to ths simple Device Centric mode.

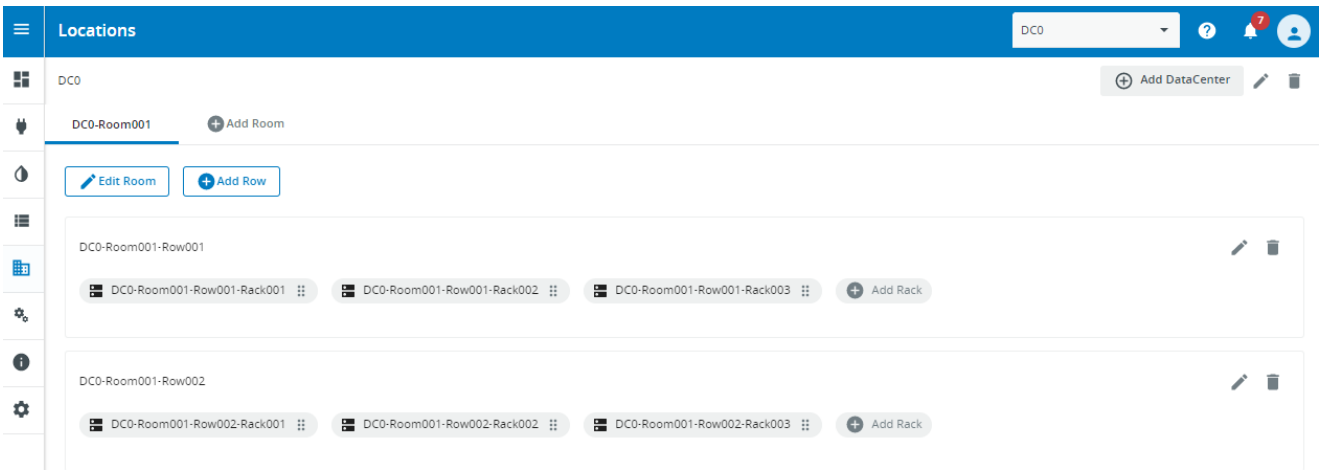


Once you have enabled Datacenter Layout, you can Generate the data center Room layout with **Number of Rows** x **Rack per row**.



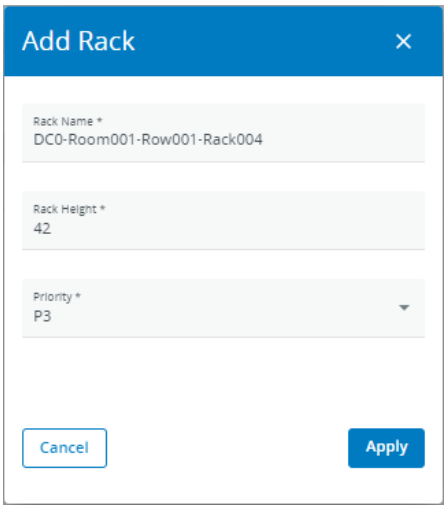
As a result: an initial Datacenter layout is generated

e.g. here **Number of Rows** =2 and **Rack per row** = 3



The application offers this visual tool for streamlining the creation of the assets used in building the data center layout topology : rooms, rows, racks.

- Additional **Datacenter**, **Rooms**, **Rows** and **Racks** may be defined with the **Add ...** buttons.
- Any data center must have at minimum a room containing a row with a rack inside.
- The rack ordering (into a row) can be changed simply by moving the Racks by drag and drop



For all the new assets added, you may change the default name before the configuration is saved. Once saved, edit operations can also be performed from this page.

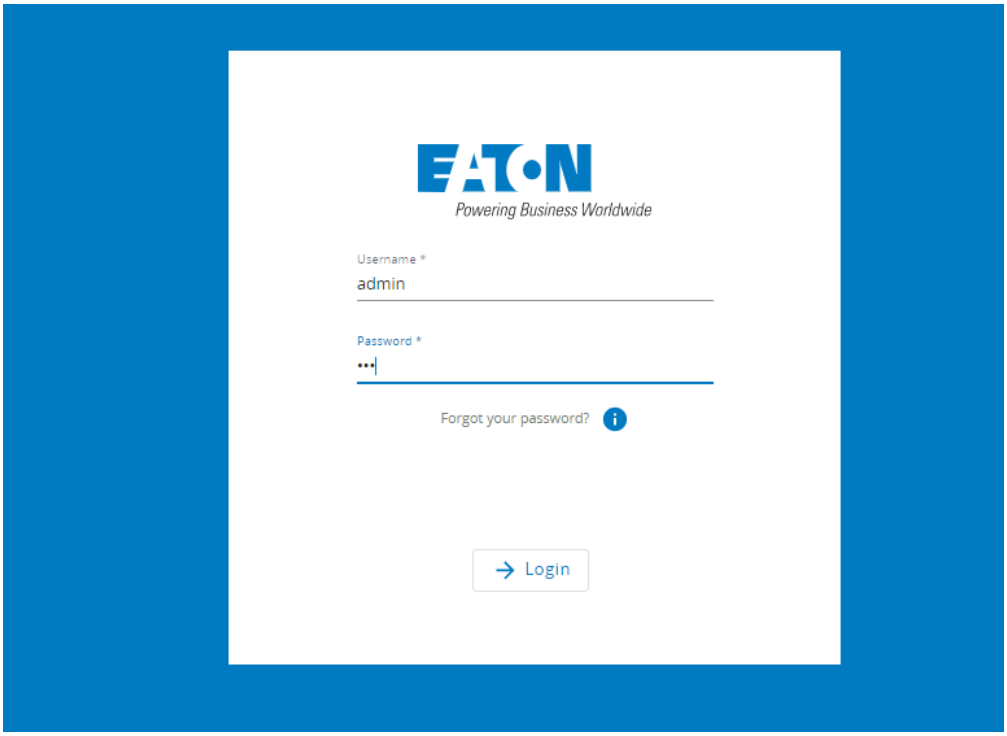
Once the full layout has been defined, simply click **Save**.

NOTE

If you want to remove a Room, Row or Rack, all child object must first be removed (e.g. all devices deleted from the rack before deleting the rack)

2 Contextual Help

2.1 Login page



2.1.1 Initial login

1. Enter default password

As you are logging into your IPM application for the first time, you must enter the factory default username and password which are set to:

Username = admin
Password = admin

As you will be able to see, the password details are obscured from view so please ensure to enter the password carefully and correctly.

> **Note**
>
> Passwords are case sensitive!

2. Enter the login wizard

As soon as the default credentials are entered successfully, the login wizard starts.

At first login, the system requires that you change the default admin password.

- You are presented with a message requesting the current admin password ("**admin**") and to enter a new password which you must also enter a second time to ensure you have entered it correctly.
- Follow the password policy recommendations included in the tooltip.
- A secure password is mandatory.

> The factory default password security policy requires that you enter a password with **at least *8 characters and that includes a minimum of 1 number, and 1 special character***.
> You may modify the password strength policy in the settings of the application. See User Management for more information.

- Click **Continue**.

For the more details on the remaining steps in the wizard, please go to the Initial setup & configuration section of the documentation.

2.2 Dashboard View

2.2.1 Overview

The purpose of the Dashboard is to give a general snapshot of the health of the Data Center via key metrics. This includes real-time data and trends over 24 hours, 1 week and 1 month periods for both Power and Environmental metrics.

> **Note**
>
> The **Datacenter Configuration** is required to get the full view. If you skipped the **Datacenter Configuration** (optional) step during the initial Installation Wizard, some panels in this view will be greyed. Just follow the link displayed in the greyed panels to complete the **Datacenter Configuration** and enable all panels.

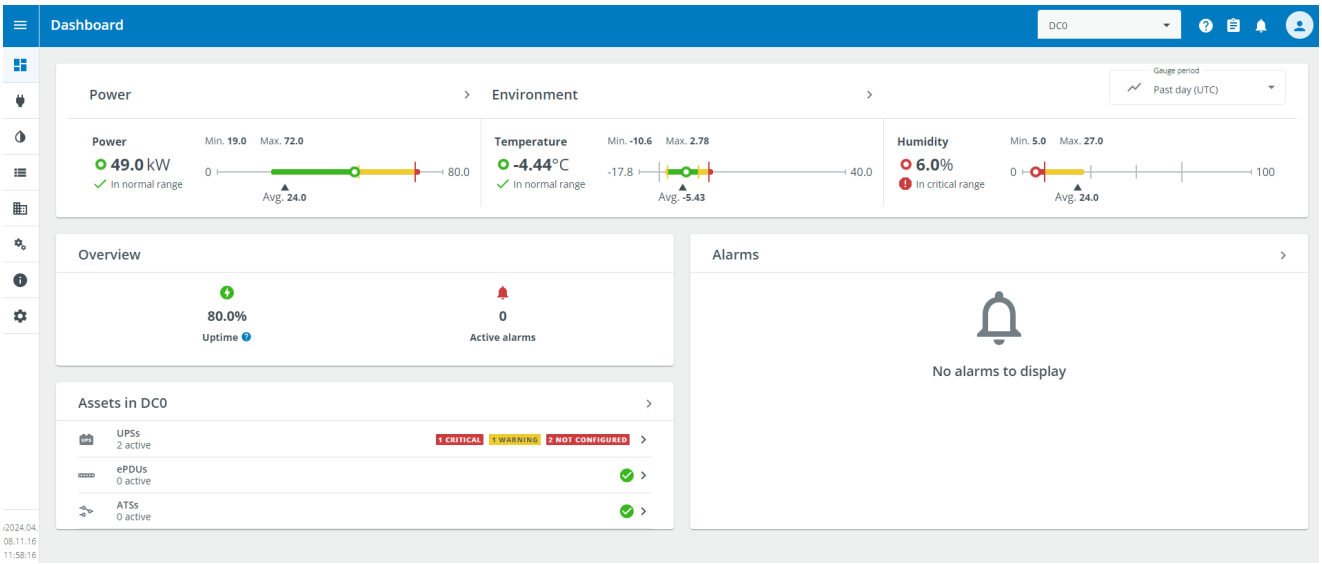
The left most **Power** gauge provides you with a view of the total power usage of your Data Center, allowing you to quickly see and understand power usage at the Data Center level.

The **Current Temperature** and **Current Humidity** gauges enable you to view the current environmental status of your Data Center, providing an aggregated value for temperature and humidity sensors deployed within your site.

The **Alarms** panel provides the user with visibility of the most recent active alerts occurring within their Data Center along with timestamps and a brief description of the issue impacting a particular device.

The **Overview** panel displays a Data Center uptime KPI based on the main feed to the UPS. It is a quick way to understand the stability of the power in the data center.

The **Equipment** panel displays an overview of the power equipments (UPS, ePDUs, ATS) according to their status



2.2.2 Navigation within the application

The application progressively exposes more detailed information via a drill-down navigation starting from the Dashboard.

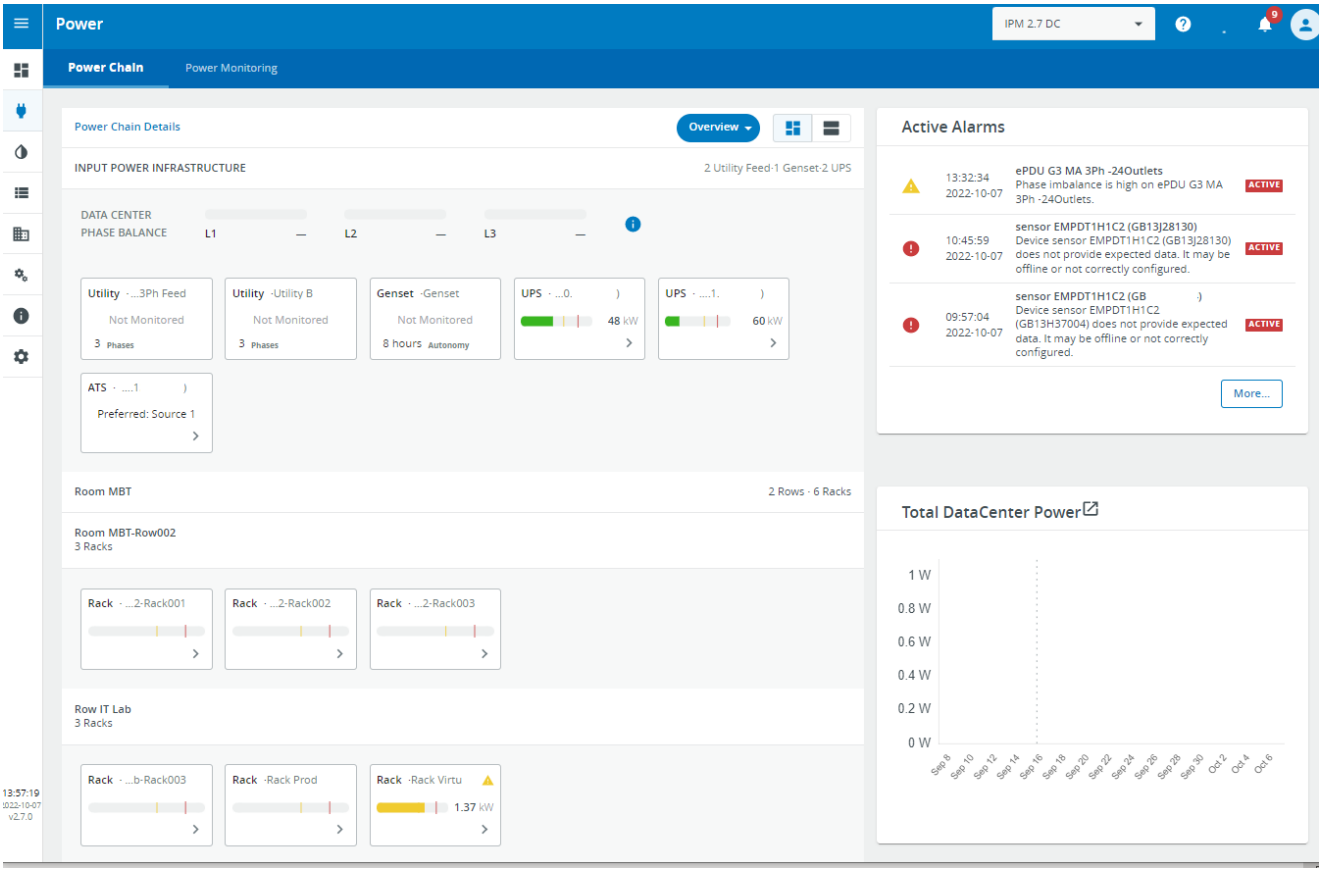
From the dashboard, you may navigate using the left or top menus or you may also click on clickable icons to advance to a more detailed view.

For example, by clicking on the **Power** icon, you'll be taken to a Power Chain view which provides you with an overview of the Data Center power distribution topology from the Utility feed down to the racks. From that page, you can click on a given Rack gauge to go further down in detail.

2.3 Power Chain View

From the main Dashboard page, you may navigate to specific areas of their Data Center such as the more detailed Power Chain view, (see below). The Power Chain view provides you with an overview of the Data Center power distribution topology from the Utility feed, through the UPS down to the rack level. To access to the Power Chain view, you click either on the power icon  in the left menu or click directly on the Power gauge on the main dashboard to drill down to this level.

> **Note**
>
> The **Datacenter Configuration** is required to get the full view. If you skipped the **Datacenter Configuration** (optional) step during the initial Installation Wizard, some panels in this view will be greyed. Just follow the link displayed in the greyed panels to complete the **Datacenter Configuration** and enable all panels.



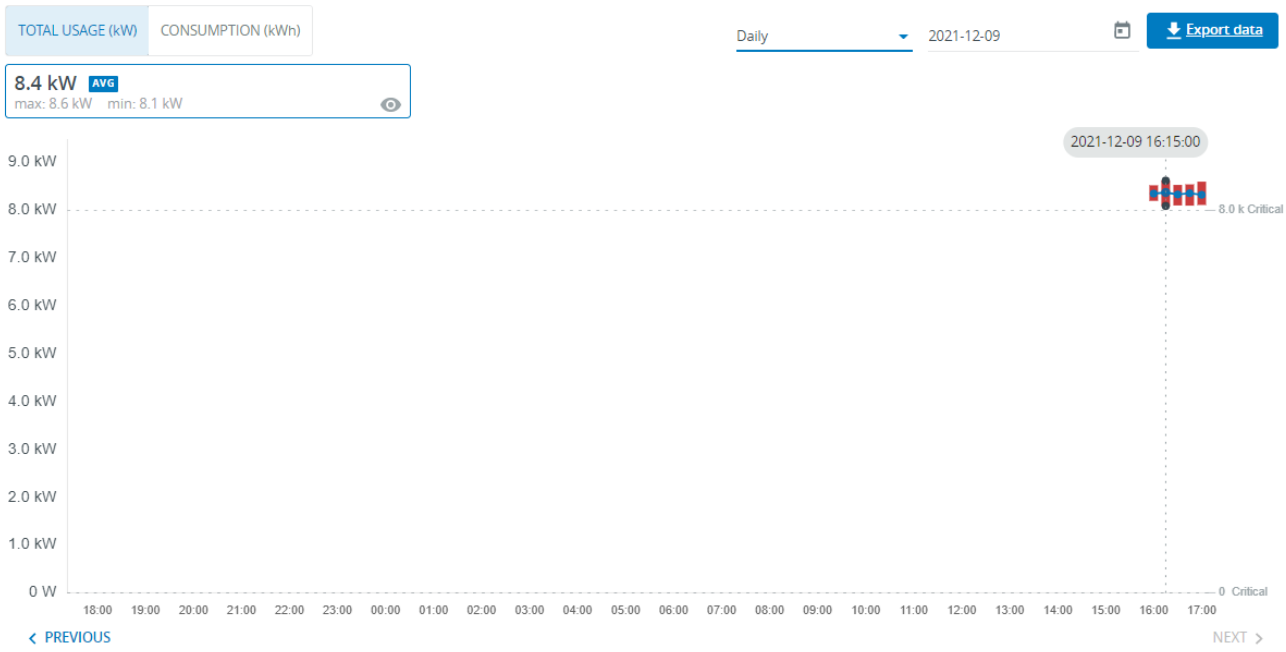
Here you are presented with a simplified line diagram of their power chain topology. You are also shown a graph of the total power consumption of your Data Center over the last 24 hours, 1 week and 1 month. A custom date range may also be entered manually. Active alarms are also shown on this page ensuring you will never miss any new alarms that may occur.

If the UPS present is a stand alone 3-phase UPS, you are also able to select a high level overview of the phase balance.

A list of possible configurations for the input power infrastructure can be found in Typical Power Chain Topologies section of the documentation.

By clicking on the **Full Page** icon in the graph tile you can access to following additional graphs with more details:

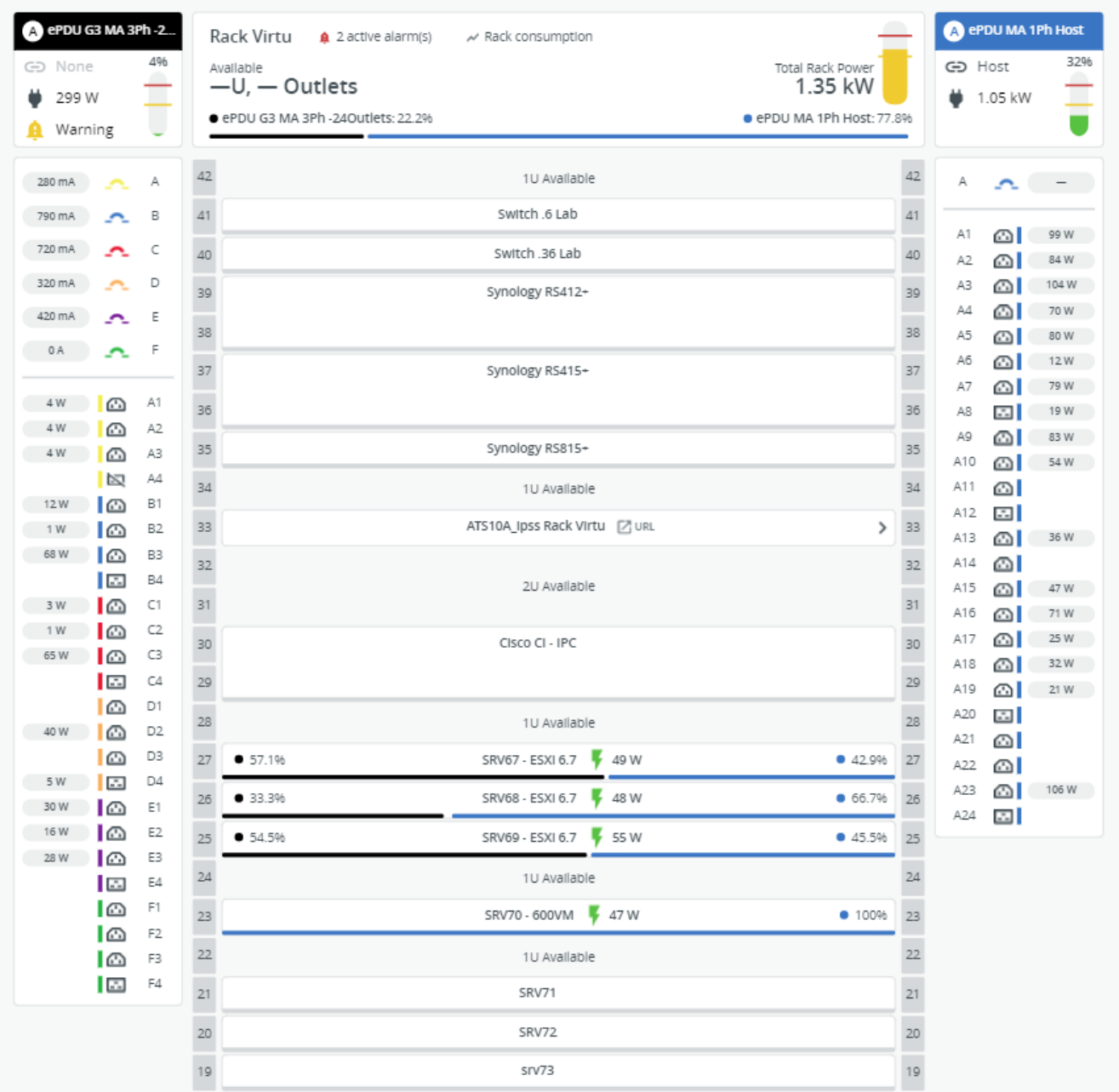
- TOTAL USAGE (kW)
- CONSUMPTION (kWh)



2.4 Rack View

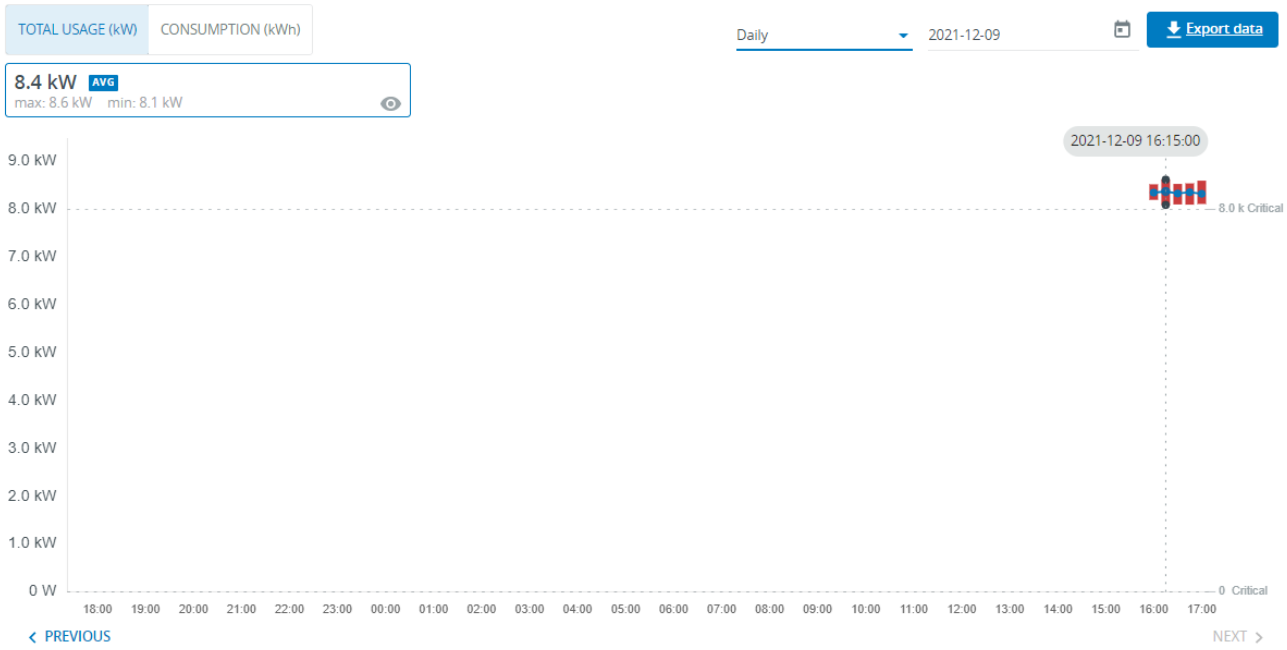
By clicking on one of the rack representations in the Power Chain View, you are taken to the Rack View.

> **Note**
>
> The **Datacenter Configuration** is required to get the full view. If you skipped the **Datacenter Configuration** (optional) step during the initial Installation Wizard, some panels in this view will be greyed. Just follow the link displayed in the greyed panels to complete the **Datacenter Configuration** and enable all panels.



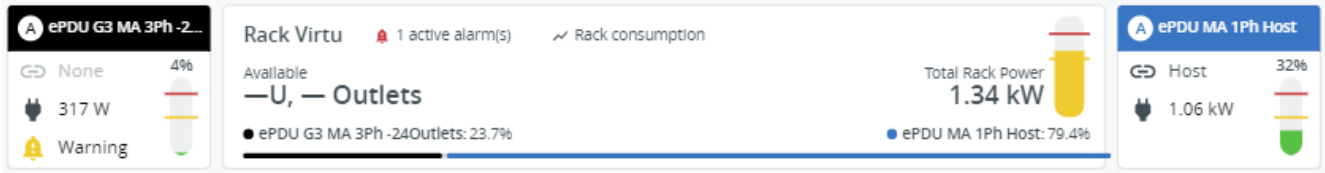
By clicking on the **Full Page** icon in the graph tile you can access to following additional graphs with more details:

- TOTAL USAGE (kW)
- CONSUMPTION (kWh)



You are able to see detailed information for this rack including total rack power, percentage of load balance between both rack ePDUs, and load levels on each rack ePDU. You may also view the power usage graphs over 24 hours, 7 days and 1 month periods. The top right panel shows you the most recent alarms.

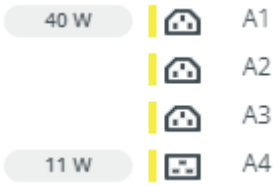
The top banner of the rack view clearly indicates the power source of each feed into the rack (E.g. UPS, Mains). See below:



Gauges are provided for Rack & ePDUs with following color code:

- **GREEN** = ePDU or Rack within threshold
- **YELLOW** = ePDU or rack above warning threshold
- **RED** = ePDU or rack above critical threshold

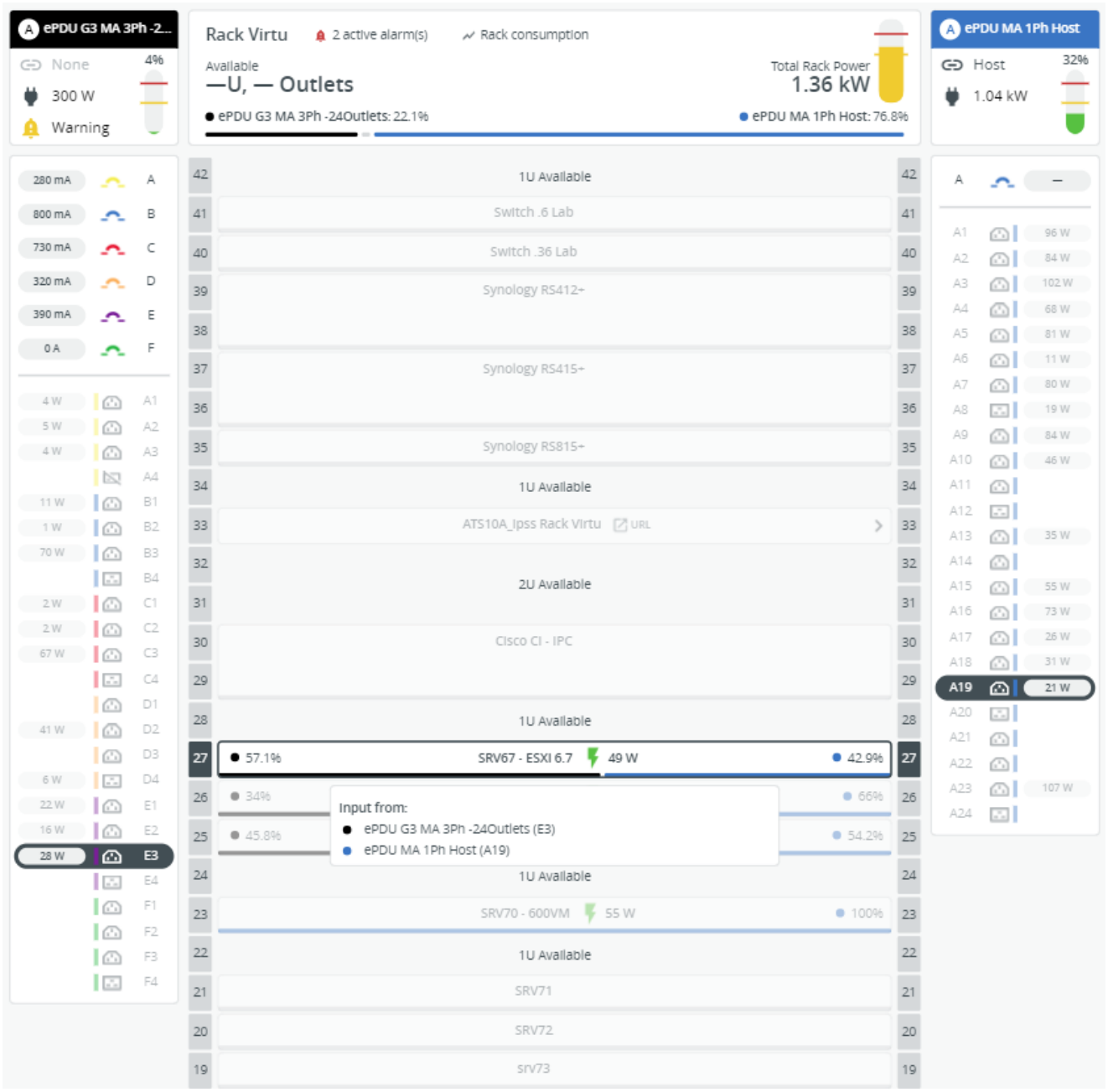
Outlet states are following ones

Icon for Outlets	Status
	Outlet On with or without power

Icon for Outlets	Status
	Outlet Off
	Outlet alarm is critical
	Outlet alarm is warning

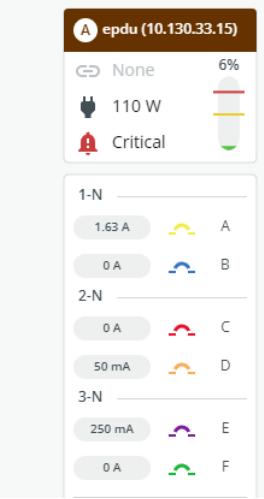
When you perform a mouse click on

- one of the outlets, the device supplied is displayed with a Bold rectangular highlight. If there is another outlet supplying the device, that (those) outlet(s) is (are) also displayed in bold.
- a rack mounted IT device in the view, a popup appears with the name of the device, the name of the power supplies and the outlet number if the device is powered by a PDU, as well as the total power consumed by the device from all outlets. Both device and outlets are displayed surrounded by a Bold rectangular border.

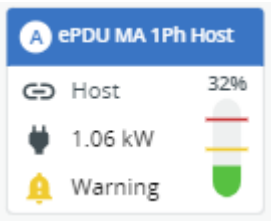


PDU sections are represented with their name in a colored rectangle and Eaton G3/G3+ ePDUs are represented in the rack view with the same colors as those applied to the HW unit itself making it easy to quickly identify the relevant section and outlet.

The colored breaker icon identifies each section. With the group name of the section, the phase powering the section and the instantaneous values of the current of the section.



A feed identifier is displayed above each of the rack PDU gauges. When available from the rack PDU, the feed color and name are displayed automatically.



You may also obtain more details related to each of the rack PDUs installed. Simply click on the **ePDU name** link

2.5 Power Monitoring View

2.5.1 **Overview**

Clicking on the **Power Monitoring** tab brings you directly to this list view.

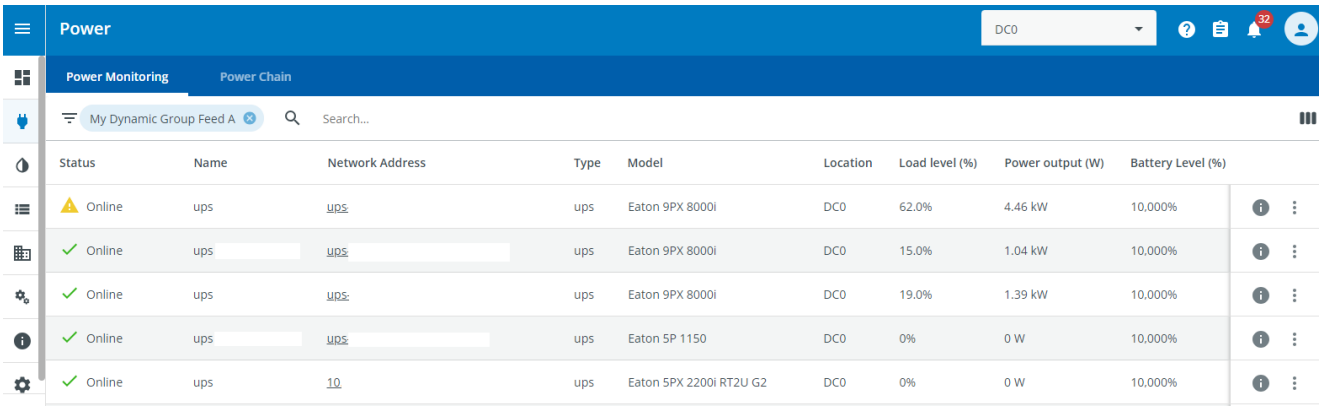
Here you may view Power devices such as UPSs, ePDUs or STS simply displayed in a list. This view is very convenient if you didn't configure datacenter topology during initial installation wizard.

- A Search field allows you to filter the Power Devices
- You can sort the devices simply by clicking the colums headers
- On each line mouse hover buttons provide you direct access to **Detailed Information** or **Rack View** or **Device Web page**
- Some metrics such as its Status, Load Level, Power Output, Battery runtime are displayed in this view

Clicking the filter icon on the top left will open the **Power Monitoring Filter** side menu.

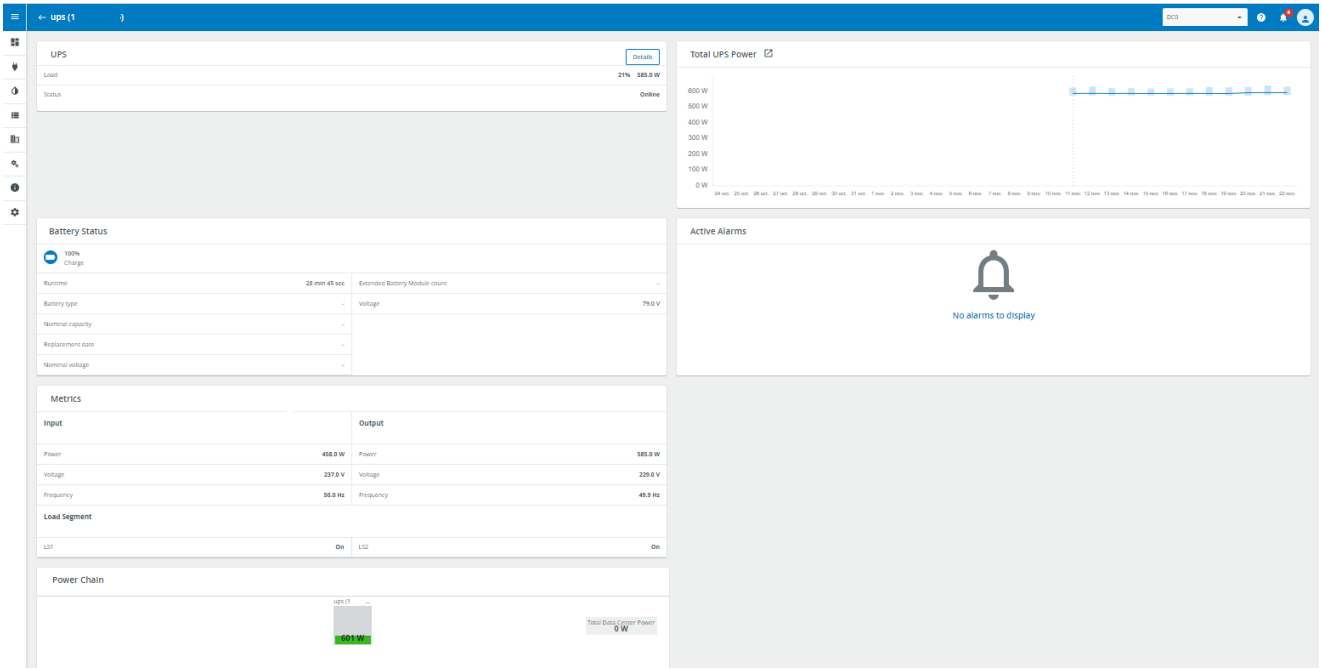
- Two types of filters are available: locations and dynamic groups
- You can select a filter by checking its corresponding check box
- Location filtering includes rooms and racks. Selecting a room will select all the racks located in this room
- Adding a filter in this menu will create a chip containing the name of the filter on the top left of the Power Monitoring table

- A filter chip can be removed by unchecking the check box corresponding to that filter or by clicking the cross icon inside the chip
- Selecting multiple filters will display all the assets that apply to each filter. (E.g. selecting **room 1** and **dynamic group 1** will display all assets from **room 1** even if they are not in **dynamic group 1** and all assets from **dynamic group 1** even if they are not in **Room 1**.) Assets that correspond to more than one filter will only appear once in the Power Monitoring table



2.6 UPS View

Clicking on the UPS gauge brings you directly to the **UPS view**.

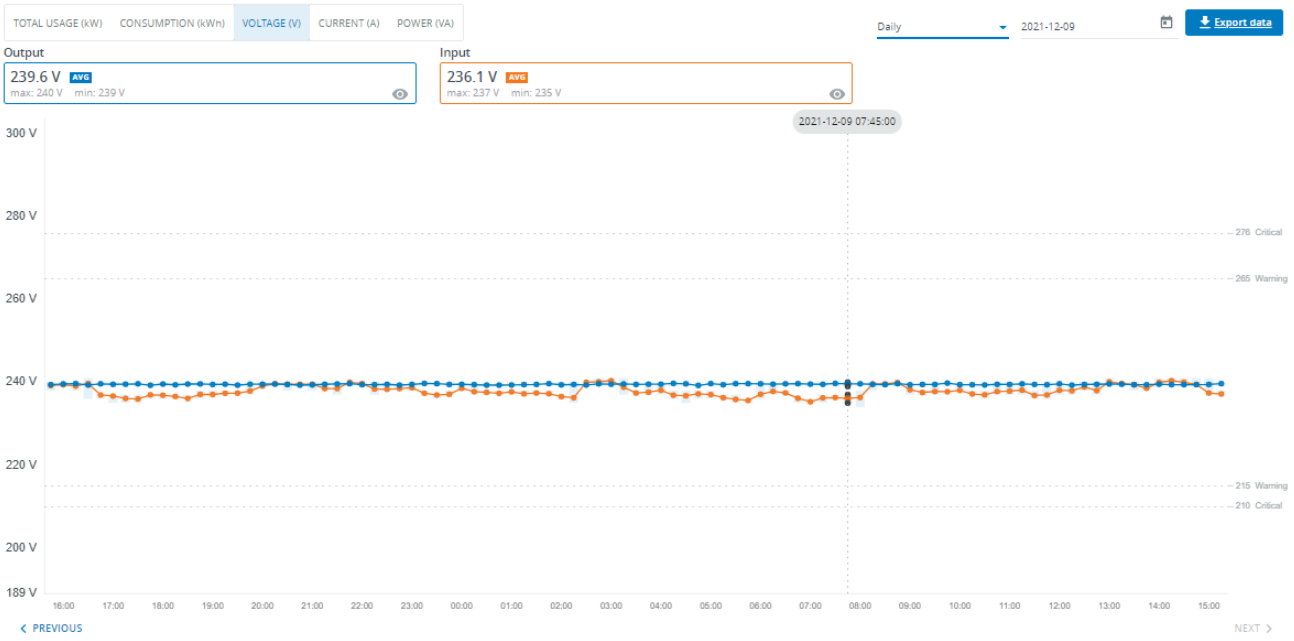


Here you may view more detailed UPS measurements such as its status, as well as the Battery, Input and Output Metrics, while still maintaining an overview of the total critical power and active alerts.

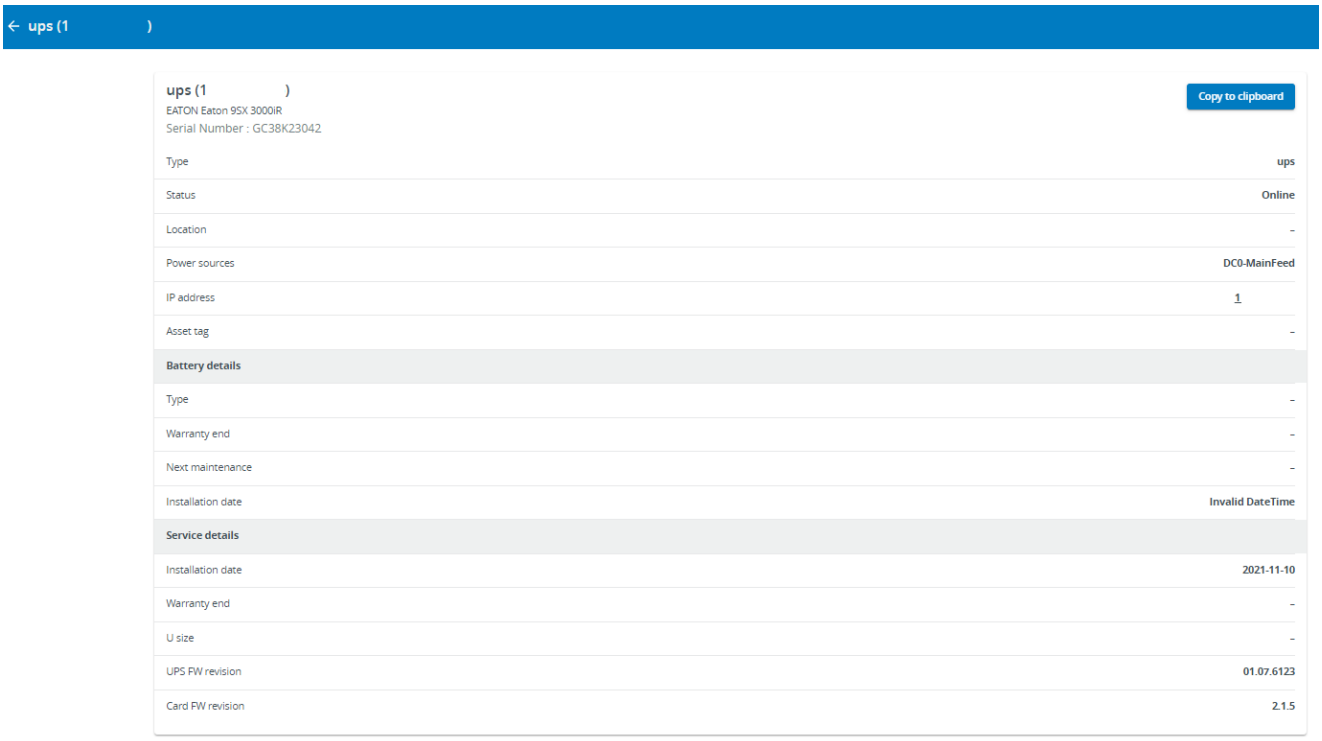
By clicking on the **Full Page** icon in the graph tile you can access to following additional graphs:

- TOTAL USAGE (kW)

- CONSUMPTION (kWh)
- VOLTAGE (V)
- CURRENT (A)
- POWER (VA)



By clicking on the **Details** button you are presented with further details related to the UPS such as its IP address, serial number, location, etc.



Alternatively, you may click on the IP Address link which will take you directly to the selected UPS' embedded web interface.

Returning to the Power View page, you may see the power consumption by rack for each rack protected by the selected UPS.

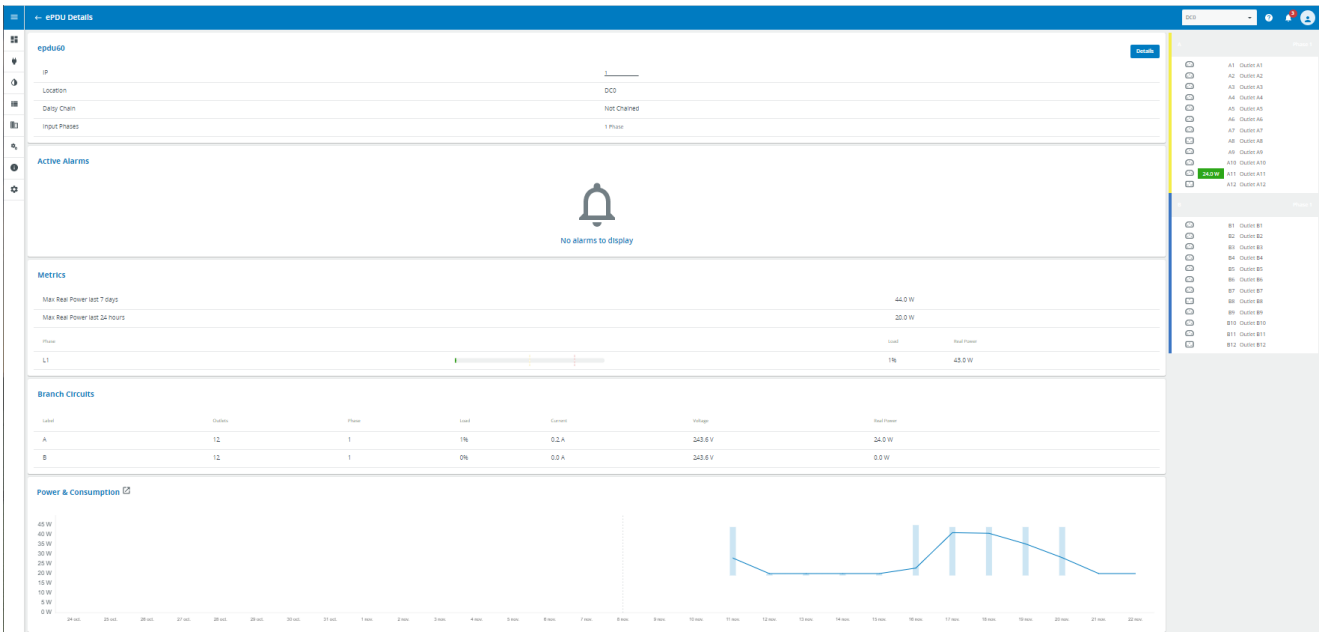
2.7 ePDU View

2.7.1 **Overview**

A detailed view of ePDU assets is available. It is called **ePDU view.**

The user can access it by openning the Power Monitoring view and hovering the line corresponding to the ePDU she/he is interested in.

