

Eaton[®] Intelligent Power Manager [®] (IPM) Editions User guide

Eaton is a registered trademark of Eaton Corporation or its subsidiaries and affiliates.

Phillips and Pozidriv are a registered trademarks of Phillips Screw Company.

National Electrical Code and NEC are registered trademarks of National Fire Protection Association, Inc.

Microsoft®, Windows®, and Windows Server® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

UNIX® is a registered trademark of The Open Group.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions.

Google™ is a trademark of Google Inc.

All other trademarks are properties of their respective companies.

©Copyright 2017 Eaton Corporation. All rights reserved.

No part of this document may be reproduced in any way without the express written approval of Eaton Corporation.

Table of Contents

1	General information	9
1.1	The virtual appliance	9
1.1.1	Technical specifications	9
1.1.2	Virtual appliance console	9
1.2	Initial setup & configuration	
1.2.1	Initial commissioning	
	Login Wizard	
	Initial Login	
	End User License Acceptance	
	Network configuration	
	Data center creation (Optional)	
	Data center layout configuration (Optional)	
	Software license or subscription configuration	
	Finalize data center asset configuration	15
1.3	Asset Management	
1.3.1	Asset Management from the User Interface	
	Asset creation	
	Input Power Chain Configuration	
	Manually add a new asset	
	Edit an existing asset	
	Asset Mass configuration	
	Dynamic groups of assets	23
1.3.2	T&H Sensors Management	25
1.3.3	ePDU G3/G3+ Daisy Chaining	27
1.3.4	How to use the CSV file for commissioning	
	Initial CSV Creation	
	CSV upload	
	Upload Errors	
1.4	Alarms Management	
1.4.1	Introduction	
1.4.2	Alarm Lifecycle	
1.5	User Management	35
1.5.1	Local Users	35
1.5.2	Remote Users	
1.6	Automation	
1.6.1	Trigger events	
1.6.2	Actions	

	IT actions supported	
1.7	Xtreme Support Process	
1.8	Supported Power Chain Topologies	43
1.8.1	Supported configurations for the input power infrastructure	43
1.8.2	Local power redundancy schemes supported	45
1.9	Cybersecurity	45
1.9.1	Eaton cyber security notifications	45
1.10	Licensing	
1.10.1	Initial trial period	
1.10.2	Online license or subscription activation	47
1.10.3	Offline license or subscription activation	
1.10.4	Other license activations	
1.10.5	What does licensing do?	
1.10.6	How node credits are counted?	
	Credit count evolution through a simple example	
	All impacts of assets activation status	51
1.11	Graphite / Grafana deployment	51
1.11.1	IPM Editions graphite connector configuration	51
	Query	53
	Using the REST API to display the Asset ID - Asset name mapping	54
	Visualization	54
2	Contextual Help	55
2.1	Login page	55
2.1.1	Initial login	55
	1. Enter default password	55
	2. Enter the login wizard	55
2.2	Dashboard View	
2.2.1	Overview	56
2.2.2	Navigation within the application	57
2.3	Power Chain View	57
2.4	Rack View	
2.5	Power Monitoring View	62
2.5.1	Overview	62
2.6	UPS View	63
2.7	ePDU View	64
2.7.1	Overview	64
2.7.2	Main view	65
2.7.3	Side view	65
2.8	Environmental View	65
2.9	Asset Management View	66

2.9.1	Types of assets	67
	Facility assets	
	Location	
	IT assets	
	Virtual Assets	
2.9.2	Primary asset actions	
	Auto Discovery	
	Upload CSV file	74
	Add New Asset	74
	Add Connector	75
	Export Assets	75
	Delete Asset	75
2.9.3	Asset list statistics and report	75
	Asset List	
2.10	Asset mass configuration view	
2.10.1	Configure NMC or G3 cards	
2.10.2	Configure Network M2 card	
2.11	Automation view	
2.11.1	Overview	
2.11.2	Automation main page	
	Automation List	85
	Automation Settings	
	Define the triggering events	
	Define the action(s)	
2.12	Status dashboard	
2.13	Setting Views	
2.13.1	Account settings	
2.13.2	Alarms settings view	
	Data Center Alarm Settings	
	UPS Alarm Settings	
	Row Alarm Settings	
	Rack Alarm Settings	
	PDU Alarm Settings	
	ATS/STS Alarm Settings	
2.13.3	Connectors	
	Overview	
2.13.4	Datacenter Layout	
2.13.5	Date & time	
2.13.6	License	
2.13.7	Monitoring	

	SNMP	107
	Graphite connector (optional)	108
2.13.8	Network settings view	109
2.13.9	Security wallet	109
	Create a new SNMP v1 credential	110
	Create a new SNMP v3 credential	110
	Create a new Basic credential	111
	Delete a credential	112
	Credential usage in user scripts	112
2.13.10	Notifications	113
2.13.11	Upgrade view	113
	Overview	113
	Upgrade Devices	115
2.13.12	Local Users View	115
	Local users accounts list	115
	Actions	116
	Global user settings	117
2.13.13	Remote Users View	119
	LDAP support	119
2.13.14	Save & Restore view	
	Overview	122
2.14	Alarms View	125
2.15	Feedback Tool	126
3	Troubleshooting	128
3.1	Connector connections	128
3.2	Factory Reset	128
3.2.1	Virtual appliance version	129
	Virtual appliance console	129
3.3	Procedure to collect all required data to get some support	129
4	Appendix I - Migrating from IPM Infrastructure 1.5 to IPM Understand Edition 2.3.0 32	or better 1
4.1	How can I get the right license to move from IPM Infrastructure to IPM Understand Edition?	132
4.2	How can I migrate my configuration from IPM Infrastructure 1.5 to IPM Understand Edition?	132
4.2.1	On IPM Infrastructure 1.5	132
4.2.2	On your computer	132
4.2.3	On IPM Understand Edition	132
5	Appendix II - Save and Restore file	133
5.1	Introduction	133
5.2	File global structure	133
5.3	List of groups and features	135

5.4	"Asset management" (group-assets)	
5.4.1	Customize Physical Assets	
	Introduction	
	Change asset name	
	Change SNMP connection settings	
5.4.2	Customize Automations	
	Introduction	
	Change automation name	
	Change automation task name	
	Change automation asset reference	
5.4.3	Customize Connectors in a file saved by IPM Editions	
	Introduction	
	Change connector URL and port	
	Change connector credentials	
6	Appendix III - Using the command line interface (CLI)	153
6.1	Introduction	
6.2	List of available commands	
6.2.1	license-agreement.sh	
	Description	
	Syntax	
6.2.2	license-activation.sh	
	Description	
	Syntax	
6.2.3	fty-srr-cmd	
	Description	
	Syntax	

1 General information

1.1 The virtual appliance

All IPM Editions (version 2.0.0 and higher for IPM Understand, 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)

(i) 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.

To access the IPM Editions VA console through ssh: Connect with ssh client to IP: 10.1 You can also select to: Login on the local interactive console 2 Factory Reset and reboot 3 Reboot 4 Execute System Diagnostic 5 Network Settings		IPM Editions VA Editions VA web interface: browser to https://10.1	
2 Factory Reset and reboot 3 Reboot 4 Execute System Diagnostic 5 Network Settings	Connect with ssh c	lient to IP: 10.1	
	234	Factory Reset and reboot Reboot Execute System Diagnostic	
		<mark>< <u>0</u>K ≫</mark>	

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

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

(i) 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.

1.2 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.

Ir	ntelligent Power Manager Infrastructure
Username	Username
Password	Password
	Login Eorgot your password 2
	Anwering Business Worldwide

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:

Jsern	ame	e = a	adm	nin
Passv	vord	= a	dm	in

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

(i) 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.

(i) 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

Change Password
Please change your password before continuing. User admin Current Password
New Password
Repeat New Password
Password Strength 🔮
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.

License Agreement	
Note: Code York, Nature 1. Node services and internate of period under this Agreement. 1.5. "Source Code" means all or any portion of human restable software code. For Clarity, Source Code Includes scripts which are in human restable format 1.5. "Software Components" means software components, modules, functional blocks, libraries and organized groups of lines of codes.	^
2. The headings in this Agreement do not affect its interpretation.	
 In the event of any conflict between this Agreement and other documents entreed into between the Parties the order of proceedings shall be: 	
3.a. any signed, written contractual Agreement between faton and the ind-User splicitly over-riding or contradicting specific terms in this agreement;	
3.b. This agreement 3.c. the Appendices to this Agreement;	
3.d. Eaton's terms and conditions of sale (if applicable); and	
3.e. any other documents referred to, incorporated into or attached to any of the documents contemplated in paragraphs a to d above.	
APPENDIX 2 ADDRESSES FOR NOTIFICATIONS	
Eaton:	
EH6A IP Group Eaton Legal Department	
Eaton Industries Haufraturing GebH	
Note: on la congersite / 1110 Monges VD, Switzerland	
I have read & agree to all terms above.	- 6
	*
•••••	

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**.

				nfiguration pa to restart the r		e automatically logged out whe es.	n all
Network configuration							
Default Location / Networ	k prefix						
Definit general 10.1 Drs Settings Donan name server 127.0.0.11	Alternate Domain name server		Proxy settings HTTP address				
Time Time Topsamic (NTP) Manual No server address * pool.ntp.org							
		••			Next		

Data center creation (Optional)

or

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

- Configure Datacenter information such as Datacenter Name, Max power consumption, Power feeds, ...
- Skip this optional step if Datacenter Power and Spatial topologies are not important for you. You will be directly re-directed to the Licensing page

	uired fields marked with an location hierarchy (Data cen		atory. Also note that the system has cks -> devices).
Datacenter Name			
Datacenter Power Location Of Congrege private targe scalar of a congrege private targe scalar of a congrege private targe scalar of the scalar	Asset Tag		
Power Feed(s)			
Feed 1 Imma FeedNe Coupe Thema I I Stans Active (default) Prany Prany Ps V			
Previous	0000	Skip Next	

Data center layout configuration (Optional)

On the following step you are able to create the Data Center Layout.

You may specify the **data center topology** including the **number of Rooms, Rows and Racks** present in the data center.

The **default Rack U size is 42**. It can be modified in the Asset page (see Asset management for more details).