An information icon will appear on the right end of the line. By clicking this icon, the user will open the ePDU view of the corresponding device.

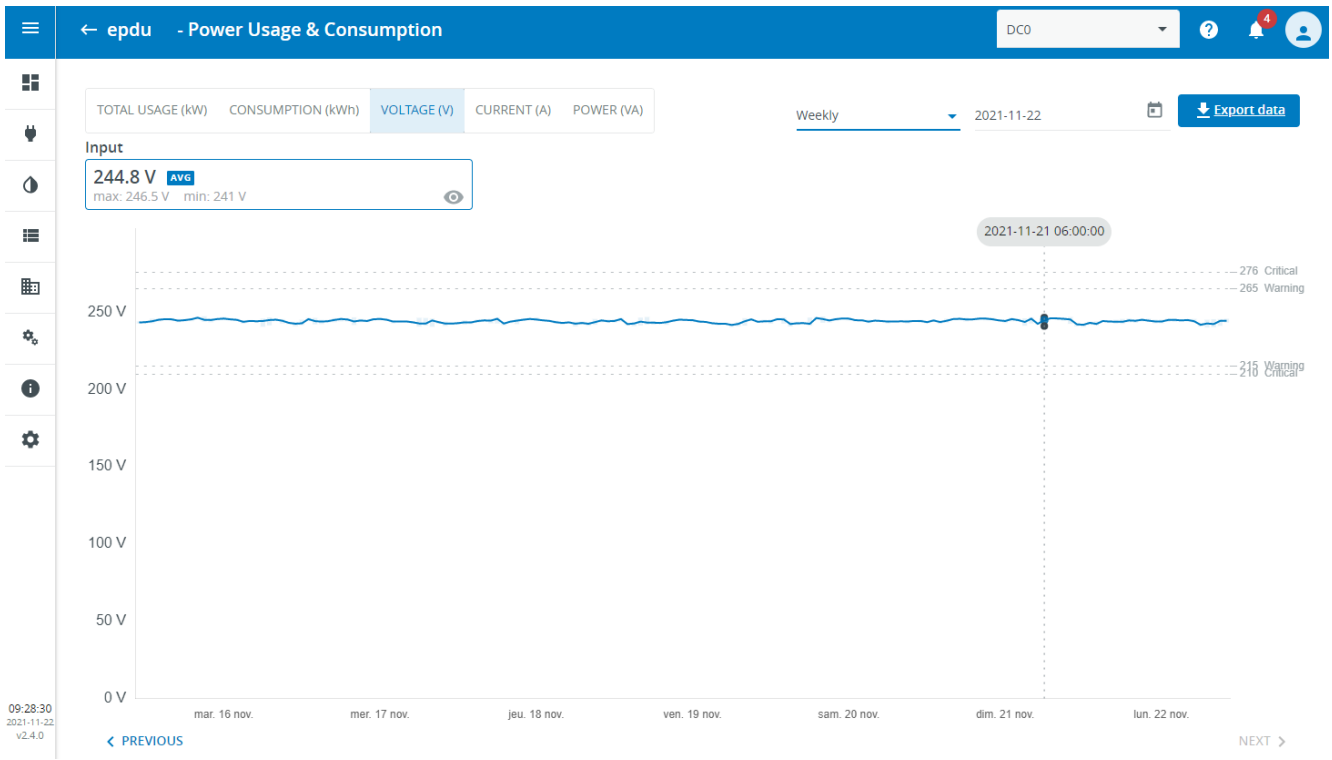


This page is made of a main view containing several panels and a side view detailing each section, outlet by outlet, on the right side of the page.

2.7.2 **Main view**

The main view is made of five panels:

1. The top panel contains the key information of the device and a button to open the detail dialog also available from the rack view.
2. The Alarms panel displays the alarms currently active on the device, if any.
3. The Metrics panel shows the main instantaneous global power values phase by phase.
4. The Branch Circuits panel shows the main metrics of each branch circuit.
5. Power & Consumption Graph (Clicking on the zoom icon will display a full page graph with additional details)



2.7.3 Side view

The side view contains as many panels as the ePDU has sections.

Each section panel presents the phase powering the corresponding branch circuit and the list of its outlets by showing for each outlet:

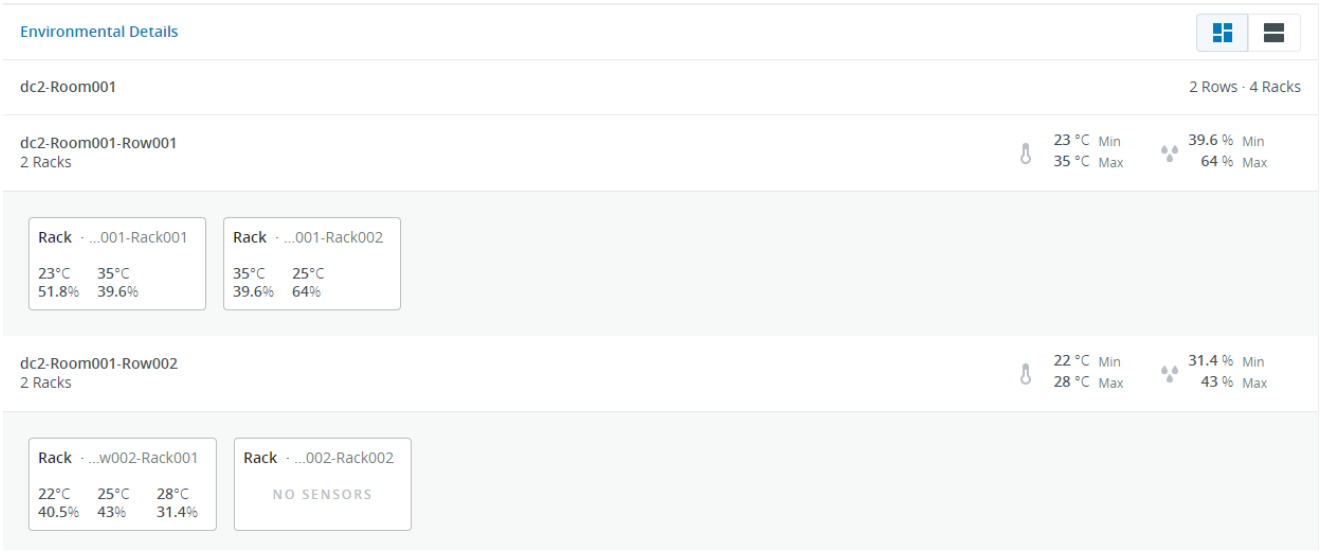
- A pictogram to represent the type of the outlet
- The power drawn from the outlet (if non-zero)
- The identifier of the outlet
- The friendly name of the outlet

2.8 Environmental View

By clicking on the temperature and humidity symbol on the left hand side of the screen, you are able to view a greater level of detail with respect to the temperature and humidity sensors deployed in your data center.

Currently, IPM Editions software monitors the temperature at the server intake level (front of rack sensor deployment), this provides the user with a view of the environmental status directly at their IT device level.

> **Note**
>
> The **Datacenter Configuration** is required to get the full view. If you skipped the **Datacenter Configuration** (optional) step during the initial Installation Wizard, some panels in this view will be greyed. Just follow the link displayed in the greyed panels to complete the **Datacenter Configuration** and enable all panels.



Similar to the layout of the power view page, you may see the telemetry from sensor(s) monitoring the air intake (front of rack).

You may change the selected view by selecting the grid format view on the top right of the temperature and humidity display in order to see change from the default hierarchical view of the location topology to a grid view with all racks in an alarm state being moved to the top of the panel in order to see them all at once.

At the top right hand side of the page, you are presented with a snap shot of your current and most recent alerts.

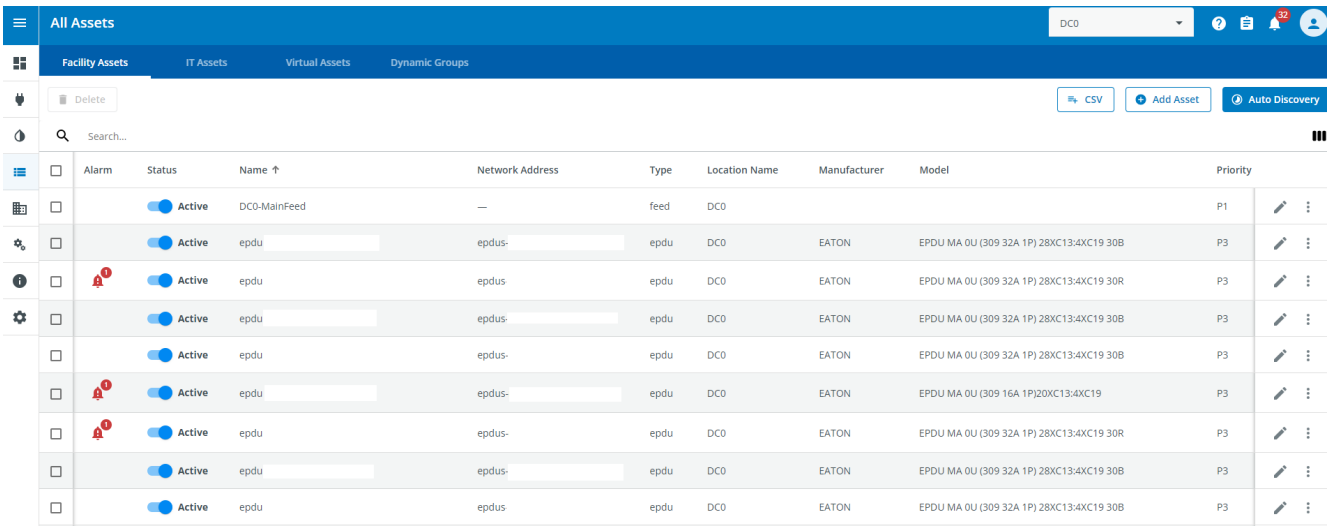
In the bottom right panel, you may also view graphs of the historical data related to either temperature or humidity

> => Clicking on the zoom icon in Graph title will display a full page graph with more details over the last day, last week or last month.

2.9 Asset Management View

One of the base functions of the system is to provide a basic asset management tool, enabling you to track all data center devices over the asset's lifecycle from installation to decommission. Along with the basic location and device type tracking,you may also enter contact details and assign a device specific priority which will be used in calculating the frequency at which alarms are resent.

At all times, you have visibility of all current issues related to this device via the alarm icon  which is displayed to the left of the asset name.

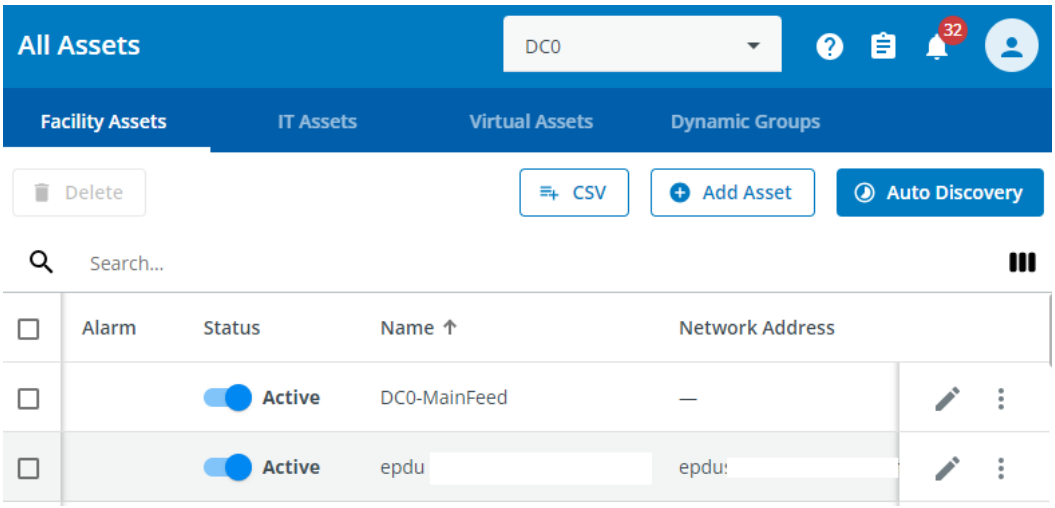


2.9.1 Types of assets

Devices are categorized by type with the top level categorization defined as follows: ***Facility assets, IT assets, Virtuals Assets, Dynamic Groups***

All are accessible in dedicated tabs.

Every time a new asset is added (discovered or created), it is assigned an asset type and displayed in the corresponding tab.



Facility assets

Power asset tab will will monitor the following types of assets :

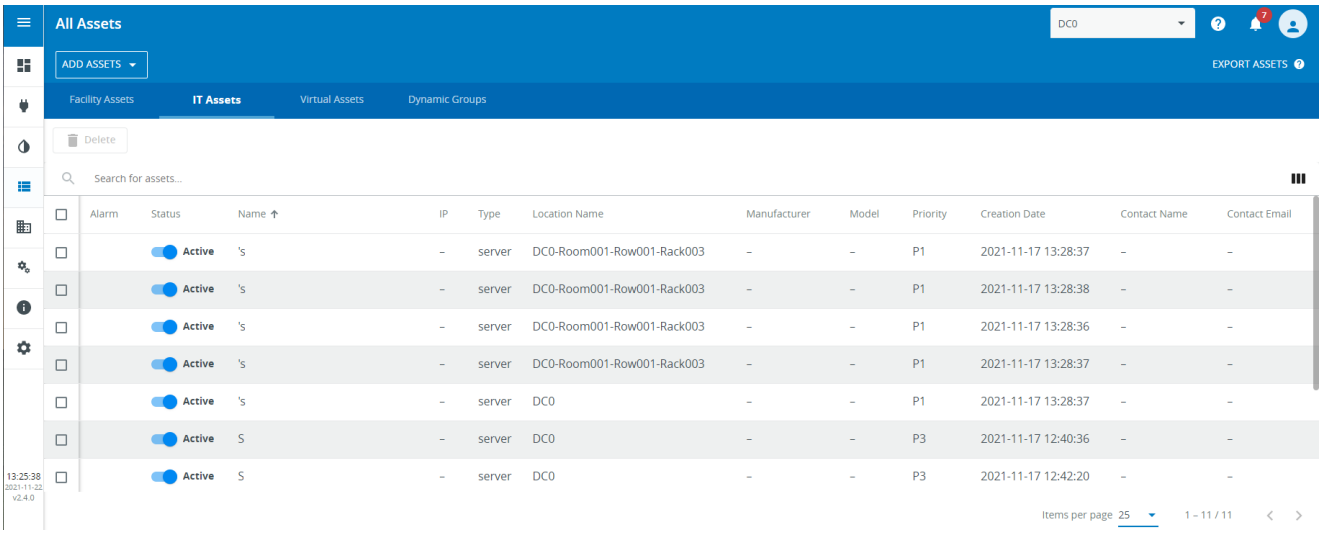
- **Power Devices**
  - Feed
  - UPS
  - ATS/STS
  - PDU
  - ePDU
  - Genset
- **Sensors & GPIOs**
  - Sensor
  - Dry contact sensor

- Actuator

IT assets

From this tab, it's possible to manage assets of the following types:

- Server
- Storage
- Switch
- Router
- Rack controller
- Appliance
- Chassis
- Patch Panel
- Other

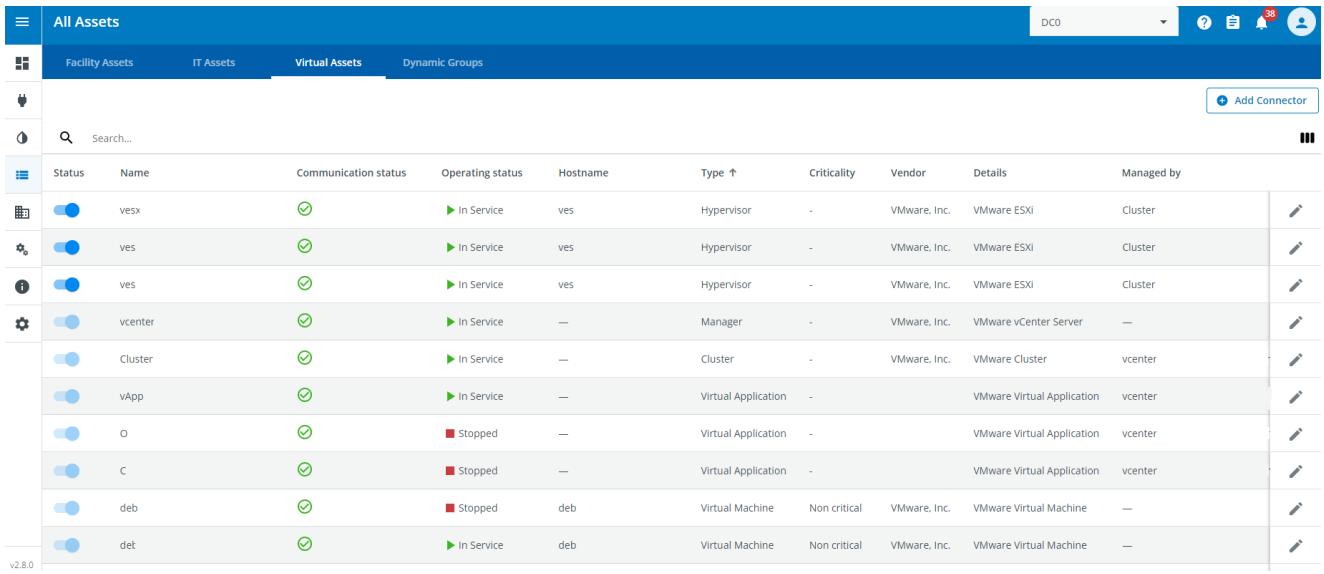


Virtual Assets

On this tab, all of the virtual assets associated to Virtualization connectors are displayed.

When a virtualization connector is correctly configured, all of the connector derived virtual assets will be displayed in this view with high level monitoring information :

- **Cluster objects :**
  - VMware
  - VxRail
  - Nutanix
- **Manager objects :**
  - VMware vCenter
  - Microsoft SCVMM
- **Hypervisor objects :**
  - VMware : ESXi
  - Microsoft Hyper-V
  - Nutanix : AHV
  - Nutanix : ESXi
- **Container Nodes**
  - Kubernetes Nodes : microk8s
- **Virtual Machine objects :**
  - VMware
  - Microsoft
  - Nutanix



Hypervisor and physical host pairing

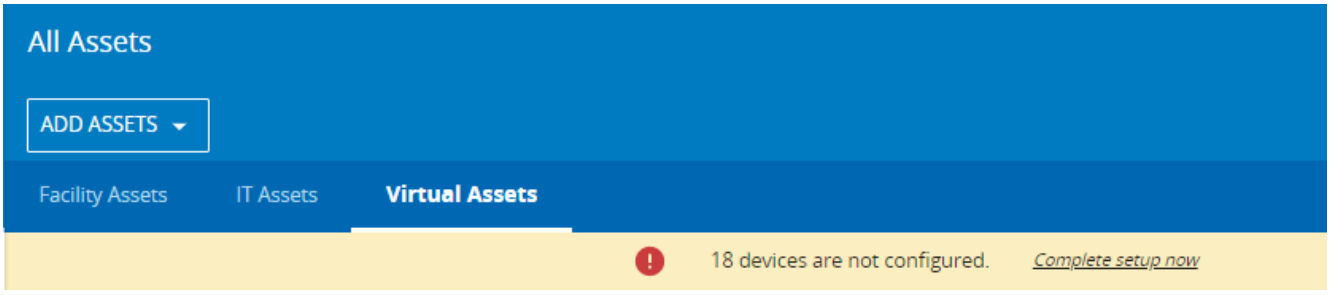
In order to benefit from contextual visibility provided by IPM, all connector discovered hypervisors should be paired to a physical server host object in order to establish a power chain link between a physical host object and the power chain topology.

However, this pairing is not mandatory. If you only wish to protect your virtual environment and not utilize the full contextual visibility features available in IPM, it is also possible to do so.

Pairing configuration assistance

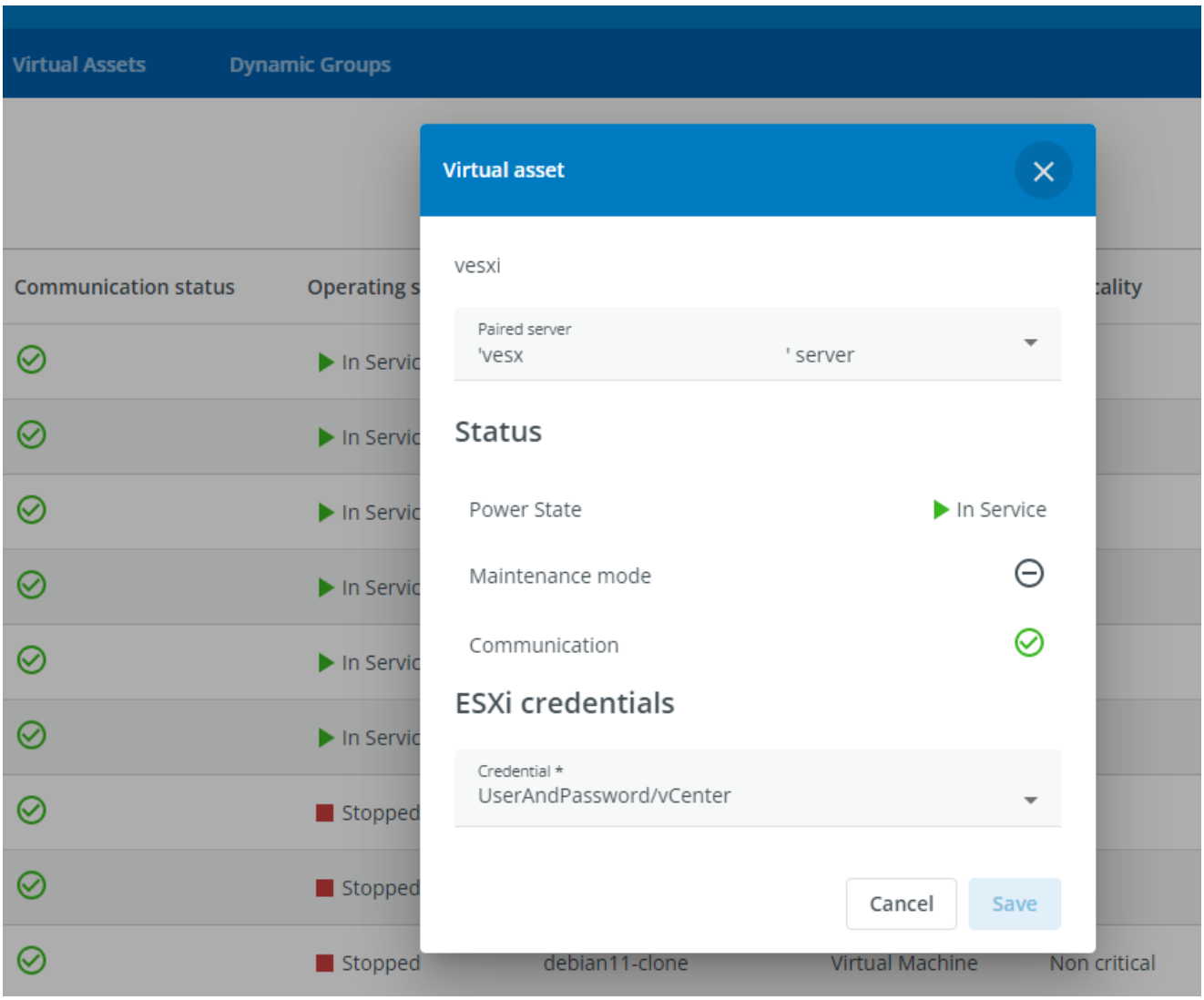
A filtered view will help you quickly identify all Hypervisors that still need to be paired with a physical host by simply clicking on the link.

> **Note**
>
> Physical hosts should be created in the IT assets page prior to beginning the pairing process.



Select a hypervisor to pair and click on **edit button**. A dialog box will open with the list of servers available in the field **Server Host**. Simply select the host on which the hypervisor is installed.

Please note that the application will not allow you to mistakenly assign more than 1 hypervisor to a host.

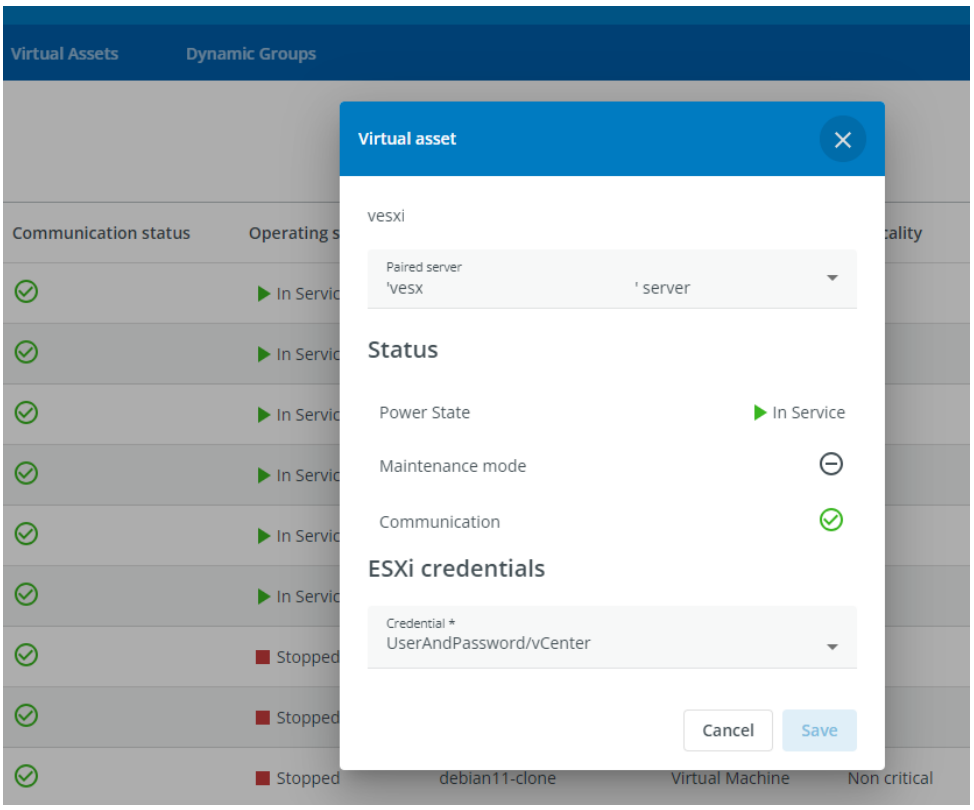


Setting Hypervisor credential

In order to tune VMware, Nutanix cluster shutdown restart sequence you can configure Hypervisor credential.

To proceed to configuration: select an Hypervisor and click on **edit button**. A dialog box will open with Hypervisor Credential

- Hypervisor credentials correspond to a super user account
- The IPM Security Wallet stores ESXi credentials, allowing you to either choose an existing credential or add a new one through **Add new credential** button
- A Yellow warning message is displayed if ssh connection is failed



Setting VMware Virtual Machine Criticity

In order to tune VMware cluster shutdown restart sequence you can configure Virtual Machines criticity.

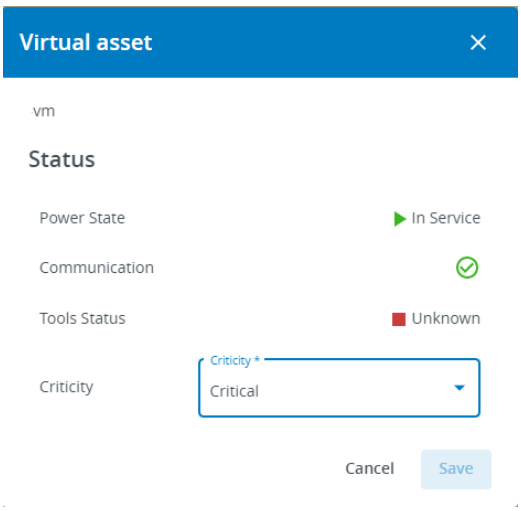
However, this setting is not mandatory.

To proceed to configuration: select a VMware virtual machine and click on **edit button**. A dialog box will open.

Following Criticity levels are possible:

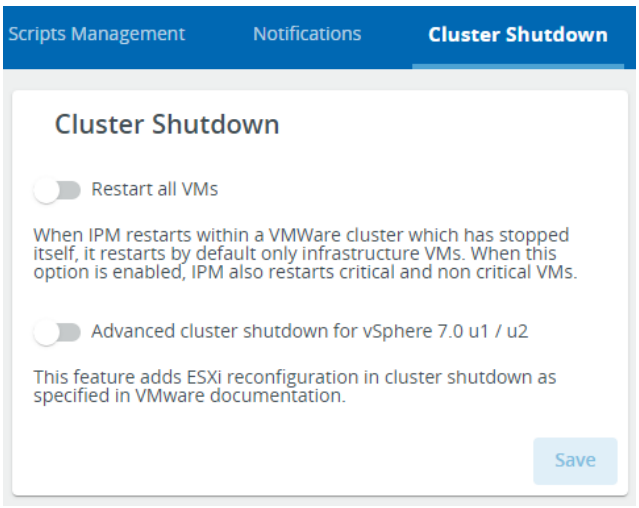
- 3 levels can be set by the user:
  - Non Critical (default value)
  - Critical
  - Infrastructure

- The level of some VMs is detected by the system and cannot be set nor modified by the user:
  - Infrastructure (autodetected)



Once Virtual Machines Criticity is configured you can activate / deactivate the **Restart all VMs** after a Cluster Shutdown action

This option is accessible from **Automation** => **Automation Settings** => **Cluster Shutdown** tab



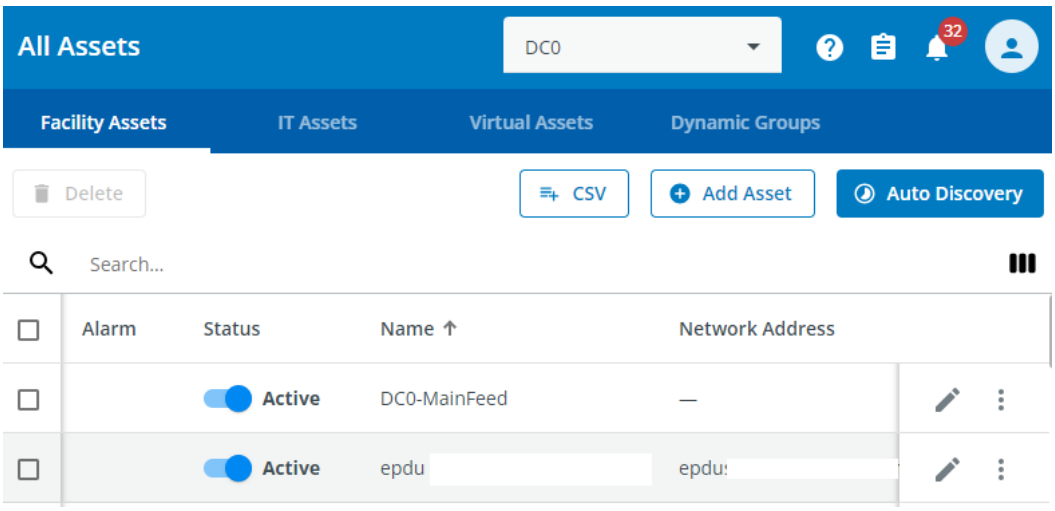
Please refer to Automation View page for more details

Dynamic Groups

Please refer to Asset Management page

2.9.2 Primary asset actions

On each Asset page, you can access the primary asset management actions via buttons located at the top of each page.



Auto Discovery

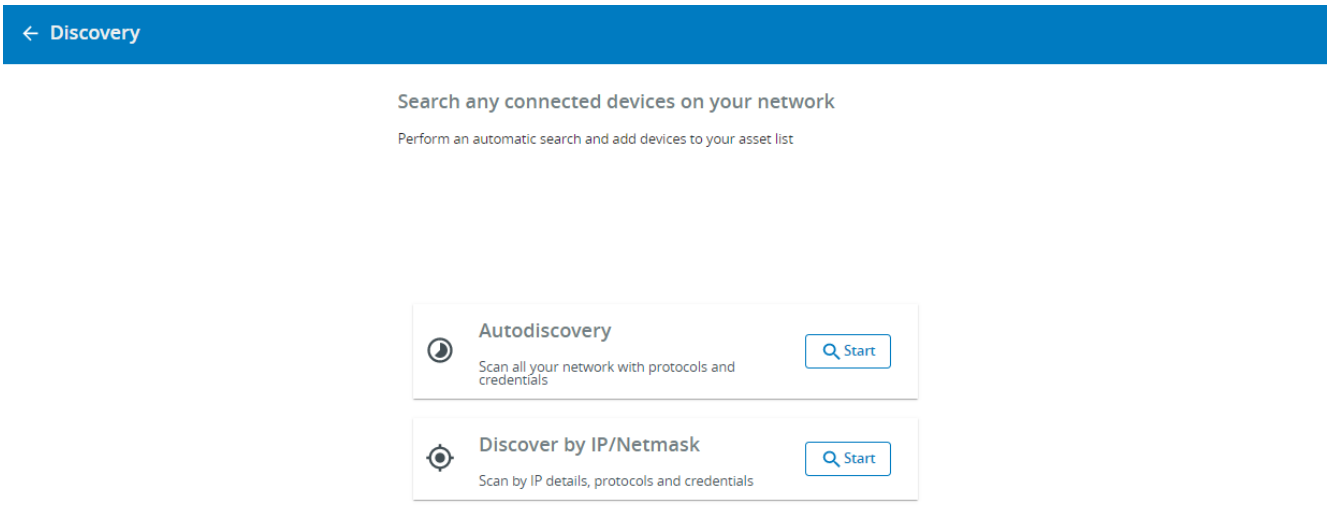
This menu item enables you to perform a scan of the network to discover connected power assets and to add them automatically to the asset list. The devices elligible to the discovery are of following types:

- **Uninteruptible Power Supply (UPS)**
- **Rack Power Device Unit (PDU)**
- **Automatic/Static Transfer Switch (ATS/STS)**

Once the Auto Discovery menu item is selected, you are presented with the Auto Discovery initial choice.

Discovery initial choice:

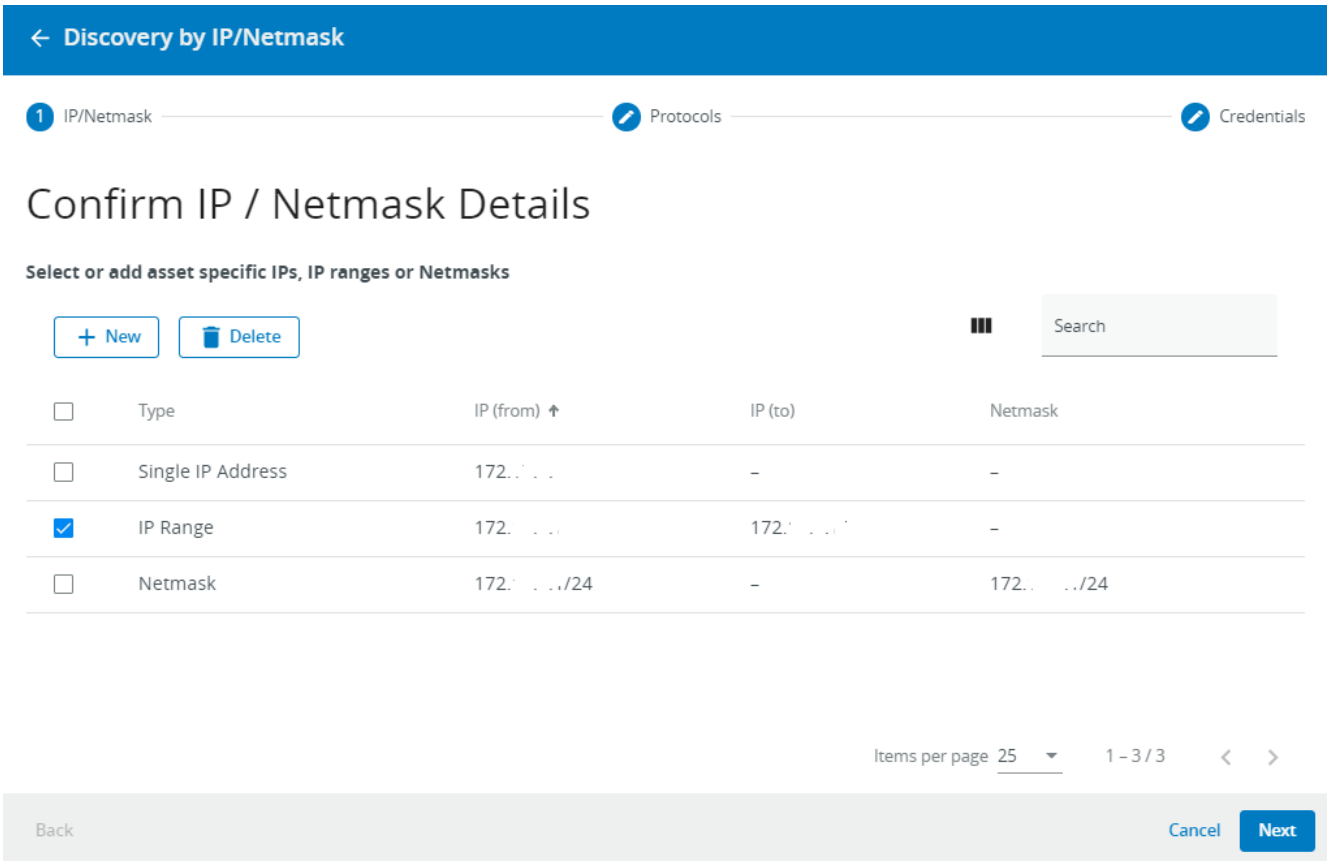
1. **Autodiscovery** will start a 2 steps wizard for **Protocols** and **Credentials** selection
2. **Discover by IP / Netmask** will start a 3 steps wizard for **IP details** then **Protocols** and **Credentials** selection



Step 1 : **IP Details** (**optional** for Autodiscovery Mode)

- You may select from one of three methods to control the scope of the discovery process over the network (**Single IP Address** or **IP Range** or **Netmask)**

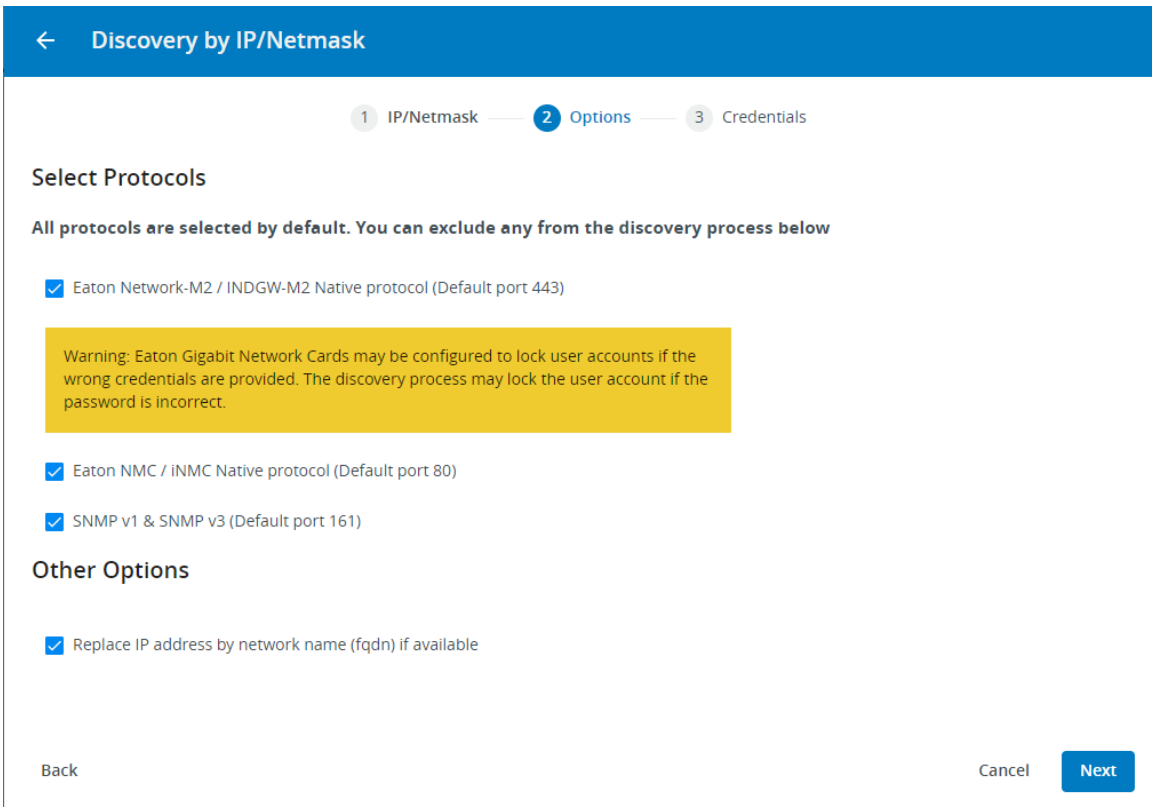
- Click on **New** button to search by **Single IP Address** or **IP Range** or **Netmask**. Depending on the context enter any relevant settings like IP address or range.
- To select a method, simply select the corresponding line.



- **Single IP**: The scan will only be performed on the individual IP address that you enter.
- **IP Range:** is a contiguous list of IP addresses defined by the first and the last addresses in the range. The scan will be processed over all the IP addresses included in the range(s) defined by the user.
- **Netmask:** is a set of addresses defined by a base IP address and a netmask. The scan will be processed over all the IP addresses included in the range(s) defined by the user.

Step 2 : Select Protocols and options

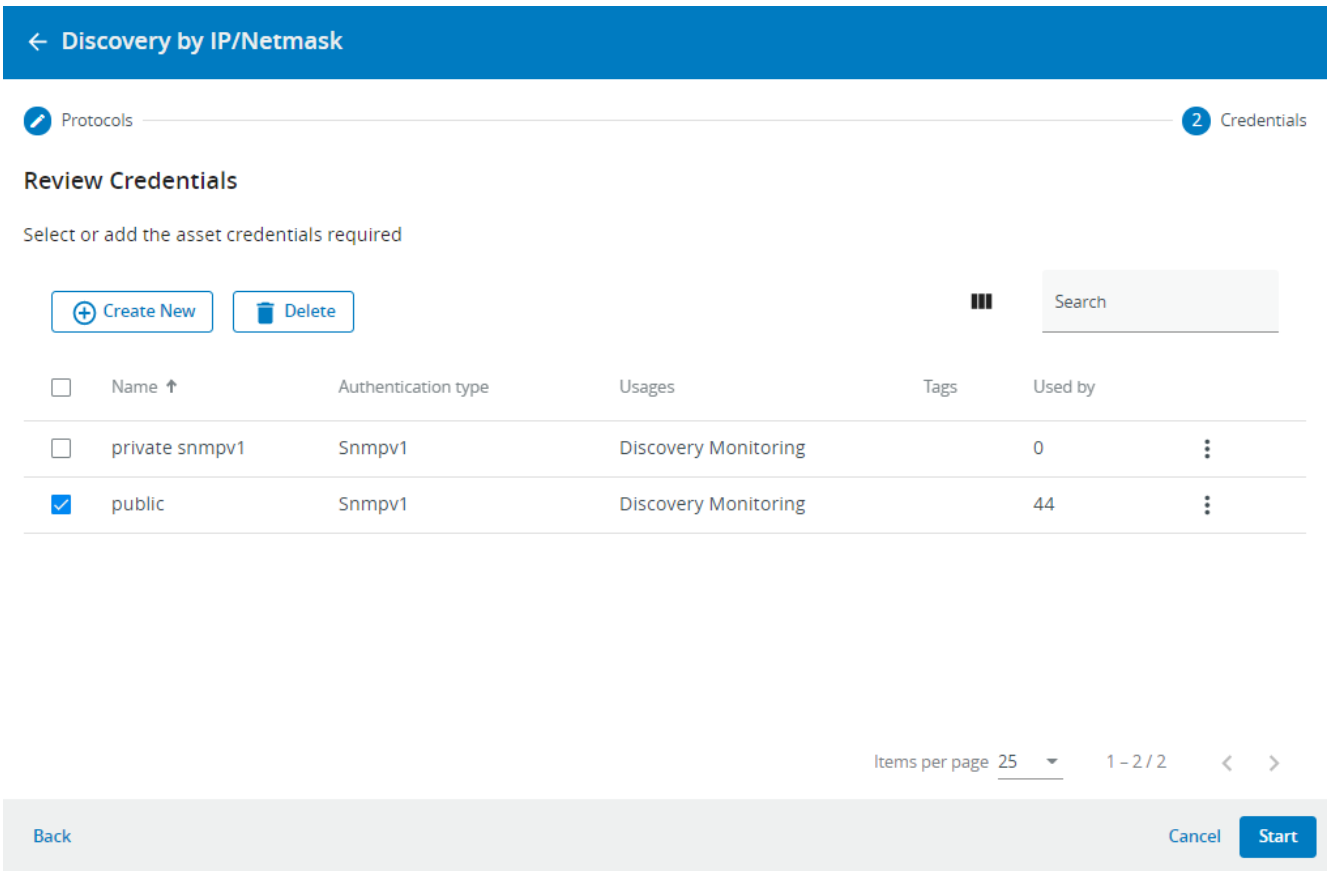
In this step you can select the target protocols for Discovery process and some extra options



Step 3 : Select Credentials

In this step you can select the target Credentials for Discovery process

Create New button allows you to create a New credential for Discovery Process



Pressing the **Start** button will launch the configured automatic discovery process.