Datacenter Layout		
Data Center Layout		
Rack Unit Default Rock Default Height 42. [5]	Layout Design Recent 0 × ADD ROOM	
This settings will create default placeholders for yout devices. Devices can be added once the auto-discovery is launched after completing this set up or any time from the Assets Manager page. Custom Locations, Layouts, Rack size and placement can be updated anytime using the	Room Name Room Role Nr Ros Room 0 4 5 (8)	
Assets Manager' feature.	Row Yaona Row O	\ominus \oplus
	Row 1	⊖ ⊕
	Row Abra	⊝ ⊕
	Row 3	⊝ ⊕
Previous	00040	Skip Next

This wizard step will automatically generate the specified topology with the desired number of Rooms, Rows and Racks.

ONOTE The data center layout can be updated later on from the Setting Views page.

Software license or subscription configuration

At this stage, you are prompted for a license key. You have 7 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.

	e activation	
Activa	on id *	
Don't	ave an activation code ? Find your reseller	
	vatë license online	
You	may activate your software license later. You will then have 7 days to do it from the menu Settings / License.	
Onl	e activation is disabled because your IPM infrastructure is not connected to internet.	
	activation	
1	Export the activation request	Export
2	Send the activation request to the Eaton website to get the license file	Open Eaton website
3	Import the license file to software (No file selected)	Import file
Previo	5	•

- To proceed without a license key, click the Skip & Import/Create devices button.
- To activate a license, enter a **valid activation ID** and click **Continue**.

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

(i) **NOTE** If network parameters have been changed, you will be automatically logged out after this screen and will be required to log in to start a new session.

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
- 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.

Asset creation

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

From the Dashboard, the user can access the page from the top menu Asset management. All possible operations on assets are accessible through the page menu:

≡	Intelligent Power Manager 2.3.0	All Assets	
	Dashboard	ADD ASSETS 👻	
٠	Power	AUTO DISCOVERY	Virtual Asset
٥	Environment	UPLOAD CSV FILE	
-	Assets	ADD ASSET	
¢,	Automation	ADD CONNECTOR	Name 🕈
0	Status	Active	EDF
\$	Settings	Active	EPDU-RACK01-E

Input Power Chain Configuration

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

- 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 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 Settings page 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.

Next

					A	1 sset type	2 Power details	Additional inf	fo		
Asset Type											
Select the device f	type you want to a	UPS	PDU	Server	Š Sensor	More					
Pdu Type *			PDU								
ePDU (Intell PDU (Basic r	igent Rack Pdu) rack PDU without i	monitoring)									
Auto-Discover A	sset Capabilities	*									
IP or hostname	*			Se	ect Protocol				-	Credential	•

(i) 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 IP Address + Protocol + Credential allows you to discover automatically Asset capabilities

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

← Create Asset (My ePDU)		
Asset type Power details Additional info		
Connect a Power Source to My ePDU		
Power Source	My ePDU	
Select a power source * Lab A1 MBT/EDF) Input : 1	
Back	Additional Information	Finish

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

← Create Asset (My ePDU)			
	00	3	
	Asset type Power de	tails Additional info	
Add additional information (opti	onal)		
Include additional details or skip this step to c	omplete the process		
Manufacturer Details			
Manufacturer name	Model	Serial Number	Warranty Expiration
Contact Details			
Contact Name		Contact Phone	
Other Information			
Asset Tag	0	HTTP Link	
Description			
			ĥ
Back			Finish

(i) **TIP** Make sure you define the **location** of your assets and set them to **Active** in order to get telemetry data.

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 and click on **Edit**.

All Assets							Datacenter LAB-A1-DEV		2021-03-24 16:17:10	?	1
ADD ASSETS	•									EXPOR	RT ASSETS ဈ
Facility Ass	ets IT/	Assets Virtual /	Assets	Location	Automatic Gro	ıps					
			9	31 devices a	are not configured.	<u>Complete setup now</u>	!				
🔍 Configu	ure 📋 De	lete							Sea	rch	
Alarm	Status	Name 🛧	Manufacturer	Model			Creation Date		Con	tact Name	
	Active	EDF					2021-02-027	10:29:29+	0000		:
	Active	EPDU-RACK01-BLUE	EATON	EPDU MA 0	U (309 32A 1P) 28	XC13:4XC19 30B	2021-02-027	10:42:13+	0000		:
	Active	EPDU-RACK01-RED	EATON	EPDU MA 0	U (309 32A 1P) 28	XC13:4XC19 30R	2021-02-027	10:41:30	Edit		
	Active	EPDU-RACK02-BLUE	EATON	EPDU MA 0	U (309 32A 1P) 28	XC13:4XC19 30B	2021-03-22T	09:08:50	6 Show	Device Infor	mation
	Active	EPDU-RACK02-RED	EATON	EPDU MA 0	U (309 32A 1P) 28	XC13:4XC19 30B	2021-03-22T	09:09:57	Show	in Rack	
	Active	EPDU-RACK03-BLUE	EATON	EPDU MA 0	U (309 32A 1P) 28	XC13:4XC19 30B	2021-03-227	09:11:44	To de	vice url	
	Active	EPDU-RACK03-RED	EATON	EPDU MA 0	U (309 32A 1P) 28	XC13:4XC19 30R	2021-03-227	09:10:51	0		

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 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.

	configuration can be copied only to the same type of c the same firmware version. e assets :	evice (card/product/vendor)
UPS/NMC	Network-MS / Modbus-MS cards	
ePDU/G3	ePDU Network management card	
UPS/M2	Network-M2 / INDGW cards (FW version 1.7 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 click on the **Configure** button on top of the asset list.

≡	All Assets					Datacenter LAB-A1-DEV	2021- 16:03	2	1 9 6
H	ADD ASSETS	•						EX	Port Assets 🕻
٠	Facility Ass	ets IT.	Assets Virtual	Assets	Location	Automatic Groups			
٥			0) 31 devices an	e not configured.	<u>Complete setup now</u>			
=	🔾 Config	ure 📋 De	lete				ш	Search	
\$	Alarm	Status	Name 🕈	Manufacturer	Model			Creation D	ate
0		Active	EDF					2021-02-	02T :
\$		Active	EPDU-RACK01-BLUE	EATON	EPDU MA OU	(309 32A 1P) 28XC13:4XC19	30B	2021-02-	02T :
		Active	EPDU-RACK01-RED	EATON	EPDU MA OU	(309 32A 1P) 28XC13:4XC19	30R	2021-02-	02T :
	~	Active	EPDU-RACK02-BLUE	EATON	EPDU MA OU	(309 32A 1P) 28XC13:4XC19	30B	2021-03-	22TI :
		Active	EPDU-RACK02-RED	EATON	EPDU MA OU	(309 32A 1P) 28XC13:4XC19	30B	2021-03-2	22TI :

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

To configure NMC (UPS) or G3 (ePDU) cards, user can select from the source device all the settings to configure or select them individually.

← ups (10.130.35.51)			Jeff-DC	
				BULK APPLY (7)
System Settings Access Control	∧ System Settings			0
Networks Settings	Contact	Eaton Global Tech Support	✓	
Outlets	Location	Labo A2-01, Mbt	~	
Emails	Default Language	ENG	\checkmark	
Network Management System	History Log Interval	180 s	\checkmark	
Environment Sensor	Environment Log Interval	300 s	\checkmark	
Shutdown Schedule Time Settings	 Access Control 		•	
Client Settings	Manager Login	admin	~	
	Password	****	~	
	Security Mode	1		
	Firmware Upload	1		
	SNMP Advanced parameters			
	Teinet Advanced parameters			
	Authentication Advanced parameters			
	 Networks Settings 			

Once all settings are selected, user can choose what are the devices where he wants to apply these settings through "BULK APPLY" function :

← Bulk Apply (7)				🛅 Jeff-DC	٤	
					APP	rLY
						8
Devi	ces to Apply these Settings			1 Devices selected		
	Name	Туре	Credential			
×	ups (10.1 1) (10.1 1)	ups	OUpdate admin NMC/G3			

To configure Network M2 (UPS) cards, user can select from the source device features and not individual settings.

← UPS-EATON-P01				LAB-A1-DEV 🔻	
					BULK APPLY (4)
Account service	~	Account service			
Card	~	Card			
Certificates Date	^	Certificates		~	
Email			50		
LDAP	country state		FR 38	✓ ✓	
Measure	location		Grenoble	✓	
MQTT	organiza	ationName	Eaton	~	
Network	organiza	ationUnit	Power Quality	×	
Power outage policy	contact			×	
RADIUS Remote user	~	Date			
Scheduled shutdown	~	Email			
Sessions settings		LDAP			
• SMTP	~	LUAP			
SNMP	~	Measure			
Syslog	~	MQTT			

Once all settings are selected, user can choose what are the devices where he wants to apply these settings through "BULK APPLY" function :

Once process is complete, IPM will notify that configuration has been applied to the devices selected.

\leftarrow Bulk Apply (3)							🛅 Jeff-DC	۰	
								API	PLY
									0
	Device	s to Apply	these Settings				No Devices selected		
		Name			Туре	Credential			
		ups (10.1	32) GENEPI (10.	.32)	ups	OUpdate admin GEN	EPI		
		ups (10.1	53) GENEPI (10.	53)	ups	OUpdate admin GEN	EPI		

vices to Apply these Settings		2 Devices selecte
Name	Туре	Credential
ups (10.1 32) GENEPI (10.1 32)	ups	OUpdate admin GENEPI
UDS (10.1 53) GENIEDI (10.1 13)	uns	Allodate admin GENED
Configuration end status		
Ø ups (10.1 53) GENEPI		
		CLOSE

Dynamic groups of assets

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

In Automatic Group Tab we provide the possibility to define a dynamic Asset Group by a dynamic rule

Rules are covering the following fields:

- Asset Name
- Asset HostName
- Asset IPAddress
- Asset Location
- Asset Contact
- Hosted By

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

≡	All Assets	5				Datacenter LAB-A1-DEV	2021- 09:22		?	6 2
:	ADD ASSET	5 🗸							EXPORT	ASSETS ᠀
Ŵ	Facility As	sets IT Assets	Virtual Assets	Location	Automatic Groups					
0	🖍 Creat	te					ш	Search		
I		Name †		Grou	ping rule					
\$ 0		BLUE assets			e contains BLUE			:		
0		Hosted by vesxi67-01		host	is vesxi67-01.mbt.lab.etn.com				Edit	
¢		In Rack 1		locat	tion is Rack1			î	Delete	
		In Rack2		locat	tion is Rack2			0		
		RED Assets		nam	e contains RED					
						ltems per	page 25	▼ 1	-5/5	$\langle \rangle$

Create/Edit a Group

- In Automatic Groups Tab click on Create button and following window will appear
- Enter following information :
 - Group Name
 - Enter a first criterion based on:
 - Asset Name
 - Asset HostName
 - Asset IPAddress
 - Asset Location
 - Asset Contact
 - Hosted By feature (e.g. to retrieve the Virtual Machines Hosted By an Hypervisor)
 - Operator is automatically filled (Contains or Is)
 - Enter the filtering expression (Free text field or Location or Host list, ...)
 - Click on Add Criteria if you want to add a second rule (the rules combine with the AND logical operator):

Edit G	roup				
Name BLU	* E assets in Rack 1				
AND	_{field} * Name	 operator * Contains 	•	BLUE	Θ
AND	field * Location	▼ operator * Is	Ţ	Location * Row1Rack1	 - O
					Add Criteria
					Cancel Save

Groups usage

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

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 Autoimation, please refer to the Automation section.

1.3.2 T&H Sensors Management

The T&H sensors are managed as standard 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 sensors connected to Eaton power devices (i.e. UPSs, ePDUs).

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

(i) NOTE

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.

← Create Asset (sensor1)				
	1 2 Asset type Additional info			
Asset Type				
Select the device type you want to add				
Ats-stress Imput Elect Imput Elect <th elect<="" imput="" th=""><th>Š Sensor More</th><th></th><th></th></th>	<th>Š Sensor More</th> <th></th> <th></th>	Š Sensor More		
Sensor Type *				
Sensor				
 Dry Contact Sensor 				
Complete asset details *				
Name* sensor1	Priority * P3		~ 🕐	
Monitoring location *				
LAB-A1-DEV			*	
ſ Sensor Model *				
EMPDT1H1C2			•	
	Offset Humidity *	Offset Temperature *	Sensor function *	
Notification The field is required				
Email contact				
			Additional Information Finish	

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.

(i) 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 relevent 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

1.3.4 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**.

All Assets					Upload CSV file				▦	LAB-A1-DEV	∰ª @ :
ADD ASSETS 👻						exporting a CSV with current DC assets.					EXPORT ASSETS 🥥
Facility Assets		ssets Virtual Assets	Lo	cation	File Choose File No file chosen	Export Assets		m			
Alarms		Name 🋧	type	location		Cancel Upload	priority	creation_date	Contact name	Contact email	site_name
	active	EDF	feed	LAB-A1	-DEV		P1	2020-04-02T09:38:32+0000			
	active	EPDU-RACK01-BLUE	epdu	Rack1	EATON	EPDU MA 0U (309 32A 1P) 28XC13:4XC19 30B	P1	2020-04-02T09:53:53+0000			
	active	EPDU-RACK01-RED	epdu	Rack1	EATON	EPDU MA 0U (309 32A 1P) 28XC13:4XC19 30R	P1	2020-04-02T09:53:53+0000			
	active	EPDU-RACK02-BLUE	epdu	Rack2	EATON	EPDU MA 0U (309 32A 1P) 28XC13:4XC19 30B	P1	2020-04-02T13:41:35+0000	Essai contact 2		
	active	EPDU-RACK02-RED	epdu	Rack2	EATON	EPDU MA 0U (309 32A 1P) 28XC13:4XC19 30B	P1	2020-04-02T13:41:35+0000	Essai contact 2		
	active	EPDU-RACK03-BLUE	epdu	Rack3	EATON	EPDU MA 0U (309 32A 1P) 28XC13:4XC19 30B	P1	2020-04-02T09:53:55+0000	Essai contact 2		

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**.

1	A	8	c	0	Ł	. 1	G		н		1		1	K	1	M		N	0	P	Q	R		5	
1	name	type	sub_type	location	status	priority	asset_ta	g power,	source.1	power,	plug_arc3	power,	input 3	description	n ip.1	compan	y site,	name	region	country	address	contact_	name	contact_em	ail conta
2	DataCenter	datacenter			active	P1																			
3	Roomi	room		DataCenter	active	P1																			
4	Room2	room		DataCenter	active	P1																			
5	Row1	row		Room1	active	P1																			
6	Row2	rów		Room2	active	P1																			
7	Rack3	rack		Row1	active	P1																			
8	Rack1	reck		Row1	active	P1																			
9	Rack2	rack		Row2	active	P1				1															
10																									
11																									
12																									
14																									

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	В	С	D	E	F	G	Н	1	J	K	L	М	N	0
name	type	sub_type	location	status	priority	power_source.1	power_plug_src.1	power_inpu	power_source.2	power_plug_s	r manufactur	model	location_u	pid
SRV31	device	server	Rack2	active	P3	EPDU-RACK02-RED	31		EPDU-RACK02-BI	. 31	l HPE	G9		8 server-11
UPS04	device	ups	Rack4	active	P1	UPS01								1 ups-12
UPS01	device	ups	Rack1	active	P1	EDF								1 ups-17
UPS02	device	ups	Rack2	active	P1	UPS01								1 ups-18
UPS03	device	ups	Rack3	active	P1	UPS01								1 ups-19
SRV54 GENEPI	device	server	Rack1	active	P2	EPDU-RACK01-RED	11		EPDU-RACK01-BI	. 11	L Dell	R6415	3	38 server-1
STS RACK01	device	sts	Rack1	active	P5	EPDU-RACK01-RED	1		EPDU-RACK01-BI	. 1	L		4	40 sts-118
HPE-PROD	device	ups	Rack1	active	P2	EPDU-RACK01-BLUE	5						3	33 ups-119
SRV32	device	server	Rack2	active	P3	EPDU-RACK02-RED	30		EPDU-RACK02-BI	. 30) HPE	G9		9 server-1
SRV33	device	server	Rack2	active	P3	EPDU-RACK02-RED	29		EPDU-RACK02-BI	. 29	HPE	G9	1	10 server-1
2 SRV34	device	server	Rack2	active	P3	EPDU-RACK02-RED	28		EPDU-RACK02-BI	. 28	B HPE	G9	1	11 server-1
SRV35	device	server	Rack2	active	P3	EPDU-RACK02-RED	27		EPDU-RACK02-BI	. 27	7 HPE	G9	1	12 server-1
SRV36	device	server	Rack2	active	P3	EPDU-RACK02-RED	26		EPDU-RACK02-BI	. 26	5 HPE	G9	1	13 server-1
SRV38	device	server	Rack2	active	P3	EPDU-RACK02-RED	25		EPDU-RACK02-BI	. 25	5 HPE	G9	1	14 server-1
i SRV45	device	server	Rack2	active	P3	EPDU-RACK02-RED	23		EPDU-RACK02-BI	. 23	B HPE	G9	1	15 server-1
7 SRV20	device	server	Rack2	active	P3	EPDU-RACK02-RED	22		EPDU-RACK02-BI	. 22	2 HPE	DL385 G8	1	16 server-1
3 SRV16	device	server	Rack2	active	P3	EPDU-RACK02-RED	21		EPDU-RACK02-BI	. 21	L FUJITSU	RX 300 S7	1	18 server-1
SRV42	device	server	Rack2	active	P3	EPDU-RACK02-RED	20		EPDU-RACK02-BI	. 20	DELL	PowerEdge R6	i 2	27 server-1
SRV43	device	server	Rack2	active	P3	EPDU-RACK02-RED	19		EPDU-RACK02-BI	. 19	9 DELL	PowerEdge R6	i 2	28 server-1
l SRV44	device	server	Rack2	active	P3	EPDU-RACK02-RED	18		EPDU-RACK02-BI	. 18	3 DELL	PowerEdge R6	i 2	29 server-1
SRV41 (x3 - VXRAIL)	device	server	Rack2	active	P3	EPDU-RACK02-RED	7		EPDU-RACK02-BI		7 VXRAIL		2	30 server-1
SRV56	device	server	Rack2	active	P3	EPDU-RACK02-RED	4		EPDU-RACK02-BI		4 HPE	G10	2	32 server-1
SRV57	device	server	Rack2	active	P3	EPDU-RACK02-RED	3		EPDU-RACK02-BI	. :	B HPE	G10	2	33 server-1
SRV39	device	server	Rack2	active	P3	EPDU-RACK02-RED	10		EPDU-RACK02-BI	. 10) Lenovo	ThinkServer	2	25 server-1
SRV40	device	server	Rack2	active	P3	EPDU-RACK02-RED	9		EPDU-RACK02-BI		ENOVO	ThinkServer	2	26 server-1
EPDU-RACK04-RED	device	epdu	Rack4	active	P2	EDF								epdu-13
BEPDU-RACK04-BLUE	device	epdu	Rack4	active	P2	UPS04								epdu-13
e chassis test	device	chassis	Rack1	active	P1	UPS04			UPS01					2 chassis-1

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.

All Assets									⊞	LAB-A1-DEV	% ⁴ 0 ∶
ADD ASSETS 👻					Upload CSV file						EXPORT ASSETS 🕑
Facility Asset	s ITA	ssets Virtual Assets	Lo	cation	Nothing to upload yet? Start by	exporting a CSV with current DC assets. Export Assets					
P Edit	🔧 Config	ure 📄 Delete			Choose File No file chosen			ш			
Alarms		Name 🕇	type	location		Cancel Upload	priority	creation_date	Contact name	Contact email	site_name
	active	EDF	feed	LAB-A1	DEV		P1	2020-04-02T09:38:32+0000			
	active	EPDU-RACK01-BLUE	epdu	Rack1	EATON	EPDU MA 0U (309 32A 1P) 28XC13:4XC19 30B	P1	2020-04-02T09:53:53+0000			
	active	EPDU-RACK01-RED	epdu	Rack1	EATON	EPDU MA 0U (309 32A 1P) 28XC13:4XC19 30R	P1	2020-04-02T09:53:53+0000			
	active	EPDU-RACK02-BLUE	epdu	Rack2	EATON	EPDU MA 0U (309 32A 1P) 28XC13:4XC19 30B	P1	2020-04-02T13:41:35+0000	Essai contact 2		
	active	EPDU-RACK02-RED	epdu	Rack2	EATON	EPDU MA 0U (309 32A 1P) 28XC13:4XC19 30B	P1	2020-04-02T13:41:35+0000	Essai contact 2		
	active	EPDU-RACK03-BLUE	epdu	Rack3	EATON	EPDU MA 0U (309 32A 1P) 28XC13:4XC19 30B	P1	2020-04-02T09:53:55+0000	Essai contact 2		

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).