Simply press the **Cancel** button to exit the discovery modal without starting a discovery process.

Upload CSV file

This button allows the import of a CSV file containing some number of asset descriptions (one per line).

A CSV file may be generated to backup all of the configured assets in CSV format (see **Export Assets**, below).

> The CSV upload requires a specific format. Please refer to the Asset Management documentation for more detailed information

Add New Asset

This button allows you to create an individual asset from the UI by entering asset details in the configuration Wizard that will appear.

This asset configuration Wizard is documented in the **Asset Management** section of the documentation.

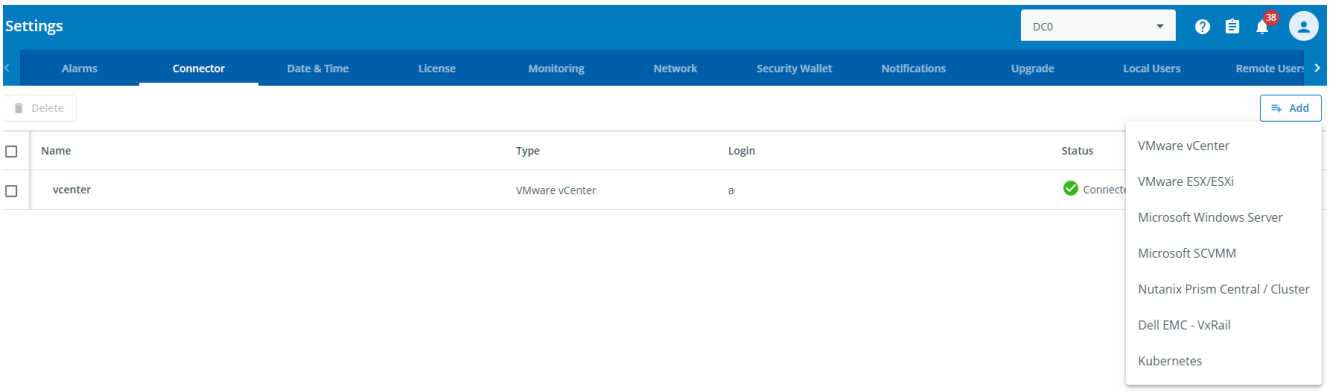
> Before proceeding with the addition of new assets to your system, please consider the comments below:
> - Create the appropriate Input Power topology for your data center. See the possible recommended topologies available in the Typical Power Chain Topologies section in the documentation.
> There is a specific Power Chain in the IPM application called the **Input Power Chain**. The input power chain is made up of power devices (Feed, Genset, stand-alone UPS) which provide power to your Data center. In order assign a device to the Input Power Chain, you simply need to set its location as **data center**.

- After defining the input power chain of the data center, we recommend that you proceed to create all rack mounted power devices (E.g. rack mounted UPSs, rack PDUs, etc.) in order to complete the power chain down to the rack power device level.
- For adding sensors to the asset list, there is a dedicated **T&H Sensors Management** sub-section in the **Asset Management** section of the documentation.
- For adding daisy chained rack PDUs to the asset list refer to the **ePDU G3/G3+ Daisy Chaining** sub-section in the **Asset Management** section of the documentation.
- To enable monitoring, you must make sure you have enabled SNMP v1 or v3 protocol from the Web interface of the devices. You will need to configure SNMP credentials in the application. Refer to the **Security Wallet** section for more information.

Add Connector

To add a connector, user is redirected to settings menu / connectors

For more information please read the Settings / Connectors documentation page.



Export Assets

This button generates a CSV file that contain the description of all the configured assets.

This file will be usable to restore the asset list later if needed (see "Upload CSV file" above).

Disable Asset

This toggle allow you to activite or not the monitirong of the asset.

If you disable an asset, all thresholds set (via the setting/Alarms page) on this asset will be lost.

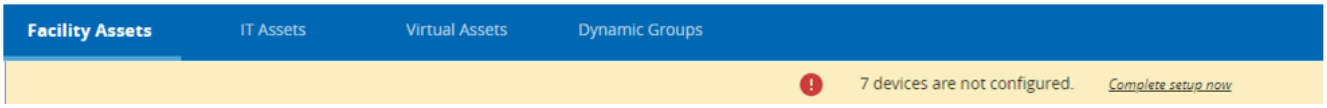
Delete Asset

This button is only active if at least one asset is selected.

When active and pressed, this button deletes all the selected assets from the list.

2.9.3 Asset list statistics and report

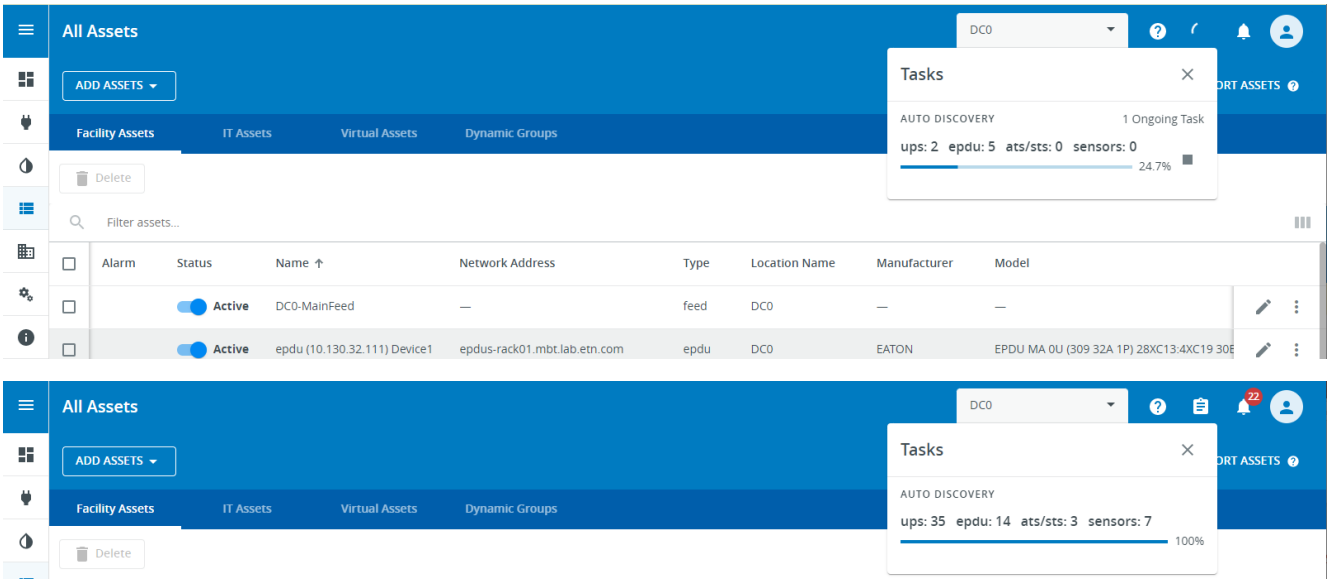
Just below the top row of buttons, the asset management view displays an optional message informing about the completeness of the configuration.



Depending on the way each asset has been added, its **power source** and **location** in the data center might not be set and it may not be set to **Active**. This information is mandatory for an asset to be monitored by the IPM application. In such a situation, a **red alert icon** will draw your attention to the need to complete the configuration.

The link gives easy access to filter the inactive devices in order to help you focus on the assets that still need further configuration in order to be monitored by the application.

The user can also access to task manager, where he will see all the tasks completed or in progress, especially regarding auto-discovery

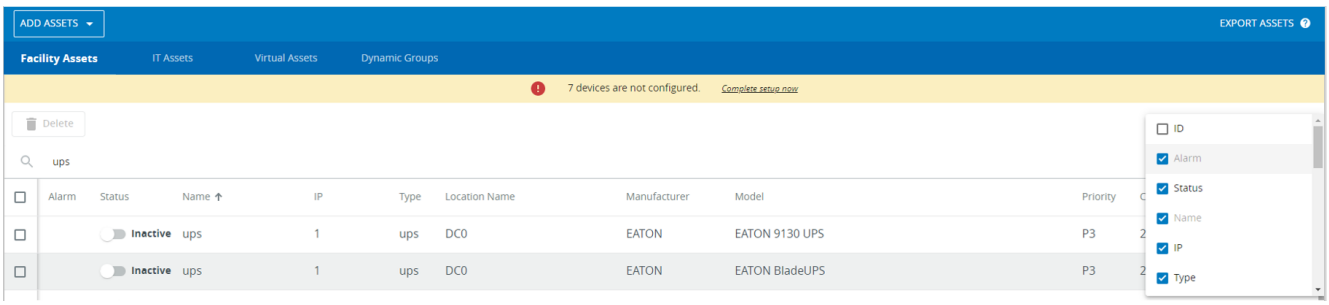


Asset List

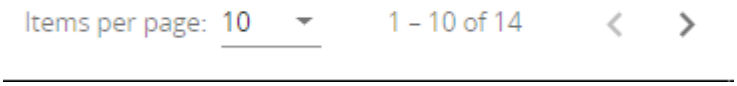
The main content of the asset management view is the asset list itself.

This list can be managed via the column icons and the search field:

- the **list icon (on the right of the search field)** enables the user to choose the columns to display in the table by selecting the related checkboxes.
- the **search field** enables you to select the type of asset to display in the list



- The pagination navigation is available at the bottom of the table along with the configuration of the number of items displayed per page (10 ; 25 or 100).



2.10 Asset mass configuration view

IPM allows you to configure multiple assets at once by selecting:

1. a correctly configured source device first,
2. all or part of the settings of this source asset,
3. the set of all target assets last.

As a result, the data set selected at Step 2 will be bulk-applied to all the target assets selected at Step 3 with the values coming from the source device selected at Step 1.

Note

Note that a configuration can be applied from one device to another if and only if they are both of the same type (hardware/vendor) and having the same firmware revision.
Examples :
It's impossible to apply a configuration from a NMC card to a Network M2 card.
It's impossible to mass configure a NMC card to another NMC card running with a different firmware version.

Note

List of eligibles assets to Mass configuration :

UPS/NMC	Network-MS / Modbus-MS cards
ePDU/G3	ePDU Network management card
UPS/M2	Network-M2 / INDGW / XSlot cards (FW version 1.7 and upper)
ATS/M2	Network-M2 (FW version 1.7 and upper)
ATS/NMC	Network-MS

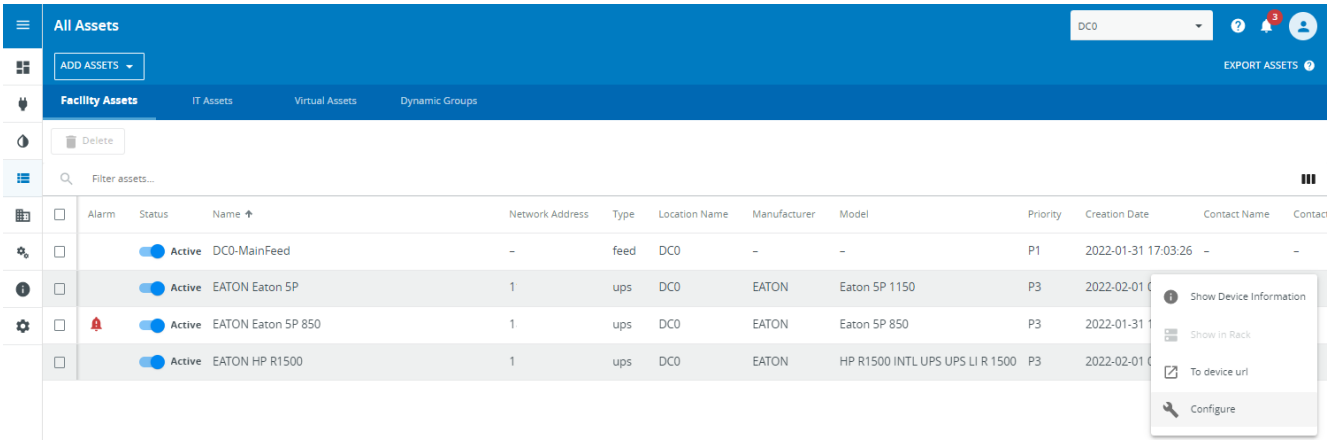
Note

Credential & Protocol Mass Management:

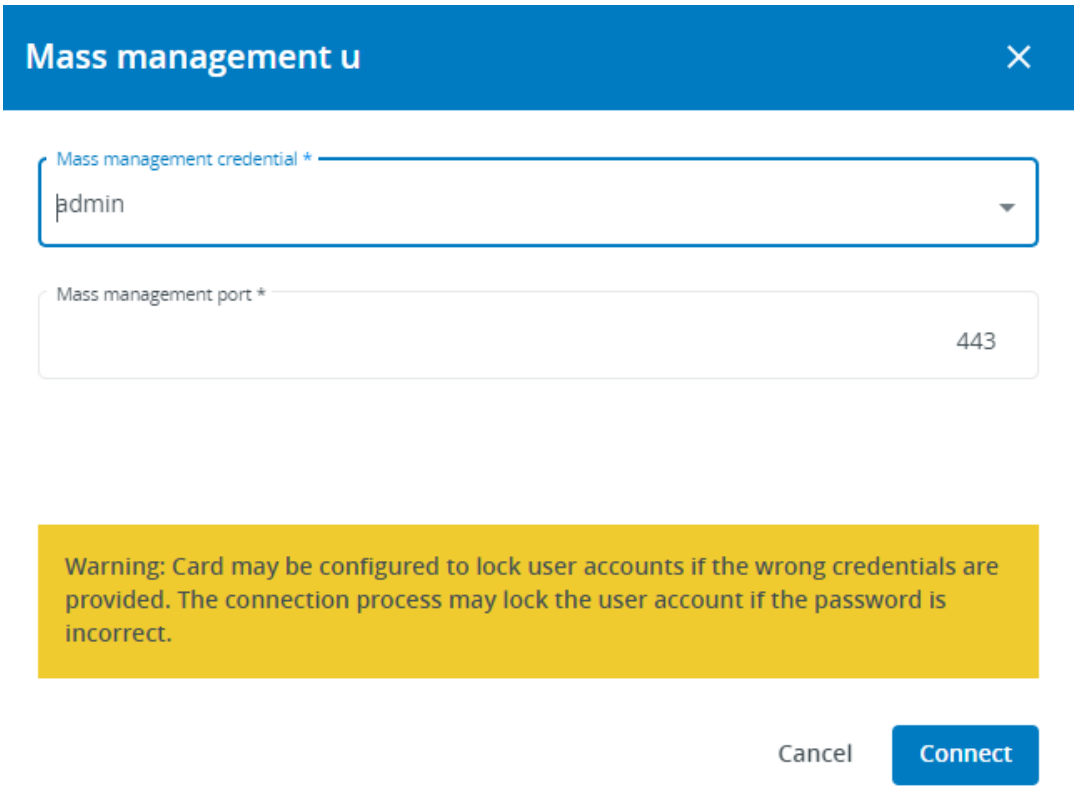
- A new section is displayed to the user in the top of the mass configuration feature/panel
- This section is called "**IPM Settings related to assets**" and displays one setting "**Connection settings for asset monitoring**", that is check-able
- If this setting is checked, then the source connection settings used by IPM2 to monitor the source device, will replace all the destination assets connection settings in IPM2, as follow :
  - Will be replaced:
    - Monitoring protocol (& other settings linked to the protocol)
    - Credential for monitoring (if exists)
    - Port to be used for monitoring
  - Will not be replaced:
    - IP address (host name)
    - Sub Address (position in the chain for ePDUs)
  - The connection settings are applied in IPM only if the settings changes are successful on the target device

- If this setting is not checked, then the source connection settings used by IPM2 to monitor the source device, will not be applied to any destination assets connection settings in IPM2 :
  - Connection settings used to monitor destination assets will be unchanged.

To begin this process, go to the **Asset => Facility Assets** view, select the source asset from which you want to copy the configuration, then access to the **Configure** feature.



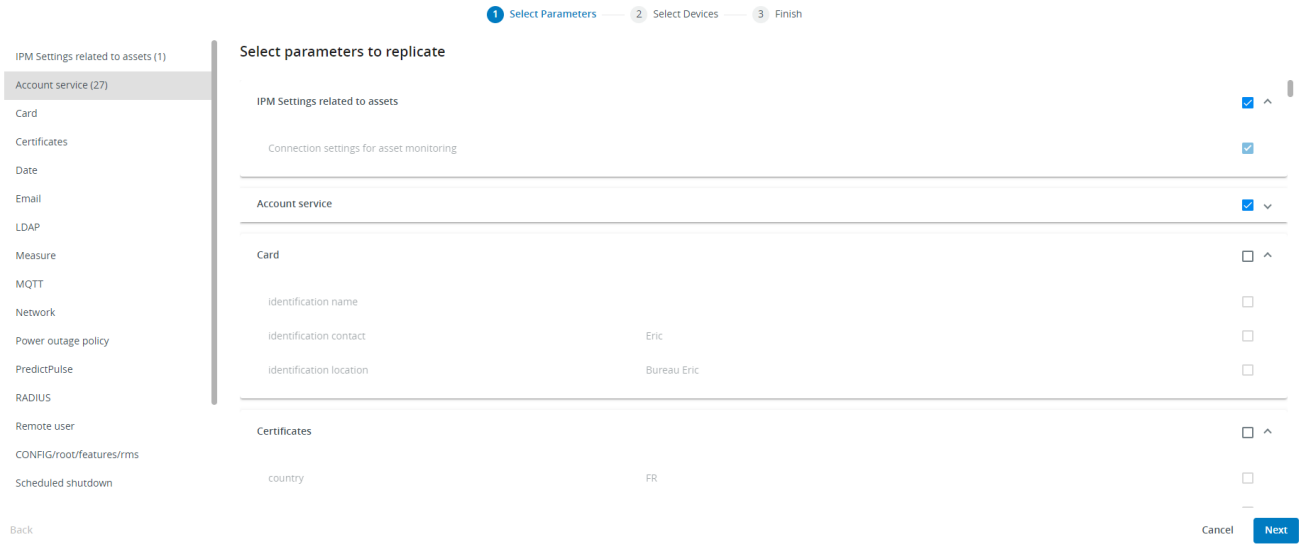
Then, select/create the credentials to authenticate to the device.



2.10.1 Step 1 Select Parameters

- IPM will display all settings available for the asset. They are grouped by categories.

- Select the settings you want to copy to another device.
- Once all / or part of settings are selected, click on the **Next** button.



This table provides typical examples of the available parameters categories

e.g. for NMC Card (communication card dedicated to UPS)	**e.g. for ePDU G3 (communication card dedicated to ePDU)**	**e.g. for Network M2 card (the list below may vary depending on the FW revision of the Network M2 cards used)**
• System settings • Access control • Network settings • Outlets • Emails • Network Management System • Environment sensor • Shutdown schedule • Time settings • Client settings	• System settings • Access control • Netwotk settings • FTP settings • HTTP settings • Network Radius settings • SMTP settings • Telnet settings • Network log settings • SNMP • Network management settings • LDAP settings • Display settings • Users • Emails • Input • Outlets • Outlets groups • Environment sensor • EnergyWise settings	• Account service : settings related to user management and card password management (Password strength, Account expiration, session expiration, preferences settings, administration password) • Card : card general information (contact, location, name) • Certificates : certificates settings • Date : Date & Time settings • Email : email sending configuration • LDAP : LDAP configuration for User management • Measure : Meters Menu / Measure logs (logs UPS measures frequency) • MQTT : MQTT certificates • Network : network settings • Power Outage Policy : protection settings / Power outage policy set on the card • RADIUS : RADIUS configuration for User management • Remote user : user preferences settings (temperature, language, date, time) • Scheduled shutdown : protection settings / scheduled shutdown • SMTP : email SMTP server settings • SNMP : SNMP card settings • Syslog : protocols settings / system logs

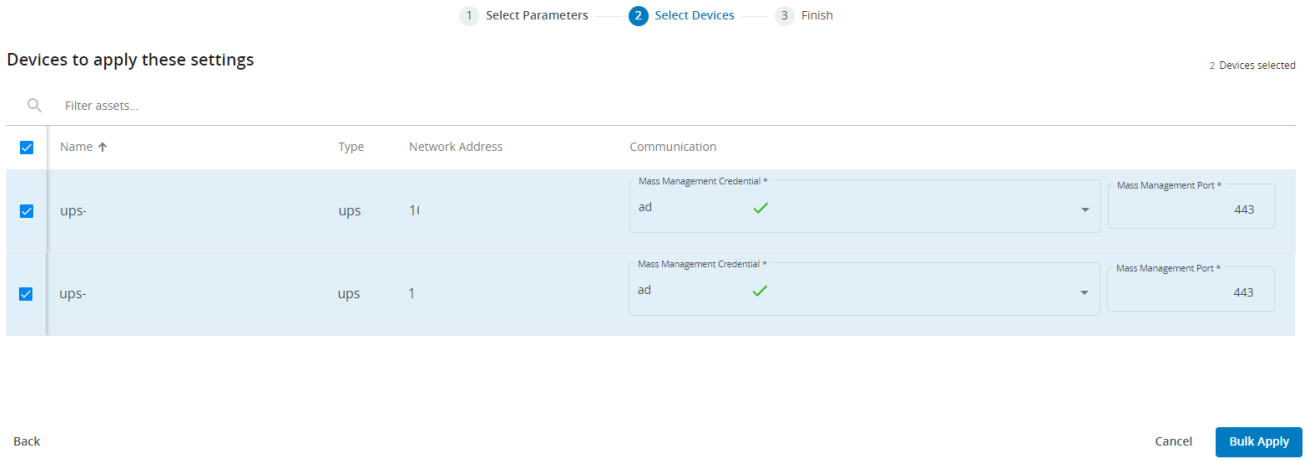
e.g. for NMC Card (communication card dedicated to UPS)	e.g. for ePDU G3 (communication card dedicated to ePDU)	e.g. for Network M2 card (the list below may vary depending on the FW revision of the Network M2 cards used)
		• Webserver : protocols settings / HTTPS server settings

Note

For Network M2 card, it's possible to select only features and not individual settings.
For full details on features content, please refer to Network card online help or user guide.

2.10.2 Step 2 Select Devices

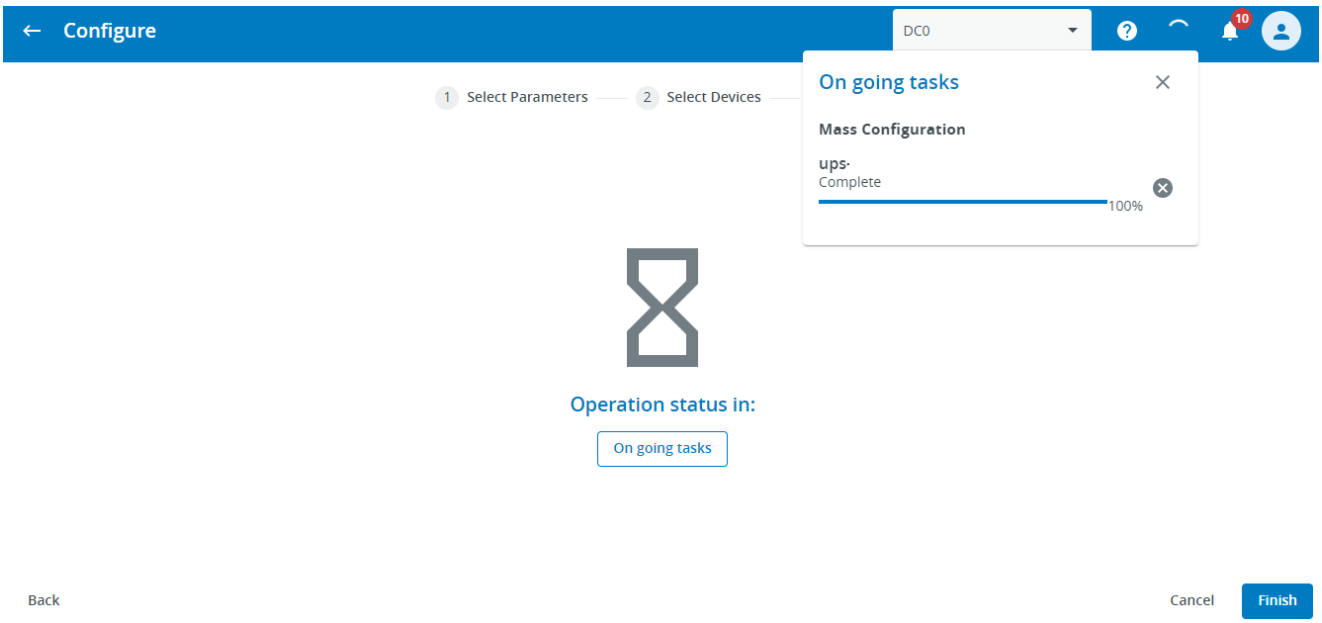
- Select the asset(s) where to copy the configuration. IPM will display only the eligible assets.



Click on "Bulk Apply" button to start the configuration on targeted assets.

2.10.3 Step 3 Finish

- IPM will show the progress of the configuration in the Task panel, and display a message once operation is done.



2.11 Automation view

2.11.1 **Overview**

IPM Editions software can keep the business continuity of your infrastructure by handling a set of policies.

The IPM Editions software guarantees the continuity of your activity by the management of automated protection policies. The configuration of these policies is provided though an intuitive step-by-step creation wizard.

The resulting policies can address both the physical and digital infrastructures.

They consist in user defined ordered list of actions triggered by some event.

Examples:

- **protection of an IT infrastructure** : example - execute an action if an event happens on one of my devices
- **notification of specific power events** : example - send an email notification in case of an event/alarm is triggered on one of my devices

One ordered list of actions and the initial trigger is what we call an *automation*.

All automations follow the same basic configuration flow:

- define the triggering event that will start your automation
- select an action to perform in case the triggering event is reached
- select the target device(s) to which to apply the action
- loop on actions/targets definitions

2.11.2 **Automation main page**

Through this menu users are able to manage all automations:

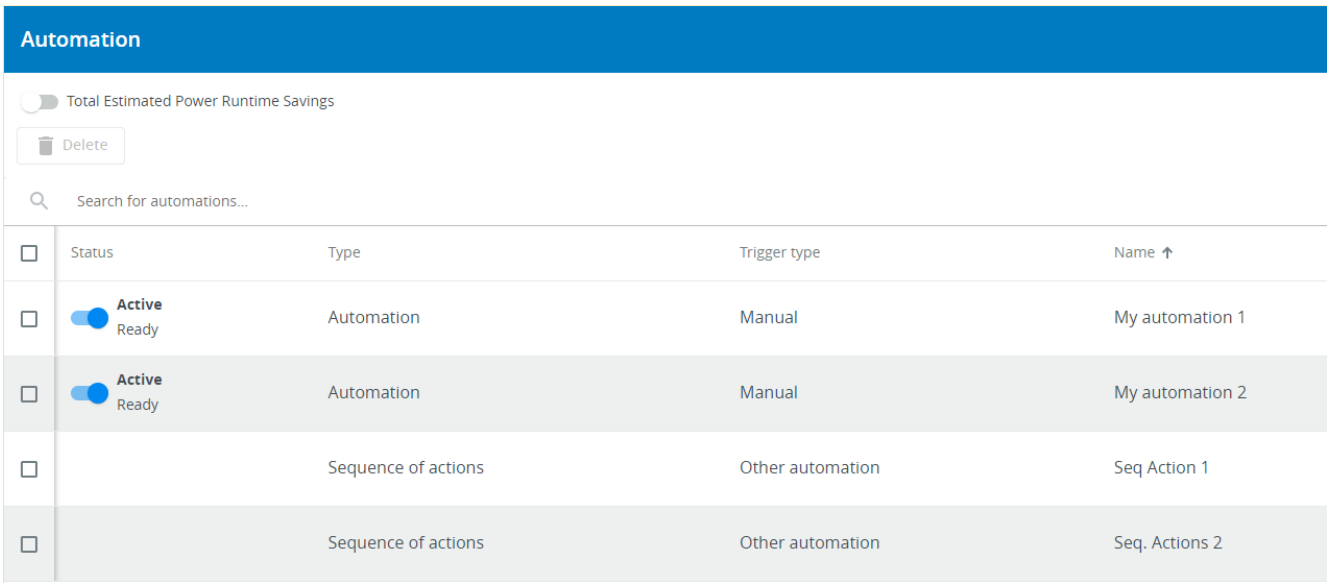
- **Create automation**
- **Create a Sequence of actions**
- **Edit automation**
- **Edit a Sequence of actions**
- Manage the **Automation settings**

The corresponding page contains some action buttons on the top and a list of all configured automations and Sequences of actions, as a main content.

Automation List

All existing automations are listed in this table. From the list you may easily:

- Activate or deactivate an Automation. An automation in an **Inactive** state will not start if the trigger event occurs. By default, an automation is inactive upon creation. You must manually activate it.
- Find all of the important information about each automation : Name, type of trigger event, execution information (last start, last end, current activity, end status, and execution history)

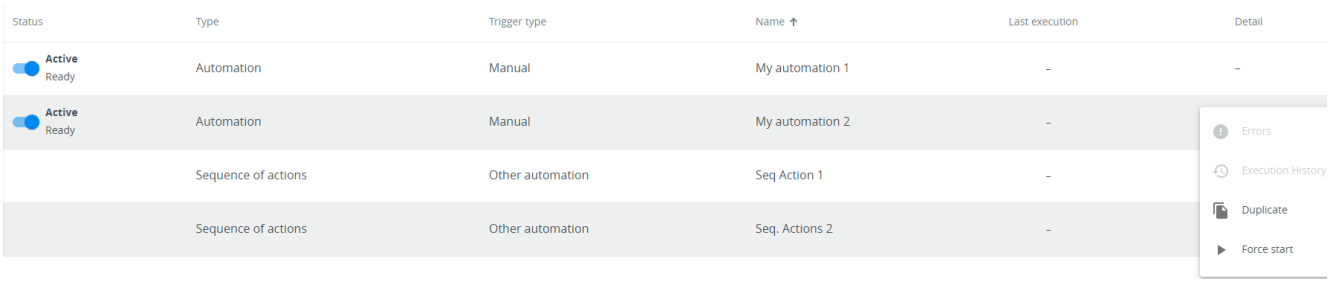


> **Note**
>
> A "Sequence of actions" cannot be activated, as it is not aimed to run outside of an If/Else action of an automation.
> A "Sequence of actions" is identified by its "Trigger type" which is always called "Other automation".

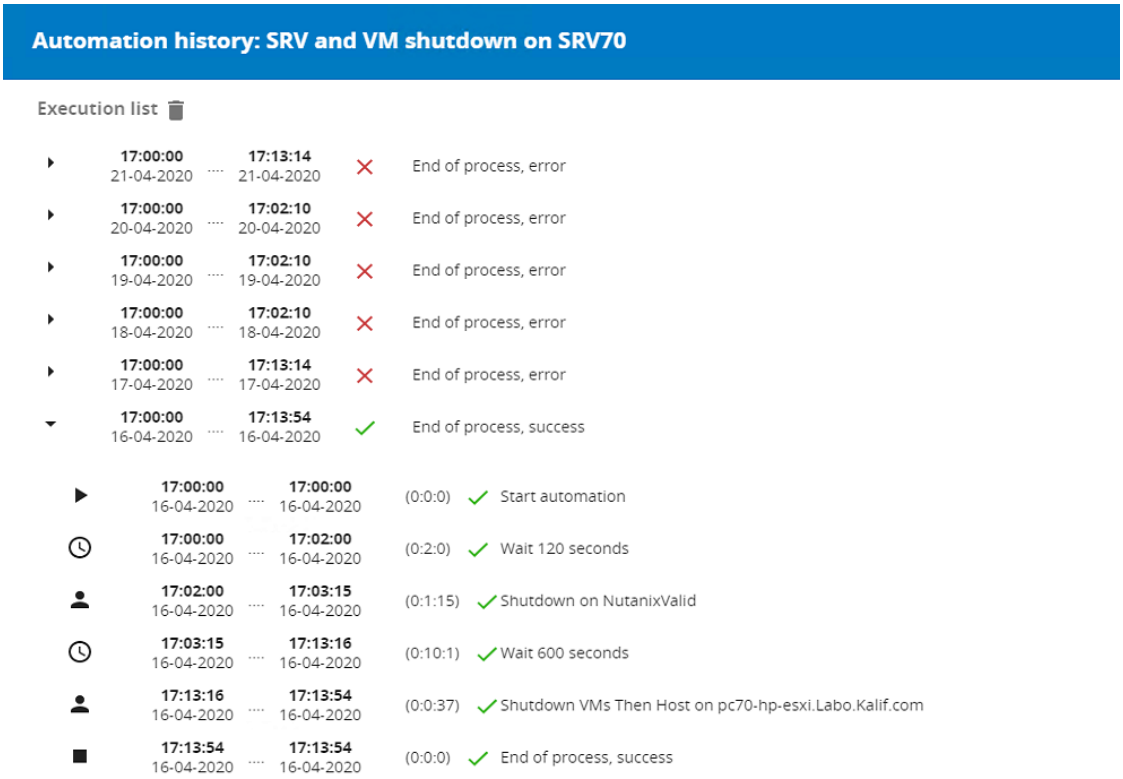
Actions buttons found to the right of the table, or accessed with a right click, allow you to:

- For an Automation object:
  - **View execution history**: here you will find all the execution histories of a policy, for each execution the detail of each stage is available as well
  - **View Errors:** here you will find all errors that have occurred during previous executions of the automation
  - **Edit** the automation
  - **Duplicate** an automation
  - **Force start**: will manually force the immediate execution of the automation as if the triggering event was just reached
- For a Sequence of actions object:
  - **Edit** the Sequence of actions
  - **Duplicate** the Sequence of actions

Detail of action buttons :



Example of execution history for an "automation" :



Automation Settings

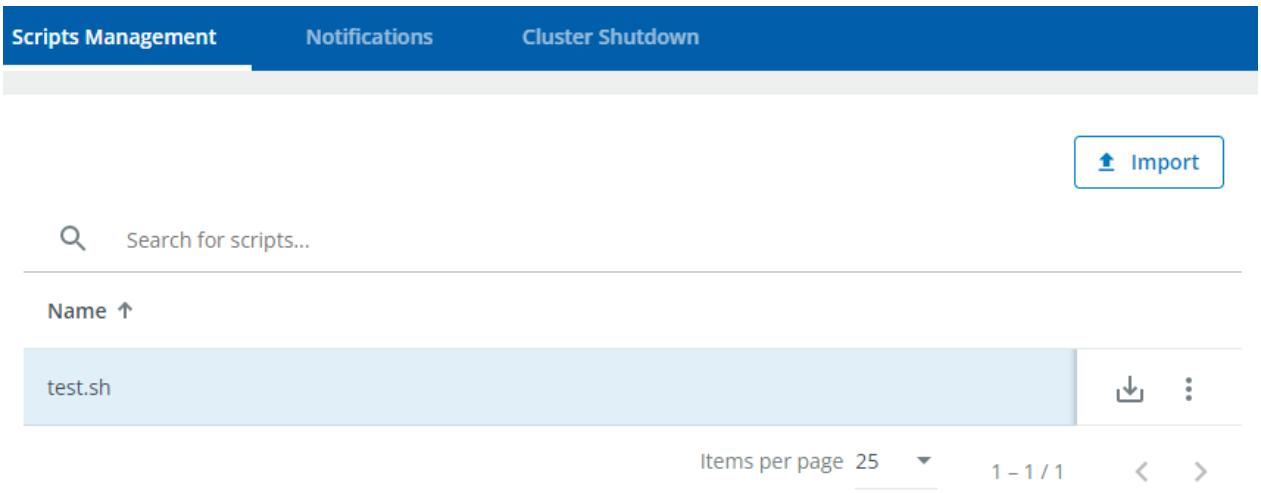
The Automation settings sub-menu enables you to configure global parameters that apply to the entire automation.

Scripts management

It is possible to configure actions based on custom user script.

To use a script as an action, you may manage available script from here with following possibilities:

- Import
- Execute for test purpose
- Download
- Delete

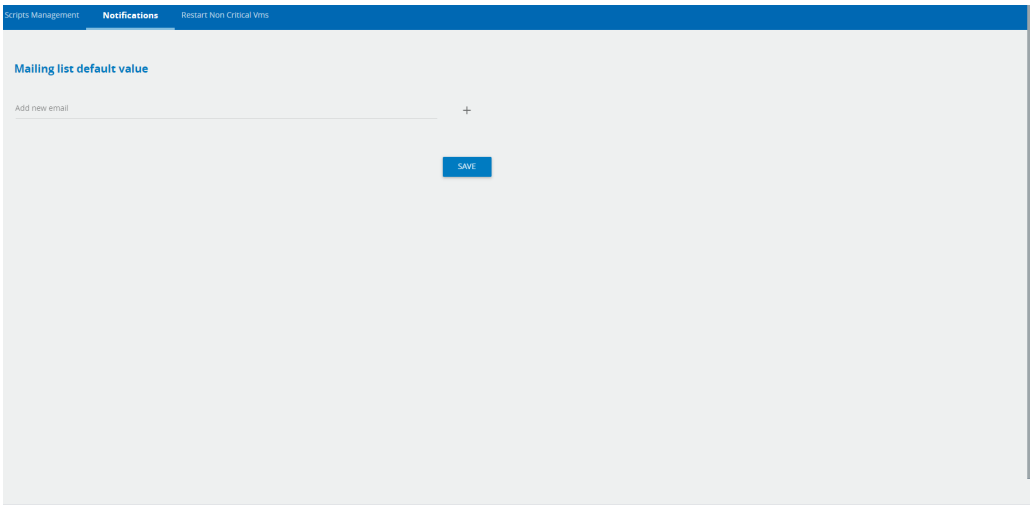


For more information on Script Management please refer to the **Action** section in **Automation** page

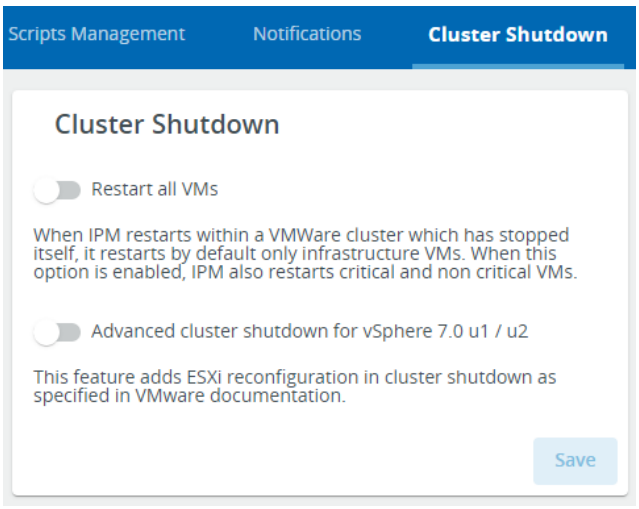
Notifications

It is possible to configure the email address(es) to use by default when you create a **Notification** action. Values set here will be retrieved automatically in the automation wizard when you configure a **Notifications** action.

However, it's still possible to change the mailing list during the automation configuration. In this case, the override value will apply only to the automation where the value is changed.



Cluster Shutdown



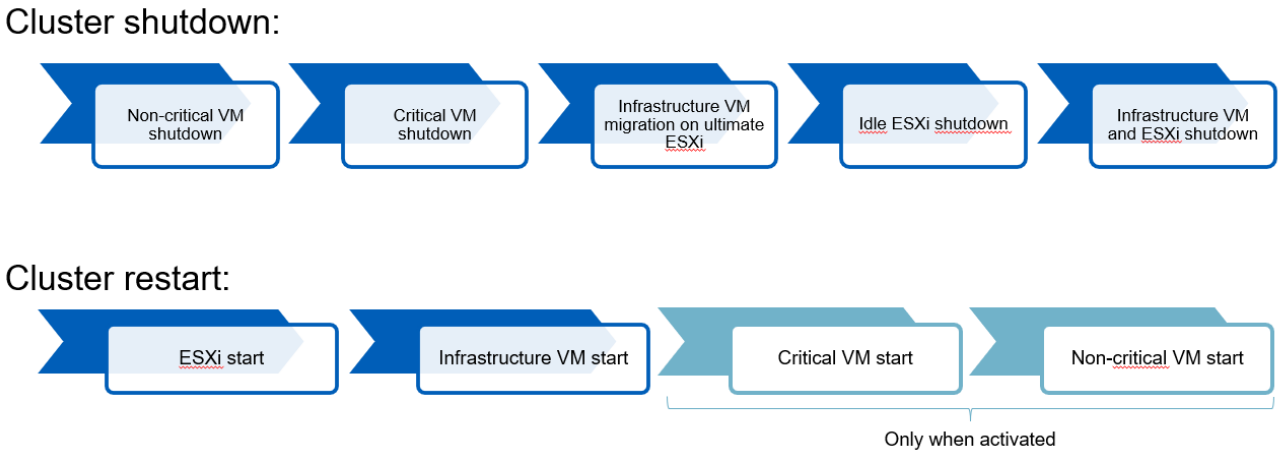
Prerequisites
This setting applies to the following specific situation:

- IPM VM is deployed inside a VMware cluster and configured to be restarted automatically when its hosting hypervisor will restart
- All the other hypervisors of the cluster hosting IPM are restarted manually afterwards

Restart all VMs toggle & Cluster Restart scenario
In the above context, if the toggle of this setting is set to enabled, IPM will trigger a restart scenario as follows:

- wait for all ESXi to be restarted and all VMs to be monitored again
- execute iteratively the power on action on each VM, one by one (prioritize Critical VMs then Non Critical VMs)

This is illustrated by following Time Diagram



Non-critical VMs definition
The set of non-critical VMs potentially restarted by the restart scenario is the set of all the VMs that were running at the time the cluster shutdown started except:

- Critical VMs
- Infrastructure VMs
    - the corresponding vCenter VM (Infrastructure auto detected)
    - the corresponding IPM VM (Infrastructure auto detected)
    - User defined Infrastructure VMs
- the VMs that are part of a vApp

Notes

- If not all ESXis are restarted after a 5min delay, the scenario continues and tries to perform the VM restarts concerning the restarted ones only
- If some ESXi were put into maintenance mode during the cluster shutdown, IPM takes care of making them exit this mode automatically
- Infrastructure VMs are always restarted when the hosting ESXi starts regardless of the status of all the VMs restart Options
- VMs that were powered off before the cluster shutdown will remain off after the cluster restart even is the restart scenario is executed
- The restart scenario only applies to the cluster IPM is deployed into
- If IPM is deployed in a non-VMware cluster, the restart scenario won't operate regardless of the toggle status of this setting

Please refer to Asset Management View for more details

Advanced Cluster Shutdown for vSphere U1/U2 toggle
If you enable the "Advanced Cluster Shutdown for vSphere U1/U2", a connection verification will be done on all ESXi connected to a vCenter 7.0 U1/U2:

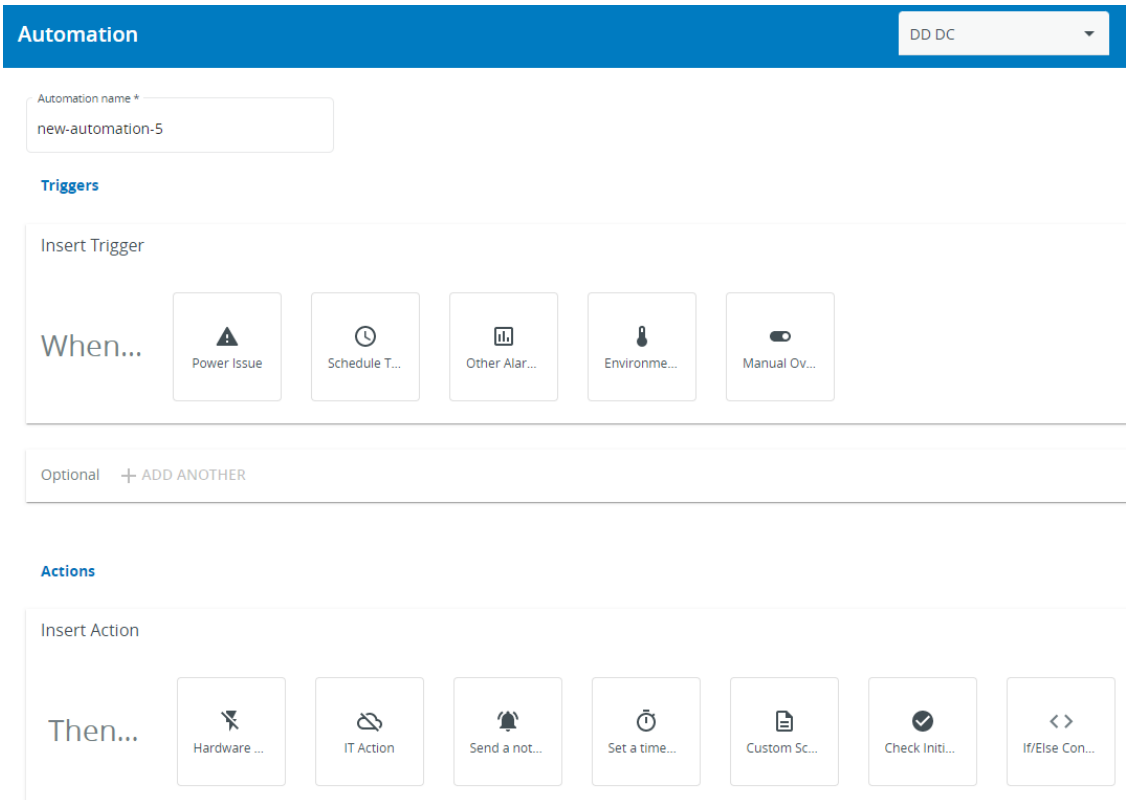
- The state of ESXi connection is verified every 10 minutes including ssh connexion state and vCenter → ESXi connexion
- Note: If the ssh connexion state is down, the communication status in the Virtual assets list is Orange, with a warning message

Automation creation wizard

This section will detail the main configuration steps for an automation and for a Sequence of actions.

Automation creation:

First of all, you must provide a name to the automation. This field is mandatory.



Define the triggering events
The triggering events are the starting point of any automation.

All triggering events available are grouped into the following categories:

- **Power issue**
- **Scheduled time**
- **Other alarm**
- **Environmental issues**
- **Manual override**

Note

A list of all triggering events per device that are managed by the IPM Editions software is available in the Automation section.

Note

The **Automation wizard** is able to detect the application context meaning that the wizard will filter triggering events in order to show only those that can be generated by devices discovered and monitored by the application. Similarly, for actions the Wizard will only propose actions that are possible given your license and virtualization connector configuration.
As a result, it is important that you've completed the setup of the application before beginning to create your automation.

Asset based triggering events
The categories "Power issue", "Other alarm" and "Environmental issues" are all requiring the selection of source asset(s).

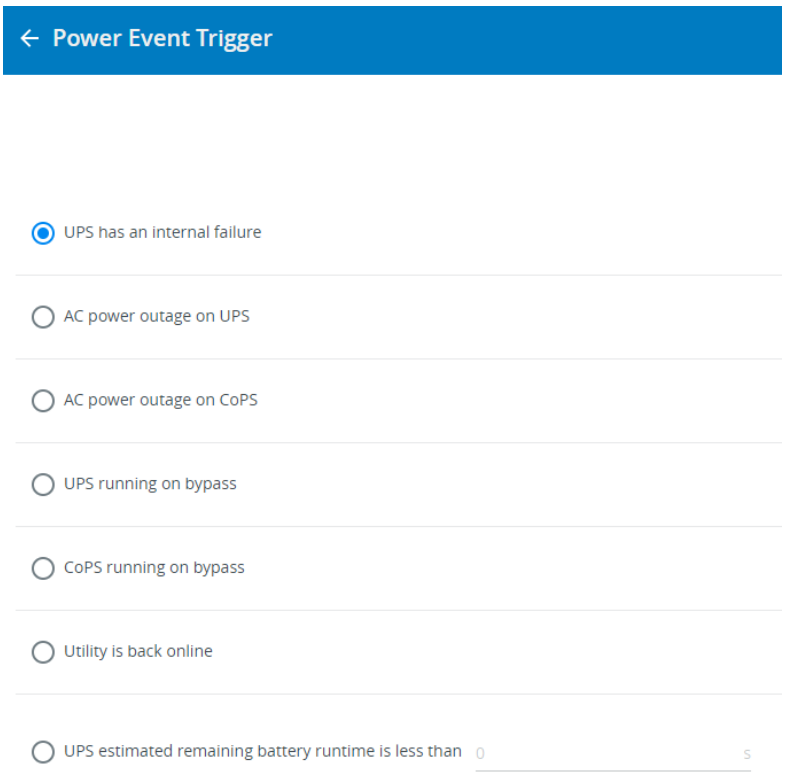
For those categories, the definition of the triggering event is a 2 steps process:

1. select the nature of the event
2. select the source asset(s) of the event

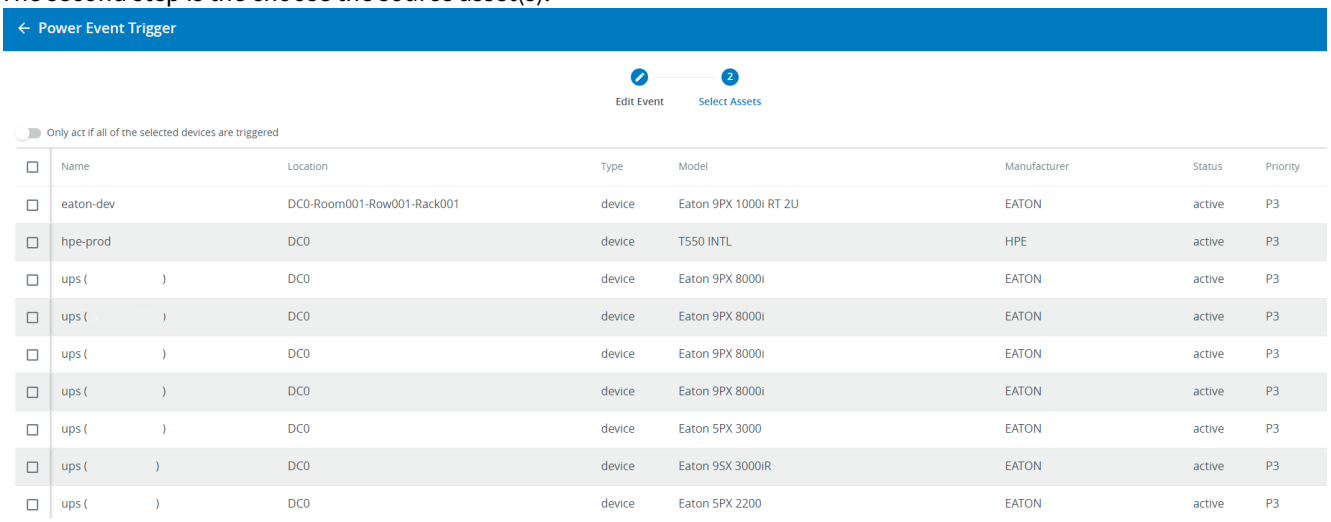
When selecting multiple source assets for a given event, an option allows to define the triggering event to be true either when the event is happening on all the source assets at the same time or at least on one of the source assets.

Example on power issue:

The first step is to define the nature of the event.



The second step is the choose the source asset(s).



Similar approach applies to environmental issues and other alarms.

Trigger Type: Scheduled time
This category of trigger allows you to schedule an automation based on the date and time.

This type of trigger can be useful to configure maintenance windows in an environment or to schedule a shutdown/ switch off devices at a specific interval.

You must select the day and time to start the automation and one of the recurrence schemes below:

- once
- every day
- every week

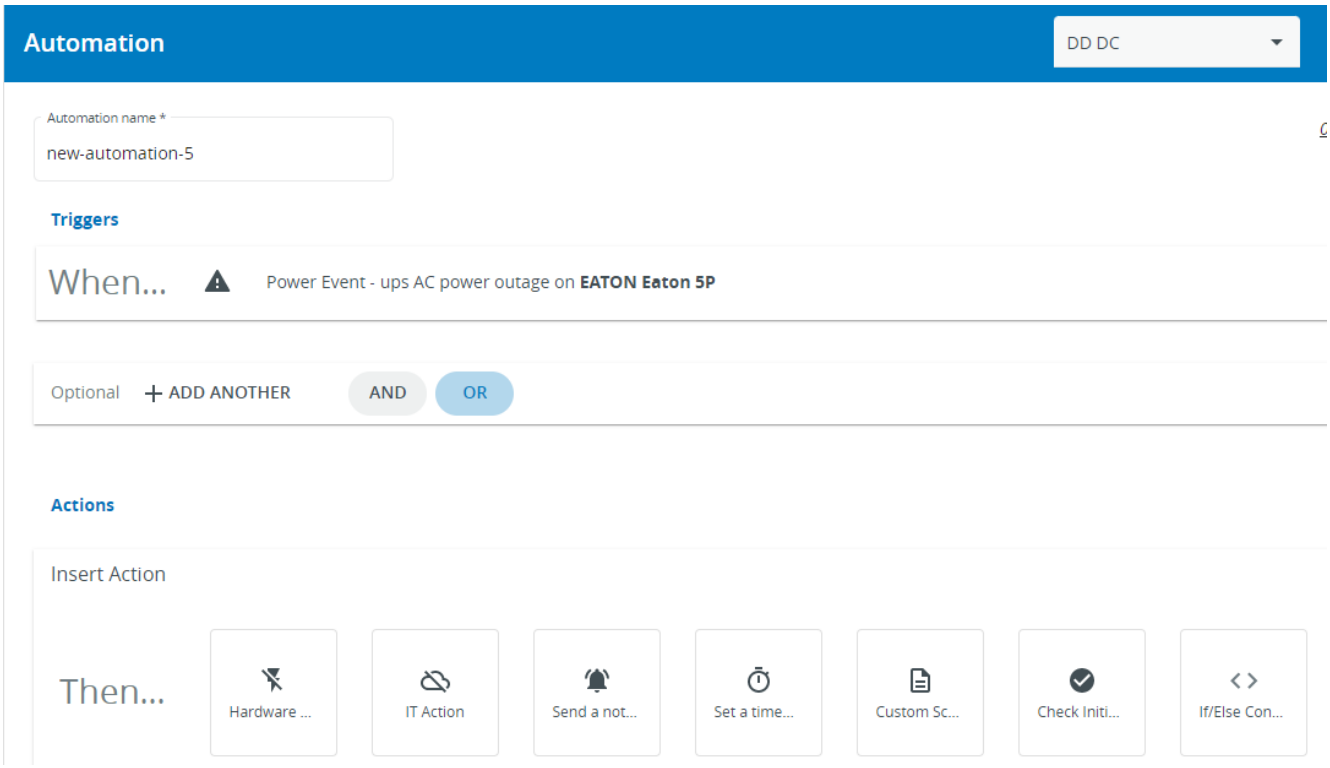
Trigger type: Manual override
This last type allows to define an automation that will only be triggered manually.

No specific event will be listened by the system to automatically start it in the background.
This only way to get it started is to manually request it.

One could use it for capturing anything that should be repeated the exact same way in various and hard to schedule situations. For example, it can be there as a "panic button" kind of policy to run in case of unplanned issue.

This is also a good choice of triggering event to define actions sequences designed only to be initiated within other automations.

Combining multiple triggers
Once the first triggering event is defined some additional triggering events can be combined as an option.



There are two modes to combine multiple triggers together.

The OR mode consists to launch the automation as soon as one of the multiple triggering events is fired while the AND mode would start the automation only when all the triggering events are true.

Define the action(s)
As soon as the triggering events are defined, it's time to specify the action(s) to perform when triggering events are reached.

General principles
You may specify multiple actions, if you want to build a chained sequence of actions.

> **Note**
>
> In the case where you have configured multiple actions, they will be sequenced by order of configuration. In the current version, wizard generated automation actions cannot be executed in parallel but multiple targets can be set for a given action.

Common behaviors for all actions definition
When you've selected the action type you want to configure and the targeted asset(s) to apply the action to, the wizard will guide you through the specifics of this action configuration. You just have to follow the process for full completion.

All action configurations (but the "If/else condition" action) are ending by the same last step about the automation behavior on action error. This step is performed in case the current action falls in error at the end of the execution of it.

You can choose to continue the next actions of the automation, end the current automation, or end the current automation, but before ending it, run another automation.

Note

As in the case of triggering events, the **Automation wizard** is able to analyze the application context meaning that the wizard will only propose actions that are possible given your devices, license and virtualization connector configuration.

Note

Please note that some restrictions in available features may apply with respect to:

- your software license
- the kind of assets configured in your IPM application
- the kind of virtualization connector you have configured as some actions are not available in all connectors

Available actions by category
Actions are split into categories into the wizard to simplify the configuration:

- Hardware Action
- IT action
- Send a notification
- Set a timed delay
- Custom script
- Check initial trigger validity
- If/Else condition action

Hardware Action
This action enables you to control :

- rack PDU devices in order to switch on/off outlets.
- physical servers to turn On/Off the device
- Dynamic group(s) to turn On/Off the devices being part of it/them (please refer to the last section of this page "Dynamic Groups")
- Actuator (Only EasyE4 PLC are supported, see the Appendix IV - Configuring EasyE4 PLC with IPM for more details)

IT actions

Note

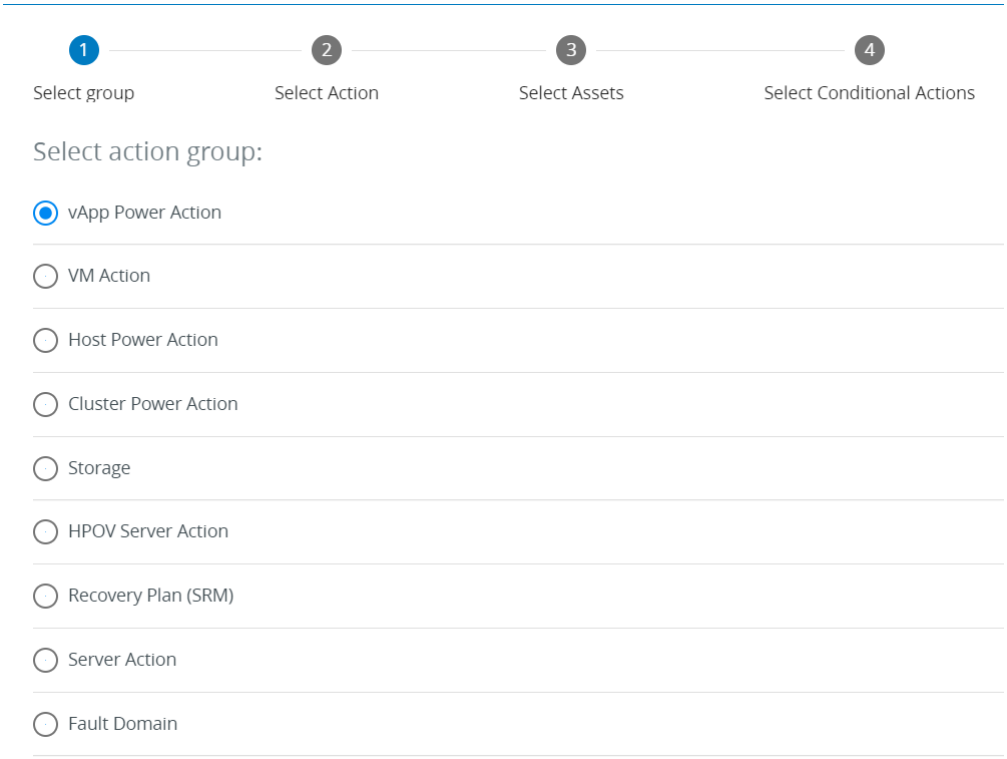
IT actions are enabled when virtualization connectors are configured in the IPM Editions software. Please check the **Setting view / Connectors** section of the contextual help for more information.
For IT actions, please note that some restrictions may apply related to your software license and the type of virtualization connector you have configured as some actions aren't available in all connectors.
Please check the chapter **Automation / IT actions supported** in **the General Information** section in the documentation for more details.

Using IT actions, you may configure actions applicable to virtual hosts and machines monitored via a virtualization connector. In addition to actions on virtual assets, the IT sections also covers the actions applicable to some physical servers directly reachable by SSH protocol.

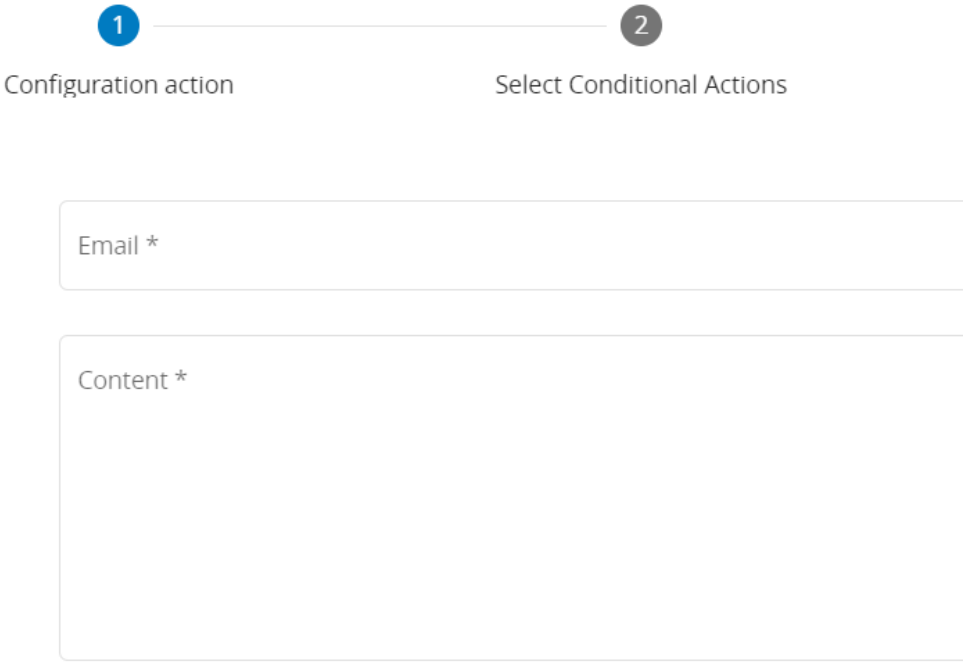
Actions are grouped by sub-categories:

- **vAPP Power Action:** These actions apply to some targeted virtual app(s)
  - power on
  - suspend
  - shutdown
- **VM action:** These actions apply to some targeted virtual machine(s) or dynamic group(s) (please refer to the last section of this page "Dynamic Groups")

    - Migrate
    - Power Off
    - Power On
    - Resume
    - Shutdown Guest
    - Suspend
- **Host Power Action:** These actions apply to some targeted hypervisor(s)
    - Enter in maintenance mode
    - Enter in maintenance mode then shutdown
    - Exit from maintenance mode
    - Power down to stand by mode
    - Power up from stand by mode
    - Shutdown host
    - Shutdown VM then Host
- **Cluster Power action:** These actions apply to some targeted cluster(s)
- **Storage:**
    - Execute a shutdown on a storage node
- **Recovery Plan (SRM)** (VMware Site recovery Manager)
    - Launch a specific recovery plan of a VMware SRM node
- **Server action:**
    - Execute a SSH command on a chosen SSH enabled target device
- **Fault Domain:**
    - Make a domain enter/exit the maintenance mode
    - Shutdown a domain via maintenance mode

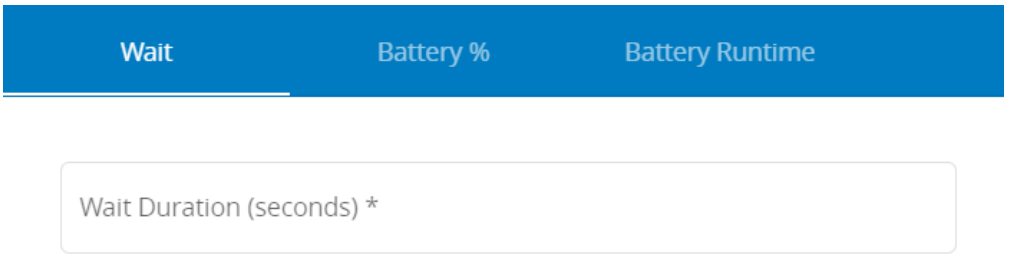


Send a notification action
It is possible to edit the email address and also customize the content of your notification message.



A valid SMTP server must be configured for the Send message action to work properly.
Please proceed to the configuration of the SMTP server to be used in Settings/Notifications page.

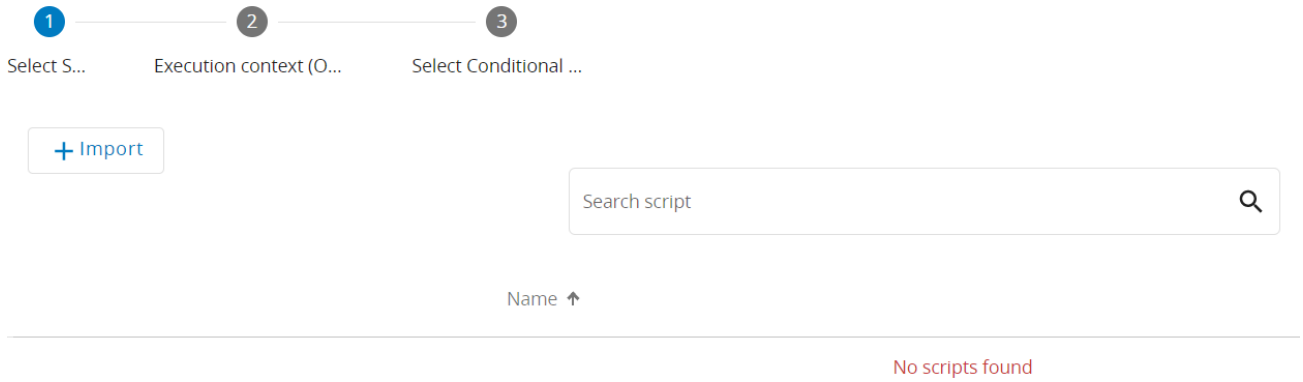
Add a timed delay action
This action is especially useful when defining a sequence of actions. Indeed, it enables you to pause an automation by adding a **timed delay**, **runtime threshold** or **% battery threshold** condition that must be reached prior to executing the next action.



Custom script action
Through this action you may configure an automation with a predefined action generated by a custom user script. The script may be uploaded before configuring the automation (Menu **Automation settings**) or directly during the configuration process by clicking on **Import**.

All scripts previously uploaded will be retrieved by the wizard and presented for selection. Only one script may be selected for execution by the action.

Command(s) defined in the script will be executed when the automation starts.



Note

The IPM Editions software embeds appropriate tools to support the following scripting languages:

- **Bash, Python, Perl** as part of the system
- **IPMI, Redfish, Wake On Lan, Expect** using additional libraries

Check trigger validity action
Use this action to insert an optional break point into the automation action sequence.
The condition tested here is about the state of the trigger of the automation.

If the state is still valid, the automation sequence will continue.

Otherwise, the automation action sequence will stop here and all the actions defined forward in the sequence won't be executed.

If/else condition action

Note

This kind of action is depending on "Sequence of actions" object. It is mandatory to first create a "Sequence of actions" object from the "Automation panel" first. Please refer to the below section to set up a "Sequence of actions".

This action is able to performs a "Sequence of actions", depending on one of the following metrics / system information:

- PowerSource status
- PowerSource capacity %
- PowerSource runtime
- PowerSource load
- Temperature
- Humidity
- Day of the week (1st day of the week is Monday)
- Time of the day (expressed as UTC time)

For example the following use case is possible with an "If/else condition" action:

```
When PowerSource#1 goes on battery, start the automation
    Do Action 1
    If PowerSource#2 is not online
        Run Sequence-of-actions#1
        Continue
    Else
        Run Sequence-of-actions#2
        End this automation
    endif
```

```
    Do Action N
End the automation
```

Note

Note that for the condition on the "Day of the Week" and "Time of the Day", the following conditions will never be true:

- Time of the day (in UTC) is lower than 12AM
- Day of the week is lower than Monday
- Day of the Week is greater than Sunday

Add Another Action : build the ordered list of actions
After each action is configured, the wizard will systematically ask you whether you want to add a new one. Click on **Save** to ignore and save your automation "as is".

If you add a new action, your automation will become a sequential business continuity policy automation.

All actions will be executed sequentially. However, it is possible to check the trigger validity when you add a New Action and the Wizard will prompt you as to whether you want to do this or not.

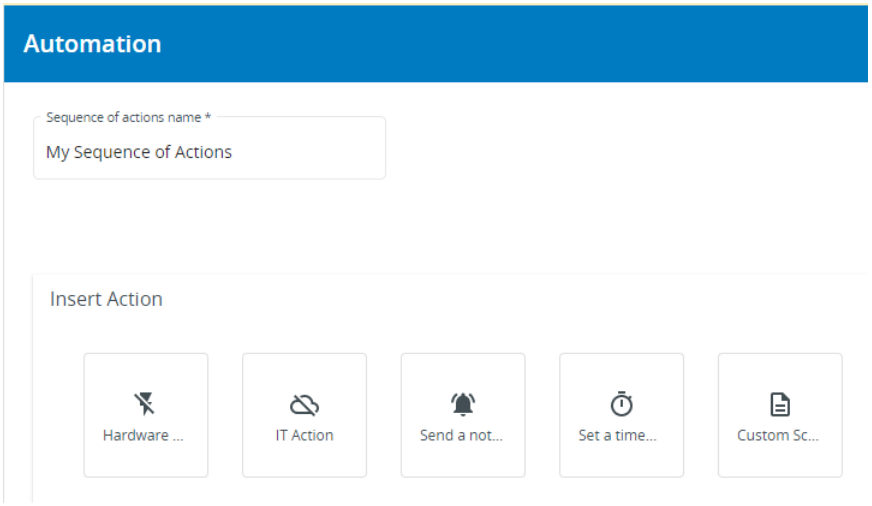
With this option you can decide to stop or continue your automation according to the status of the initial trigger. In this manner, you can ensure that the trigger status is verified between each action.

The condition will be added to your automation sequence summary as a "**Check trigger Validity**" step.

You may then add a new action in order to continue the configuration of your automation sequence, or click on save to complete your automation.

Sequence of actions creation

First of all, you must provide a name to the "Sequence of actions". This field is mandatory.



As a "Sequence of actions", it cannot be triggered by an event, and is only used in a "If/else condition" action.

The general principle for setting up an action in a Sequence of actions, is the same than the one for creating an action in an Automation.

The available actions that can be added to a Sequence of actions are :

- Hardware Action
- IT action
- Send a notification
- Set a timed delay
- Custom script

All theses actions are configurable the same way than actions in Automation, described in the above section. The wizzard will guide you through the different steps.

Common behaviors for all actions definition in a Sequence of actions :
When you've selected the action type you want to configure and the targeted asset(s) to apply the action to, the wizard will guide you through the specifics of this action configuration. You just have to follow the process for full completion.

All actions configured in a Sequence of action are ending by the same last step about the automation behavior on action error. This step is performed in case the current action falls in error at the end of the execution of it.

You can choose to continue the next actions of the automation or to end the current automation.

The difference between an action in an Automation and an action in a Sequence of actions is that, in case of error, it is not possible to run another Automation before ending. Actually as a Sequence of action does not handle the context of the executed Automation, this feature cannot be available.

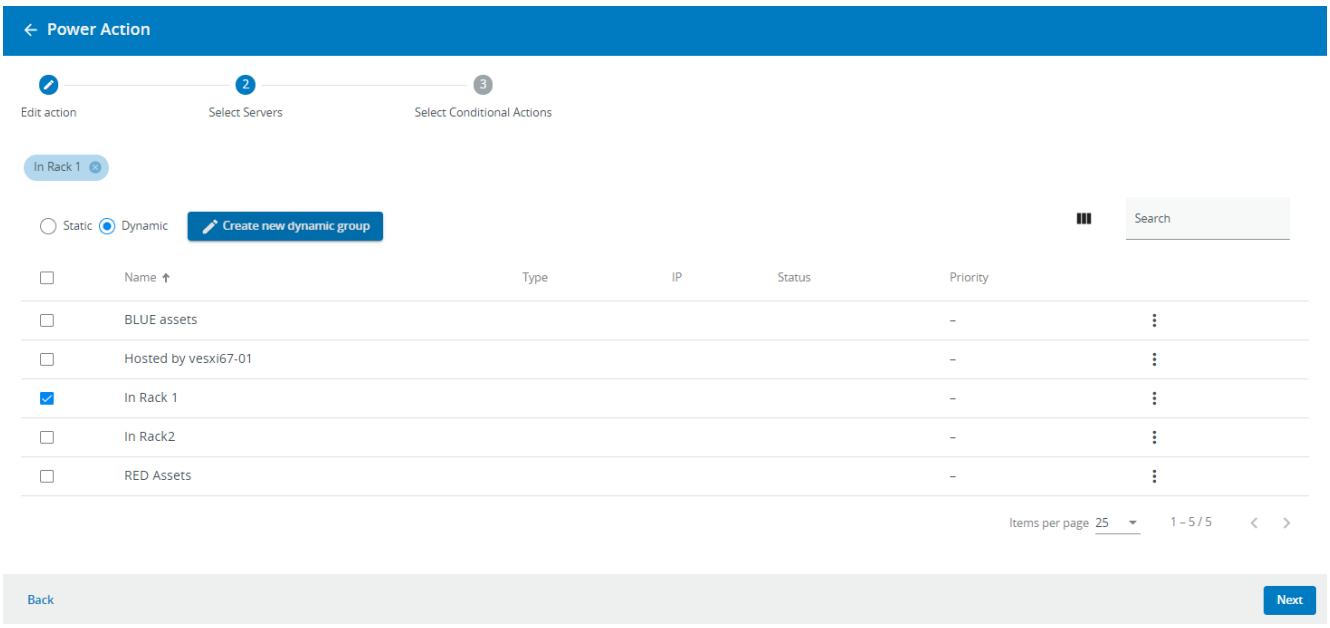
Dynamic Groups

On some Power and IT actions, you have the possibility to select a dynamic group as the target of the Action.

A Toggle choice allows you to select between **Static** and **Dynamic** asset selection.

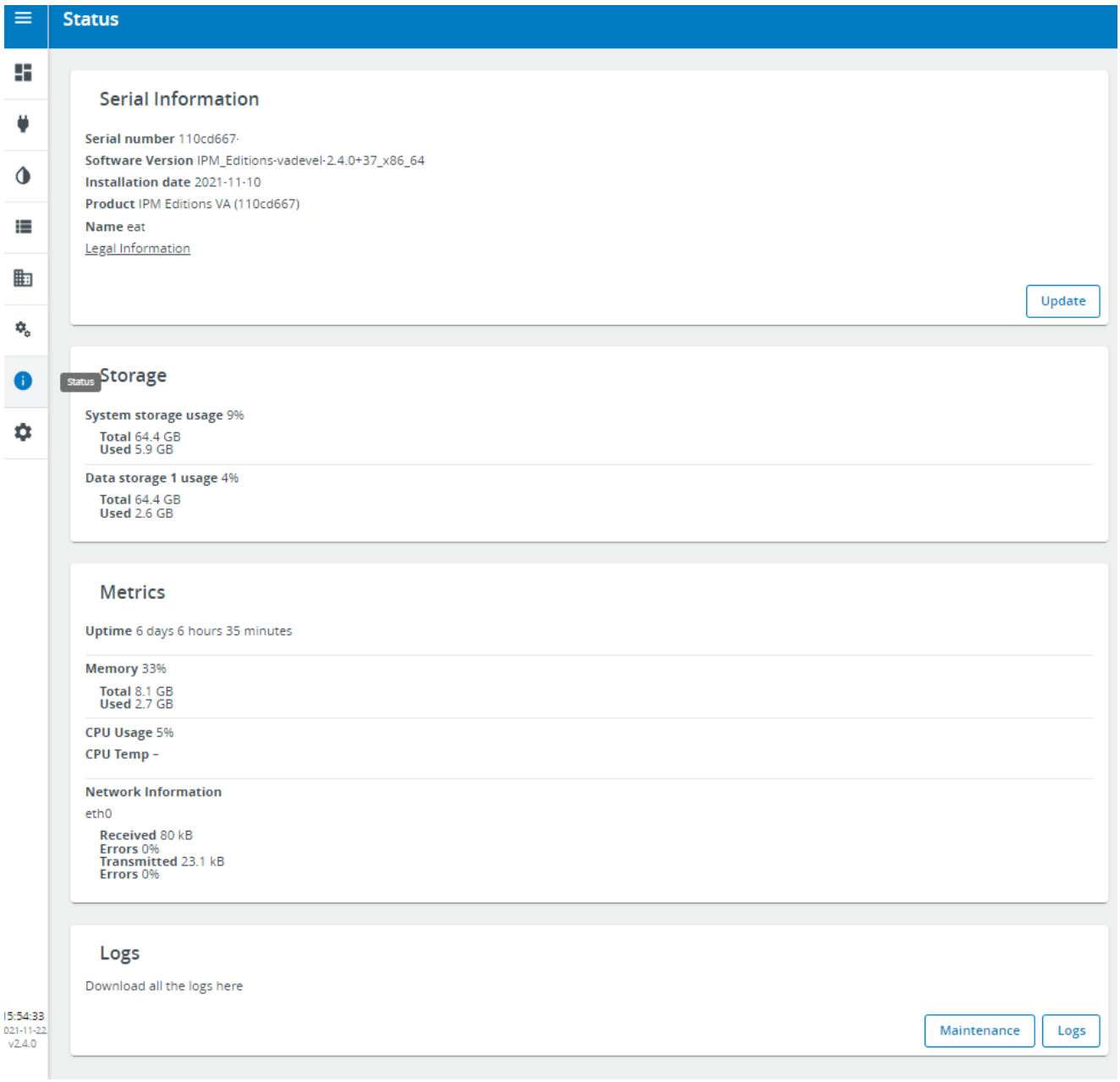
If the dynamic group has been already created it appears automatically in the list (refer to Asset Management page of the User Manual to create Dynamic Groups).

You can also create a new Dynamic Group on the fly with the **Create new dynamic group** button.



2.12 Status dashboard

The status dashboard page may be accessed by clicking on the **Status** menu item in the left menu.



It provides you with application information and real-time metrics related to application health (E.g. storage usage, uptime, memory usage, cpu usage, and network usage).

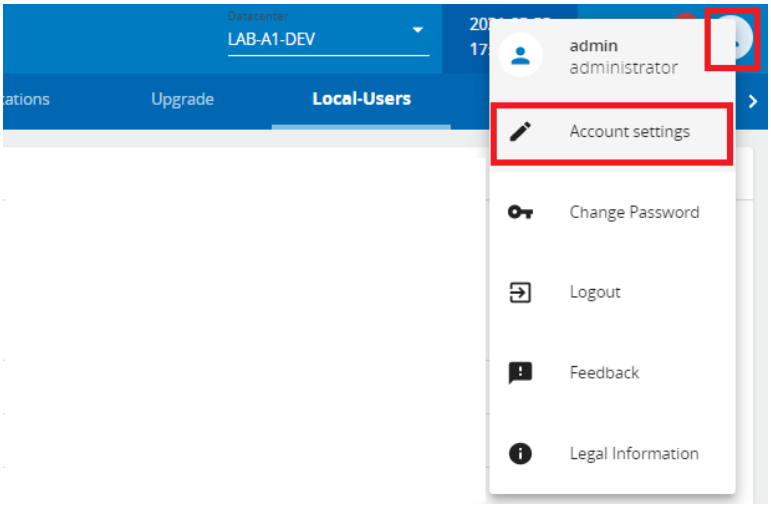
It also allows to download and archive following logs for troubleshooting purpose:

- **Maintenance**
  and
- System **Logs**

2.13 Setting Views

2.13.1 Account settings

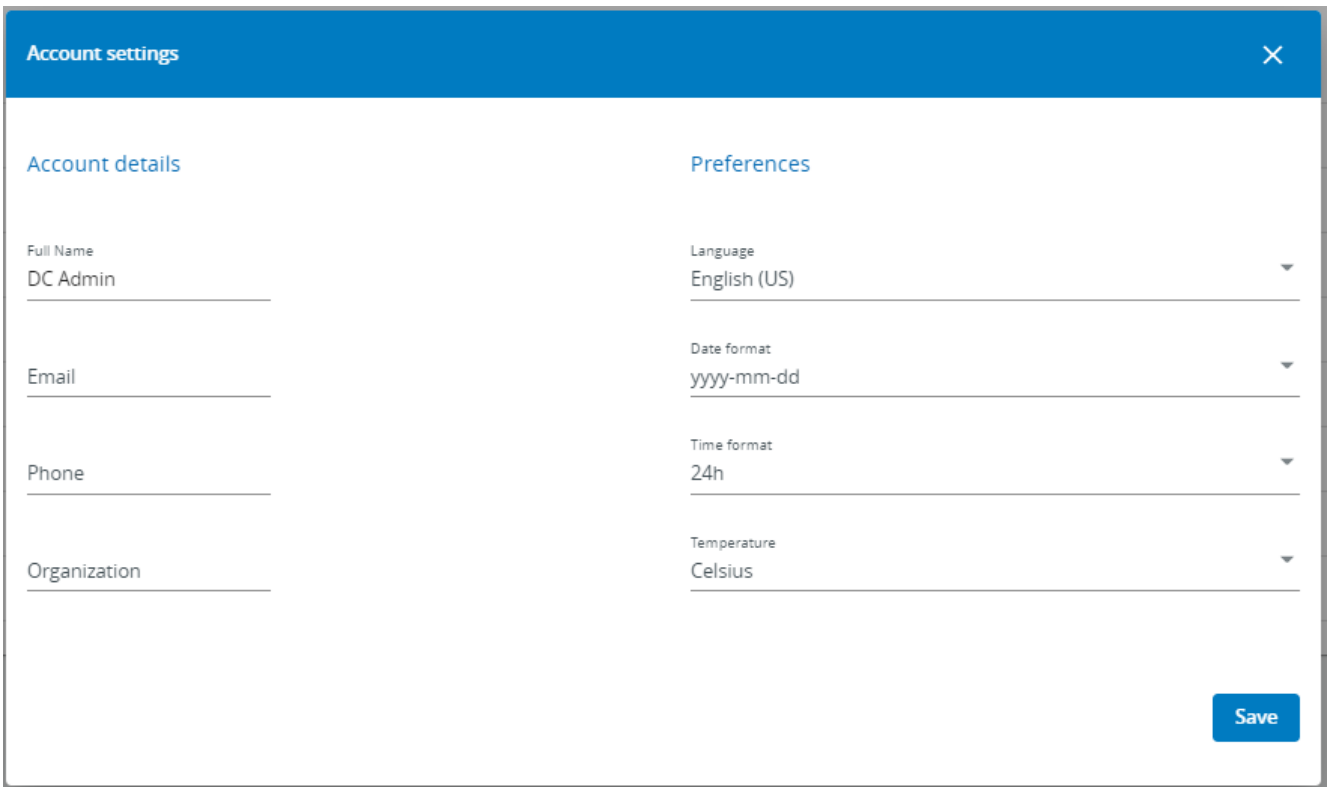
The **Account settings** feature is accessible from the **right hand** icon in the **Top bar**.



Note: Your password, can also be changed from the **right hand** icon in the **Top bar**.

In **Account settings** you can change:

- Your Account details such as:
  - Full Name,
  - Email,
  - Phone,
  - Organization
- Your user preferences such as
  - Preferred user interface language
  - Date Format,
  - Time format
  - Temperature scale in Celsius or Fahrenheit,



2.13.2 Alarms settings view

The **Alarm settings** tab is accessible from the **Settings** menu item in the left navigation menu.

The alarm settings page is organized into 6 subsections including :

- **Data Center**
- **UPS**
- **Row**
- **Rack**
- **PDU**
- **ATS**

Specific alarm thresholds such as temperature and humidity levels in the Data Center are prepopulated with industry standards defaults to facilitate configuration.

Temperature & Humidity default settings		
Temperature Critically High	30°C	85°F
Temperature Warning High	27°C	80°F
Temperature Warning Low	17°C	62°F
Temperature Critically Low	14°C	57°F
Humidity Critically High	70%	
Humidity Warning High	60%	

Temperature & Humidity default settings		
Humidity Warning Low	40%	
Humidity Critically Low	30%	

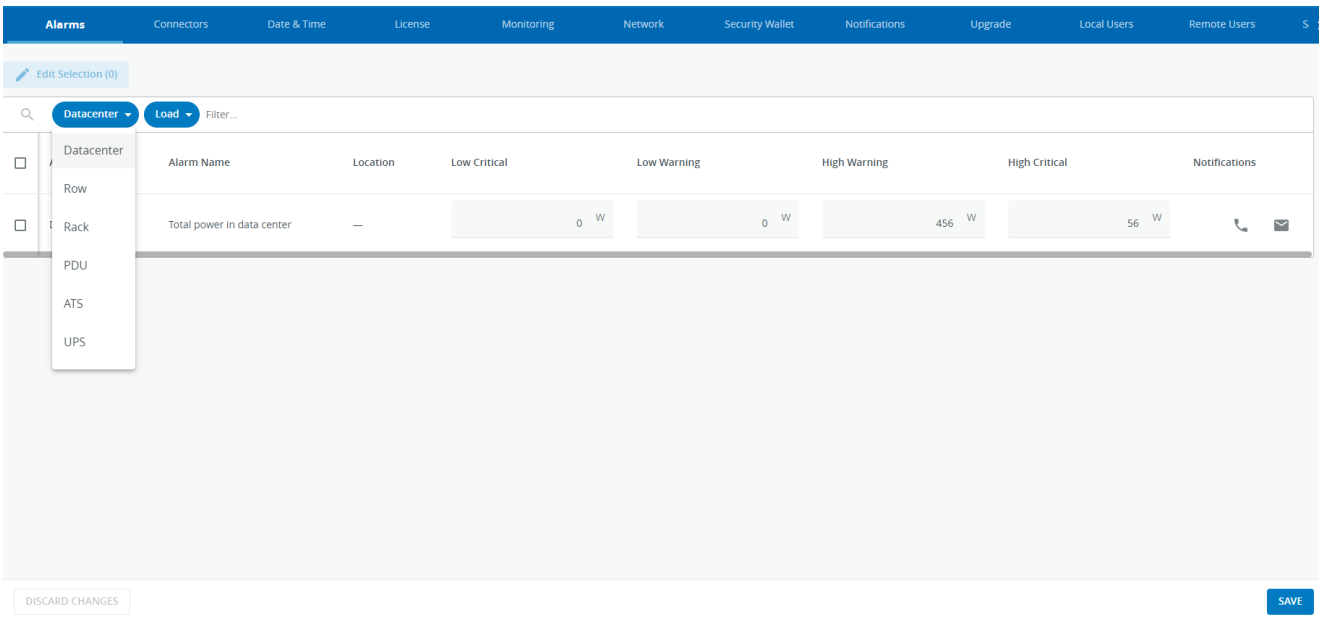
Although the temperature and humidity settings have default values, you may adjust them to a more suitable setting reflective of the standards you have defined for your data center environment

All alarms can be set to send additional notifications to specified users by email, email to SMS gateway or both.

Alarm Settings filtering

- A double filtering mechanism is available on the right end corner of the page
- First selection is the **Asset** or **Location** type:
    - Datacenter
    - Row
    - Rack
    - PDU
    - ATS
    - UPS
- Second selection is the **Alarm category**:
    - Load
    - Battery
    - Phase Imbalance
    - Input Current
    - Output Current
    - Input Voltage
    - Output Voltage
    - All
    - Temperature
    - Humidity
    - Licensing & Warranty

In order to configure alarms for Data Center / Row / Rack please first define these entities in **Location** view.

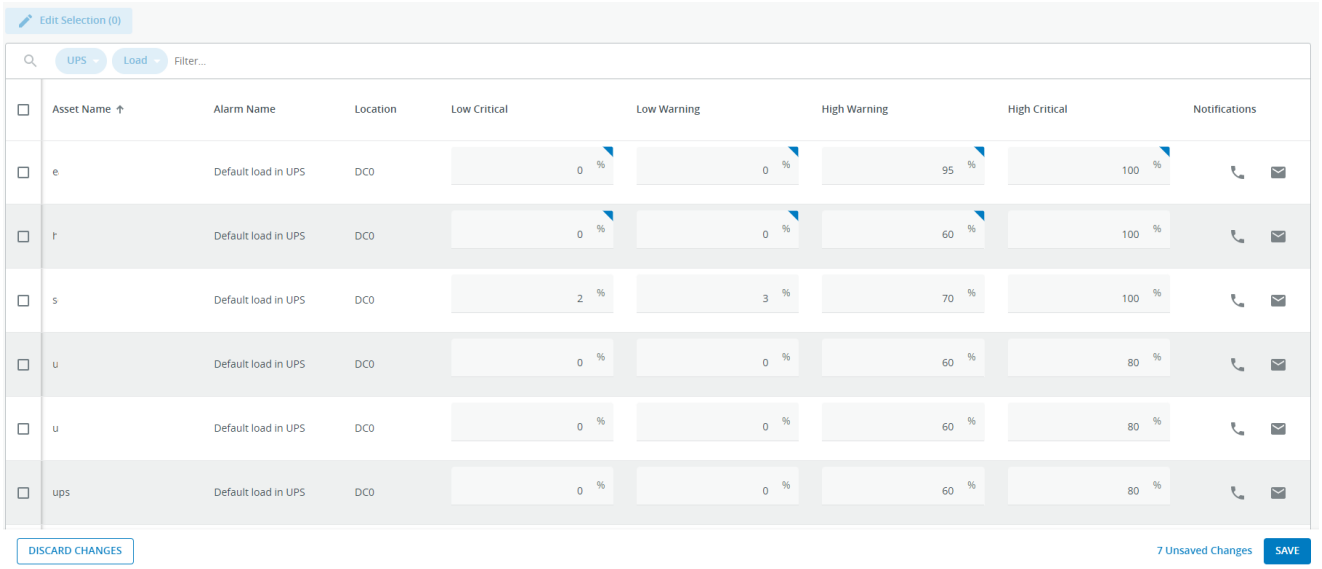


Alarm Settings

Individual value settings through table

To set individual values through the table you can proceed like this:

- Select **Asset type** then **Alarm category** as explained on previous paragraph
- Click on each cell you want to modify and enter a new value
- A blue triangle appears on each modified cell
- Then you can **Save** or **Discard Changes**

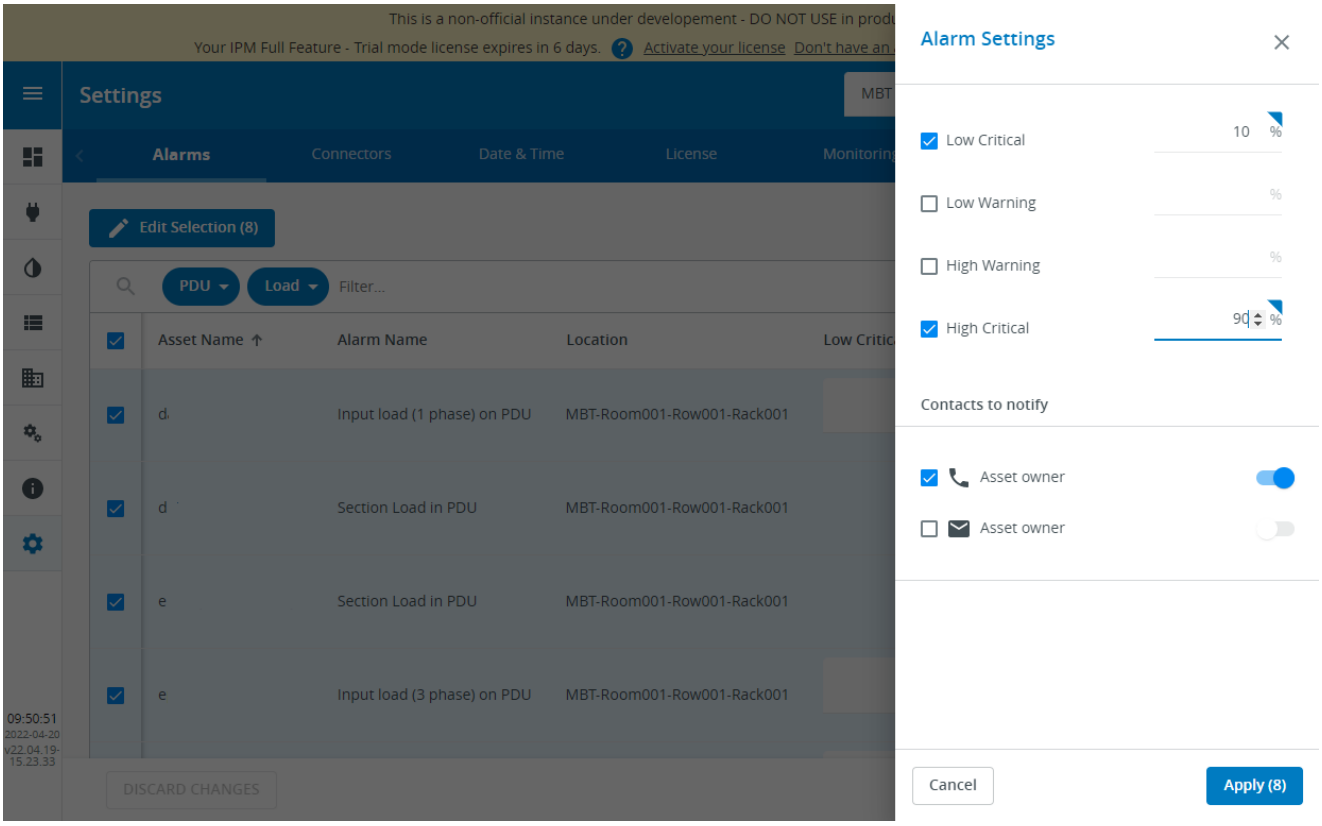


> **Note**
>
> Some values are in read only mode as these values are defined at the device level

Mass settings through Right Hand Panel

To set homogeneous values on several assets you can proceed like this:

- Select **Asset type** then **Alarm category** as explained on previous paragraph
- Select several Assets through checkboxes on each line of the table (you can also **select all assets** through the check box in the table header)
- Click on **Edit Selection** button and a right hand panel appears
- Enter the alarms values you want to apply to all selected devices
- Click **Apply** or **Cancel**
- A blue triangle appears on each modified cell
- Then you can **Save** or **Discard Changes**



ATS Alarm Settings

On the ATS/STS alarm setting page, you may set the specific alarms related to ATS/STS. No thresholds can be defined here. Only the **source change events** or **malfunction notifications** are accessible from an STS/ATS.