Error	
Please fix the following lines and upload your CSV file again: - Line 2 : Element 42' cannot be processed because of conflict. M duplicate entry.	/lost likely
	Close

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.

Error	
2 lines were successfully processed from your file Please fix the following lines and upload your CSV file again: - Line 2 : Element ' 42' cannot be processed because of co duplicate entry.	onflict. Most likely
	Close

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

All Assets		
ADD ASSETS 👻	Success	
Facility Assets IT Assets Virtual Assets Location	CSV Import Successful 49 lines were successfully processed from your file	
Edit Configure Delete	Close	
Alarms Status Name 🛧 type location	_name Manufacturer Model	priority creation_date Contact na

Import Error Code Details

Error Condition	Code
Method is not allowed	45
Content size is too big	53
File "assets" is missing	46
File "assets" has bad coding or bad format	47

Error Condition	Code
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 42 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	lgnore	Silence	Pause	Work in Progress	Resolved

(i) 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	Visibl e 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	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

|--|

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
	р3	
	p4	
	р5	
Warning	p1	1h
	p2	4h
	р3	
	p4	
	р5	
Info	p1	8h
	p2	24h





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

i 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.



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 : **If a power outage is detected on** *this* **UPS then Shutdown my hypervisor and switch off the powering ePDU outlets**.

The automation wizard, enables you to configure sequences of actions.

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

≡	Intelligent Power Manager 2.3.0	Automation			LAB-A1-DEV 2021-03- 16:28:53	
	Dashboard	Create new	on Settings	Q _{search}		
٠	Power			- 300101		
٥	Environment	Status	Trigger Type	Name 🛧	Last Execution	Detail
≔	Assets	Ready	Power	IT-automation-2	-	-
۰.	Automation	C Active Ready	Power	Power-automation	-	-
0	Status					
۰	Settings					
(i) 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 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.

(j)	 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 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 if a given UPS lose the power OR if 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 application to trigger an automation policy :

	Datace nter	Rack	Row	sensorg pio	UPS	ePDU	STS
Average Humidity	0		0	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	I	N/a	N/a
Door Contact State Change	N/a	N/a	N/a	0	N/a	N/a	N/a
Load default	N/a	N/a	N/a	N/a	•	N/a	N/a
Load.input_1phase	N/a	N/a	N/a	N/a	N/a		N/a
Load.input_3phase	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
On battery	N/a	N/a	N/a	N/a	v	N/a	N/a
On bypass	N/a	N/a	N/a	N/a	Ø	N/a	N/a
Phase imbalance		Ø	N/a	N/a	•	Ø	N/a
Pir-motion- detector.state-change	N/a	N/a	N/a	•	N/a	N/a	N/a
Realpower.default		N/a	N/a	N/a	N/a	N/a	N/a
Realpower.default_1ph ase	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-detector.state- change	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	Ø
Temperature.default	N/a	N/a	N/a	N/a	Ø	N/a	N/a
Vibration-sensor.state- change	N/a	N/a	N/a			N/a	N/a
Voltage.input_1phase	N/a	N/a	N/a	N/a	Ø		N/a
Voltage.input_3phase	N/a	N/a	N/a	N/a			N/a
Water-leak- detector.state-change	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	v	N/a	N/a

1.6.2 **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 :

Actions						
Insert Action						
Then	K Shutdown	X IT Action	Send a not	Ō Set a time	Custom Sc	Check Initi

- Shutdown 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
- IT actions you may configure actions to target your IT infrastructure including physical servers and virtualized assets when virtualization connectors are configured :
 - Host Power Action: this action executes a command on the targeted hypervisor.
 - VM Power Action: this action executes a power command on a virtual machine.
 - vApp Power Action: this action executes a power command on a virtual application.
 - Cluster Actions : this action wil initiate a cluster shutdown. Cluster Configuration supported :
 - VMware
 - VMware HA + DRS
 - VMware vSAN
 - VxRail
 - Nutanix
 - SRM (Site Recovery Plan) : this starts a predefined recovery plan in fail-over mode. (only for VMware connectors)
 - Fault Domain Action (VMware only)
 - Server IT action : execute a command on a physical serser, like Power on or Power Off
 - Power capping : cap the power consumption on physical asset(s) targeted by the action
 - Storage IT actions : execute the shutdown on a storage node
 - SSH command
 - Windows Server Shutdown
- Send a notifications (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 :
 - Dedicated page in Automation settings for script management : Import/Read/Update/Delete
 - Possibility to select an imported local script to configure an action
 - The commands defined in the local user script are applied when executing the automation policy
 - 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

• 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

(i) 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.

IT actions supported

	Operati ng systems (Windo ws / Linux / .)	vm ware [,]	Microsoft	■ NetApp	NUTANIX.	Hewlett Packard Enterprise
Host IT Actions						
Shutdown Host	n/a	0		n/a	8	n/a
Shutdown VMs Then Host		0			8	
Enter Maintenance Mode		v			Ø	
Enter Maintenance Mode Then Shutdown		0			8	
Exit From Maintenance Mode		•	Ø		Ø	
Power Down To Standby Mode		Ø	n/a		n/a	
Power Up From Standby Mode		0	n/a		n/a	
Shutdown commands						

Windows Shutdown		n/a	n/a	n/a	n/a	n/a
SSH						
VMs IT Actions						
Power On	n/a	0	v	n/a	Ø	n/a
Power Off	II/a	•	I		Ø	
Shutdown Guest		0	v		Ø	
Shutdown Guest With Timeout		I	n/a		n/a	
Suspend		0	I		Ø	
Resume		⊗	I		⊗	
Migrate		0	I		⊗	
Fault Domain						
Enter Maintenance mode then shutdown	n/a	0	n/a	n/a	n/a	n/a
Enter Maintenance Mode		I				
Exit Maintenance Mode		I				
SRM						
Recovery plan activation	n/a	0	n/a	n/a	n/a	n/a
vApp IT actions						
Power On	n/a	0	n/a	n/a	n/a	n/a
Shutdown						
Suspend						
Cluster IT Action						
(check info note below for cluster configurations supported by IPM)						
Cluster shutdown	n/a	(including VxRail cluster shutdown)	0	n/a	0	n/a
Servers IT Actions						HP servers

Xtreme Support Process

Power capping	n/a	n/a	n/a	n/a	n/a	
Power On						•
Power Off						0
Storage IT action				storage		
Shutdown	n/a	n/a	n/a	⊘	n/a	n/a

Blue	e cell = connectors/actions available with "Optimize" license
Gree	en Cells = connectors/actions available with "Manage" license
(i)	 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)
i	 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

1.7 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.

(i) 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 <u>john.doe@organization.com</u>
- 3. Send the archive received by mail to <a>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 Supported Power Chain Topologies

1.8.1 Supported 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

	ATS	
UTILITY A	υτιμηγ	UTILITY B
3 ph		3 ph

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

	ATS	
UTILITY	UTILITY	GEN SET
3 ph	UPS 100 KW	8 hours of autonomy
	50 kw	

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

UTILITY A	UTILITY	UTILITY B
2 ph	UPS	2 ob
3 ph	100 kW	3 ph
	50 kW	

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 in parallel connected to a Power Control Unit (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-considerationselectrical-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

1.10 Licensing

1.10.1 Initial trial period

All IPM Editions come with one week 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.

(i) 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**

	Your trial expires in 6 days. Activate your license <u>Don't have an activation code? Find your reseller</u>			
DCLAB-A		46 Alarms	P rde	Intelligent Power Manager Infrastructure
Dashboard	Account Alarms Datacenter Layout Date & Time License Monitoring Network Notifications Users			
🗩 Power	License			
Environment				
(i) Status	O Trial period expires in 6 days ✓ License for software is valid until 11-07-2018 • Max active power nodes: 200			
Assets	✓ License for maintenance is valid until 11-07-2018			
Settings	Activate license			
K Denny danar Harbart				

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

Activate license	
Activation ID	
Don't have an activation code? Find your reseller	
☑Activate license online	

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.

As a consequence, the checkbox Activate license online is available and checked by default.

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.

(i) 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 <u>network settings</u> tab described in the contextual help chapter of this document for more details on configuring the proxy.

Initial activation

Online activation will not be available for the first activation.

Only Offline activation will be allowed after a self-registration that will create an account on licensing portal.

(i) 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
- 2. Click on the **Open Eaton website** button
 - 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)

Login	
With User Name	
Username	

- 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**

Devices v Icense has been generated successfully, please click here to download the new license. Offfine Device Management Manually upload either a Capability Request or Synchronization History Files for offline processing. The application will offer you a response file to download. Upload type: Generate license Upload synchronization history Choose File No file chosen 	FAT•N	
Offline Device Management Manually upload either a Capability Request or Synchronization History Files for offline processing. The application will offer you a response file to download. Upload type: O Upload synchronization history		
Janually upload either a Capability Request or Synchronization History Files for offline processing. The application will offer you a response file to download. Upload type: Generate license Upload synchronization history	License has been	generated successfully, please click here to download the new license.
Ianually upload either a Capability Request or Synchronization History Files for offline processing. The application will offer you a response file to download. Upload type: Generate license Upload synchronization history	Offline F)evice Management
Upload synchronization history		
Choose File No file chosen		-
	[Choose File No file chosen
Upload	Upload	

- e. Click on Choose File and select the capability request you generated in Step 1
- f. Click on **Upload**. You should be notified of the license generation success.
- g. Click on the "**click <u>here</u>**" 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
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 independant server count for 1
Activate 8 hypervisors	16	Each independant hypersidsor 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.

requency (seconds) * 30		
Server IP Address *		
erver Port * 2003		
Basename 3		
Activate		
		Save
Graphite Connector	Status	

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

Graphite Connector Status



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 :

uhite

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

	Queries to	r myGraphite	•					Add Query	Query Inspecto	or ?
										œ û
		select metric								
Ţ										
*										
	Cache timeout		Max data points	Relative time	Time shift					
J										

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 <u>https://[your_IPM</u> <u>Edition_IP address_or_hostname]/api/v1/assets</u>. 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.