2.13.3 Connectors

The **Connectors settings** tab is accessible from the **Settings** menu item in the left navigation menu.

Overview

The IPM application can monitor and orchestrate business continuity policy when virtualization connectors are used.

This feature enables the IPM application to manage and interact with your third party products or your virtualized IT environment.

IPM can be configured to use the following virtualization connectors:

- VMware vCenter
- VMware ESX / ESXi
- Microsoft Windows Server
- Microsoft SCVMM (Secured or unsecured connection)
- Nutanix Prism Central / Cluster
- Dell EMC - VxRail
- Kubernetes

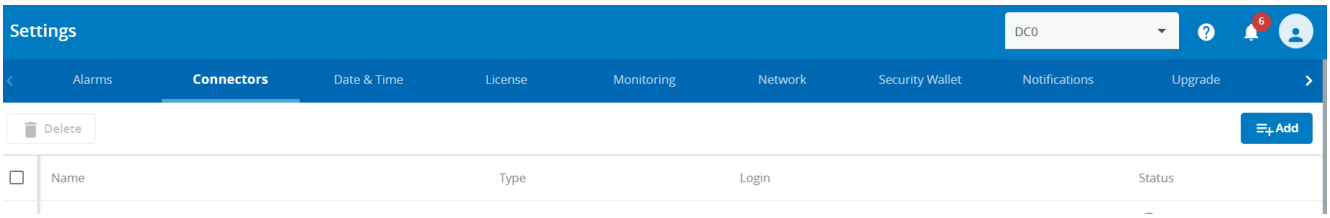
Once a connector is properly configured, all assets managed by the connector are retrieved by IPM2 in an asset management page (Assets menu / virtual Assets tab) : Virtual machines, Hypervisor, Manager, VMs, Cluster.

Connectors also enable the IPM application to interact with the assets monitored by the connectors and for you to define business continuity policies using the IPM automation features.

> **Note**
>
> The virtualization connectors and IT actions supported per connector are detailed in the IPM Documentation section Automation / IT actions supported
> Please note that some restrictions may apply with respect to your software license and type of virtualization connector configured as some actions are not available on all connectors.

Add new connector

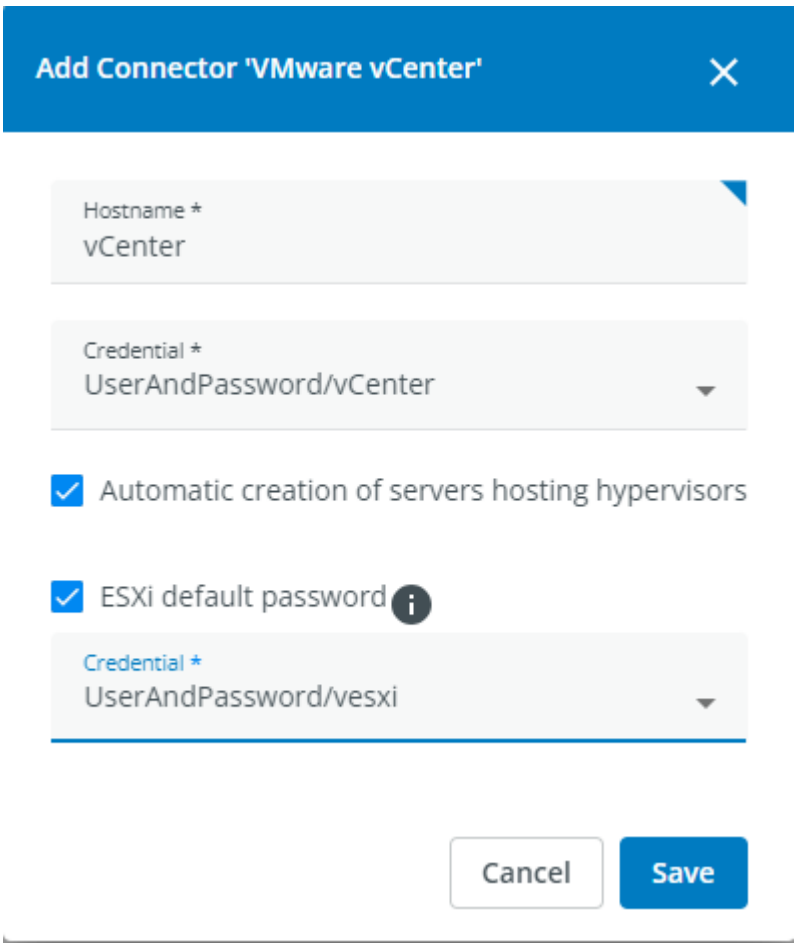
Click on +**ADD** and select the type of connector you want to configure :



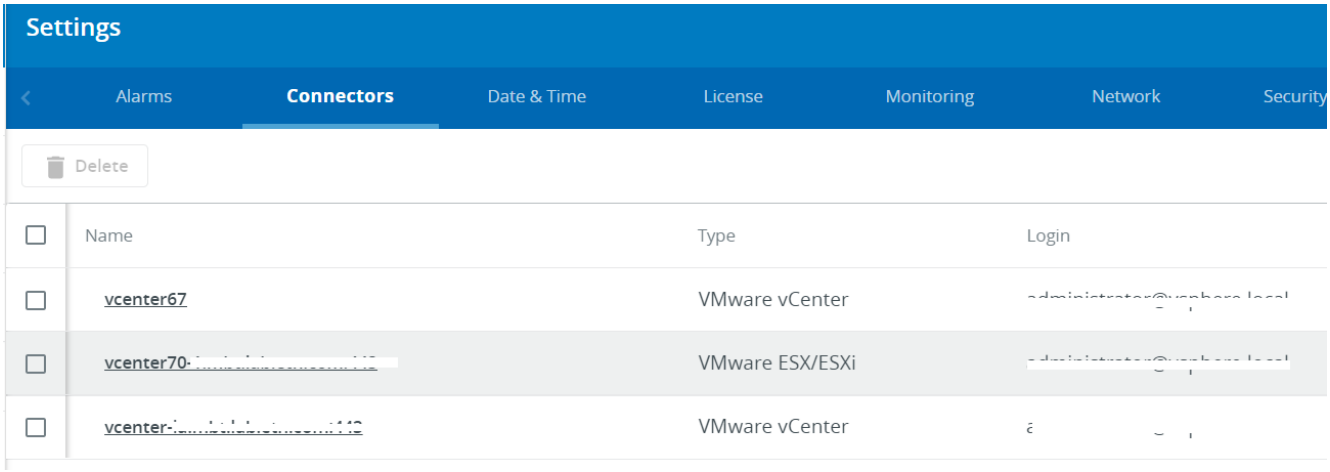
Then enter valid credentials to finalize the connector configuration,

VMware options

- check the "Automatic creation of servers hosting hypervisors" if you want that IPM automatically creates the physical servers in the IT Assets management
- check the "ESXi default credential" if you want that IPM uses a common ESXi User and Password for all supervised ESXi
    - The default credential corresponds to a super user account
    - The IPM Security Wallet stores ESXi credentials, allowing you to either choose an existing credential or add a new one with **Add new credential** button



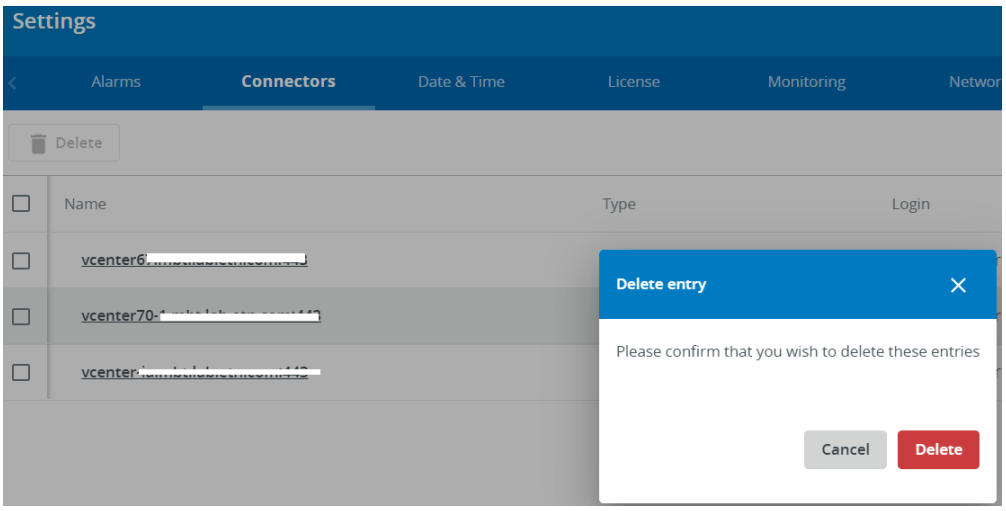
Once a connection is established, the connector is added to the list:



Delete connector

To delete a connector, select it from the the list and then click on **DELETE** .

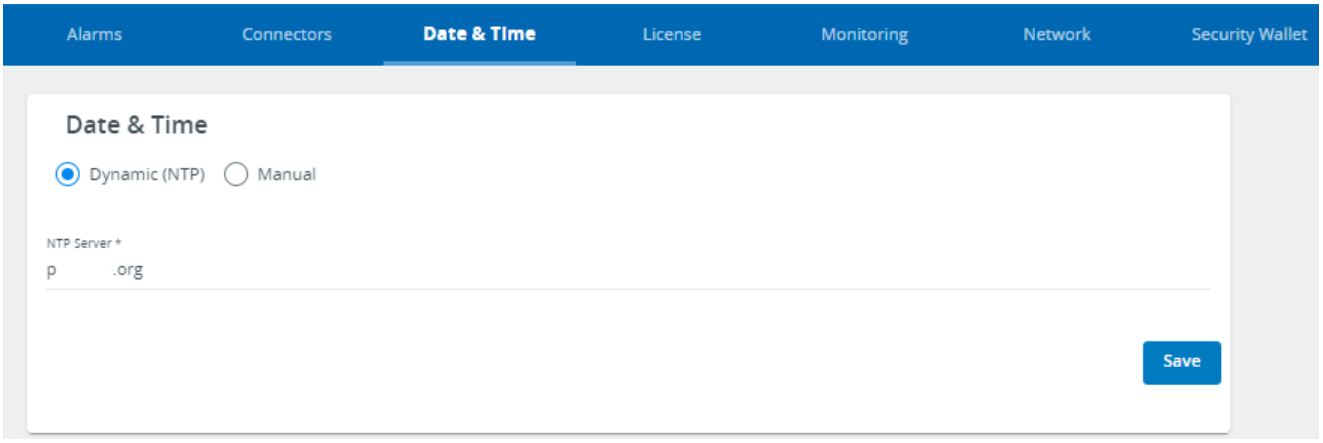
The connector and all assets discovered via the connector will be automatically removed.



2.13.4 Date & time

The **Date & time settings** tab is accessible from the **Settings** menu item in the left navigation menu.

Date and time may be set manually or by configuring an NTP server, if available.



Attention

Some compatibility issues have been observed with some NTP servers based on MS-Windows OS.
If any issues are encountered, it's advised to use Manual time settings or to configure another NTP server.

2.13.5 License

The **License settings** tab is accessible from the **Settings** menu item in the left navigation menu.

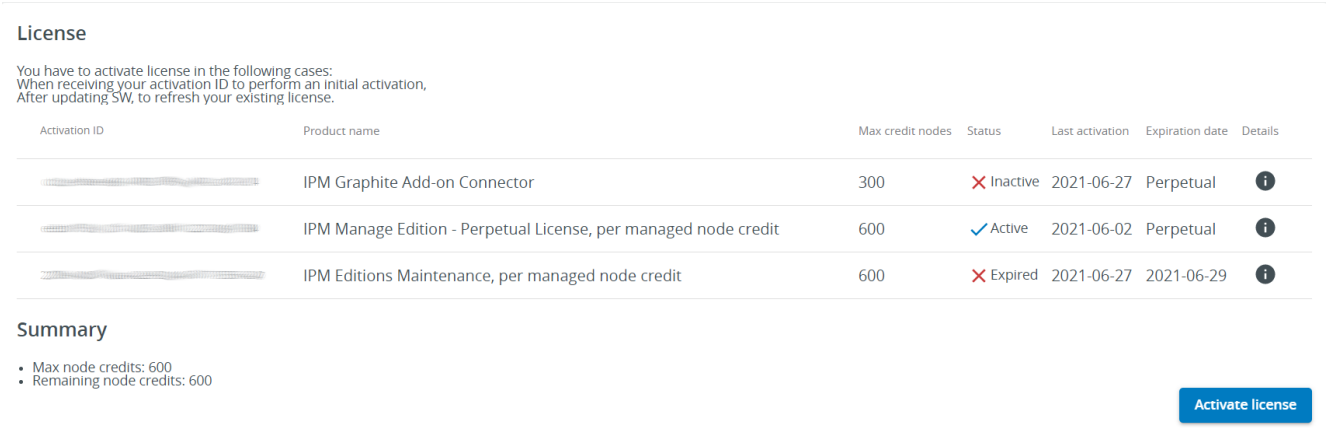
The License settings displays the status of each license that was activated, and details of these for your IPM application.

All information regarding the features that your instance of IPM application is entitled to use, through each License, as well as relevant information of each license, are displayed here.

IPM Editions comes with a one week initial trial License. Longer duration trial licenses are also available upon request.

Other licenses may be purchased and require activation.

To activate a license, click on the **Activate license** button which will take you to the activation wizard modal. Information detailing license activation may be found in the **Licensing** subsection of the General Information section.



Licenses status

In the above example:

- the main license "IPM Manage Edition - Perpetual License, per managed node credit" is valid and **Active**,
- the maintenance license "IPM Editions Maintenance, per managed node credit" has **Expired**, and should be renewed by contacting your Reseller,
- the license "IPM Graphite Add-on Connector" is **Inactive**, because of its Max credit nodes that is lower than the main license Max credit nodes.
  In such cases, contact your License Reseller to remediate this issue.

Licenses expiration

In case of license expiration for Virtualization or Automation features:

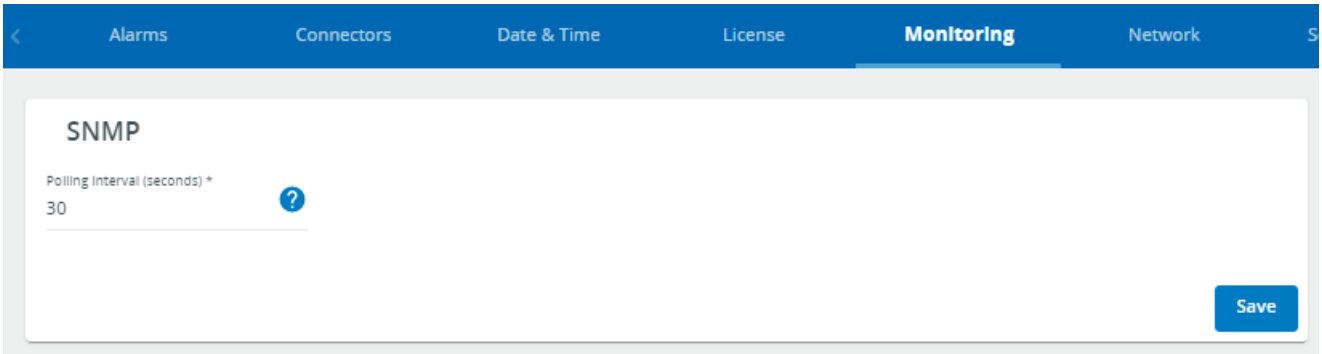
- user is still able to delete an Automation or a Virtualization connector, to clean up the configuration.

2.13.6 Monitoring

The **Monitoring settings** tab is accessible from the **Settings** menu item in the left navigation menu.
This tab includes SNMP polling interval and Graphite/Grafana connector settings configuration.

SNMP

The SNMP polling interval may be configured in this view. The default polling rate is **30 seconds**.



You may add **SNMP v1** community names and/or **SNMP v3** credentials in each asset to be monitored through SNMP.
See the **Security Wallet section** for more information on SNMP credential configuration.

Graphite connector (optional)

Prerequisite

A graphite database server must be up, running and accessible for IPM to use this feature. IPM will act as a data provider to your existing server (The Graphite and Grafana servers are not embeded in the IPM OVA image).

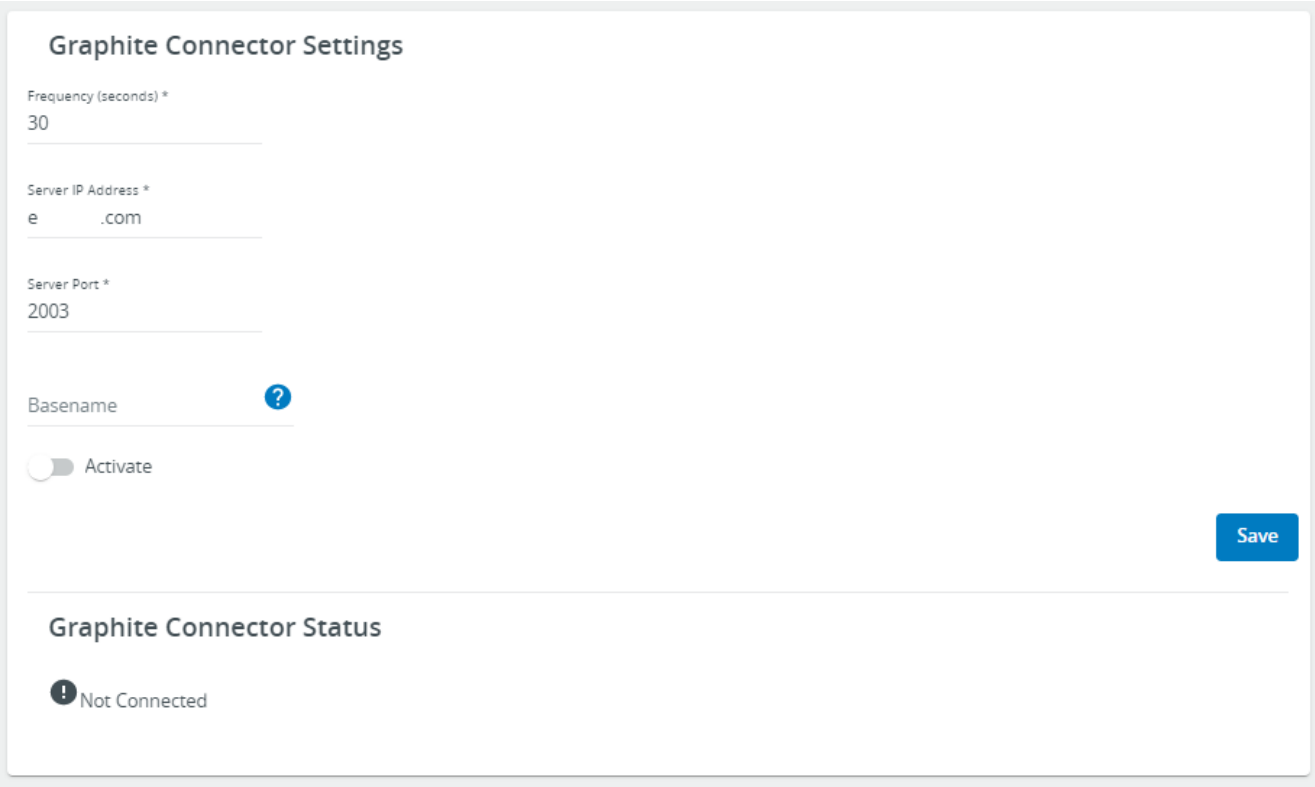
Prerequisite

An IPM Graphite Plug-In license is required to unlock this feature.

Please see the General information > Graphite / Grafana deployment section of the documentation for more detailed information on setting up a Grafana environment.

IPM Editions Graphite connector configuration

The **Graphite Connector Settings** panel may be accessed from the **Monitoring tab** in the **Settings** menu item from the left navigation menu.



Frequency (seconds) defines the Graphite data push frequency. **Default value is 30**.

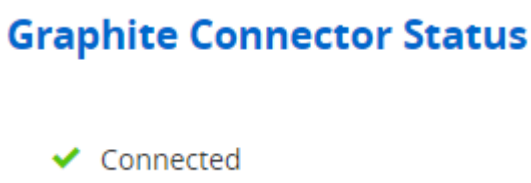
Server IP address should be configured with the IP address of your Graphite server

Server Port is the port number to be used for your Graphite server. **Default value is 2003**.

Basename is the name which will be display on the Graphite server for the IPM Edition connection. If none is set, your IPM Edition will send its hostname as the Basename.

Activate is a toggle to turn on / off the Graphite server connection. Please keep in mind that you must click **Save** to start the connection between the applications.

If everything is configured correctly, the **Graphite Connector Status** should turn to a green **Connected** state



Using Tags and Aliases

When the Graphite connector is set up properly in IPM, all metrics IPM is monitoring through its active assets are sent to the Graphite connector.

In addition to those, all the metrics about IPM virtual appliance system (cpu usage, memory etc..) are provided under "system" asset_id.

Dealing with all those metrics can be difficult. To have an easier usage and readability, it is recommended to use Tags and Aliases.

For more information about Graphite tags refer to the official documentation here : https://graphite.readthedocs.io/en/latest/tags.html

Below is the table of the different tags made available by IPM.

Tag name	Description
name	Default tag concatenating the basename, the asset_id and the metric_name
asset_name	Display name of the asset based on the IPM asset name in replacing white spaces by underscores
asset_id	A unique identifier of the asset or "system" to identify IPM virtual appliance system itself
metric_name	Display name of the metric based on the one provided by IPM replacing white spaces by underscores.
instance_name	"hostname" or custom hostname from IPM configuration for Grafana
metric_type	Type of the value of the metric from "value" , "arithmetic_mean_15m", "arithmetic_mean_30m" ... "min_15m",..."max_24h". The goal is to distinguished normal values from aggregated ones

Using tags and aliases allow to query multiple metrics identified by a common tag pattern at once and to associate to each of those metrics a meaningful name.

Here is an example to query the nonaggregate metric of all "voltage input" from instance "myInstance" and to return them aliased by "<asset_name>.<metric_name>".

```
seriesByTag('instance_name=myInstance', 'metric_name~=voltage.input.*', 'metric_type=value'
 ) | aliasByTags('asset_name', 'metric_name')
```

The seriesByTag() function queries multiple metrics at once based on tags patterns you choose.

In the example:

- *instance_name* identifies the IPM instance you want to collect metrics from.
- *metric_name* allows you to get just (but all) the voltage inputs seen from the previous instance

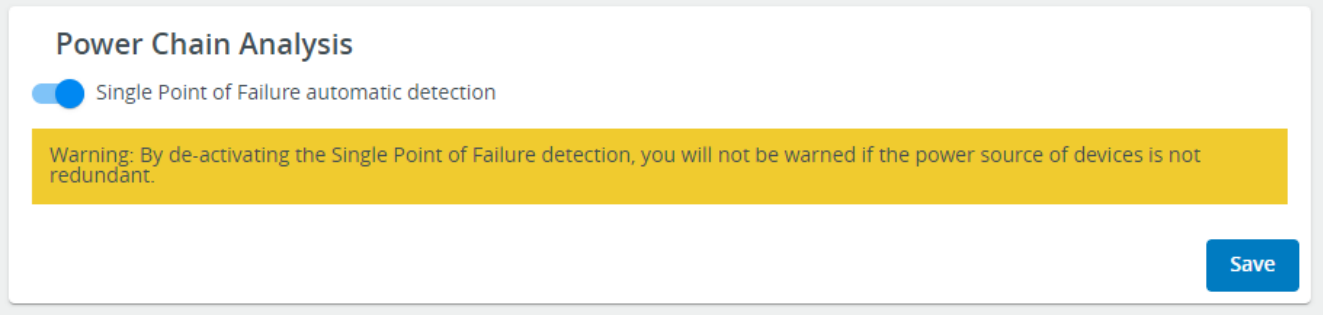
- *metric_type* is there to focus on unitary metrics ignoring any average, minimum, maximum... (any aggregated ones)

The aliasByTags() function postprocesses metrics series and substitutes a name pattern to all elements.

In the example: the concatenation of the asset name and the metric name will allow a straightforward identification of each single metric by putting those as their name.

Power Chain Analysis

On IPM2, you can disable "Single Point of Failure" automatic detection alarming. A single point of failure appear when all the inputs of a device are connected directly or indirectly to the same power source . If a power outage happened your device may not be protected correctly. IPM2 is triggering an alarm to inform that it detect a single point of failure in the power chain.



2.13.7 Network settings view

The **Network settings** tab is accessible from the **Settings** menu item in the left navigation menu.

Network details for each of the available LAN ports including:

- DHCP or Static addressing
- IP address
- Subnet mask
- Default gateway

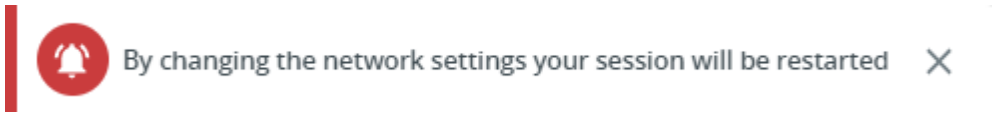
DNS server details including :

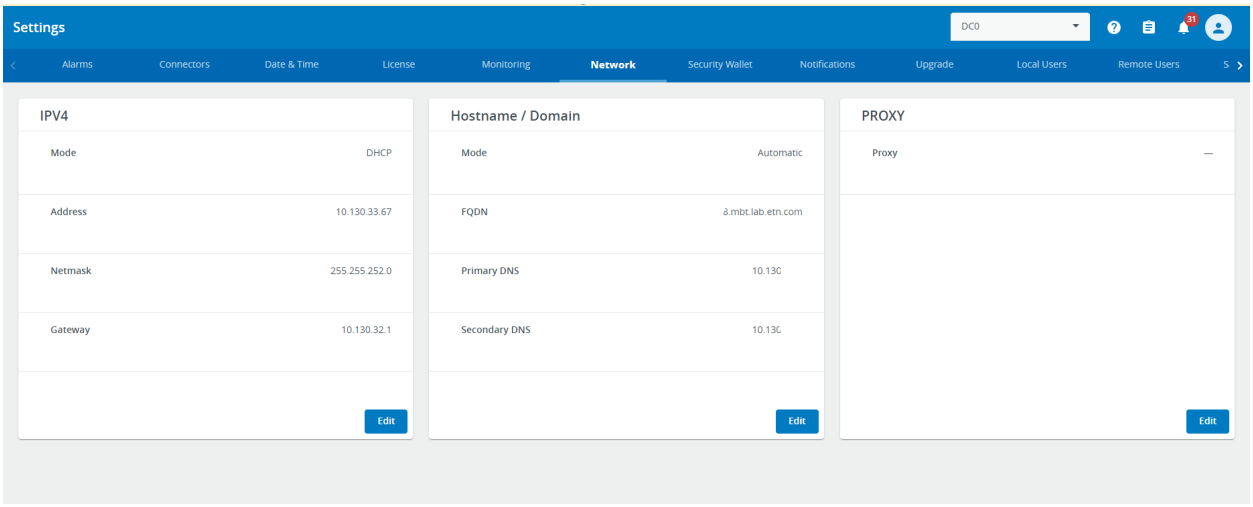
- preference of configured DNS name servers or DHCP supplied name servers

HTTP(s) proxy details including :

- a valid url for your proxy server, e.g. http://proxy.company.com:8080

Once correct details are entered you must click on **Save AND Logout** to apply the changes. Following warning message is displayed:





2.13.8 Security wallet

The **Security wallet settings** tab is accessible from the **Settings** menu item in the left navigation menu.

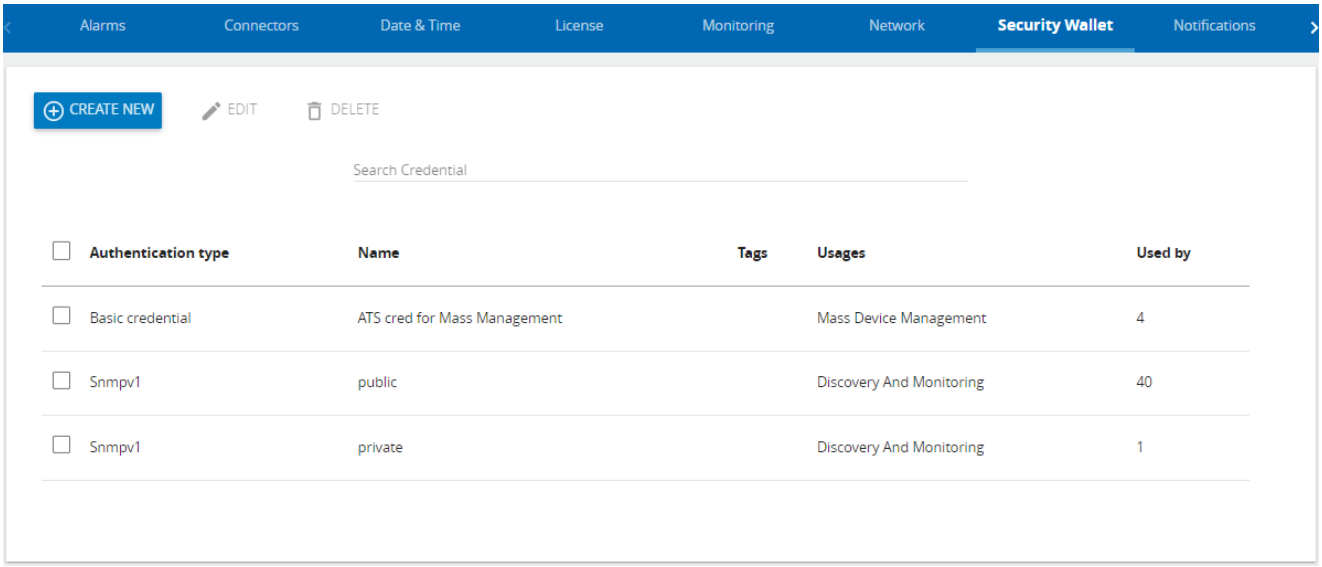
Your IPM Edition potentially connects to many remote systems including communication cards and virtualization platforms for monitoring and management purposes.

As a result, IPM must authenticate through various protocols with appropriate credentials for different purposes. This sensitive data is managed and encrypted in the **Security wallet**.

Security wallet provides a secure and centralized repository to manage all credentials IPM Edition may use to authenticate to 3rd party systems.

Credentials currently stored in the security wallet include the following purposes :

- **Discovery and monitoring**
- **Mass-management** (including mass-configuration & mass-upgrade) of communication cards
- **User Script**
- **Virtualization Connector**



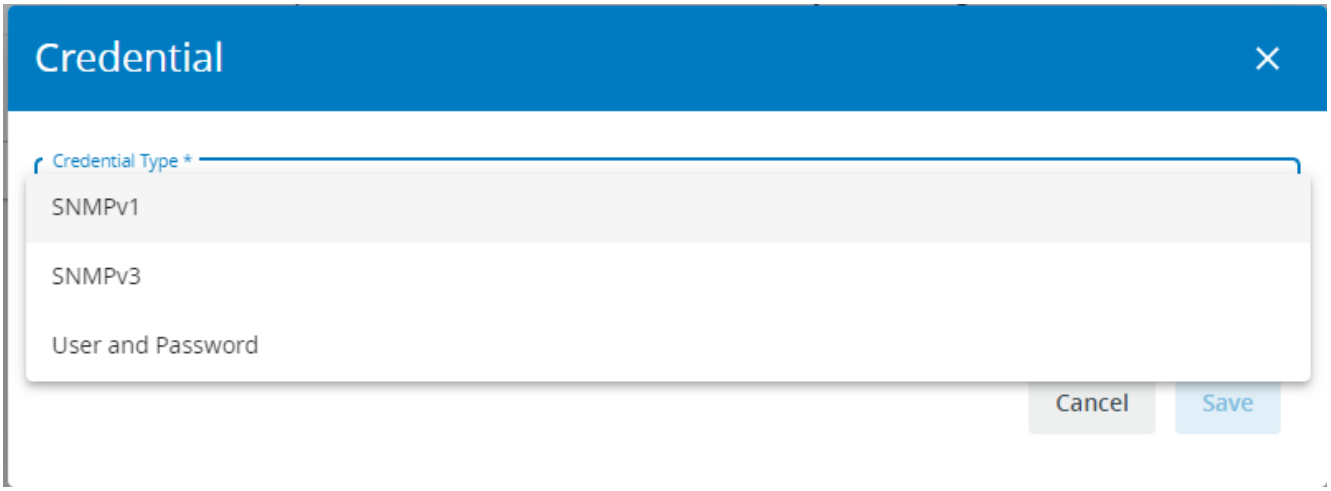
The security wallet is represented as a list of credentials which may be sorted by clicking on any column.

A search engine is also available to quickly select a specific credential by typing all or a part of its name.

Once a security wallet item is selected, it may be either modified or deleted using the corresponding action button at the top of the panel.

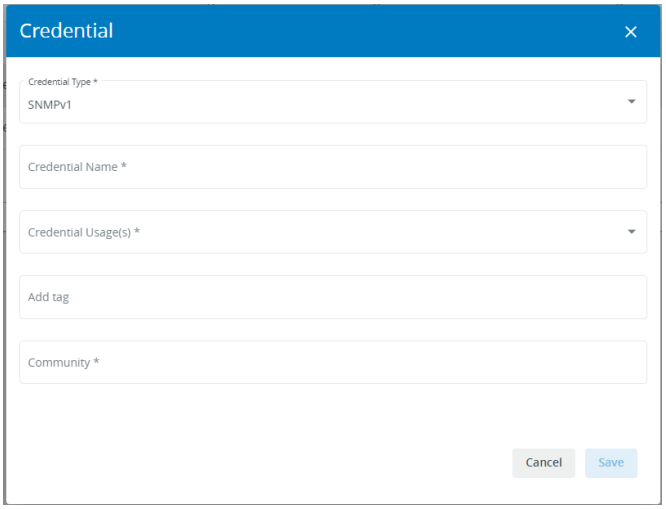
Create a new credential :

1. Click on the **Create new** button.
2. Select the Credential type in the drop down list:



Create a new SNMP v1 credential

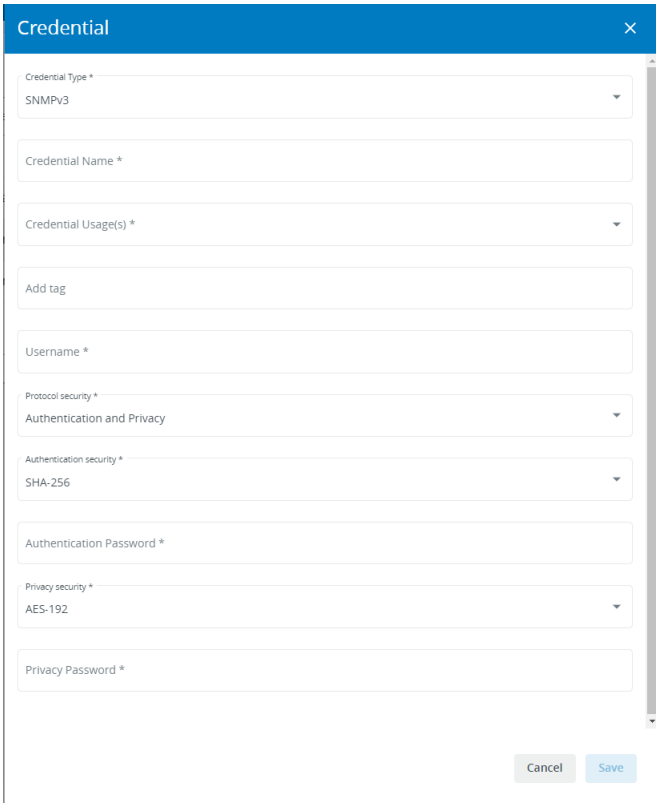
1. Enter a Credential name
2. Set the **Usage** field to **Discovery and monitoring**
3. You may set user specified tags. E.g. **Management vlan 2**
4. Enter the community name E.g. **public**
5. Click the **Save** button



Create a new SNMP v3 credential

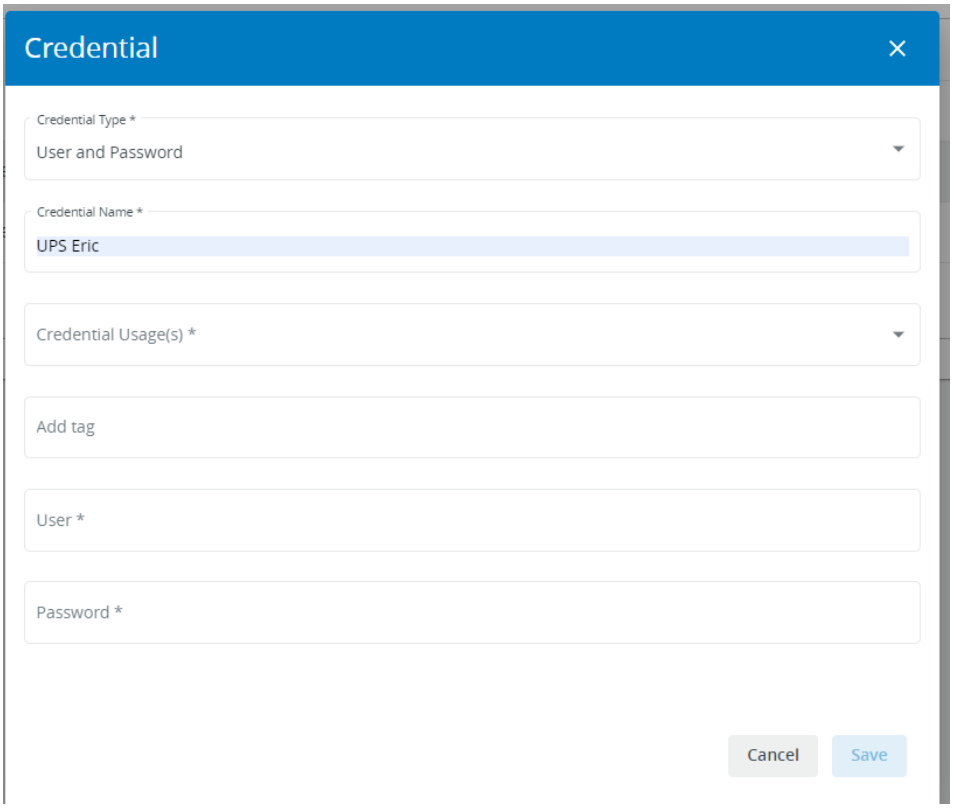
1. Enter a Credential name
2. Set the **Usage** field to **Discovery and monitoring**
3. You may set user specified tags. E.g. **Management vlan 2**
4. Enter the **Username**
5. Select the Authorization and Privacy Security level
    a. **NO_AUTH_NO_PRIV** => No Authentication & no privacy (encryption)

   b. **AUTH_NO_PRIV** => Authentication but no privacy
   c. **AUTH_PRIV** => Authentication & privacy
6. Depending on the security level you have selected, you will be prompted to add more information
7. Select the **Authentication security** algorithm (if applicable)
   a. MD5
   b. SHA-1
   c. SHA-256
   d. SHA-384
   e. SHA-512
8. Select the **Privacy security** algorithm (if applicable)
   a. DES
   b. AES
   c. AES-192
   d. AES-256
9. Click the **Save** button



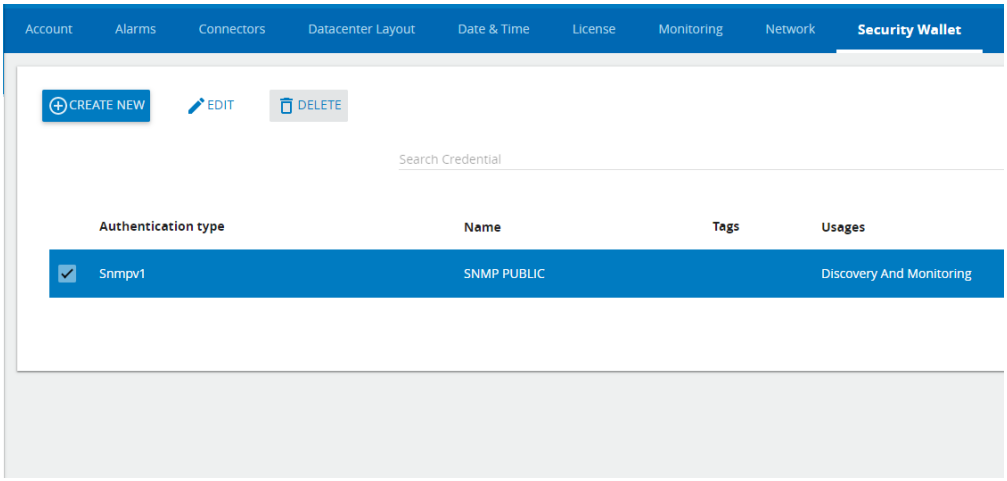
Create a new User and Password credential

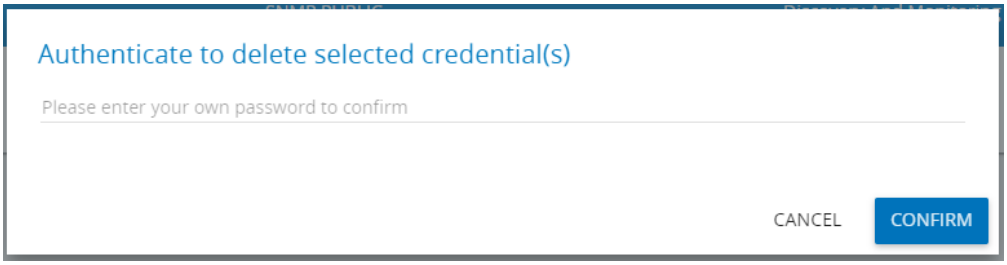
1. Enter a Credential name
2. Select the **Usage** field to **the behaviour you want to manage**
3. You may set user specified tags. E.g. **ePDUs**
4. Enter the **Username**
5. Enter the **Password**
6. Click the **Save** button



Delete a credential

1. Select one or several credentials from the list
2. The **Delete** button will become active
3. Click on the **Delete** button. You will be presented with a modal dialog which will request your password.
4. Enter your **Password**
5. Click on **Confirm**





Credential usage in user scripts

User scripts can be uploaded through the Automation module to be triggered on demand by IPM Edition (see custom script action in Automation view page).
All credentials stored in the security wallet can be used in those scripts to avoid to type them in clear.

As an example, imagine a script with the following line:

```
connect "192.168.0.2" "login" "password"
```

If the purpose of this line is to pass an IP address followed by a login and a password, both given in clear to the "connect" command, the security wallet allows the following syntax:

```
connect "192.168.0.2" $(etn-secwcmd -u "My credential") $(etn-secwcmd -p "My credential")
```

"etn-secwcmd" stands for "Security Wallet Command" and gives access to the login and password detail of a credential stored in the security wallet of IPM Edition by just mentioning its name,

"-u" option is used to get the username (or login) of the credential.

"-p" option is used to get the password of the credential.

As a result, in case the script source would be leaked, it does not contain any cyber-critical data.

The following is an example of using *etn-secwcmd* inside an automation script:

```
#!/usr/bin/env bash

# etn-secwcmd is an IPM-specific command that allows us to retrieve credentials

user=$(etn-secwcmd -u "name-of-the-entry-inside-security-wallet")

password=$(etn-secwcmd -p " name-of-the-entry-inside-security-wallet")

echo "$user and $password"
```

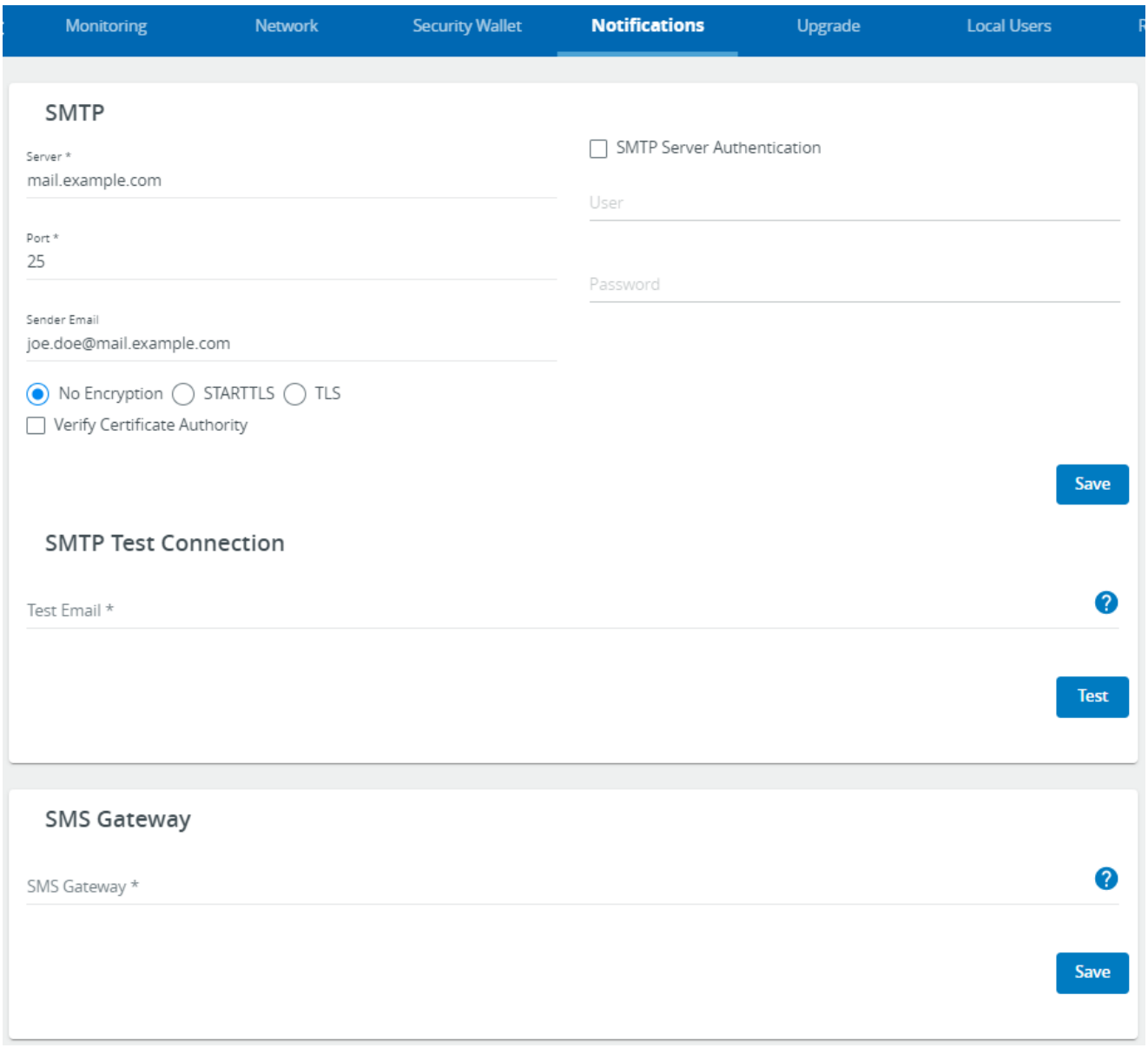
2.13.9 Notifications

Email notifications require an accessible SMTP server to be configured and a sender email address to be entered.

To test the configuration, the Test Email field can be used to enter a recipient for the test.

If you have an SMS gateway, configure it in the SMS Gateway field to also receive SMS notifications.

The Save button on the bottom right corners persists the configuration into the system.



Sending emails through Microsoft 365 or Office 365 requires some server side configuration. The following article might help in this process:
https://docs.microsoft.com/en-us/exchange/mail-flow-best-practices/how-to-set-up-a-multifunction-device-or-application-to-send-email-using-microsoft-365-or-office-365

2.13.10 Upgrade view

Overview

The **Upgrade** tab is accessible from the **Settings** menu item in the left navigation menu.

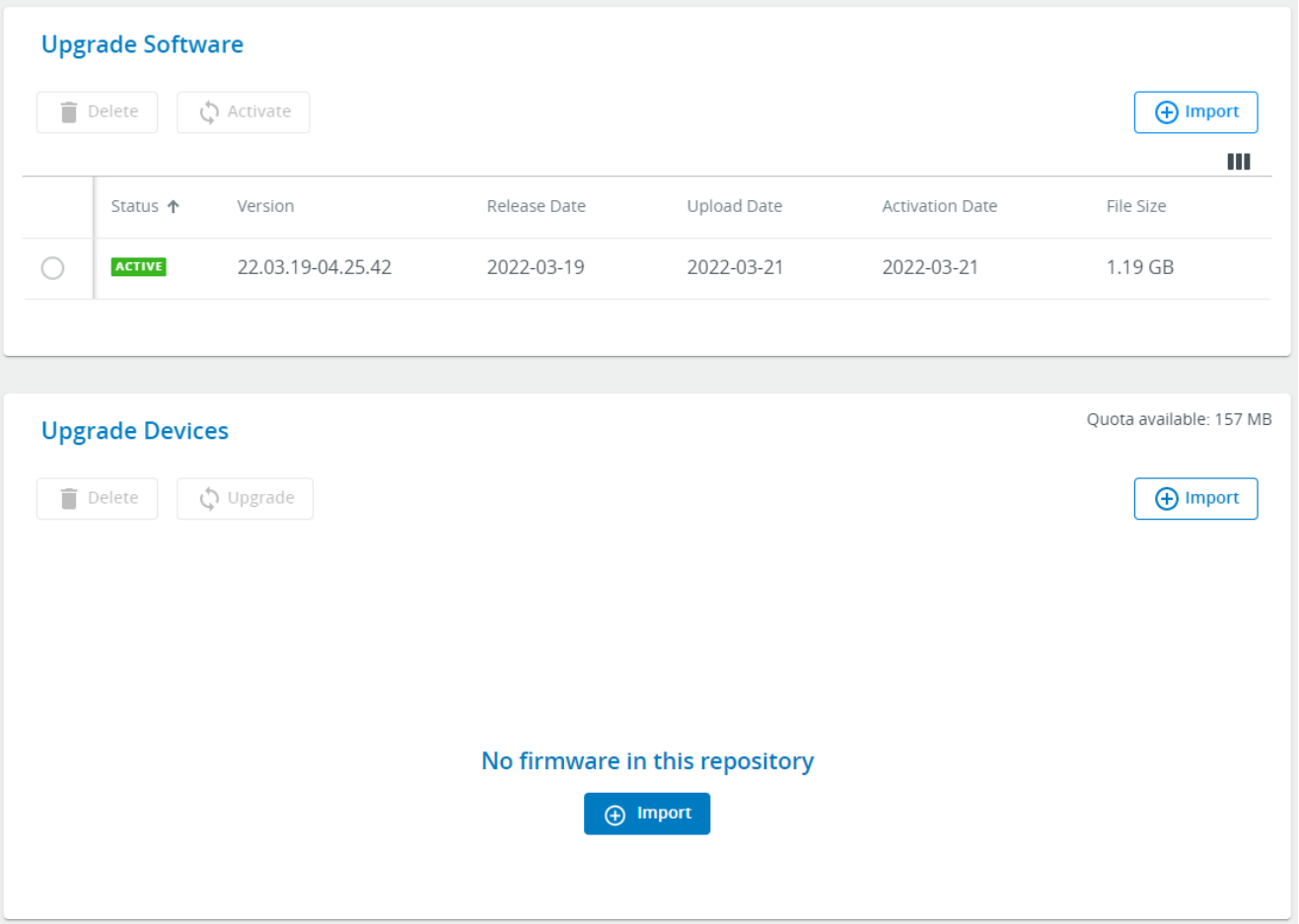
The Upgrade tab enables you to manage the application of new:

- **IPM Edition software versions**
  and
- **Devices Firmware versions (communication card firmware and UPS Firmware)**

The Upgrade Settings page is split into two panels:

- the top panel enables you to update the IPM software itself

- the bottom panel enables you to update the communication card firmware



Upgrade Software

The top panel is dedicated to the IPM software upgrade process.

It provides a view on the IPM software versions you have downloaded in addition to the version that is currently running.
Initially, the view presents the active version only (the one currently running).
Newer versions of IPM can be downloaded from our website and then uploaded to the system by clicking on "Import" and browsing to the downloaded local copy of the package.
An unused version can be removed from the system by selecting it and clicking on "Delete" button.

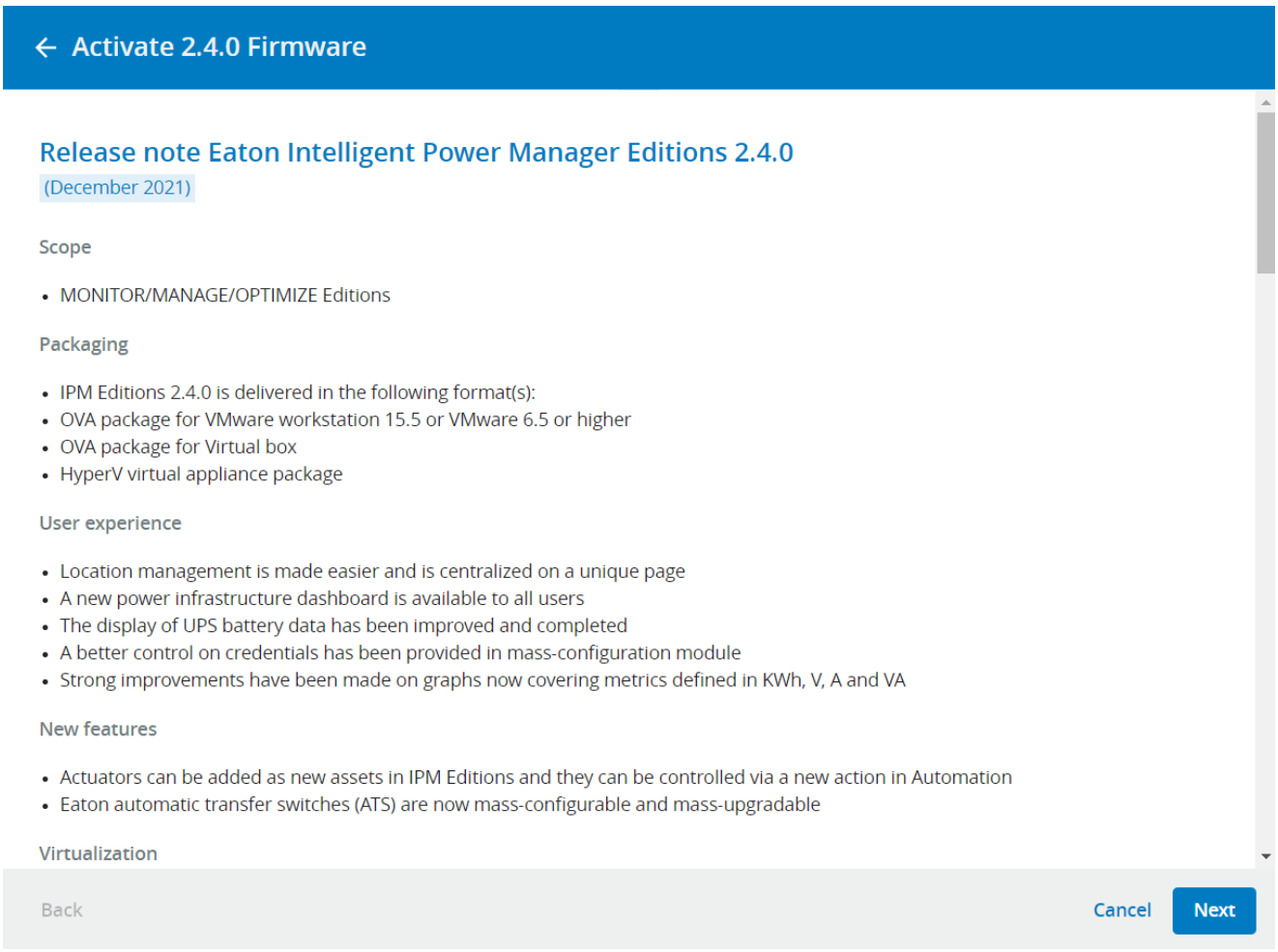
To upgrade your IPM software, please follow the steps below.

Step 1

- **Download** the latest upgrade package from **powerquality.eaton.com**
- **Import** it into the system using the **Import** button
- Once imported, select it and click on the **Activate** button

Step 2

The release note is displayed for your review. Click on next when ready to proceed or click on Cancel to interrupt the process.

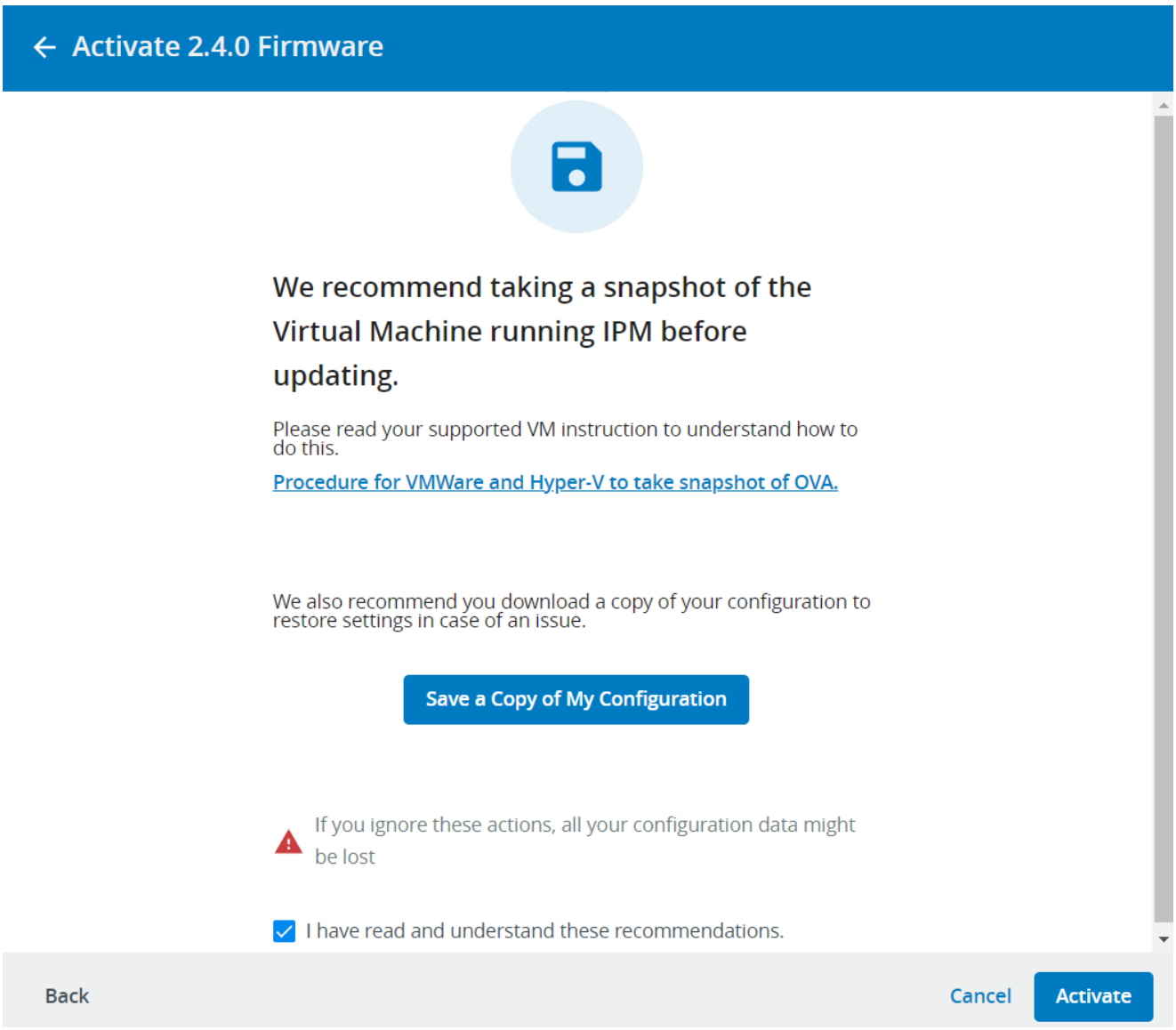


Step 3

Once you have read the release note (Step 2), you are encouraged to secure your IPM configuration.

Following actions are proposed:

- You can snapshot your entire virtual machine. This will allow you to redeploy a fully configured IPM instance from scratch if needed.
- You can also save your IPM configuration. This will allow you to restore this configuration in a fresh IPM instance you would have deployed as a replacement of this one.



We recommend you to take appropriate actions from the above list as the upgrade process, if interrupted unexpectedly, can lead to weird situations where your instance could be broken.
If this unlikely issue happens to you, the above approaches will significantly reduce the cost of the remediation.
To proceed to the upgrade, please check the box to confirm you have understood the benefit of backing-up your IPM instance before moving forward.
You can now press the Activate button to proceed to the upgrade.

Potential IP address change

Note that after reboot, your IPM instance IP address may change, depending on your network infrastructure. Prefer to use the system Name, from the System information on the Status dashboard, to connect to your IPM Edition instance.

Image listing and deletion

- Only Active and imported images are listed.
- Upon activation, the previous software version will be automatically deleted.
- An imported but unused version can be removed from the system by selecting it and clicking on "Delete" button.

Downgrade is not currently supported. Use this feature to switch only to newer versions of IPM.

Upgrade Devices

The bottom panel is dedicated to firmware upgrades for Eaton communication cards that IPM is managing:

- **Eaton Gigabit Network Card** firmware can be downloaded at eaton.com
- **Eaton G3 ePDU Network Management and Control Module** (eNMC) firmware can be downloaded at eaton.com
- **Eaton Network Mangement Card** (NMC) firmware can be downloaded at eaton.com

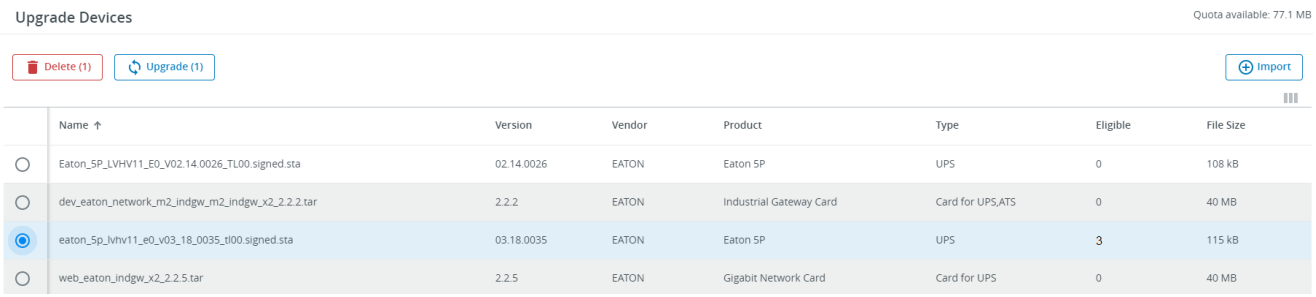
UPS firmware upgrade is a new feature of IPM version 2.6.0 with the same process described hereafter. The prerequisites for UPS Firmware upgrade are following ones:

- **IPM** minimal version 2.6.0
- **Eaton Gigabit Network Card** minimal version 3.0
- **UPS** with remote firmware upgrade capability (refer UPS User Manual for more information)

- It is not possible to downgrade Card or UPS firmware through IPM.

Step 1

- Once a firmware (UPS or Card firmware) has been downloaded, it maybe imported into IPM by clicking on the **Import** button, then selecting the firmware with the file browser,
- Once imported into IPM, it appears in the firmware repository list,
- Select a firmware in the list; the number of **Eligible** Devices is computed and displayed,
- Click on the **Upgrade (x)** button to proceed to next step.

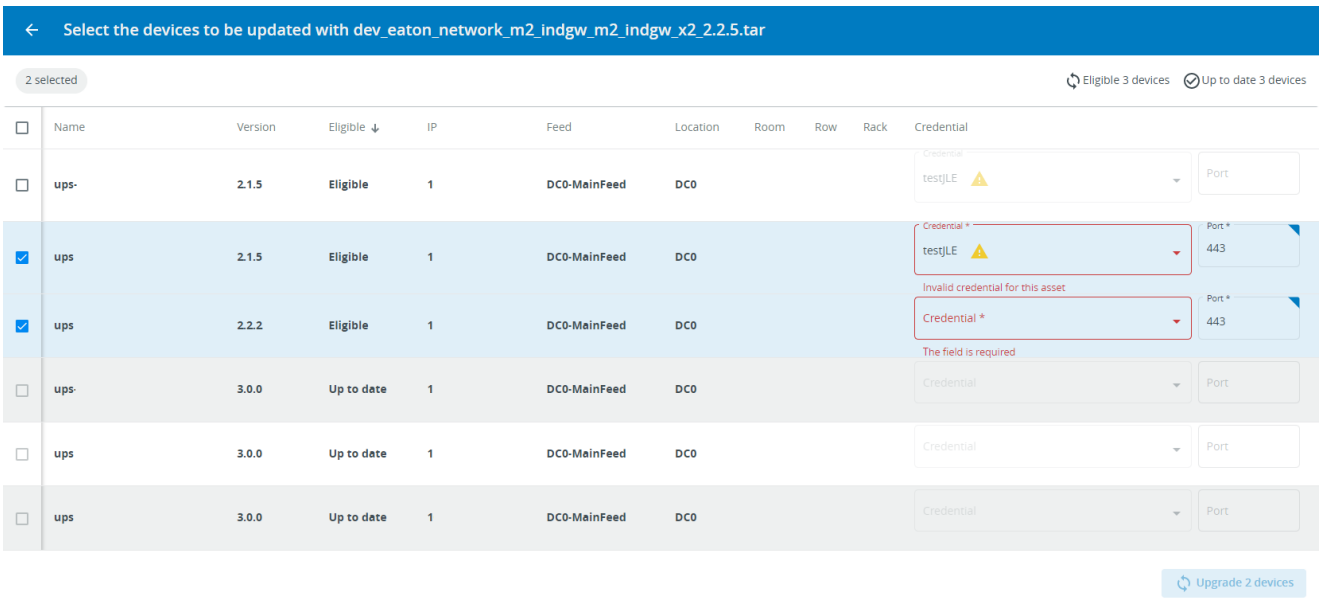


Step 2

- At this point, you can select the device(s) you want to upgrade
- Click on the **Upgrade (x devices)** button to start the firmware upgrade process

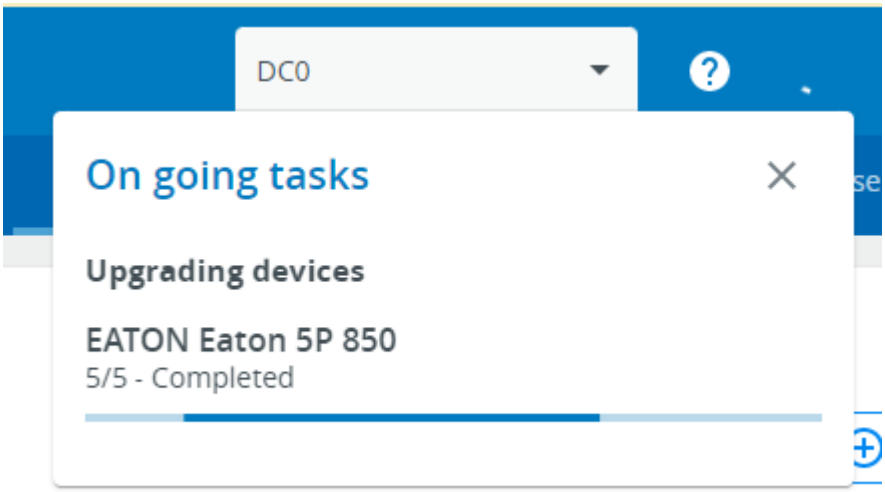
Credential Management

- **Credential** and **Port** need to be correctly configured to proceed to device upgrade
- **Credential** is used during Mass Upgrade process. If authentication fails a warning message is displayed and warning Icon is reported in the selection view



Step 3

- The Upgrade progress is then displayed in Task panel

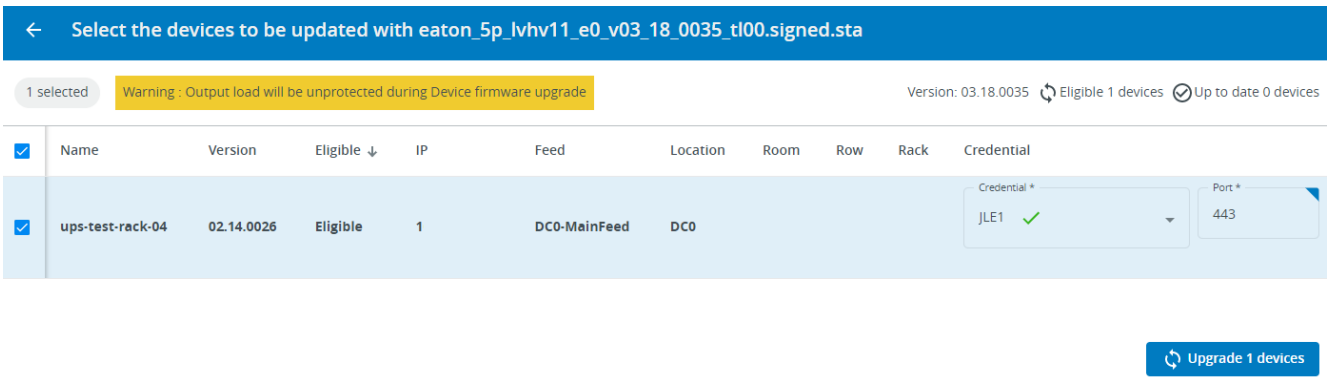


Specific warning messages for UPS Firmware Upgrade process:

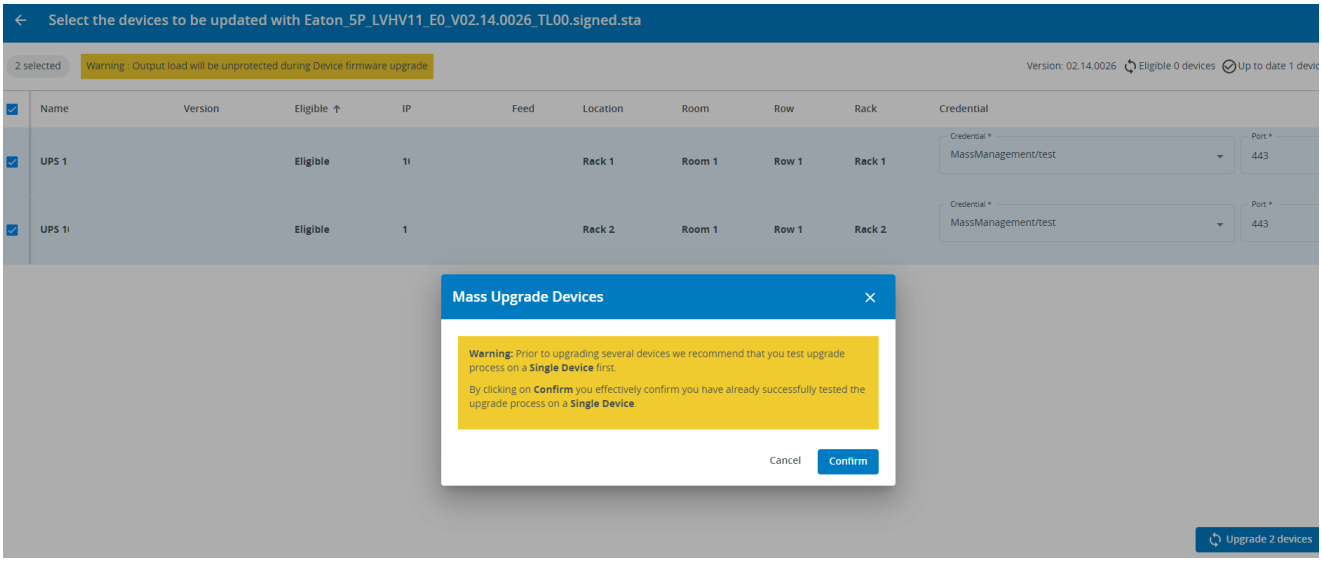
The **Upgrade Devices** process described in previous chapter applies to both "Card Firmware" and "UPS Firmware". However some warning messages are specific to UPS Firmware Upgrade process.

- UPS Firmware upgrade process can take up to 30 minutes

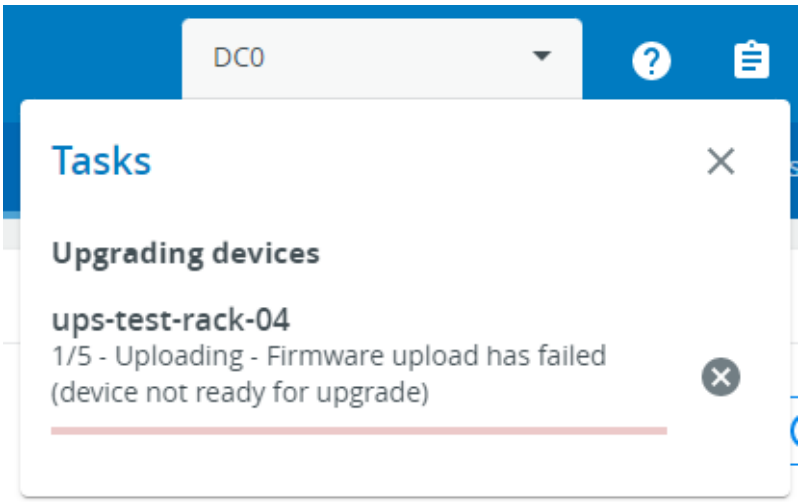
- Warning message when upgrading single UPS:



- Warning message when upgrading multiple UPSs:



- Error message when UPS is not ready to upgrade:



- Refer to UPS User Manual to get the necessary operations before UPS FW Upgrade (e.g. UPS on By Pass or UPS Output off or ...**)**

2.13.11 Local Users View

The **Local Users view** tab is accessible from the **Settings** menu item in the left navigation menu.

This menu is decated to manage user accounts :

- Create a new user
- Edit an existing user account
- Delete a user account

It is also possible to configure the security policy for :

- password strength
- account expiration
- session expiration

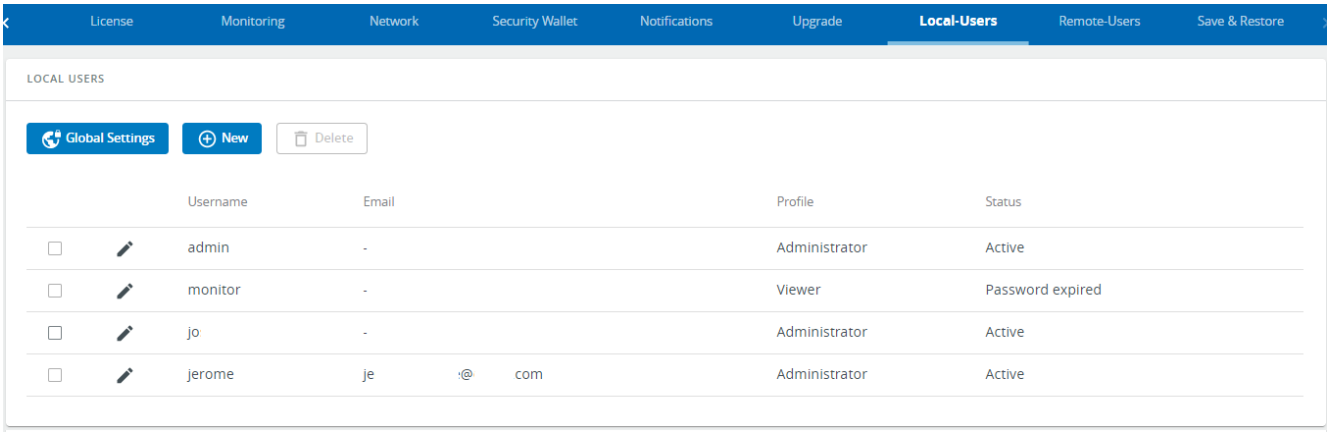
Security policy settings appy to all user accounts.

Only users with an **admin** profile have permission to access to this settings menu.
Administrators may **create a new account**, **edit**, **delete,** and **activate / deactivate** existing accounts.

Primary administrator

By default on the first install of IPM Editions, two user accounts are created : **admin** and **monitor**. (see default password below)
This initial **admin** account will be automatically defined as the **Primary administrator account**. This means that this account may not be edited by other user accounts with an administrator profile.
The first connection is only possible with the "admin" account created by default. The password change will be requested on first connection.

Local users accounts list



The table shows all the supported local user accounts and includes the following details:

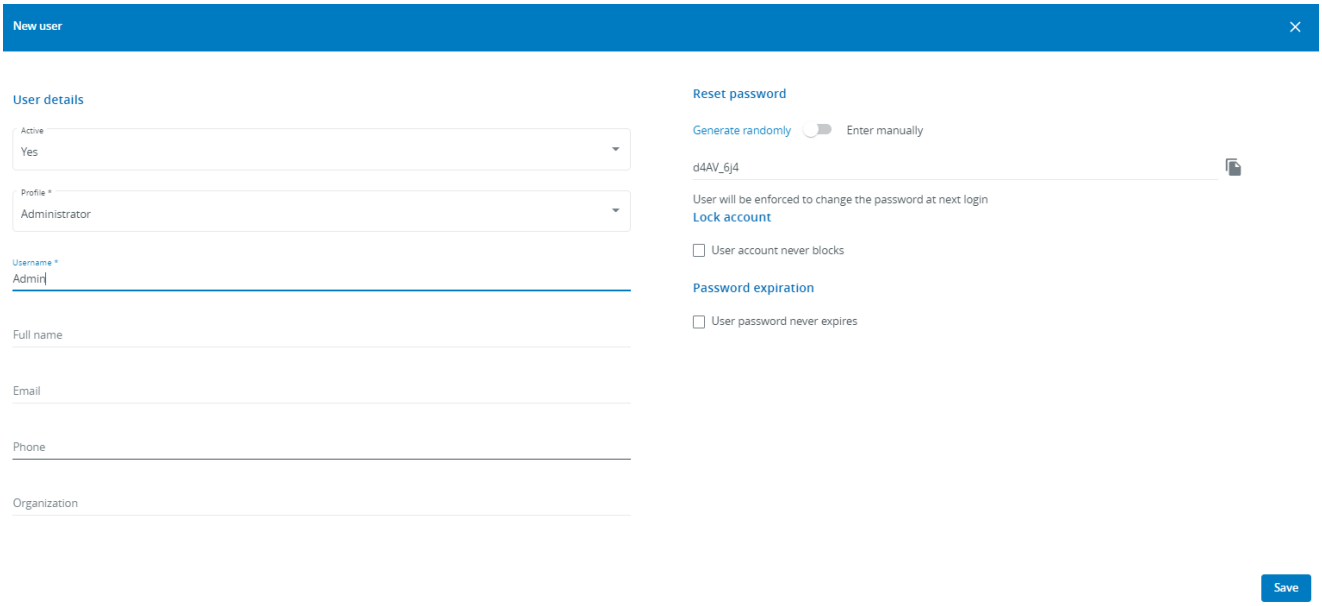
- **Username**
- **Email**

- **Profile**
- **Status –** Status could take following values – Inactive/Locked/Password expired/Active

Actions

Add

Press the **New** button to create up to ten new users.



When completed:

- the new account appears in the Local user table
- the password change will be required on first connection to the new Local user account.

Remove

Select a user and press the **Delete** button to remove it.

Edit

Press the pen icon to edit user information:

- User Details
  - Active: allows to activate or deactivate account
  - Profile: administrator or viewer
  - Username: this value will be used as login ID
  - Full name
  - Email
  - Phone
  - Organization – Notify by email about account modification/Password
- Reset password
  - Generate randomly: the system will automatically create a random password
  - Enter manually: you create your own password, taking care to respect the parameters defined in password strength policy
    Note: The new user will be required to change his password upon his/her first connexion.
  - Confirmation Password: In order to finalize the user account creation, the administrator currently logged into the application will have to reauthenticate by entering his/her own password after pressing Save button.
    A similar reauthentication behavior is required to reset a user account password. Same behaviour when an administrator wants to reset a user account password.
- Lock account information
- Password expiration information

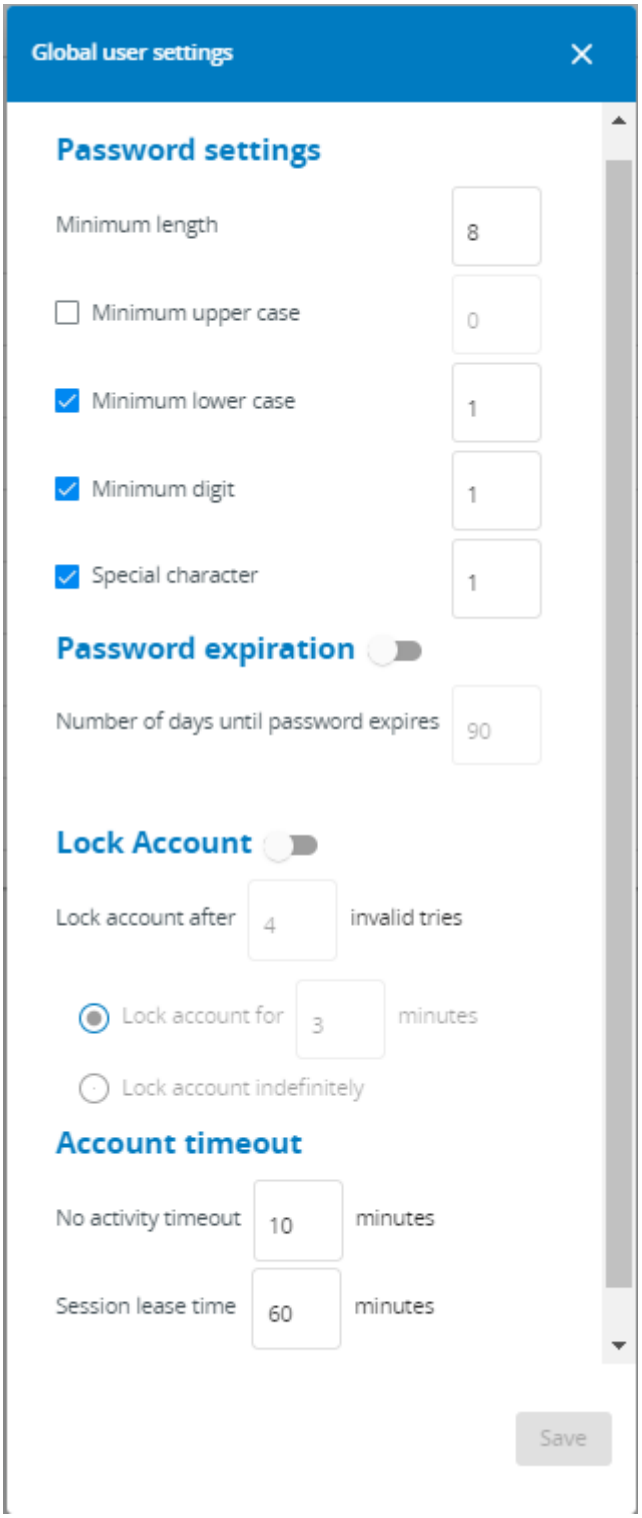
Global user settings

Password strength policy parameters may be managed by administrator profiles.

Administrators may also configure parameters for **Password expiration, Lock Account and** and **session expiration**

> Security policy configuration changes apply to all accounts created in your IPM application.

For a more detailed explanation of User settings configuration, see the User Management section of the documentation.



Press **Save** after modifications.

Password settings

It's possible to define the complexity of the password, but not mandatory. By default the minimum length is 8 with 1 special character and 1 digit.

You must save in order for the account modifications to be applied.

To set the password strength rules, apply the following restrictions:

- Minimum length
- Minimum upper case
- Minimum lower case
- Minimum digit
- Special character

Password expiration toggle

To set the password expiration rules, apply the following restrictions:

- Number of days until password expires
  A password change will be requested once the password expiration delay is reached.

Lock account toggle

- Lock account after a number xx of invalid tries
- Lock account for xx minutes
  or
- Lock account indefinitely

Account timeout

To set the session expiration rules, apply the following restrictions:

- No activity timeout (in minutes).

  If there is no activity, session expires after the specified amount of time.

- Session lease time (in minutes).

  Session still expires after the specified amount of time.

2.13.12 Remote Users View

LDAP support

Activate LDAP toggle will activate/deactivate the ability to configure and use LDAP.

When the toggle s active, all the related actions might be used.

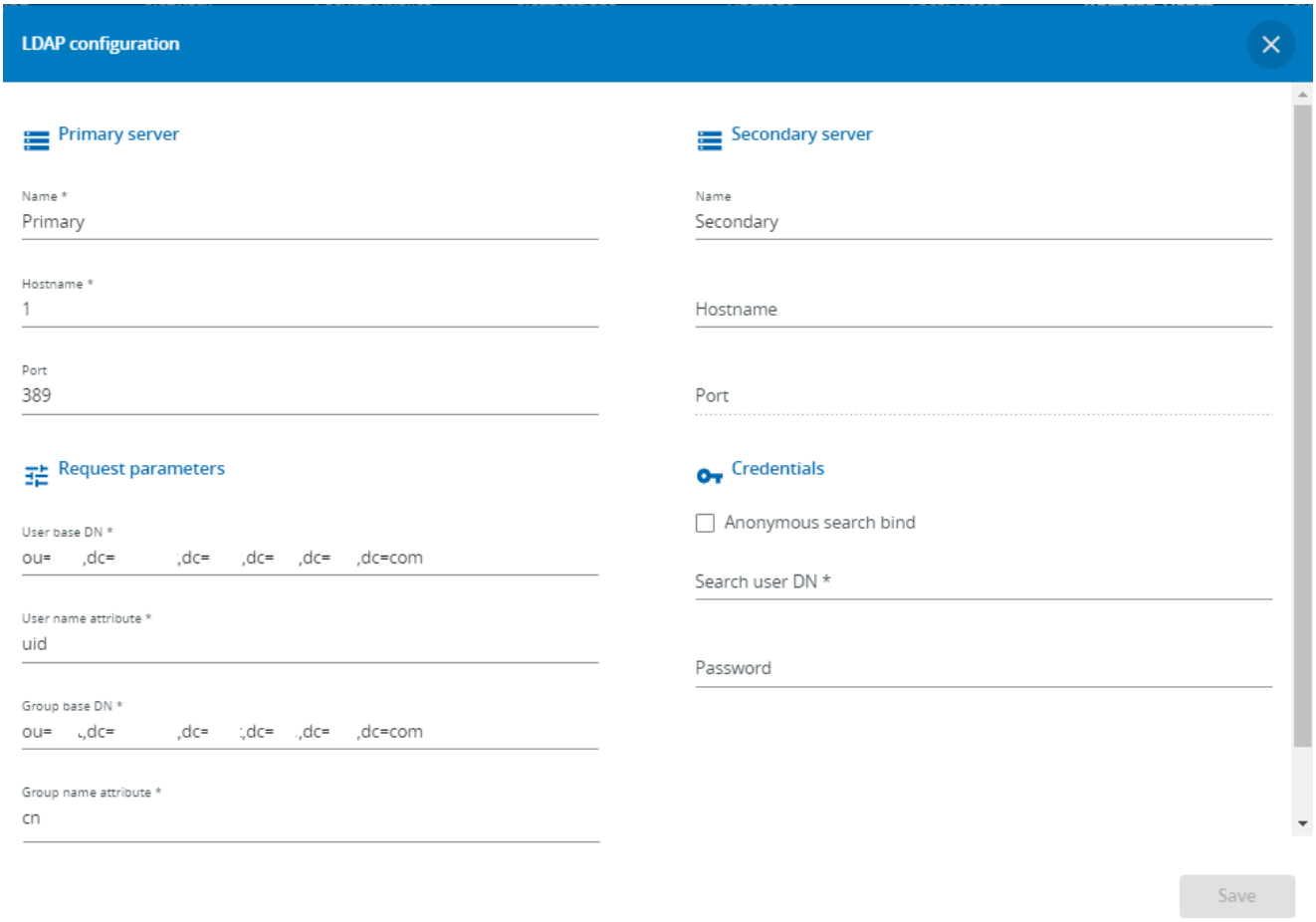
Configure action

1. Press **Configure** to access the following LDAP settings:

- Primary server
  - Name
  - Hostname
  - Port
- Secondary server
  - Name
  - Hostname
  - Port
- Credentials
  - Anonymous search bind
  - Search user DN
  - Password
- Request parameters
  - User base DN
  - User name attribute

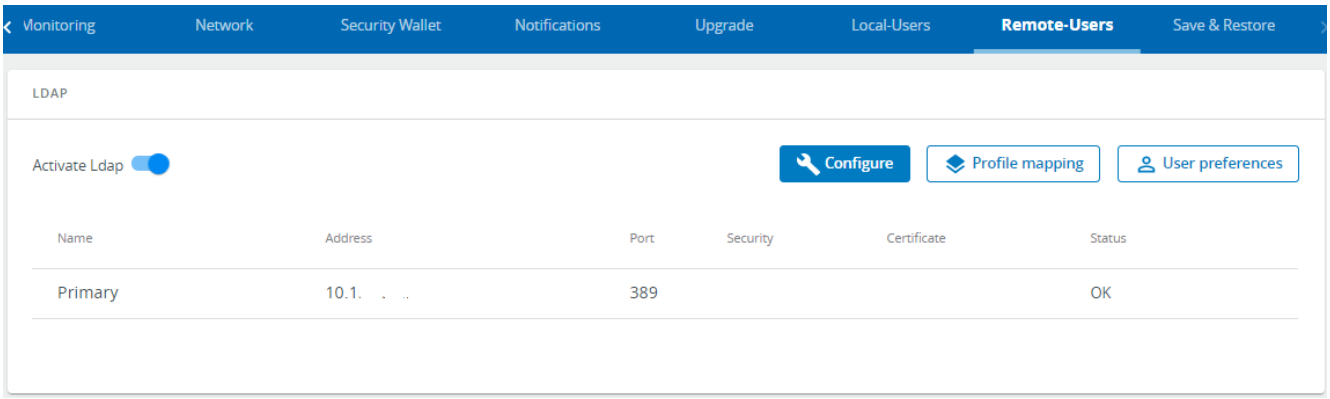
- Group base DN
- Group name attribute

2. Click **Save**.



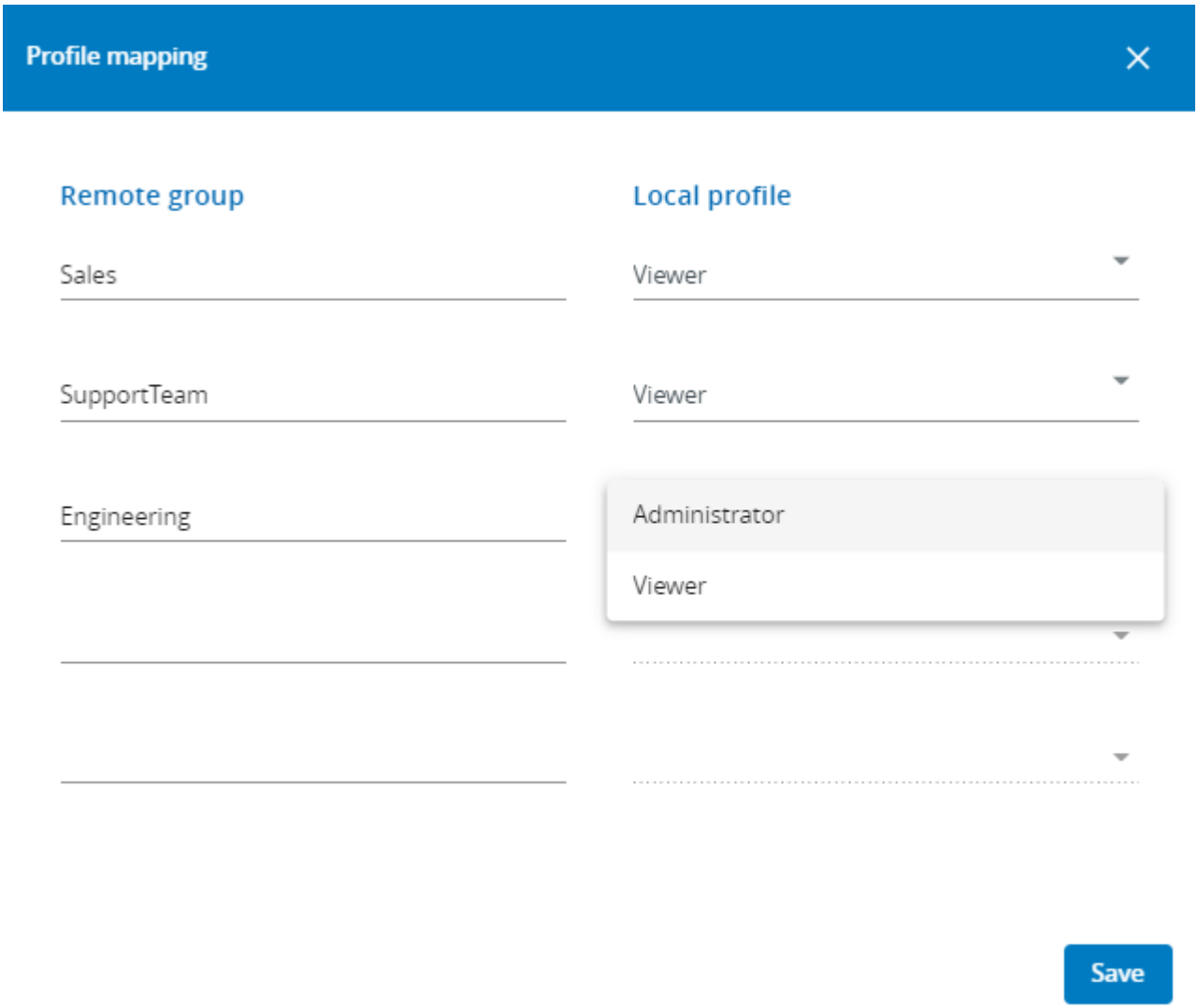
Each configured server will appear in the below table with the following details:

- Name
- Address
- Port
- Security
- Certificate
- Status



Profile mapping

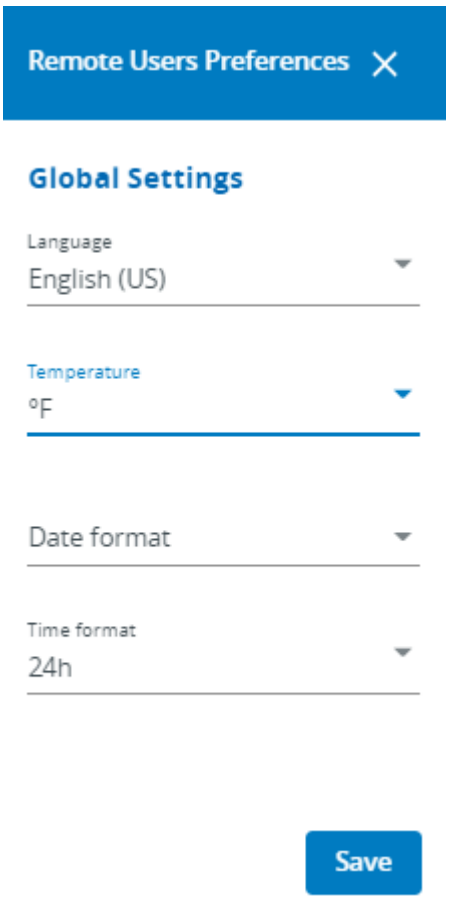
The feature is about mapping remote groups to local profiles.