Visualization

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

、 、	Visualizat	ion 📺	Graph 👻							
)	Draw Mod	es	Mode Options		Hover tooltip		Stacking & Nu	ll value		
	Bars		Fill		Mode	All series	Stack			
	Lines		Line Width		Sort order	None	Null value	null		
	Points		Staircase							
	+ Add se	eries override G	•							

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



Each visualization has its own configuration panels.

2 Contextual Help

2.1 Login page

Powering Business Worldwide	
Username * admin	
Password *	
Forgot your password? 👔	
→ Login	

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.

```
(i) 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.

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.

(i) 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 Temperature and 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 top right Active Alerts 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 bottom right 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.



[•] Click Continue.

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 a gauge to advance to a more detailed view.

For example, by clicking on the Power guage, 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.

(i) 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.

≡	Intelligent Power Manager 2.3.0	Power			Datacenter	2021-03-22 13:18:51	?	1
55	Dashboard	Power Chain	Power Monitoring					
	Power	Power Chain	Overview O Power per phase	Data Center Phase Balance	Active Alarms			
٩	Environment				2021-03- 22 10:13:41 > Total power in	datacenter I AB-A	1-DEV is	criticall
=	Assets			L1 L2 L3	22 10:13:41 Float power in 22 2021-03- 10:12:41 > Total power is			
۰,	Automation		EDF		▲ 2021-03- 16:08:16 > Humidity in da			
0	Status		3 phase					More
\$	Settings							
			LAB-A1-DEV-Room1 / Row1		Total Data Center Power			
			Rack1 Rack2 Avg Rack3	Ard 23994W	24h 7d	30d Min Average 97:18		D 3:18 xport data
	FAT-N Powering Business Worldwide						-	

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 Supported Power Chain Topologies section of the documentation.

2.4 Rack View

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



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:

Availability	Power Source 🕜	
35U 62 outlets	Feed A () UPS01	Feed A UPS02

The system also displays the state of each outlet and which outlet of a rack PDU a device is connected to by simply rolling over either a device or an outlet.

The Question Mark icon at the top right of the Rack topology provides a legend for the outlet colour:

- GREEN = Management on & device connected and within threshold
- **YELLOW** = Management on & device connected and above warning threshold
 - **RED** = Management on & device connected and above critical threshold
- WHITE = Management on & no device connected
- GREY = Management off

٠

• Grey with strike-through = Communication lost or belongs to PDU with no communication capabilities

When you perform a mouse-over on one of the outlets, the device supplied is displayed with a Bold rectanglular highlight. If there is another outlet supplying the device, that (those) outlet(s) is (are) also displayed in bold.



When you mouse-over 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 rectanglular 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.

You may mouse-over the top of the label in the colored rectangle identifying each section. When doing so, each device powered by the selected section's outlets is displayed with a bold border.

A tooltip is also displayed with the group name of the section, the phase powering the section and the instananeous values of the active power, current and load % 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.



G3MA 3PH

You may also obtain more details related to each of the rack PDUs installed. Simply click on the **Details** button. Details such as serial number, installation date, warranty expiration date, etc are provided.

Power Monitoring View



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

Power Chain	Power Monitoring									
					Q Search		All L	ocation 👻 🚻		
Status	Name	IP		Туре 🕁	Model	Location	Load Level(%)	Power Output(W)	Power Output(W)	Battery Runtime
🕗 Online	HPE-PROD	10	50	ups	T550 INTL	Rack1	0%	420W	100%	1:30:0
🕗 Online	UPS-EATON-P03	<u>10</u>	122	ups	Eaton 9PX 8000i	Rack3	3%	71W	100%	6:25:48
🚫 Online	UPS-EATON-P02	<u>10</u>	<u>121</u>	ups	Eaton 9PX 8000i	Rack2	1996	1316W	100%	0:54:0
🕗 Online	UPS-EATON-P04	<u>10</u>	123	ups	Eaton 9PX 8000i	Rack4	15%	1086W	100%	1:7:46
🔗 Online	UPS-EATON-P01	<u>10</u>	120	ups	Eaton 9PX 8000i	Rack1	63%	4454W	100%	0:11:39 🚯 🔚 🖸
\otimes	EPDU-RACK02-BLUE	<u>10</u>	112	epdu	EPDU MA 0U (309 32A 1P) 28XC13:4XC19 30B	Rack2	1996	1300W		Show Device Information
\oslash	EPDU-RACK04-RED	<u>10</u>	114	epdu	EPDU MA 0U (309 32A 1P) 28XC13:4XC19 30B	Rack4	20%	1472W		
\otimes	EPDU-RACK04-BLUE	<u>10</u>	114	epdu	EPDU MA 0U (309 32A 1P) 28XC13:4XC19 30B	Rack4	16%	1076W		
\oslash	EPDU-RACK01-RED	10	111	epdu	EPDU MA 0U (309 32A 1P) 28XC13:4XC19 30R	Rack1	10%	615W		
\otimes	EPDU-RACK01-BLUE	10	.111	epdu	EPDU MA 0U (309 32A 1P) 28XC13:4XC19 30B	Rack1	7%	295W		

2.6 UPS View

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

← UPS-EATON-P01			atacenter AB-A1-DEV	2021-03-22 13:49:00	?	<mark>•</mark> •
Load Status Battery Charge 58% 3.92kW Online 100%	Details	Active Alarms				
Temperature: R Location LAB-A1-DEV-Room1 > Row1 > Rack1 T N N	Battery Runtime 14min Type Mainenance: Warranty end	No alarms to display				
Power L1: 4.54 kW Power voltage L1: 237 V voltage	tputs ver L1: 3 92 kW age L1: 239 V quency: 30 Hz					
Power Chain UPS-EATON 3916 W	Total Data Center Power 10931 W	Total UPS Power 24h 7d 4198 W 7d	30d	● Min ● Average	• Max	8
LAB-A1-DEV-Room1 Rack1 Rack2 Rack3 Rack4 B201- 84/001- 84/002- 84/00	/ Row1	4100 W 4000 W 3990 W 3765 W 43347 19-47	01.47	2021-03-22 12:00 Max 4037 W 07:47		3:47

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

Type UPS	Asset tag
Status Online	Serial number G208C32063
Make/Model / Eaton 9PX 8000i	IP address 10.1 120 대학
Location Room1 > Row1 > Rack1	Installation date
U size 6	Warranty end
UPS FW revision 01.10.0032	Power Sources EDF
Card FW revision 1.4.9	
Battery	
Туре	Next Maintenance
Warranty End	Installation Date

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.

← ePDU Details								ta u	AB-A1-DEV 🛕	0 :
EPDU-RACK01-BLUE							Details	A		Phase 1
IP								•	A1 Outlet A1	
Location								6 114 60	0 W A2 Outlet A2	
Daisy Chain				Device1					A3 Outlet A3 A4 Outlet A4	
Input Phases				1 Phase					0 W A5 Outlet A5	
									A6 Outlet A6 A7 Outlet A7	
Alarms								5.0	W AS Outlet AS	
									0 W A9 Outlet A9	
No alarms								0	A10 Outlet A10 A11 Outlet A11	
								0	A12 Outlet A12	
Metrics									A13 Outlet A13	
Max Real Power last 7 days						447.0 W		 22.0 32.0 	A14 Outlet A14 A15 Outlet A15	
Max Real Power last 24 hours						306.0 W			A16 Outlet A16	
Phase						Load	Real Power	В		Phase 1
u		•				7%	294.0 W		B1 Outlet B1 B2 Outlet B2	
								•	B3 Outlet B3	
Branch Circuits									B4 Outlet B4	
Label	Outlets	Phase	Load	Current	Voltage	Real Power			B5 Outlet B5 B6 Outlet B6	
	0.000	1100		Carron.	10.000	near one		0	B7 Outlet B7	
A	16	1	8%	1.4A	239.6 V	203.0 W			OW B8 Outlet B8	
8	16	1	7%	1.2.A	239.6 V	69.0 W			B9 Outlet B9 B10 Outlet B10	
								0	B10 Outlet B10 B11 Outlet B11	
								0	B12. Outlet B12	
								1.0	W B13 Outlet B13	
									W B14 Outlet B14	
									B15 Outlet B15	
								16.0	0 W B16 Outlet B16	

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 four panels:

- 1. The top panel contains the key informations 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.

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.

(i) 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.

10:56:28	Environment 2021-03-29 10:5628 2021-03-29 10:
	Environment Sensors
in datacenter LAB-A1-DEV is critically high. is critically high in rack Rack3. More 30d 0 Min • Average • Max	 L48A1-DEV L48A1-DEV Temperature Humidity L35C 330% L48A1-DEV/Room1 / Rov1 L15C 330% L48A1-DEV/Room1 / Rov1 L15C 330% L215C 30% L215C 30%
is cri	• LAB-A1-DEV-Room1 / Row1 21.5 C \$3.0% 0 2021-03 10:12:41 > Total power is cn • 22.0% 38.0% 38.0% 0 2021-03 10:12:41 > Total power is cn • 22.0% 38.0% 38.0% 0 2021-03 10:12:41 > Total power is cn • 22.0% 38.0% 38.0% 0 0 Temperature 0 0 Temperature 0 10:12:41 > Total power is cn 0 0 10:12:41 > Total power is cn 0 2021-03 10:12:41 > Total power is cn

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 over the last 24hrs, 7 days or 30 days.

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 \clubsuit which is displayed to the left of the asset name.

<u></u>	All Assets									⊞ D(LAB-A0 🝷	🧶 🕲 :
brument	ADD ASSETS											EXPORT ASSETS
ccount 🗸	Facility Ass	ets										
DASHBOARD	Edit	🔍 Cor	nfigure 📋 Delete			Q _{Search}						
POWER						• pearch			111			
ENVIRONMENT	Alarms	Status	Name 🛧	type	location_name	Manufacturer	Model	priority	creation_date	Contact name	Contact email	site_name
ASSETS		active	ATS16A - Rack IPC A0	sts	Rack IPC A0	Dummy Manufacturer	Eaton ATS	P3	2020-04-07T13:44:50+0000			
		active	ATS16A - Rack IPSS A0	sts	Rack IPSS A0		Eaton ATS	P5	2020-04-07T13:44:50+0000			
AUTOMATION		active	EMP - 9PX6kVA A0	senso	or Eaton 9PX Titan A0	Eaton	EMP001	P1	2020-04-07T13:44:50+0000			