1. Press **Profile mapping** to map remote groups to local profiles.
2. Click **Save**.

Users preferences

User preferences are common to all users authenticated through LDAP.



1. Press **Users preferences** to define preferences that will apply to all LDAP users
    - Language
    - Temperature
    - Date format
    - Time format
2. Click **Save**.

2.13.13 Save & Restore view

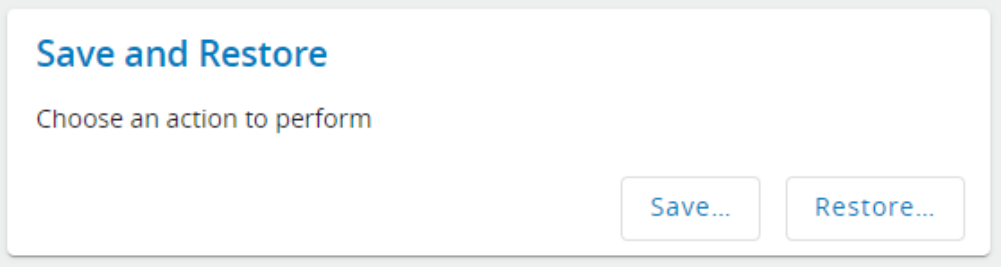
Overview

The **Save & Restore settings** tab is accessible from the **Settings** menu item in the left navigation menu.

Using SRR in between version is possible starting from IPM2, version 2.3.0, on the following conditions :
If Xs.Ys.Ws is the version where the saved happened and Xr.Yr.W.r the version where the restore happened :

- Upgrade where Xs != Xr not supported:
    - 2.3.0 to 3.0.0 will failed
- Upgrade where Ys > Yr is not supported:
    - 2.4.0 to 2.3.1 will failed
    - 2.4.0 to 2.5.0 will success
- Upgrade where Ys == Yr and Ws > Wr are allowed with loss of data:
    - 2.4.0 to 2.4.1 will success
    - 2.4.1 to 2.4.0 will success with loss of data : the new data present in 2.4.1 are lost in the 2.4.0 restauration

The Save & Restore tab enables you to Save and Restore all parameters of your **IPM Edition** software instance.

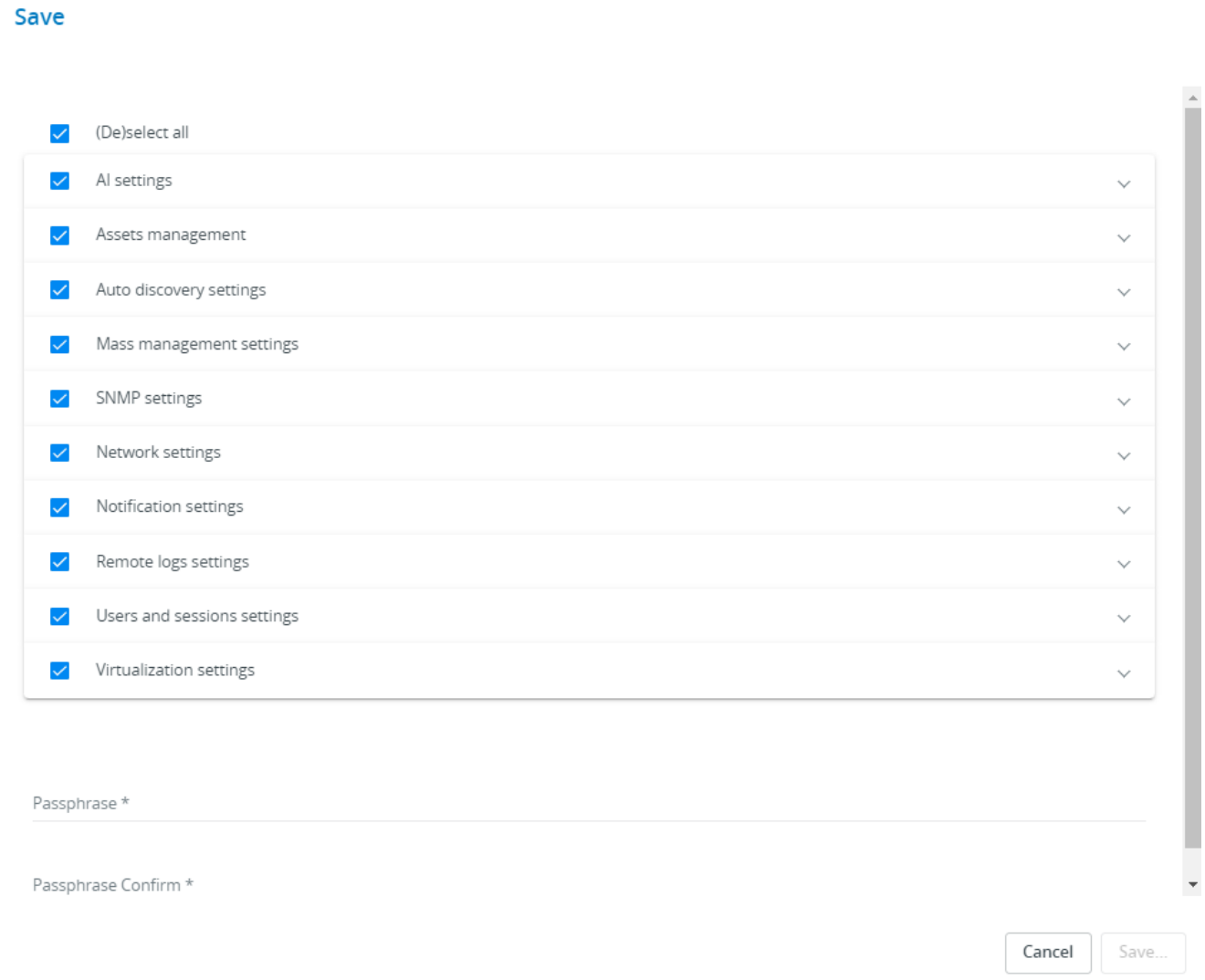


Saving IPM Editions settings

The Save & Restore tab prompts the user to choose either to save or restore some settings.

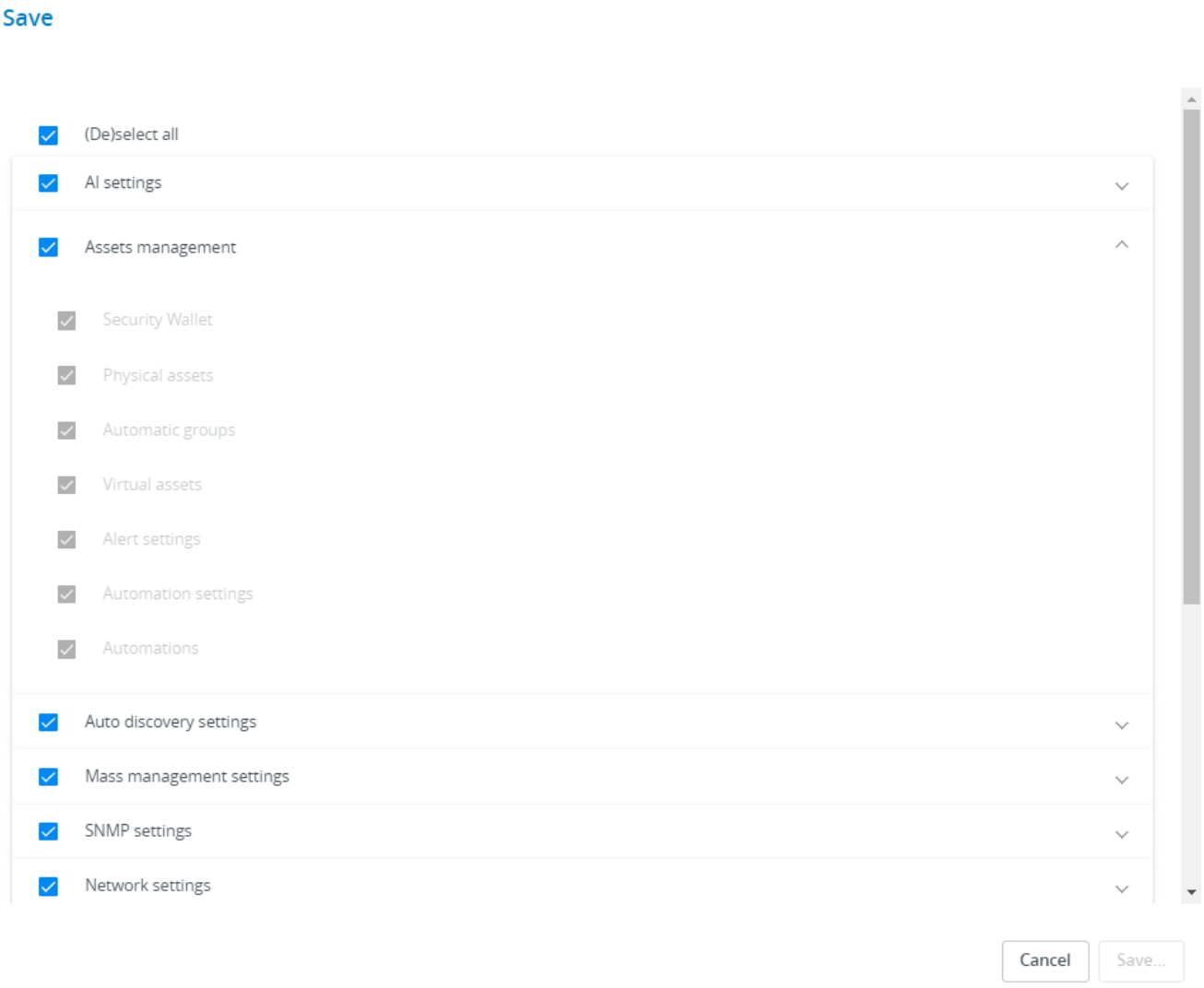
In order to save some settings, the user must click on the **Save ...** button and follow the process illustrated below.

After clicking on the **Save ...** button, the user is prompted with the list of all categories of settings available.



In addition to the list of categories, the user must provide a passphrase to encrypt the sensitive data that might be present in the saved file.

In order to help the selection of the appropriate categories some detail can displayed for each category by hitting the control present at the end of each category line.



Once the selection of the settings categories is done and the passphrase is typed and confirmed, the user can proceed and **Save** the selected settings.

> The user will have to provide the chosen passphrase to restore all or part of the saved settings later. Therefore, this passphrase must be chosen and noted carefully.

Restoring IPM Edition settings

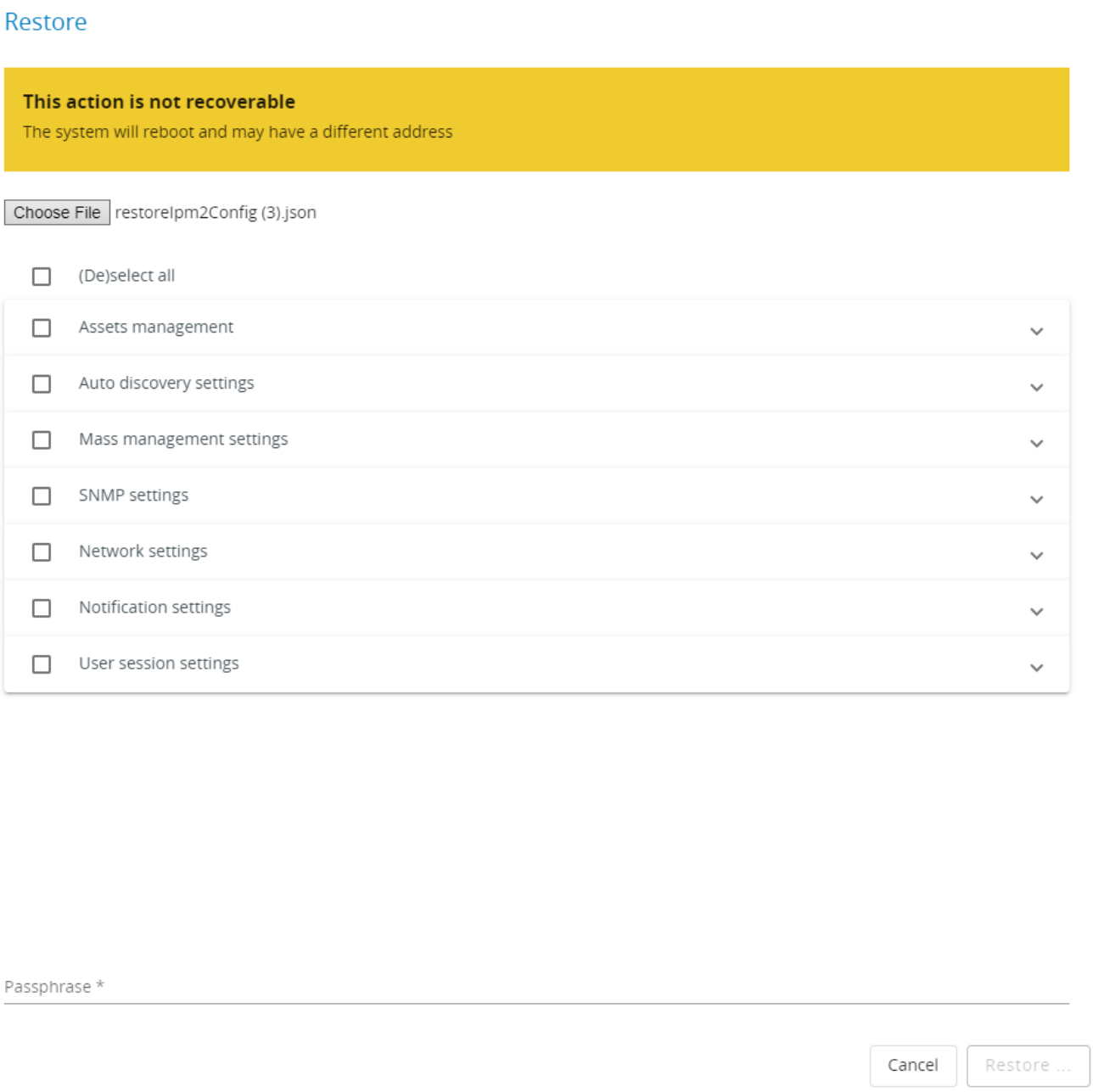
The Save & Restore tab prompts the user to choose either to save or restore some settings.

In order to restore some settings, the user must press the Restore button and follow the process illustrated below.

After pressing the **Restore ...** button, the user is prompted to choose the file from which the settings will be restored.

This file must have been generated by an earlier "Save" action.

Once the file is selected, all the settings categories it contains are proposed to be restored.



The categories can be restored independently and the user is free to select all or some of them.

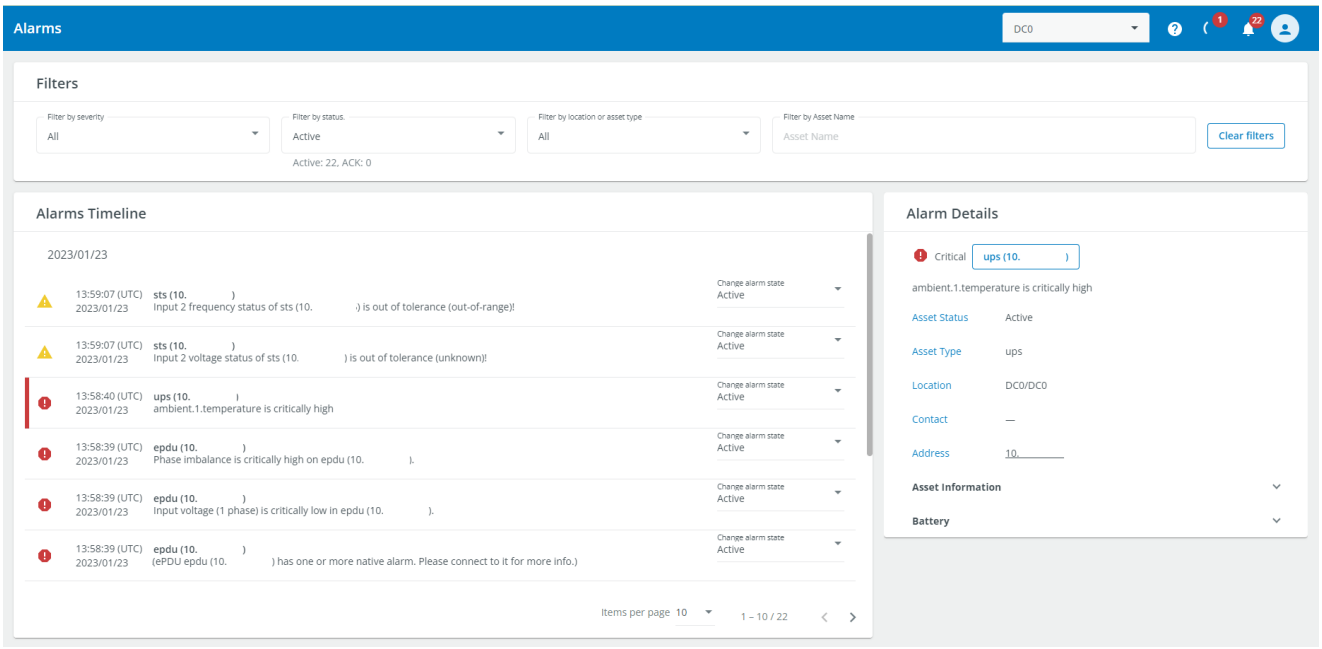
Once the selection of the settings categories is done and the passphrase entered at Save time is typed again, the user can proceed and restore the selected settings.

2.14 Alarms View

You may view and manage the state of all alarms from the Alarms view page.

By default, you are presented with all **current active alarms** in the system.

Each alarm displays the system name generating the fault condition, a timestamp of when the alarm occurred, and a short description of the alarm taking place.



Users may place Alarms into one of several possible states enabling you to move the alarm through your internal workflow and take appropriate action when addressing an incident.

All alarm states may be filtered by using of the Filter function at the top of the page.

Filter attributes include :

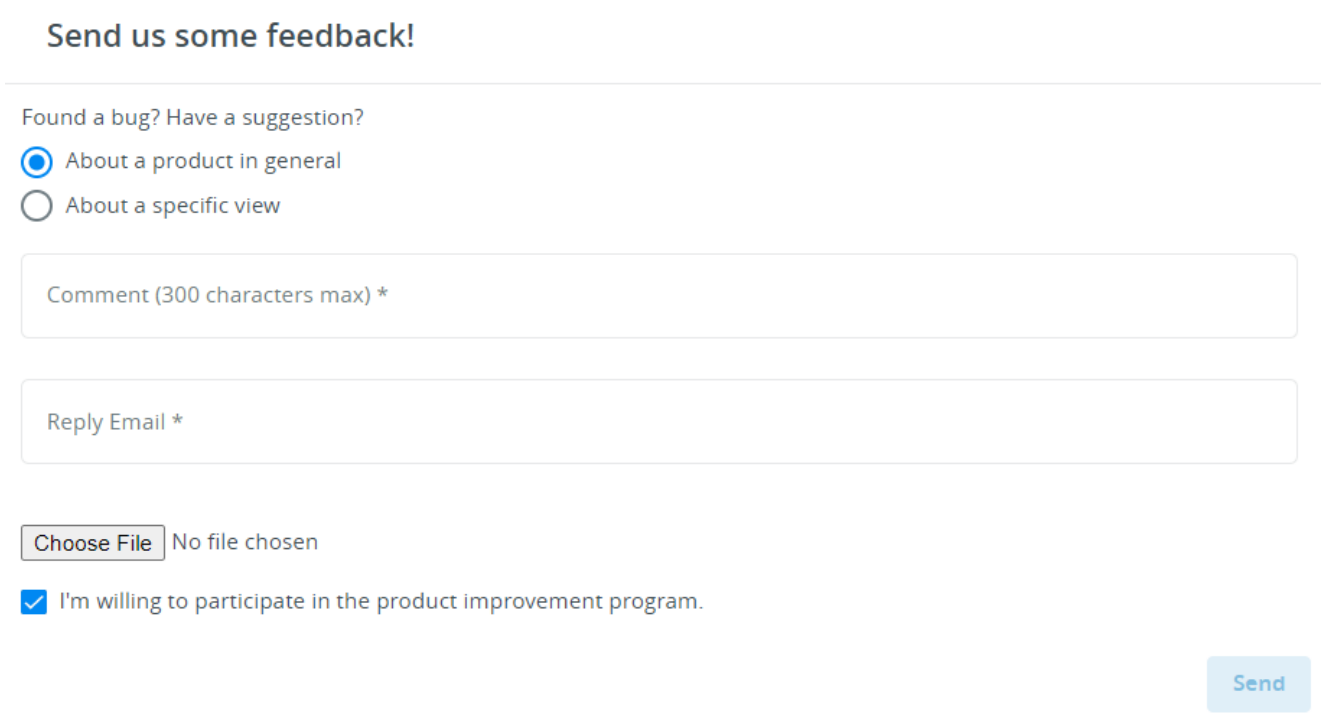
1. **Severity**
2. **Status**
3. **Location or asset type**
4. **Asset Name**

Refer to the Alarms Management section of the documentation for a more detailed description of the management features.

2.15 Feedback Tool

> Eaton would love to know more about your experience. You may send your feedback directly to us by using the Feedback Tool.

The Feedback tool allows you to communicate questions or comments directly to Eaton.



1. Select the appropriate **radio button** with respect to the type of feedback you are providing :
    a. **General feedback** about the IPM application
    b. Relative to the **current page**
2. In the **Comment** field, please try to describe all the details of the issue you want to report. Please provide us with any relevant information about the context in which you are using your IPM application.
3. If you'd like us to reply to your submission, please enter a **reply email** address.
4. You may optionally add a file (e.g. screenshot) that can complement your text description by clicking on **Choose File** and selecting a file from the file browser.
5. Click **Send**.

It is also possible to manually send an email to EATON support at this address: EatonProductFeedback@Eaton.com

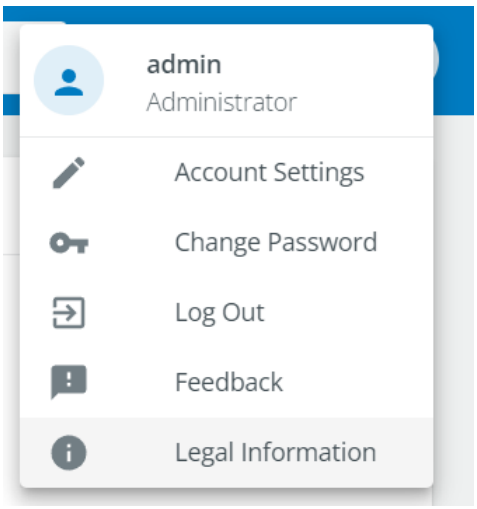
2.16 Legal Information

Legal Information

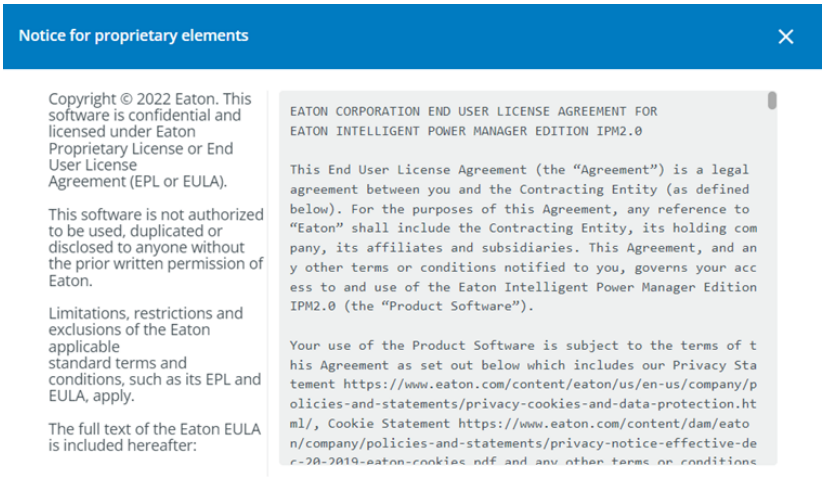
Eaton Intelligent Power Manager includes software components, which are licensed under various open source licenses, or under a proprietary license.

The Legal Information provides all Copyright notices and Licenses text, for both open source and proprietary software.

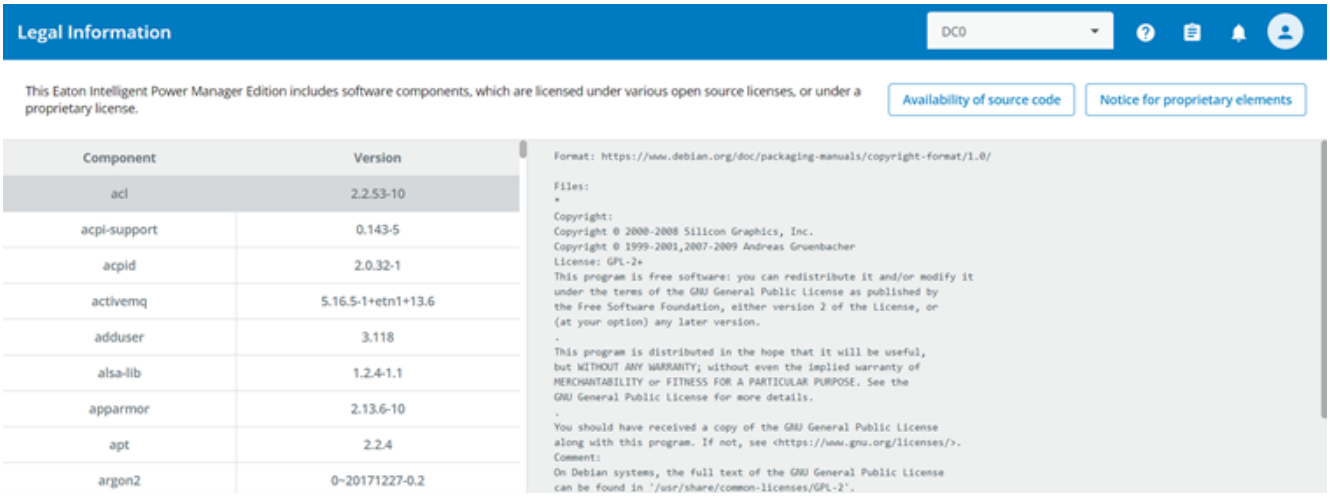
Legal Information can be accessed from the User menu:



Information are provided for proprietary source code, including the Eaton EULA that was accepted during the initial commissioning:



The page also provide all legal information for each software, both proprietary and open source:



Finally, open source code can be requested using the mentioned email address:

Availability of source code

The source code of open source components which are made available by their licensors (including Eaton where applicable) may be obtained upon written express request by contacting: ipc-opensource@Eaton.com

Eaton reserves the right to charge minimal administrative costs, in compliance with the terms of the underlying open source licenses, when necessary.

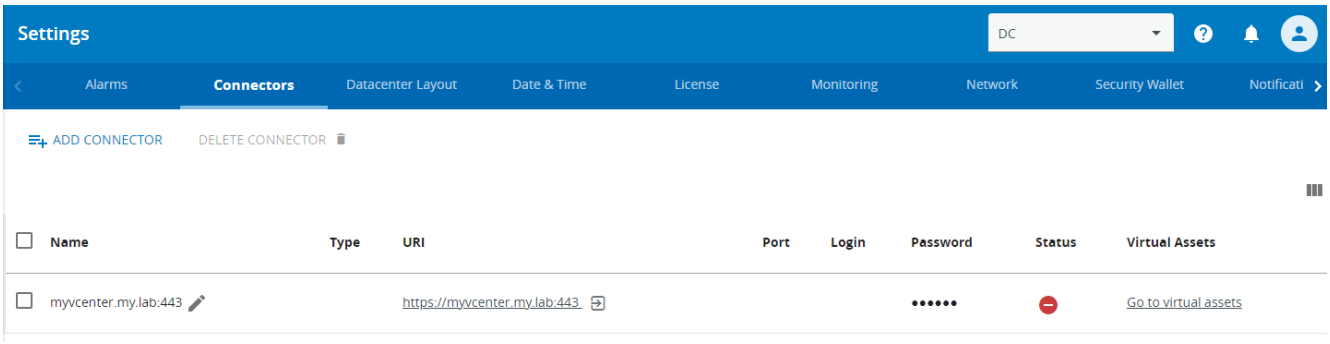
3 Troubleshooting

3.1 Connector connections

At creation time or during monitoring, a connector can have a connection error symbolized by a red icon in the “Status” column.

These errors prevent the connector and all subsequent monitoring and automation actions to work correctly.

On the red icon, the mouse over tooltip displays the root cause.



Frequent errors are:

- **Unknown host** : the targeted host is unknown. Try to check if the host name or IP address exists or is correctly spelled.
- **No route to host** : the targeted host is not accessible. Try to check if the host is accessible through the network route.
- **Invalid credentials** : entered credentials are not accepted by targeted service. Try to verify if the user is valid and user and password are correctly spelled.
- **Connection refused** : entered user is not authorized. Try to verify if the user is valid and authorized.
- **Connection timeout** : targeted service is low or doesn’t respond. Try to check if the service is healthy and correctly configured.
- **API Mismatch** : targeted service doesn’t match expected API. Try to check if hostname or IP address of the service is correct. Try to check if the type of connector corresponds to the type of service. Try to check if the version of the service is supported by the version of IPM.
- **Unexpected connection error** : Another unspecified error. Try to check all other tips before, particularly the hostname, IP address, user name or password are spelled correctly, the service is healthy and correctly configured- and in a supported version.
  Moreover, some connectors needs to be time-synchronized with the remote service and error can occur when date and time are not well synchronized. Try to check if their respective time are almost synchronous (i.e. less than 5 minutes of dyssynchronization), particularly when at least one of them have a manually set date and time. If both are synchronized through NTP, try to check if they are synchronized on the same NTP server or their respective NTP servers are synchronized.

3.2 Factory Reset

> **CAUTION**
>
> **Performing a factory reset will delete all data and reset the software to its initial state. All monitored data, application updates, configuration settings and passwords will be deleted.**

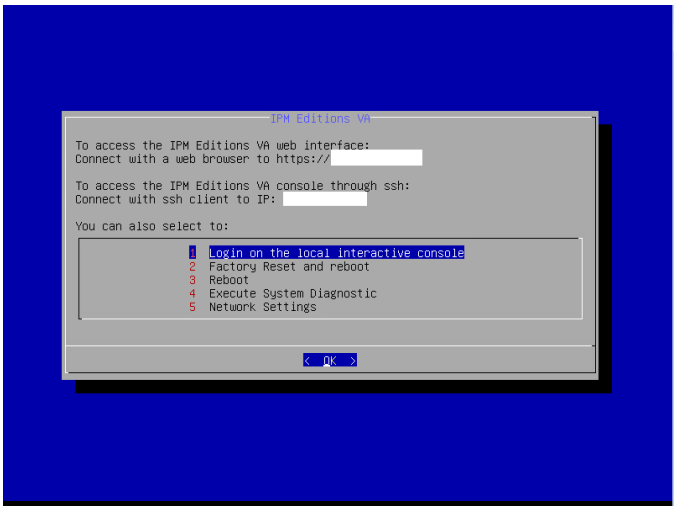
3.2.1 **Virtual appliance version**

If your instance of the software runs in a virtual machine, you may perform a factory reset by using the virtual appliance console and select **Factory Reset** option of the menu.

Virtual appliance console

Some administration functions are made available via the vCenter console including the Factory Reset.

You may connect to the console via SSH and your preferred SSH client.



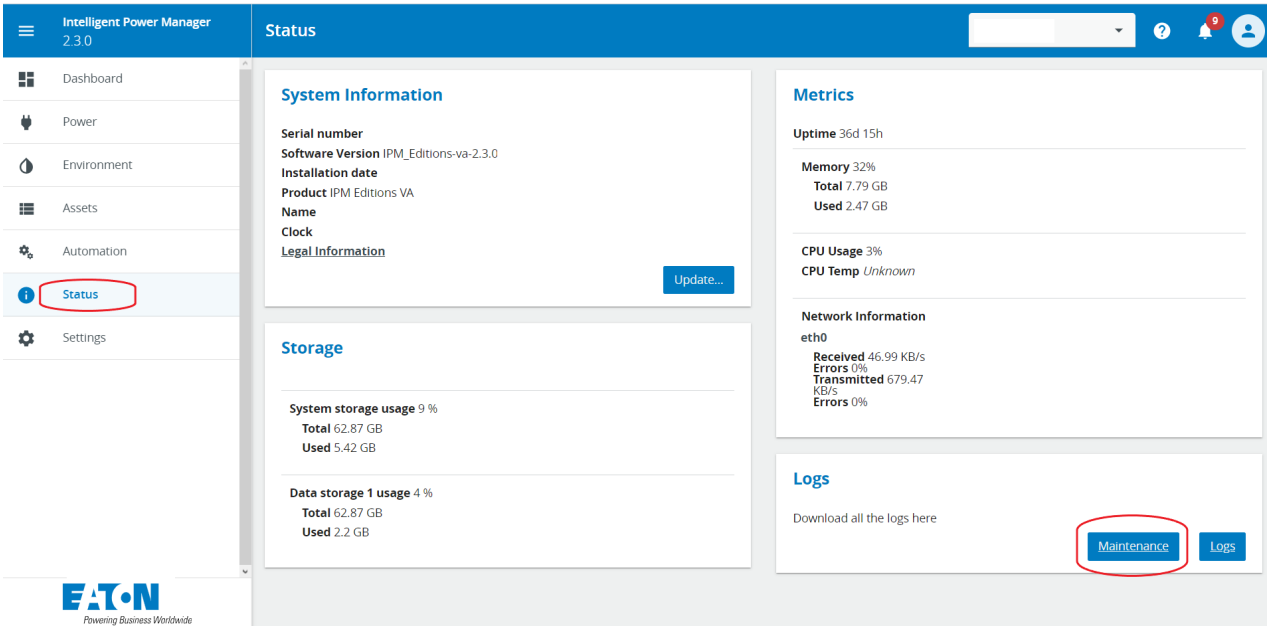
3.3 Procedure to collect all required data to get some support

If you experiment some issues using the SW and want to get some support from our support team, please follow these steps to collect the required information.

First, you need to log in to your instance and then perform the actions below through the user interface.

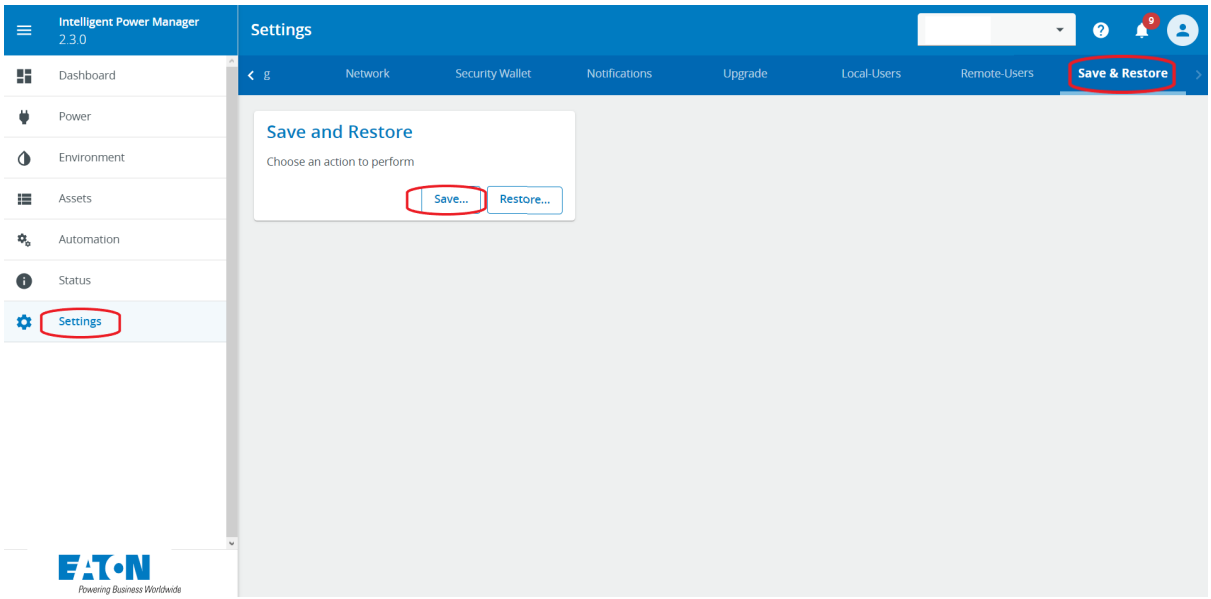
1. Retreive the maintenance report and share it

    - Open the status page
    - Click on "Maintenance retport" button
    - This will generate a password protected encrypted archive you can share with our support team (e.g. providing a link to an accessible storage).



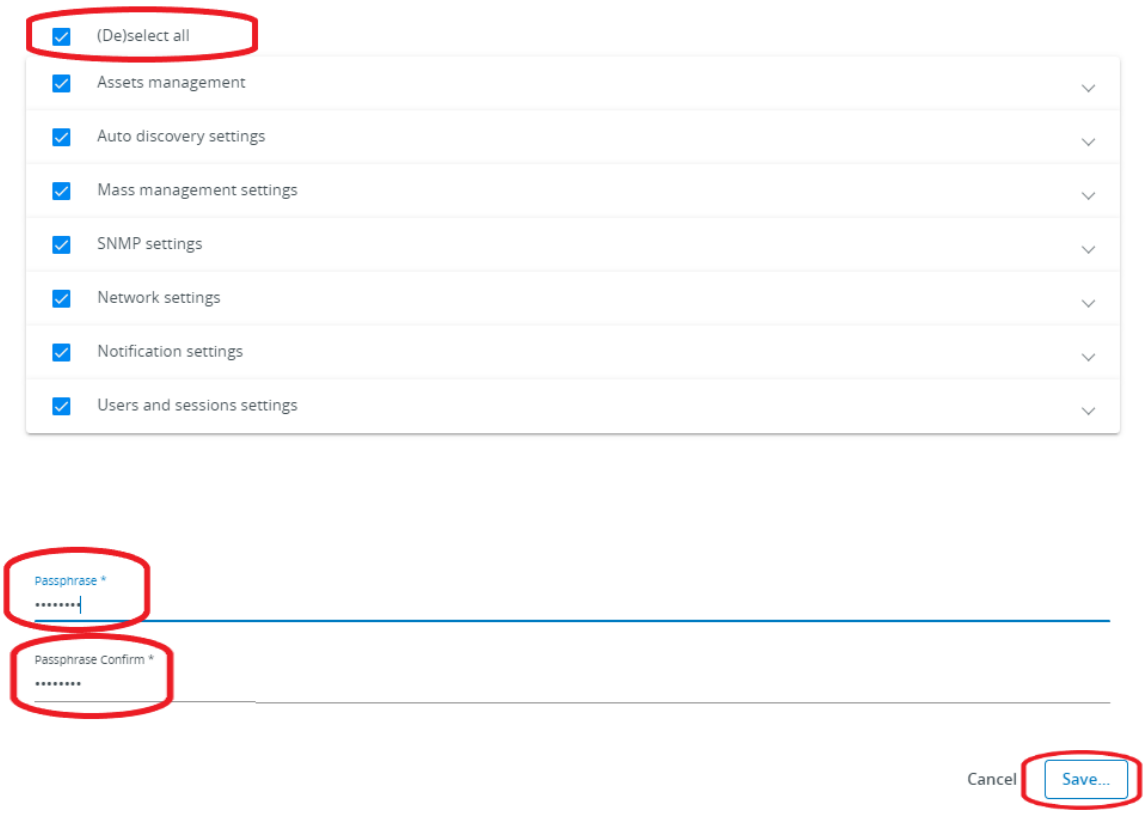
2. Save your configuration and share it

- Open the settings page
- Get to the Save & Restore tab
- Click on the Save button



- Select all categories
- Enter a passphare and confirm it
- Click on Save
- This will generate a text file in JSON format you can share with our support team (e.g. providing a link to an accessible storage).

Save


(De)select all
Assets management
Auto discovery settings
Mass management settings
SNMP settings
Network settings
Notification settings
Users and sessions settings
Passphrase *
Passphrase Confirm *
Cancel
Save...

4 Appendix I - Migrating from IPM Infrastructure 1.5 to IPM Monitor Edition 2.3.0 or better

4.1 How can I get the right license to move from IPM Infrastructure to IPM Monitor Edition?

In case you purchased an IPM Infrastructure license, please contact your local sales representative to retrieve a license for IPM Monitor Edition.

4.2 How can I migrate my configuration from IPM Infrastructure 1.5 to IPM Monitor Edition?

The migration from IPM Infrastructure 1.5 to IPM monitor Edition is limited to the asset list. The rest of the settings have to be set manually on the new instance of IPM monitor Edition.

4.2.1 On IPM Infrastructure 1.5

To be able to get the assets data from your IPM Infrastructure instance, you have to go to the "Assets" page and press "Export Assets" . You will get an file in csv format.

4.2.2 On your computer

- Open the csv file using Excel or your favorite spreadsheet program.
- Remove the second line of the file: This line should contain the rackcontroler information (type: device, sub_type: rackcontroler).
- Remove the column containing the "id". This column is the last one of the csv file.
- Save the file.

4.2.3 On IPM monitor Edition

- Start your IPM Edition instance.
- Change the password.
- Accept the license and wait. This can take few minutes.
- Change your network configuration if needed. Press Next.
- Create a datacenter and a feed with a different name as the one of your IPM Infrastructure. This datacenter will be removed at the end of the process. Press Next.
- Do not change the datacenter layout. Press Next.
- Enter the new licensing key from IPM monitor Edition. Press Next.
- Go to "ASSETS" Page, click on "ADD ASSETS" and "UPLOAD CSV FILE". Choose the file you modify and press upload.
- The system will import as much asset he can. Some may fail.
- Then we need to clean the temporary datacenter: In "ASSETS" Page, "Facility Assets" section, delete the feed and in "Location" section, remove all the assets. If everything is successful, you will switch to one of the datacenter you imported.
- You can check all the settings and add what is missing.

5 Appendix II - Save and Restore file

5.1 Introduction

In this section we will give you some example of payload which you will find in the saved file from Save and Restore feature.