STATUS		active	EMP - GA MA3ph A0	senso	or G3 MA3Ph - IPSS Right A0	Eaton	EMP001	P1	2020-04-07T13:44:50+0000			
SETTINGS		active	Eaton 5PX A0	ups	Rack IPC A0	EATON	Eaton 95X 3000iR	P1	2020-04-07T13:44:50+0000			
		active	Eaton 9PX 3000i A0	ups	Rack IPSS A0	Eaton	Eaton 9PX	P1	2020-04-07T13:44:50+0000	Computer Room Manager		
		active	Eaton 9PX Titan A0	ups	Rack IPC A0	EATON	Eaton 9PX	P1	2020-04-07T13:44:50+0000	Computer Room Manager		
		active	G2 MA0Ph - IPSS Left A0	epdu	Rack IPSS A0	EATON	Eaton ePDU MA 1P IN:C14 10A OUT:16xC13	P2	2020-04-07T13:44:50+0000	EATON - PDU Managed		
	□ 🌲	active	G3 MA3Ph - IPSS Right A0	epdu	Rack IPSS A0	EATON	EPDU MA 0U (309 32A 3P)18XC13:6XC19	P1	2020-04-07T13:44:50+0000			
		active	G3-1Ph MA - IPC Left A0	epdu	Rack IPC A0	EATON	EPDU MA 0U (C14 10A 1P)16XC13	P2	2020-04-07T13:44:50+0000			
First Power Nanager 2.0										Items per page: 10) - 1-10	0 of 14 < 🗲 🕹

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, and location.*

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.

All Assets			
ADD ASSETS 👻			
Facility Assets	IT Assets	Virtual Assets	

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
 - Output contact

Location

In the current version, it is also possible from the power asset view to create & manage:

- Location topology
 - Data Center
 - Room

- Row
- Rack

All Assets						DCLAB-A0 👻
ADD ASSETS 👻						
		ssets Location				
🖍 Edit	Delete		Q _{Search}			
	Alarms	Status	Name 🛧	type	location_name	priority
	A	active	DCLAB-A0	datacenter		P1
	A	active	Rack IPC A0	rack	Row IT Lab A0	P1
		active	Rack IPSS A0	rack	Row IT Lab A0	P1
		active	Room A0	room	DCLAB-A0	P1
	A	active	Row IT Lab A0	row	Room A0	P1

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

i Note : IT	servers re	elated to HPE On	eView con	nector a	ire no	t monitored b	y IPM2		
All Assets								🛅 DCL	AB-A0 👻
ADD ASSETS 👻									
Facility Assets IT Assets	Virtual Assets	s Location							
🖋 Edit 📋 Delete			Q _{Search}				····		
Alarms	Status	Name 🛧		type	IP	location_name	Manufacturer	Model	priority
	active	Cisco CI Bios A0		server		Rack IPC A0			P2
	active	Dell DHCP Server A0		server		Rack IPC A0			P1
	active	Fuji01 - Hyper 2012R2 A0		server		Rack IPC A0	Fujitsu	RX100	P4
	active	Fuji02 - Hyper 2012R2 A0		server		Rack IPC A0	Fujitsu	RX100	P4
	active	HPE 2920 Switch A0		switch		Rack IPC A0	HPE	2920	P1
	active	HPE01 - ESXi 6.5 A0		server		Rack IPC A0	HPE	DL 320e G8	P1
	active	HPE02 - ESXi 6.5 A0		server		Rack IPC A0	HPE	DL 320e G8	P1
	active	HPE03 - ESXi 6.5 A0		server		Rack IPC A0	HPE	DL380 G9	P1
	active	IBM XM3530 M4 Server A0		server		Rack IPC A0	IBM	X3530 M4	P3
	active	PC78 - ESXi 6.7 SetUp A0		server		Rack IPSS A0			P2

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
- Virtual Machine objects :
 - VMware
 - Microsoft
 - Nutanix
- Storage objects :
 - NetApp : ONTAP

All Assets					DCLAB-A0	• 🏴 📀 🗄
ADD ASSETS 🔻						EXPORT ASSETS
Facility Assets IT Assets Virtual Assets						
	4 devices	are not configured.	<u>Complete setup now</u>			
🖋 Edit	Q _{Search}	-				
041259-4x0F3429-549e-708705c4641c	VHYPERV2019WS	\odot	Running	Hypervisor	Microsoft Hyper-V / Server	
0104aati20-a525-444f 87a0-ee42a0248da9	IPM_Editions-va-2.1.0+76_x86_64_4cpu_8192mem	${\boldsymbol{ \oslash}}$	Running	Virtual Machine	Microsoft VM	
c331e462-a277-4542-a5e2-5771d1483cde	vmtest	\oslash	Suspended	Virtual Machine	Microsoft VM	
5ad2f565-e5d2-432a-9126-95cf572d71ff	Tutu	\otimes	Running	Virtual Machine	Microsoft VM	
domain-c7-de?f8464-cdb7-4767-6796-1566c12081c3	cluster-dev-67.3 (vSAN)	\oslash	Unknown	Cluster	VMware Cluster	
nost-23-67a48d7a-8057-4066-6d76-5917a2ee76d3	vesx om	${\boldsymbol{ \oslash}}$	Running	Hypervisor	VMware ESXI	
Dool: 12-5522e40a-d644-4c56-b6e3-7261acd31a82	vesxion	\otimes	Running	Hypervisor	VMware ESXI	
Door 26-86c9d576-57c8-434c-a4ae-095efb6e67c5	vesx	\otimes	Running	Hypervisor	VMware ESXI	
+2430x2b-a937-4c5a-878b-4c044e15a3e0	vcen ib.etn.com	\otimes	Unknown	Managers	VMware vCenter	
wm-81-0x88x99d-65x9-4651-8945-88x203a8xx77	Empty 01	${\boldsymbol{ \oslash}}$	Running	Virtual Machine	VMware VM	
m 25-3471890-9917-4/5-8306-ba99e5456ecb	vcenter67u3-vsan	${\boldsymbol{ \oslash}}$	Running	Virtual Machine	VMware VM	
vm-28-6255104c-04559-4826-6614-0x305a6dc422	Debian 8 - 03	${\boldsymbol{ \oslash}}$	Running	Virtual Machine	VMware VM	

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 paried with a physical host by simply clicking on the link.

All Assets
ADD ASSETS 👻
Facility Assets IT Assets Virtual Assets Location
18 devices are not configured. <u>Complete setup now</u>

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.

All Assets					Ē] DCLAB-A0 🔹 🎾 ? 🕴
ADD ASSETS 🔻						EXPORT ASSETS
Facility Assets IT Assets Virtual Assets Location						
	. 4 device	es are not configured.	<u>Complete setup now</u>			
🖍 Edit	Virtual asset	×		m		
id id	ves) com	hic	ation status	Operating status	Туре 🕹	Sub type
host-23-				Running	Hypervisor	VMware ESXI
nost 12 5322440a d844 4/56 0645 7261acd91a82	Server Host	· ·		Running	Hypervisor	VMware ESXI
B0412786-64073425-6494-702705c4641c	Status			Running	Hypervisor	Microsoft Hyper-V / Server
hose 26 Bit 2015 STr.S.434c adue 055e/bite07c5	Power State Communication Linked VMs	► ⊘		Running	Hypervisor	VMware ESXI
	Number of VMs	2 Cancel Save				

2.9.2 Primary asset actions

The main asset management actions are accessible in the **Add Assets** drop down menu in the top row of the page.

All Assets	
ADD ASSETS 👻	
AUTO DISCOVERY	Virtual Assets
UPLOAD CSV FILE	Delete
ADD ASSET	
ADD CONNECTOR	type 🛧

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

← Discovery	
	earch any connected devices on your network erform an automatic search and add devices to your asset list
	Autodiscovery Scan all your network with protocols and credentials Q Start
	Discover by IP/Netmask Scan by IP details, protocols and credentials Q Start

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 (Singl e 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.

← Discovery by IP/Netmask							
1 IP/Net	tmask	Prot	cocols		Credentials		
Confirm IP / Netmask Details							
Select or add asset specific IPs, IP ranges or Netmasks							
+ 1	New 📋 Delete			Search			
	Туре	IP (from) 🕈	IP (to)	Netmask			
	Single IP Address	172	-	-			
~	IP Range	172	172.	-			
	Netmask	172 /24	-	172/24			
			ltems	sper page 25 💌 1 – 3 / 3	< >		
Back				Ca	ancel Next		
• 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

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



Review Protocols

All protocols are selected by default. You can exclude any from the discovery process below

Eaton NMC / iNMC Native protocol (Default port 4679)

SNMP v1 & SNMP v3 (Default port 161)

Back

Cancel Next

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

Pro	tocols					2 Credential
evie	w Credentials					
lect o	or add the asset credent	ials required				
Œ	Create New	lelete			Search	
	Name 🕈	Authentication type	Usages	Tags	Used by	
	private snmpv1	Snmpv1	Discovery Monitoring		0	:
	public	Snmpv1	Discovery Monitoring		44	:

	Items per page 25 👻	1-2/2 <	>
Back		Cancel	Start

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).

(i) 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.

- (i) 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 Supported 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 subsection 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).

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 the number of assets and an optional message informing about the completeness of the configuration.



Auto Discovery completed: 1 Assets found

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** (displayed below the indicator of the number of assets) will draw your attention to the need to complete the configuration.

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

Filter inactive devices							
	All Missing Details	1/103					
	Missing Activation	1/103					
	Missing Power Source Detail	1/103					
	Missing Location Detail	0/103					
	Missing IP Address Detail	1/103					



The checkboxes in the **Filter inactive devices** dialog are helpful to finalize the configuration by topic (e.g. start by completing missing power sources and then move on to missing locations, etc.).

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.

All Assets	7						DCLAB-A0	· 42
ADD ASSETS 👻								EXPOR
Facility Assets	_	Virtual Assets Location						
🖍 Edit	Configure	Delete	Q _{Searc}	h		id		
Alarms	Status	Name	type 🛧	location_name	Manufacturer	✓ status		priority
□ \$	active	G3 MA3Ph - IPSS Right A0	epdu	Rack IPSS A0	EATON	🔲 ip 9		P1
~	active	G2 MA0Ph - IPSS Left A0	epdu	Rack IPSS A0	EATON	🗹 type 🛛 🛛 🛛	13	P2
	active	G3-1Ph MA - IPC Left A0	epdu	Rack IPC A0	EATON	Iocation_name		P2
	active	G3-1Ph MA - IPC Right A0	epdu	Rack IPC A0	EATON	EPDU MA 0U (C14 10A 1P)16XC13		P1
	active	Main EDF Feed A0	feed	DCLAB-A0				P1
	active	Main Feed EDF A0	feed	DCLAB-A0				P1
	active	EMP - GA MA3ph A0	sensor	G3 MA3Ph - IPSS Right A0	Eaton	EMP001		P1
	active	EMP - 9PX6kVA A0	sensor	Eaton 9PX Titan A0	Eaton	EMP001		P1
	active	IPSS Rack Door A0	sensorgpio	EMP - GA MA3ph A0		DCS001		P3
	active	ATS16A - Rack IPSS A0	sts	Rack IPSS A0		Eaton ATS		P5

• the search field enables you to select the type of asset to display in the list

🖍 Edit 🔍 C	onfigure	Delete	Q ep	rch duj		ш	
Alarms	Status	Name	type 🛧	location_name	Manufacturer	Model	priority
	active	G3-1Ph MA - IPC Left A0	epdu	Rack IPC A0	EATON	EPDU MA 0U (C14 10A 1P)16XC13	P2
	active	G3-1Ph MA - IPC Right A0	epdu	Rack IPC A0	EATON	EPDU MA 0U (C14 10A 1P)16XC13	P1
□ ≜	active	G3 MA3Ph - IPSS Right A0	epdu	Rack IPSS A0	EATON	EPDU MA 0U (309 32A 3P)18XC13:6XC19	P1
<u>~</u>	active	G2 MA0Ph - IPSS Left A0	epdu	Rack IPSS A0	EATON	Eaton ePDU MA 1P IN:C14 10A OUT:16xC13	P2
	active	EMP - GA MA3ph A0	sensor	G3 MA3Ph - IPSS Right A0	Eaton	EMP001	P1

• 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).

ltems per page: 10 🔹 1 – 10 of 14 < 🔪

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 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.

⁽i) Note

\sim	Note List of eligibles assets to Mass confi	guration :
	UPS/NMC	Network-MS / Modbus-MS cards
	ePDU/G3	ePDU Network management card
	UPS/M2	Network-M2 / INDGW cards (FW version 1.7 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 click on the **Configure** button on top of the asset list.

≡	All Assets							Datacenter LAB-A1-DEV)21-03-29 :03:19	?	¢ 😕
5	ADD ASSETS 👻										EXPOR	T ASSETS 🥐
	Facility Assets	п	Assets Virtua	Assets	Location	Automatic Groups						
٥					0	31 devices are not configured.	<u>Complete setup</u>	now				
=	Configure	📋 De	elete							Search		
۵.	Alarm S	tatus	Name 🕈	Manufacturer	Model			Creation Date	Contact Name	Contact	Email	í
0		Active	EDF					2021-02-02T10:29:29+0000				:
۵		Active	EPDU-RACK01-BLUE	EATON	EPDU MA	0U (309 32A 1P) 28XC13:4XC1	9 30B	2021-02-02T10:42:13+0000				:
		Active	EPDU-RACK01-RED	EATON	EPDU MA	0U (309 32A 1P) 28XC13:4XC1	9 30R	2021-02-02T10:41:30+0000				:
		Active	EPDU-RACK02-BLUE	EATON	EPDU MA	0U (309 32A 1P) 28XC13:4XC1	9 30B	2021-03-22T09:08:50+0000	Essai contact 2			:

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

÷

Create Credential	Select	Credential				
Basic credential			Search Credential			
Credential Name		Authentication type	Name	Tags	Usages	Used by
Usares " Mass Device Management 🐨		Basic credential	PDU credentials		Mass Device Management	3
	~	Basic credential	UPS Public-IPM2 Demo		Discovery And Monitoring Mass Device Management	3
Add a tag and tap enter		Basic credential	MM		Mass Device Management	0
Username						
Password	_ c	hange Default Ports 443				

2.10.1 Configure NMC or G3 cards

From the asset list, select the source asset, click on configure and select the credential to authenticate to the device.

Then, IPM will display all settings available for the asset. They are grouped by categories :

For NMC Card : communication card dedicated to UPS

- System settings
- Access control
- Network settings
- Outlets
- Emails
- Network Management System
- Environment sensor
- Shutdown schedule
- Time settings
- Client settings

&	← ups (10.1		b Jeff-DC	%⁹ ∶
tbr				BULK APPLY
Account 🗸	 System Settings 	 System Settings 		0
DASHBOARD	Access Control	system settings		
POWER	Networks Settings	✓ Access Control		
	Outlets Emails	 Networks Settings 		
ASSETS	Network Management System	✓ Outlets		
STATUS	Environment Sensor	✓ Emails		
SETTINGS	Time Settings	 Network Management System 		
	Client Settings	 Environment Sensor 		
		V Shutdown Schedule		
		✓ Time Settings		
		✓ Client Settings		
Assering Burdent Power Manage 2.0	er			

For ePDU G3 : communication card dedicated to ePDU

- System settings
- Access control
- Network 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

tbr	← epdu (10 10000 58)		🛅 Jeff-DC	BULK APPLY
Account 🗸	System Settings			0
DASHBOARD	Access Control	V System Settings		
POWER	Networks Settings	 Access Control 		
ENVIRONMENT	FTP Settings	 Networks Settings 		
ASSETS	Network RADIUS Settings	✓ FTP Settings		
AUTOMATION STATUS	SMTP Settings	✓ HTTP Settings		
SETTINGS	Telnet Settings Network Log Settings	✓ Network RADIUS Settings		
	SNMP Network Management System	✓ SMTP Settings		
	LDAP Settings	✓ Telnet Settings		
	Display Settings Users	 Network Log Settings 		
	Emails	✓ SNMP		
Part N Party Rever Tradeids Intelligent Power Manager 2.0	Input	 Network Management System 		

Then, select the settings you want to copy to another device.

It's possible to select a group of settings, or only one.

Select the check box :

- front of the group settings will select all the values for that group,
- front of the settings : open the group and select individualy the settings.

← ups (10.14)			I Jeff-DC	4 9 ÷
				BULK APPLY (7)
System Settings			_	0
Access Control	 System Settings 			
Networks Settings	Contact	Bernard Tech Support	~	
Outlets	Location	Labo A2-01, Mbt	~	
Emails	Default Language	ENG	~	
Network Management System	History Log Interval	60 s	~	
Environment Sensor	Environment Log Interval	300 s	~	
Shutdown Schedule Time Settings	✓ Access Control			
- Client Settings	V Networks Settings			
	✓ Outlets			
	∧ Emails		=	
	Sender	E @eaton.com	~	
	Subject	Network Management Card	~	
	Include UPS name	1		

Once all / or part of settings are selected, click on the button "BULK APPLY".

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

← Bulk Apply (7)		🖿 Jeff-DC 🧳 📫	
		APPLY	5
		Ū	0
	Devices to Apply these Settings	1 Devices selected	
	Name Type Credential		
	ups (10.1:		

Click on "APPLY" to start the configuration on targeted assets. IPM will show the progress of the configuration, and display a message once operation is done.

	Devices to Apply these Settings			1 Devices selected
	Name	Туре	Credential	
Savir	ng Settings to Devices	Ay.		
0 0	f 1 Devices			DONE
Config	uration end status			
\oslash	ups (10 54)			CLOSE

2.10.2 Configure Network M2 card

From the asset list, select the source asset, click on configure and select the credential to authenticate to the device. Then, IPM will display all settings available for the asset. They are grouped by features :

&	← UPS-EATON-P01			🖿 LAB-A1-DEV 🔹 烨 💡 ᠄
tbrument				BULK APPLY
Account 🗸		~	Card	
DASHBOARD	Account service			
	• Card	~	Certificates	
POWER	Certificates	~	Date	
ENVIRONMENT	Date		Date	
ASSETS	Email	~	Email	
AUTOMATION	LDAP	~	LDAP	
STATUS	Measure			
SETTINGS	мұтт	~	Measure	
	Network	~	MQTT	
	Power outage policy			
	RADIUS	~	Network	
	Remote user	×	Power outage policy	
	Scheduled shutdown			
	Sessions settings	~	RADIUS	
	SMTP	×	Remote user	
	SNMP			
	Syslog	~	Scheduled shutdown	
Factors Preserve Discuss Restorate Intelligent Power Manager 2.0	Web server	~	Sessions settings	

With the possibility to expand the group content to display the settings of the group :

← UPS-EATON-P01			🗈 LAB-A1-DEV 🝷	P 🤉 🕴
				BULK APPLY
	^ Card			
Account service				
Card	identification name			
Certificates	identification contact			
Date	identification location			
Email			_	
LDAP	 Certificates 			
Measure	-	FR	_	
	country	38		
ΜQTT	state			
Network	location	Grenoble		
Power outage policy	organizationName	Eaton		
RADIUS	organizationUnit	Power Quality		
Remote user	contact			
Scheduled shutdown	^ Date			
Sessions sottings				
Sessions settings	ntp enabled	true		
SMTP	ntp getServersFromDhcp	false		
SNMP	ntp servers preferredServer	n, m		
Syslog	ntp servers alternateServer			
Web server	timeZone	Europe/Paris		

(i) 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.

Following features are available for the mass configuration (the list below may vary depending on the FW revision of the Network M2 cards used):

- 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
- Webserver : protocols settings / HTTPS server settings

Once one or more groups of features are selected, click on the button "BULK APPLY".

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

← Bulk Apply (1)				LAI	B-A1-DEV 🝷	4 <mark>0</mark>	?	÷
							APP	LY
	Device	es to Apply these Settings		3 Device	es selected			
		Name	Туре	Credential				
		UPS-EATON-P03 (10.1 22)	ups	L Update				
	\checkmark	UPS-EATON-P01 (10.1 20)	ups	O Update UPS Public-IPM2 Demo				
	~	UPS-EATON-P04 (10.1 23)	ups	O Update UPS Public-IPM2 Demo				
	~	UPS-EATON-P02 (10.1 21)	ups	O Update UPS Public-IPM2 Demo				

Click on "apply" to start the configuration on targeted assets. IPM will show the progress of the configuration, and display a message once operation is done.

		← Bulk Apply (1)						4		
tbrument									APPLY	
Account 🗸										
DASHBOARD							_			
VOWER	Saving S	ettings to Devices								
ENVIRONMENT										
ASSETS	3 of 3	Devices								
automation										
STATUS							DONE			
🔅 SETTINGS	_		UPS-EATON-P02	(10.1 21)	ups	O Update UPS Public-IPM2 Demo	_			
FAT-N Perenty Exclusion										
Intelligent Power 2.0	wanager									

Conf	iguration end status	
\oslash	UPS-EATON-P04	
\oslash	UPS-EATON-P02	
\oslash	UPS-EATON-P01	
		CLOSE

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 sequences 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 sequence 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
- Edit automation
- Manage the Automation settings

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)

≡	Automation					Datacenter LAB-A1-DEV	•	08:32:09	?	1
:: *	Create new	Automation Settings	Delete	Q _{search}						II
0	Status	Trigger Type	Name 🕈		Last Execution		Detail			
	□ □ Inactive	Multiple triggers	Cluster Shutdown		-		-			
۰	Active Ready	Manual	Maintenance Pow	er Off	08:28:43 08:28:55	\checkmark	End	of process, su	ICCESS	
0	Active Ready	Power	Protection Policy		-		-	0	0	· • •
\$										
							ltems per pag	e <u>25 -</u>	1-3/3	$\langle \rangle$