In case you would have multiple instances of IPM Editions and you would like to configure all of them in a similar way, one approach is:

- to configure a first instance via the intuitive IPM Editions user interface
- to save your configuration to a file
- to customize the file to adapt it to the other instances
- to force the restoration of the modified files into the target instances

> The customisation of those files is reserved to advanced user.
> The restoration of an incorrect files can lead to the loss of the IPM Editions instance or to unexpected behaviors.
> To help you do the modifications in a safe and efficient way, we describe below typical examples and how to perform them successfully.

This section shows typical examples of files generated with IPM 2.x.y

The file is in Json format. In this document we are describing partial json by adding "...".

5.2 File global structure

The file is organized by group:

High file payload


```
{
  "checksum": "d903bk/69h4yMv3zwO56+A==:wQalNg4XBCT2/3E1sVG1eQ==",
  "status": "success",
  "version": "2.1",
  "data": [
    {
      "group_name": "group-assets",
      "group_id": "group-assets",
      "features": [ ... ],
      "data_integrity": "1f7a23e0f86448b5e7b7b8234e630bbad61411f1141546908ccbc647621c0d70"
```

High file payload

```
},
....
  ]
}
```

Each file have a mandatory fields:

- checksum - It ensure that the file can be restored on IPM Editions. When this file is modified, a warning message is displayed during "Restore" step explaining that the file might be corrupted.
- status - This status is the global status of your save action
- version - This is the version of the save file. It can not be modified
- data - This section will contain a list of groups. In order to guaranty the coherence of the data in IPM Editions, you can only save and restore groups. Each group have a mandatory fields:
    - group_name and group_id - Id for IPM Editions to identify the feature
    - features - all features which are part of this group
    - data_intergrity - Check on the data integrity of the group. During a restore, If the data integrity check fails, we will request you a confirmation through the UI to force the restore.

Example of a feature

```
"automations": {
  "status": "success",
  "version": "1.0",
  "error": "",
   "data": {...}
}
```

Each feature have a mandatory fields:

- status - Status of this feature when you did your save action
- version - This is the version of the feature pauload. It can not be modified
- error - Error during save if any.
- data - This section will contain the data for the restore. it can be a Json or a text string depending of the feature.

5.3 List of groups and features

Here are the groups and their features available for IPM 2.7.0 version:

Note: New features are identified with (New: xxx)

1. "group-ai-settings"
    - "ai-settings"
2. "group-assets"
    - "security-wallet"
    - "credential-asset-mapping" (New: assets mapping with the secw)
    - "asset-agent"
    - "automatic-groups"
    - "virtual-assets"
    - "alert-agent"

    - "automation-settings"
    - "automations"
3. "group-datetime-settings"
    - "timezone-settings" (New: client timezone settings)
    - "ntp-settings" (New: NTP server settings)
4. "group-discovery-ng"
    - "discovery-ng-settings"
    - "discovery-ng-agent-settings"
5. "group-mass-management"
    - "etn-mass-management"
6. "group-monitoring-feature-name"
    - "monitoring"
7. "group-network"
    - "network"
    - "network-host-name"
    - "network-agent-settings"
    - "network-proxy" (New: Network proxy settings)
8. "group-notification-feature-name"
    - "notification"
9. "group-remote-syslog"
    - "rsyslog"
10. "group-user-session-management"
    - "user-session-management"
11. "group-virtualization-settings"
    - "virtualization-settings"

5.4 "Asset management" (group-assets)

Here are some example of customization you can do on the feature of asset group

5.4.1 Customize Physical Assets

Introduction

Physical assets (ups, epdu, ...) are saved into the feature called “asset-agent”.

High level asset-agent payload

```
"asset-agent": {
  "status": "success",
  "version": "1.0",
  "error": "",
  "data": {
  "version": "1.0",
  "data": [
    {...},
    {...}
  ]
}
```

Partial example of one asset


```
{
   "priority": 5,
   "tag": "",
   "ext": {
       "endpoint.1.protocol": {
        "readOnly": false,
        "value": "nut_snmp"
       },
       "endpoint.1.nut_snmp.secw_credential_id": {
        "readOnly": false,
        "value": "b4e60d7e-dd0c-4515-94cc-791242dd51ae"
       },
       "endpoint.1.port": {
        "readOnly": false,
        "value": "161"
       },
       "name": {
        "readOnly": false,
        "value": "ups (10.130.35.81)"
       },
       "ip.1": {
        "readOnly": false,
        "value": "10.130.35.81"
       },
....
   },
   "id_secondary": "",
   "linked": [],
   "status": 2,
   "subtype": "ups",
   "parent": "",
   "id": "ups-89890588",
   "type": "device"
}
```

Change asset name

Warnings

- Asset name must be unique amongst all IPM Edition assets.
- Asset name must NOT be null or empty.

Payload without modification	Updated payload
{ "priority": 5, "tag": "", "ext": { "name": { "readOnly": false, "value": "My name" }, ... }	{ "priority": 5, "tag": "", "ext": { "name": { "readOnly": false, "value": "My new name" }, ... }

Change SNMP connection settings

Warnings

- All asset monitored with snmp must have as protocol "nut_snmp"
- Asset extended attribut "endpoint.1.nut_snmp.secw_credential_id" value must be an snmpv1 or snmpv3 credential id from security wallet
- Asset ip.1 can be ip or fqdn

Payload without modification	Updated payload
{ "priority": 5, "tag": "", "ext": { "endpoint.1.protocol": { "readOnly": false, "value": "nut_snmp" }, "endpoint.1.nut_snmp.secw_credential_id": { "readOnly": false, "value": "b4e60d7e-dd0c-4515-94cc-791242dd51ae" }, "endpoint.1.port": { "readOnly": false,	{ "priority": 5, "tag": "", "ext": { "endpoint.1.protocol": { "readOnly": false, "value": "nut_snmp" }, "endpoint.1.nut_snmp.secw_credential_id": { "readOnly": false, "value": "ace584855-47847485-477854ew-58844-447778544" }, "endpoint.1.port": { "readOnly": false, "value": "8161"

Payload without modification	Updated payload
"value": "161" }, "ip.1": { "readOnly": false, "value": "192.168.0.1" }, ... }, "id_secondary": "", "linked": [], "status": 2, "subtype": "ups", "parent": "", "id": "ups-89890588", "type": "device" }	}, "ip.1": { "readOnly": false, "value": "myups.mynetwork.com" }, ... }, "id_secondary": "", "linked": [], "status": 2, "subtype": "ups", "parent": "", "id": "ups-89890588", "type": "device" }

5.4.2 Customize Automations

Introduction

Automations are saved into the feature called “automations”.

All configured automations are described into automation List in json format.

High level automations payload
{ "automations": { "version": "1.0", "status": "success", "error": "", "data": { "bundleVersion": "2.3.14", "automationList": [*{...},* *{...}*] }

High level automations payload

```
  }
}
```

Example of one automation

```
{
  "name": "My automation name",
  "comments": "",
  "createdBy": "admin",
  "active": false,
  "schedule": "",
  "initialTrigger": "{0}",
  "triggerType": "CAT_OTHER",
  "triggers": {
    "ipmInfraEvent": [],
    "metricEvents": [
      {
        "index": 0,
        "asset": "rackcontroller-0",
        "metric": "uptime@rackcontroller-0",
        "operation": ">",
        "threshold": "107428"
      }
    ]
  },
  "tasks": [{
    "index": 0,
    "name": "Wait 10 seconds",
    "group": "WAIT",
    "subgroup": "DELAY",
    "properties": [{
      "key": "duration",
      "value": ["10"]
    }],
    "timeout": 3600,
    "onSuccess": null,
    "onFailure": null
```

Example of one automation
}], "notification": { "notifyOnFailure": false, "emails": [] } }

Below is a list of what is allowed to change into each automation.

Change automation name

Simply edit the current one to a new one.

Warnings

- Automation name must be unique amongst all IPM Edition automations.
- Automation name must NOT be null or empty.
- Automation comment could be null or empty

Example

Payload without modification	Updated payload
{ "name": "My old automation name", "comments": "", "createdBy": "admin", "active": false, "schedule": "", ... }	{ "name": "My new automation name", "comments": "New automation comment!", "createdBy": "admin", "active": false, "schedule": "", ... }

Change automation task name

Simply edit the current one to a new one.

Warnings

- Automation task name must NOT be null or empty.

Example

Payload without modification	Updated payload
{ "name": "My automation name", "comments": "",	{ "name": "My automation name", "comments": "", "createdBy": "admin",

Payload without modification	Updated payload
"createdBy": "admin", "active": false, "schedule": "", "initialTrigger": "{0}", "triggerType": "CAT_OTHER", "triggers": { .... }, "tasks": [{ "index": 0, "name": "Wait 10 seconds", "group": "WAIT", "subgroup": "DELAY", "properties": [{ "key": "duration", "value": ["10"] }], "timeout": 3600, "onSuccess": null, "onFailure": null }], "notification": { "notifyOnFailure": false, "emails": [] } }	"active": false, "schedule": "", "initialTrigger": "{0}", "triggerType": "CAT_OTHER", "triggers": { ... }, "tasks": [{ "index": 0, "name": "Task waiting for 10 seconds", "group": "WAIT", "subgroup": "DELAY", "properties": [{ "key": "duration", "value": ["10"] }], "timeout": 3600, "onSuccess": null, "onFailure": null }], "notification": { "notifyOnFailure": false, "emails": [] } }

Change automation asset reference

This must be aligned to the asset part of the file (TODO ref part from document). Asset reference values in automation must be present in the asset part.

Asset reference into automation task

Each task have a map of properties of type key<String> and value[<String>].

- Key "groupIds" represent a list of automatic group references.
- Key "asset" represent a list of asset references.

To change those properties edit them for the new value.

Warnings

- Property value could NOT be null or empty.

Example


```
{
  "name": "new-automation",
  "active": false,
  "comments": "",
  "notification": {
    "notifyOnFailure": false,
    "emails": []
  },
  "schedule": null,
  "initialTrigger": "",
  "triggerType": "Manual Override",
  "triggers": {
    "ipmInfraEvent": [],
    "ipmItEvent": null,
    "metricEvents": []
  },
  "tasks": [{
    "index": 0,
    "timeout": 3600,
    "name": "It Action powerOff",
    "group": "ACTION",
    "subgroup": "IT",
    "properties": [{
      "key": "group",
      "value": ["vms"]
    }, {
      "key": "command",
      "value": ["powerOff"]
    }, {
      "key": "asset",
      "value": []
    }, {
      "key": "groupIds",
      "value": ["5"]
    }],
    "onSuccess": null,
```

```
{
  "name": "new-automation2",
  "active": false,
  "comments": "",
  "notification": {
    "notifyOnFailure": false,
    "emails": []
  },
  "schedule": null,
  "initialTrigger": "",
  "triggerType": "Manual Override",
  "triggers": {
    "ipmInfraEvent": [],
    "ipmItEvent": null,
    "metricEvents": []
  },
  "tasks": [{
    "index": 0,
    "timeout": 3600,
    "name": "It Action powerOff",
    "group": "ACTION",
    "subgroup": "IT",
    "properties": [{
      "key": "group",
      "value": ["vms"]
    }, {
      "key": "command",
      "value": ["powerOff"]
    }, {
      "key": "asset",
      "value": []
    }, {
      "key": "groupIds",
      "value": ["2"]
    }],
    "onSuccess": null,
    "onFailure": null
  }]
```

```
{
  "name": "new-automation3",
  "active": false,
  "comments": "",
  "notification": {
    "notifyOnFailure": false,
    "emails": []
  },
  "schedule": null,
  "initialTrigger": "",
  "triggerType": "Manual Override",
  "triggers": {
    "ipmInfraEvent": [],
    "ipmItEvent": null,
    "metricEvents": []
  },
  "tasks": [{
    "index": 0,
    "timeout": 3600,
    "name": "It Action powerOff",
    "group": "ACTION",
    "subgroup": "IT",
    "properties": [{
      "key": "group",
      "value": ["vms"]
    }, {
      "key": "command",
      "value": ["powerOff"]
    }, {
      "key": "asset",
      "value": [
        "vm-125-…075b",
        "vm-127-…075b"
      ]
    }, {
      "key": "groupIds",
      "value": []
    }],
```

<table>
<tr>
<td>

<pre>
    "onFailure": null
  }]
}}
</pre>

</td>
<td>

<pre>
}}
</pre>

</td>
<td>

<pre>
    "onSuccess": null,
    "onFailure": null
  }]
}}
</pre>

</td>
</tr>
</table>

The first payload (1st column) represents the original payload with action on automatic group 5.

The second one is modified on automatic group from 5 to 2.

The third one is now on some virtual machine assets but not on automatic group anymore.

Asset reference into automation trigger

Field “ipmInfraEvent” is a rule-based trigger list. This MUST be aligned to alert engine part. (TODO reference alert engine srr part)

Field “metricEvents” is a metric based trigger list.

To change the asset reference from those kinds of trigger please modify the 'assets' field which represents the asset list used for this trigger.

Example

<table>
<tr>
<td>

<pre>
{
  "name": "My automation name",
  "comments": "",
  "createdBy": "admin",
  "active": false,
  "schedule": "",
  "initialTrigger": "{0}",
  "triggerType": "CAT_OTHER",
  "triggers": {
    "ipmInfraEvent": [{
      "index": 0,
      "operator": "and",
      "templateName":
"input_voltage_low@__name__.rule",
      "assets": [
        "ups-23"
      ],
      ...
}
</pre>

</td>
<td>

<pre>
{
  "name": "My automation name",
  "comments": "",
  "createdBy": "admin",
  "active": false,
  "schedule": "",
  "initialTrigger": "{0}",
  "triggerType": "CAT_OTHER",
  "triggers": {
    "ipmInfraEvent": [{
      "index": 0,
      "operator": "and",
      "templateName":
"input_voltage_low@__name__.rule",
      "assets": [
        "ups-42"
      ],
...
}
</pre>

</td>
</tr>
</table>

This is to change a trigger source (here, the one of trigger index 0) from asset “ups-23” to asset “ups-42” in ipmInfraEvent case.

Below is the equivalent in the metricEvents case.

<table>
<tr>
<td>

```
{
  "name": "Utility return",
  "comments": "",
  "createdBy": "admin",
  "active": false,
  "schedule": "",
  "initialTrigger": "{0}",
  "triggerType": "CAT_OTHER",
  "triggers": {
    "ipmInfraEvent": [],
    "metricEvents": [
      {
        "index": 0,
        "assets": [
          "ups-59489058"
        ],
        "operator": "OR",
        ...
}
```

</td>
<td>

```
{
  "name": " Utility return ",
  "comments": "",
  "createdBy": "admin",
  "active": false,
  "schedule": "",
  "initialTrigger": "{0}",
  "triggerType": "CAT_OTHER",
  "triggers": {
    "ipmInfraEvent": [],
    "metricEvents": [
      {
        "index": 0,
        "assets": [
          "ups-2256789"
        ],
        "operator": "OR",
...
}
```

</td>
</tr>
</table>

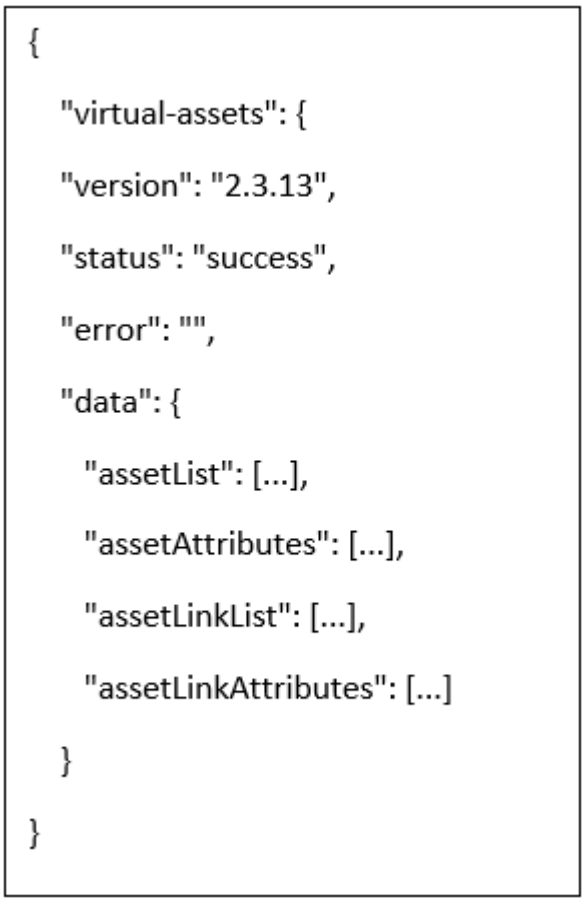
5.4.3 Customize Connectors in a file saved by IPM Editions

Introduction

Virtual assets are saved into the json object called “virtual-assets” and inside this object the assets are represented generically under two main json objects:

- "assetList" : which holds the identifier and type infos of virtual assets.
- "assetAttributes": which holds their attributes.

Note that the only virtual assets that are configurable in this json are connectors, when a connector is well configured, all the other virtual assets (Clusters, Hypervisors, vApps, VMs, etc.) are automatically discovered by IPM.



Below is a list of what is allowed to change into each connector.

Change connector URL and port

Under assetAttributes, look for the attribute object with the key equals to "URI" and modify the corresponding "value" accordingly.

Warnings

- Make sure the attribute linked asset is the corresponding connector that you want to modify.
- Both hostname and IP Address of the connector are accepted.
- the value field cannot be null or empty and should follow the RFC 3986 - Uniform Resource Identifier (URI) standard.

Example


```
{
  "virtual-assets": {
  "version": "2.3.13",
  "status": "success",
  "error": "",
  "data": {
    "assetList": [...],
    "assetAttributes": [
      {...},
      {
        "id": 420,
        "asset": {
          "id": 31,
          "name": "connector-31"
        },
        "key": "URI",
        "value": "https://my.vcenter.com:443"
      },
      {...}
    ],
    "assetLinkList": [...],
    "assetLinkAttributes": [...]
}
```

```
{
  "virtual-assets": {
  "version": "2.3.13",
  "status": "success",
  "error": "",
  "data": {
    "assetList": [...],
    "assetAttributes": [
      {...},
      {
        "id": 420,
        "asset": {
          "id": 31,
          "name": "connector-31"
        },
        "key": "URI",
        "value": "https://192.168.100.200:8443"
      },
      {...}
    ],
    "assetLinkList": [...],
    "assetLinkAttributes": [...]
}
```


Change connector credentials

Under assetAttributes, look for the attribute object with the key equals to "credentials" and modify the corresponding "value" accordingly.

Warnings

- Make sure the attribute linked asset is the corresponding connector that you want to modify.
- the value field cannot be null or empty and should follow the following format: "*login::<USERNAME>|password::<PASSWORD>|adaptorType::<ADAPTOR>*".
- Do NOT modify the adaptorType.

Example


```
{
  "virtual-assets": {
  "version": "2.3.13",
  "status": "success",
  "error": "",
  "data": {
    "assetList": [...],
    "assetAttributes": [
      {...},
      {
        "id": 417,
        "asset": {
          "id": 31,
          "name": "connector-31"
        },
        "key": "credentials",
        "value":
"login::myuser|password::mypwd|adaptorType::vmware"
      },
      {...}
    ],
    "assetLinkList": [...],
    "assetLinkAttributes": [...]
```

```
{
  "virtual-assets": {
  "version": "2.3.13",
  "status": "success",
  "error": "",
  "data": {
    "assetList": [...],
    "assetAttributes": [
      {...},
      {
        "id": 417,
        "asset": {
          "id": 31,
          "name": "connector-31"
        },
        "key": "credentials",
        "value":
"login::user2|password::otherpwd|adaptorType::vmware"
      },
      {...}
    ],
    "assetLinkList": [...],
    "assetLinkAttributes": [...]
```

6 Appendix III - Using the command line interface (CLI)

6.1 Introduction

IPM Editions comes with some commands one can use in a shell console or inside scripts.
This allow to interact with the system without starting the graphical user interface and to streamline some processes one would like to automate.

The commands are accessible using the hypervisor console or using ssh on the port 22 or 4222.

6.2 List of available commands

6.2.1 license-agreement.sh

Description

This command allows to go through EULA acceptance step programmatically.
This is useful when starting a new IPM Editions instance for the first time.
This acceptance step blocks the start of some key services of the system and must be passed to have a fully functional instance of IPM Editions.

Syntax

```
$ /usr/share/fty/scripts/license-agreement.sh -h
Usage: license-agreement.sh [options...]
   --host|-h <hostname> (default: 'localhost')
   --port|-p <port> (default: '443')
   --user|-u <username> (default: connected user 'admin')
   --ntry|-n <number-of-tries> (default: 3, min: 1)
   --help

Example (connected as admin):
$ /usr/share/fty/scripts/license-agreement.sh
Confirm that you agree with the EULA by entering password for user
'admin' (<CTRL+C> to cancel): [password + enter]
{"accepted":"yes","version":"1.0","accepted_version":"1.0","accepted_at":"16116464
41","accepted_by":"admin"}
License is accepted
```

6.2.2 license-activation.sh

Description

This command allows to do a online activation of a licensing id. You must be registered on licensing portal before to be able to do online activation. An internet connect is required and a proxy could be needed.

Syntax

```
$ /usr/share/fty/scripts/etn-license-activation.sh -h
 Usage: etn-license-activation.sh [options...] <command>
 Commands:
 test_online
 activate_online [options...]
 --id|-i <activationID>
 --help|-h


Example to test network capabilities for activation (as 'admin'):
 $ /usr/share/fty/scripts/etn-license-activation.sh test_online

Example to activate a license id (as 'admin'):
 $ /usr/share/fty/scripts/etn-license-activation.sh activate_online -i
myActivationID
 Note: test of network caps is done automatically
```

6.2.3 certcmd

Description

Command line interface for certificate manager daemon (certmanagd)

Syntax

```
$ /usr/bin/certcmd
```

--help : Display help info
--list : List the types of services supported.
--reload :
  <--reload network> : Notify the network about change in networks to all services depend on that network.
  <--reload time> : Notify the time change in time to revoke/add a certificate.

```
Usage: certcmd <service id> <target> <action> [<parameter>]
```

<service id> : Id of the service
<target> :
  - server - action: getcsr/createcsr/applycrt/getkey/revoke/info/detail/details/getcert
  - ca - action: revoke/add/list/info/details/path/getcert
  - client - action: revoke/add/list/info/details/path/getcert
  - config - action: reload
<action> :
  - reload - Only works with 'config' target option but not defined yet.
  - getcsr - Get the server CSR contents.
  - getcsrinfo - Get the server CSR detailed information.
  - getcsrtimestamp - Get the server CSR generation timestamp in GMT.
  - createcsr - Create a CSR for a server target.
  - applycrt [file] - Upload a user given certificate for the server CSR. This will replace the CSR with the certificate given.
It takes the certificate in PEM format from standard input if no file is given.
  - getkey - Get the private key of the active server certificate.
  - revoke [certId1] ([certId2] ...)
    - For server, it revoke the server active certificate. No arg needed.
    - For ca, it revokes the requested CA certificates.
    - For client, it revokes the requested Client certificates.
  - add <path> - Only works for ca/client with arg. it will add the new certificate given.
  - list - Only works for ca/client with arg. Get the CA/Client certificate list.
  - info [certId]
    - For server, it provides active certificate information.
    - For CA/Client, it provides requested certificate information.
- details [certId]

  - For server, it provides active certificate detailed information.
  - For CA/Client, it provides the requested certificate detailed information.
- getcertinfo [certId]
  - For server, it provides active certificate information, similar to detail command.
  - For CA/Client, it provides the requested certificate information similar to detail command.
- path
  - For Server, it returns the active certificate path.
  - For CA/Client, it returns the requested certificate path.
- getcert [certId]
  - For server, it returns the active certificate contents.
  - For CA/Client, it returns the requested certificate contents.
- help

```
Example to revoke the certificate for https service (produces a new self-signed
one)

 $ certcmd https server revoke

Example to generate a CSR for https service and export the request in PEM format

 $ certcmd https server createcsr
 $ certcmd https server getcsr

Example to import a signed certificate for https service

 $ certcmd https server applycrt <path/to/cert/file>
```

6.2.4 fty-srr-cmd

Description

This command allows to use Save and Restore in command line. I can be use to do mass configuration using a restore file as template.

Syntax

```
$ /usr/bin/fty-srr-cmd

Usage: fty-srr-cmd <list|save|restore|reset> [options]

 -h, --help Show this help
 -p, --passphrase Passphrase to save/restore groups
 -pwd, --password Password to restore groups (reauthentication)
 -t, --token Session token to save/restore groups if needed [default:
1Hvq2h89t5TslTAgXuWbDzRy]
 -g, --groups Select groups to save (default to all groups)
 -f, --file Path to the JSON file to save/restore. If not specified, standard
input/output is used
 -F, --force Force restore (discards data integrity check)

Example to save to a file in /tmp/my-save.json
 $ fty-srr-cmd save -p myPassphrase -f /tmp/my-save.json

### - No group option specified
Saving all groups
### Groups available:
 - group-assets
 - group-discovery
 - group-mass-management
 - group-monitoring-feature-name
 - group-network
 - group-notification-feature-name
 - group-user-session-management
Request status: success
```

```
Example to restore from a file stored in /tmp/my-restore.json
 $ fty-srr-cmd restore -p myPassphrase -pwd myLogginPassord -f /tmp/my-
restore.json
```

6.2.5 setUpFqdnForCertificate.sh

Description

This script check that the string is an fqdn and add it to system. If syntax correct => add it to /var/lib/fty/certmanagd/domain/fqdn.txt.

Syntax

$ /usr/bin/setUpFqdnForCertificate.sh

```
Usage: ./setUpFqdnForCertificate.sh <fqdn-string>
```

```
Example: $ cd /usr/bin/ && ./setUpFqdnForCertificate.sh some.fqdn-string
```

6.2.6 Remote syslog

Description

Following tools allow the setup of a remote syslog server.

Syntax

syslogconfig [OPTION] [<args>]

OPTION:

--help
display help

--show
display current server configurations

--delete-all
delete all server configurations

--delete <index>*N
delete server configuration by indexes <index> : integer > 0

--add
declare a new server configuration get user input from console variables are: 'friendlyName' : name of the configuration (string value, non empty) 'address' : the address of the server (string value, non empty) 'port' : the port to connect the server (integer value, strictly positive) 'enabled' : enabled state of the configuration (string value, <yes|no|1|0>)

--update <index>
update single server information to skip field press Enter

--enable <index>*N
if no index => activate remote syslog from server(s) configuration if index presented => activate server(s) with index <index> : integer > 0

--disable <index>*N
if no index => deactivate remote syslog from server(s) configuration if index presented => deactivate server(s) with index <index> : integer > 0

--global
get user input from console activate or deactivate remote syslog from server(s) configuration

Examples

display help
```
syslogconfig --help
```

display all server configurations
```
syslogconfig --show
```

delete all server configurations
```
syslogconfig --delete-all
```

delete server configuration at index 1
```
syslogconfig --delete 1
```

add a new server configuration (console inputs)
```
syslogconfig --add
```

edit a server configuration at index
```
syslogconfig --update 1
```

activate remote logging from the current server configurations
```
syslogconfig --enable
```

deactivate remote logging
```
syslogconfig --disable
```

activate server with indexes
```
syslogconfig --enable 1 3 2
```

deactivate server with index
```
syslogconfig --disable 1
```

7 Appendix IV - Configuring EasyE4 PLC with IPM

Using EATON EasyE4 PLC with IPM2 requires the following:

- an EATON EASY-E4-UC-12RC1, wired and powered
- the EasySoft application and a license to use it, to configure EasyE4 and load the program to run it and interact with IPM2.
  You can download this application from easySoft | Eaton.

In order to configure EasyE4, please follow the below instructions.

7.1 Wiring and powering of your EasyE4

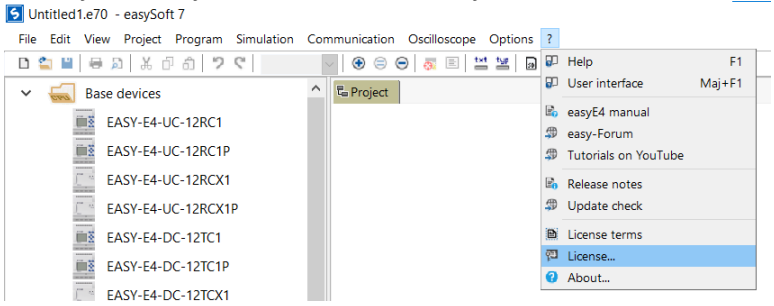
Prior to powering on your EasyE4, you need to connect:

- the power supply (*DC 12/24 V*) on the *+UC* connector
- the neutral on the first *0V*

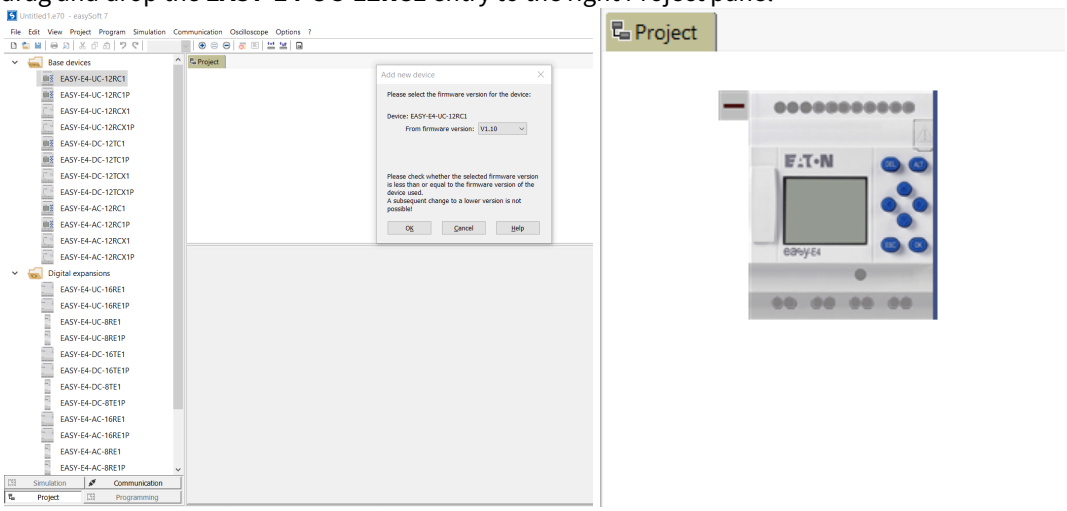
For more information, please refer to the EasyE4 User Documentation.

7.2 Connect to EasyE4

- Launch EasySoft
- Possibly activate your license, if not already done, from the *?* → *License* menu

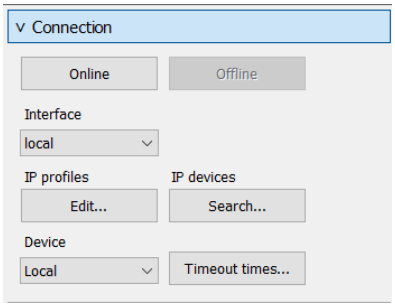


- From the *Project* section (bottom left corner)
  - drag and drop the **EASY-E4-UC-12RC1** entry to the right Project panel

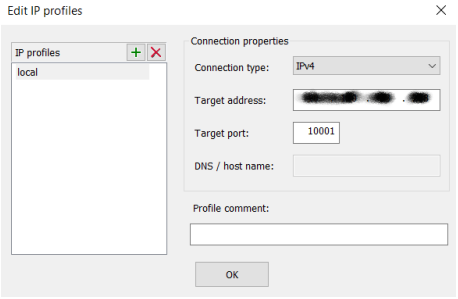


  - Click OK when prompted to *Add new device*
- From the *Communication* section (bottom left corner)

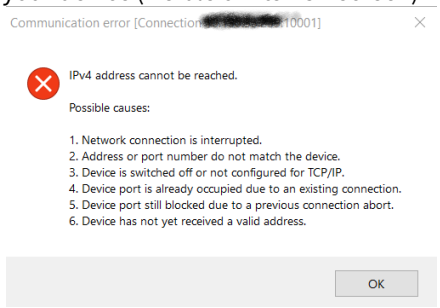
- Under the *Connection* section



- Select *IP Profiles* → *Edit...* and enter the IP address of your EasyE4 in the *Target address* field



- Verify the connectivity using the *Online* button
  - If the connection is established, the *Online* button should be greyed
  - Otherwise, an error will be displayed. In this case, please verify your settings and the IP address of your device (visible on its LCD screen)

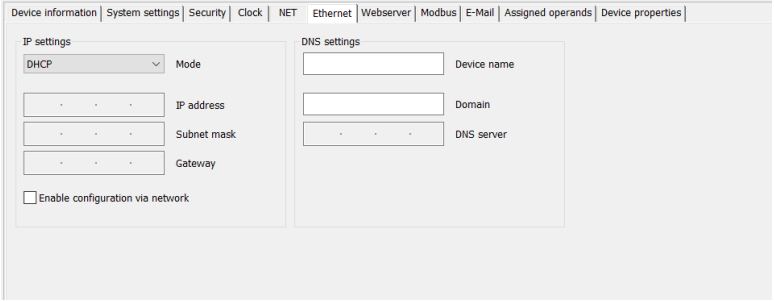


- Now save your project, using File → Save

7.3 Complete the configuration and activate the Modbus protocol

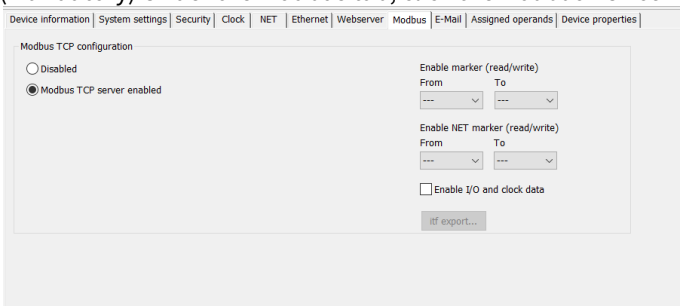
Still from the *Communication* section (bottom left corner)

- You may possibly modify the device configuration, according to your needs.
  - For example, you can modify its network configuration (DHCP, static IP, ...) under the Ethernet tab



  - For more information, please refer to the EasyE4 User Documentation

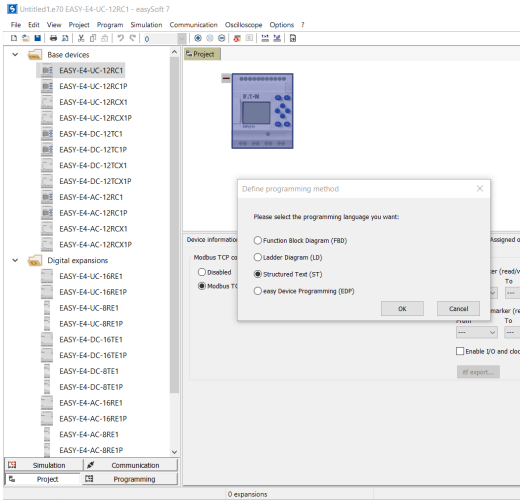
- (Mandatory) Under the Modbus tab, click the *Modbus TCP server enabled* radio button



7.4 Upload the Program to the EasyE4 PLC

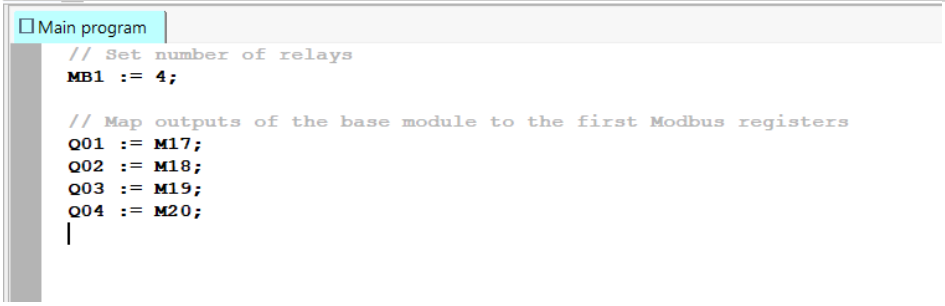
Click on the *Programming* (bottom left corner)

- Select *Structured Text (ST)*



- Copy and Paste the following program

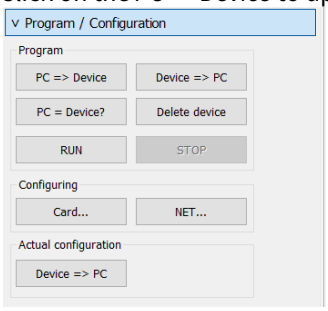
```
// Set the number of relays
MB1 := 4;

// Map outputs of the base module to the first Modbus registers
Q01 := M17;
Q02 := M18;
Q03 := M19;
Q04 := M20;
```



7.5 Apply these changes to your EasyE4

From the *Communication* section (bottom left corner)

- Under the *Program / Configuration* section,
  - Click on the *PC => Device* to upload the program and configuration to your unit



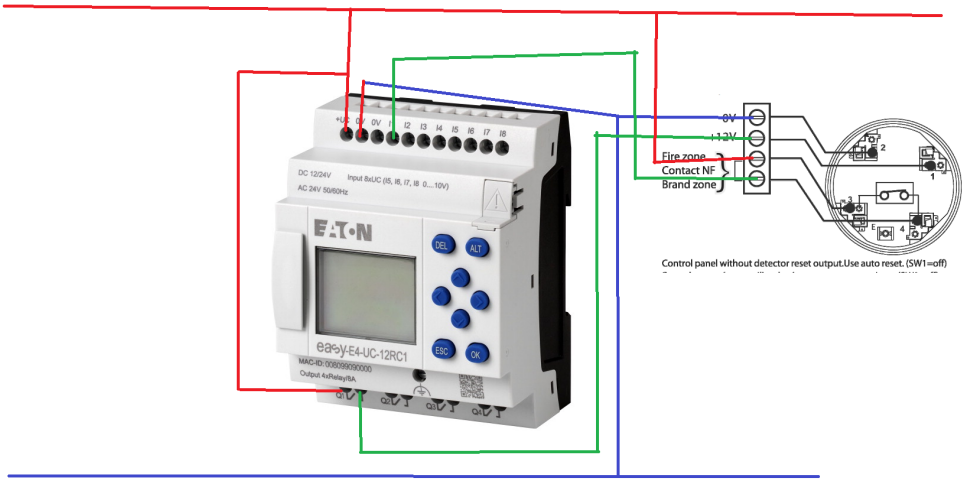
  - Now click on the *RUN* button, to put your unit into production mode

7.6 Connecting devices to the relays of EasyE4

Here are some example of connecting devices to EasyE4 outputs:

- Eaton SL4 LED signal towers

- Eaton M12 fire detector



7.7 Connecting your EasyE4 to IPM2

You are now ready to connect your EasyE4 to IPM2, and start to use it.
Please refer to the section ??? for information on how to add and use your EasyE4 with IPM2.

8 Appendix VI - How to set Windows Connector on IPM2

8.1 IPM-2 Microsoft Server/Hyper-V/SCVMM Connectors' Technical Documentation

Here we list the perquisites required to successfully connect to a Microsoft Server/Hyper-V/SCVMM infrastructure from IPM-2

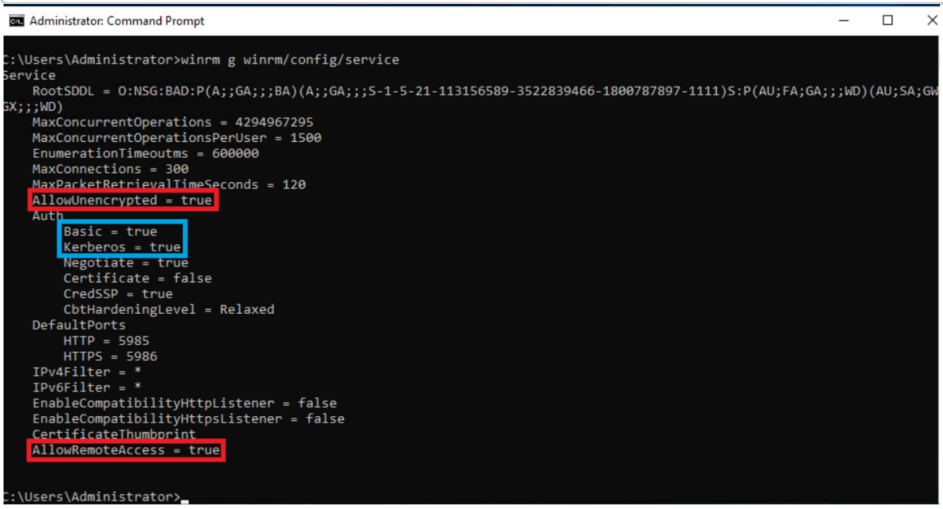
IPM-2 uses WinRM (wsMAN) in order to successfully connect to a Microsoft system, sometimes a special setting is needed to be configured properly

- To quickly configure WinRM for the first time use the following command:

```
winrm quickconfig
```

- To access WinRM configuration in the Microsoft System you want to connect to, execute the following command in a Command Prompt with Administrator privileges:

```
winrm g winrm/config/service
```



8.1.1 Create Microsoft Server/Hyper-V/SCVMM Connector - Prequesties:

First, In the Microsoft System you want to connect to, make sure that WinRM is configured to allow remote access and with the following command:

```
winrm s winrm/config/service @{AllowRemoteAccess="true"}
```

8.1.2 IPM-2 supports two different connection modes with a Microsoft System:

Unsecured Connection

If you want to use Unsecured connection (using the HTTP port) to connect to the Microsoft System, make sure to allow unencrypted access with the following command:

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

Also make sure that you already have an HTTP listener configured with the following command:

```
winrm e winrm/config/listener
```

Secured Connection

If you want to use secured connection (using the HTTPS port) to connect to the Microsoft System, make sure to have the HTTPS listener already set with the following command:

```
winrm e winrm/config/listener
```

To configure an HTTPS listener in the Microsoft System that already have a personal certificate installed (certificate must not be expired, revoked, or self-signed and has a CN matching the hostname) simply run the following command:

```
winrm quickconfig -transport:https
```

Otherwise, you need to open powershell then have to create a self-signed certificate and manually configure the HTTPS listener with the following commands:

```
New-SelfSignedCertificate -DnsName "Hostname" -CertStoreLocation Cert:\LocalMachine\My
```

Then copy the thumbprint of the self signed certificate to clipboard and use it for the following command:

```
winrm create winrm/config/Listener?Address=*+Transport=HTTPS '@{Hostname="Hostname";
CertificateThumbprint=" 998BC9E23E7292FCA3135BE9C658FECEB193A55E"}'
```

Then add a firewall rule to allow the WinRM HTTPS port (5986 by default) with the following command:

```
netsh advfirewall firewall add rule name="Windows Remote Management (HTTPS-In)" dir=in
action=allow protocol=TCP localport=5986
```

8.1.3 IPM-2 supports two different Authentication methods with a Microsoft System:

Basic Authentication

To use Basic Authentication, make sure that WinRM allows Basic authentication with the following command:

```
winrm s winrm/config/service/Auth @{Basic="true"}
```

Then in IPM-2 create your connector with the local user credential, for example: *Administrator*

NOTE: Secured Connection with Basic Authentication is not supported for SCVMM. however, to use Unsecured Basic the local user user must have enough rights to access the SCVMM inventory (see appendix-1 for more info).

Kerberos Authentication

To use Kerberos Authentication, make sure that WinRM allows Kerberos Authentication with the following command:

```
winrm s winrm/config/service/Auth @{Kerberos="true"}
```

/!\ In addition, IPM-2 must be configured properly to be able to authenticate with the Kerberos Domain Controller /!

One of the following must apply:

- IPM-2 OVA in integrated into the domain's Active Directory: (see how-to)
- IPM-2 OVA is deployed in a hypervisor belonging to the domain.
- the Domain Controller IP address is set as a DNS in the IPM-2 Network configuration.

Then in IPM-2 create your connector with the domain user credential, the user name must have the form
user@FULL.QUALIFIED.DOMAIN.NAME or FULL.QUALIFIED.DOMAIN.NAME/user
for example: Administrator@MBT.LAB.ETN.COM or MBT.LAB.ETN.COM/Administrator

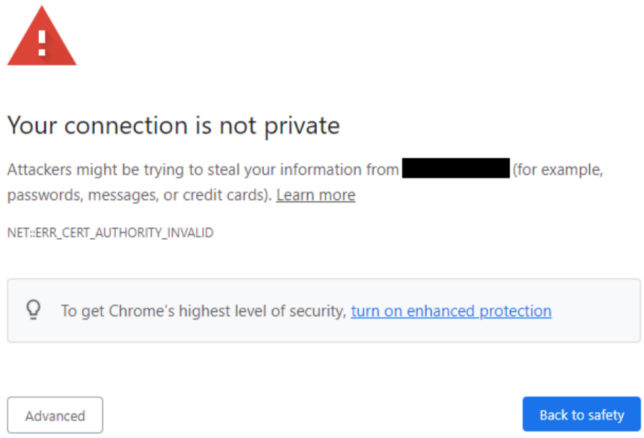
8.1.4 Appendix-1: Connection/Authentication status table

Connector type	Connection mode	Authentication mode	Status
Server/HyperV	HTTP	BASIC	Ok
		Kerberos	Ok
	HTTPS	BASIC	Ok
		Kerberos	Ok
SCVMM	HTTP	BASIC	Ok
		Kerberos	Ok
	HTTPS	BASIC	Ko
		Kerberos	Ok

9 Appendix VII - How to add certificate on IPM2

9.1 Explaining how to create a certificate

By default, every Eaton device is containing a self-signed certificate. This one permits us to use the https connection but, due to the self generation, the certificate is displayed as unsecured by web browsers.



The goal of this documentation is to explain how-to add a signed certificate to IPM2.

As a reminder, there is, for the moment, no capability to add the certificate from the Web User Interface on IPM 2.

9.1.1 Generating the certificate signing request (CSR)

If you want to certify your web server, it will be necessary to use the Command Line Interface.

1. Open a ssh connection (putty can be used for the connection)
2. Log with your admin account
3. Create the CSR to share with your Certificate Authority : certcmd https server createcsr
4. Display the CSR and copy it : certcmd https server getcsr

9.1.2 Adding the certificate to IPM2 (CRT)

1. Once you have this part, the next one is to obtain your CRT from your certificate authority. Once you have retrieved this CRT, this one can be added to the PEM or to the CRT format on IPM2.
2. Open Winscp and connect by using SCP protocol to your IPM2
3. Put the CRT file into /tmp/yourcertificate.crt
4. Open putty again then go to your account
5. Type certcmd https server applycrt /tmp/yourcertificate.crt
6. Your IPM2 web server is now certified.