Actions buttons found to the right of the table allow you to:

- 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
- 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

Detail of action buttons :



Example of execution history for an "automation" :

Automation history: SRV and VM shutdown on SRV70

Execution list 👕

•	17:00:00 17:13:14 × 21-04-2020 ×	End of process, error
•	17:00:00 17:02:10 × 20-04-2020	End of process, error
•	17:00:00 17:02:10 X 19-04-2020	End of process, error
•	17:00:00 17:02:10 X 18-04-2020	End of process, error
•	17:00:00 17:13:14 X 17-04-2020	End of process, error
•	17:00:00 17:13:54 16-04-2020 16-04-2020	End of process, success
►	17:00:00 17:00:00 16-04-2020 16-04-2020	(0:0:0) 🗸 Start automation
S	17:00:00 17:02:00 16-04-2020 16-04-2020	(0:2:0) 🗸 Wait 120 seconds
<u>.</u>	17:02:00 17:03:15 16-04-2020 16-04-2020	(0:1:15) 🗸 Shutdown on NutanixValid
S	17:03:15 17:13:16 16-04-2020 16-04-2020	(0:10:1) 🗸 Wait 600 seconds
<u>.</u>	17:13:16 17:13:54 16-04-2020 16-04-2020	(0:0:37) 🗸 Shutdown VMs Then Host on pc70-hp-esxi.Labo.Kalif.com
•	17:13:54 17:13:54 16-04-2020	(0:0:0) 🗸 End of process, success

Automation Settings

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

From this menu, it's possible to

Manage Scripts :

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 :

- Upload new scripts
- Edit existing scripts

+ Automation Settings		
Scripts Management Notifications		
IMPORT		
Script Name		
Shutdown-Policy1.sh.txt		
	Upload Script ×	
	File	
	Choose File No file chosen	
	CANCEL UPLOAD	

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.

← Automation Settings				
Scripts Management Notifications				
Mailing list default value				
user1-test@eaton.com	×			
user2-test@eaton.com	×			
Add new email	+			
	SAVE			

Automation creation wizard

This section will detail the main configuration steps for an automation.

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

Automation name * -		<u>ipient(s)</u>	
Triggers	Neve	r Expires Ō	
Insert Trigger	r	Î	
lf	Opwer issue Opwer issue Other Alar Image: Comparison of the province in the provinc		
Optional +	Optional + ADD ANOTHER		
Actions			
Insert Action			
Then	K Č Shutdown IT Action Send a not Set a time Custom Sc Check Initi		

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

(i) Note

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

(i) 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.

1 2 Edit Event Select Assets	
O UPS has an internal failure	
O AC power outage on UPS	
O AC power outage on CoPS	
O UPS running on bypass	
O CoPS running on bypass	
O UPS estimated remaining battery runtime is less than	1 0 s

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

Automation view

-	2			
Edit Event	Select Assets			
Only act	if all of the selected devices are trigg	ered		
Search		٩		
	Name 🕇	Location	Туре	Model
	PROD	Rack1	ups	-
	UPS-EATON-P01	Rack1	ups	-
	UPS-EATON-P02	Rack2	ups	-
	UPS-EATON-P03	Rack3	ups	-
	UPS-EATON-P04	Rack4	ups	-
	ups	Rack01	ups	Eaton 9SX 3000i

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.

Manufacturer

EATON

Status

active

active

active

active

active

active

Priority

P2

P1

P1

P1

P1

P5

You must select the day and time to start the automation and one of the recurence 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.

Automation name * Automation example 001			<u>O Recipientis</u>) 🗹 Never Expires - Ō
Triggers			
If A Power Event - ups AC pow	outage on 1 asset		ā 🖍
Optional + ADD ANOTHER AND	OR		
Actions			
Insert Action			
Then K	IT Action Send a not Õ	Custom Sc	

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

Action sequences

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

(i) **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 are ending by the same last step about the automation behavior at the end of the execution of each action.

You can ask the system to either check the initial trigger state at this point and, in case it would be no longer valid, stop the action sequence right here or you can ask the system to ignore the initial trigger validity and continue whatever is its state.

This allow to control if the sequence has to be performed entirely wathever happens after it has been triggered or if it has to stop as soon as the initial conditions that triggered it are no longer valid.

An independant check point of the initial trigger state can also be added as an independant action.

Example 1



Once started, this sequence may only stop after Action 30 making Action 40 an optional step performed only if the initial trigger is still true at this point.

Example 2



This second example performs the same as the first except the check point is made independant from Action 30 by adding a specific check initial trigger action of its own. This gives more flexibility on the ordering and addition of new steps keeping the check point at the same place (before Action 40 in the example).

(i) Note

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

(i) Note

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

- your software licence
- the kind of assets configured in your IPM application
- the kind of virtualisation 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:

- Shutdown hardware
- IT action
- Send a notification

- Set a timed delay
- Custom script
- Check initial trigger validity

Shutdown 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

First, you must select the type of device (ePDU or Server), then an action On or Off.

1 —	2		3				
dit action	Select Outlets		Select Conditional A	Actions			
Vhat should	d turn on/off?						
이 ePDU							
 Server 							
urn Off	Turn On						
elect ePDU							
elect ePDU							
Search epd	dus		Q				
	Name 🛧	Туре	IP	Location Name	Manufacturer	Status	Prio
	Name 1	Type epdu	IP	Location Name Rack1	Manufacturer EATON	Status	Prior P1
			Ρ				

IT actions

(i) 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 licence 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 aplicable to some physical servers either discovered by a 3rd party connector (e.g. connector to HPE OneView) or directly reachable by SSH protocol.

Actions are grouped by sub-categories:

- vAPP 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)
 - powerOn
 - powerOff
 - shutdownGuest
 - shutdownGuestWithTimeout
 - suspend
 - resume
 - migrate

- Host Power Action: These actions apply to some targeted hypervisor(s)
 - Shutdown host
 - Shutdown VM then Host
 - 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
- Cluster shutdown action: These actions apply to some targeted cluster(s)
- Storage action:
 - Execute a shutdown on a storage node
- HPE OneView server action:
 - Power On
 - Power Off
 - Power Capping
- 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

1	2	3	4
Select group	Select Action	Select Assets	Select Conditional Actions
Select action group	:		
• vApp Power Action			
VM Action			
Host Power Action			
Cluster Power Action			
Storage			
HPOV Server Action			
Recovery Plan (SRM)			
Server Action			
Fault Domain			

Send Message action

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

nfiguration action	Select Conditional Actions	
Email *		
Content *		

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.

Wait	Battery %	Battery Runtime	
Wait Duration (sec	conds) *		

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.

1	2	3		
Select S	Execution context (O	Select Conditional		
+ Impo	ort			
			Search script	Q
		Name 1	•	
			No scripts found	

(i) 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.

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 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.

action	2 Select Servers	3 Select Conditional Actions				
n Rack 1 🙁						
🔿 Static (Opnamic Create new dynamic grou	p				Search
	Name 🕇	Туре	IP	Status	Priority	
	BLUE assets				-	:
	Hosted by vesxi67-01				-	:
~	In Rack 1				-	:
	In Rack2				-	:
	RED Assets				-	:
						page 25 👻 1-5/5 <

Add Another Action : build a sequence

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.

Automation		Lab A1 MBT	-		?	
Automation name * Automation Power Los	is or High Temp		<u>0 Recip</u>			ĺ
Triggers			Never I	Expires	0	
lf ▲	Power Event - ups AC power outage on 1 asset			Ō,		
OR 8	Environmental Event - High temperature (60 °C) on 1 asset			Ō,		
Optional + ADD AI	NOTHER AND OR					
Actions						
Then	It Action - group:server - hostname:host.com -port:12345 On Action Error: Start 'Automation new-automation' + stop		Ō	/	H	
Then	O Wait 360 second(s) - -		Ō			
Then	Check Initial Trigger validity On Initial Trigger Loss: Stop		Ō		•	
Then	Power Action on e-PDU: 2 assets selected On Action Error: Stop		Ō		H	
Insert Action						
					Sav	

2.12 Status dashboard

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

≡	Status	Uzadenter 2021-03-29 LAB-A1-DEV 11:11:33	?	P B
:: ♥ ● ::: \$ 0	System Information Serial number 391849eb-84d8-4872-91e9-69108223144b Software Version IPM_Editions-va-2.3.0+30_x86_64 Installation date 2021-03-25 Product IPM Editions VA Name eaton:rc-0050586aca84 Clock 11:10 2021-03-29 Legal Information	Metrics Uptime 6d 23h Memory 32% Total 7.79 GB Used 2.45 GB CPU Usage 2% CPU Temp Unknown		
\$	System storage usage 7 % Total 62.87 GB	Network Information eth0 Received 14.95 KB/s Errors 0% Transmitted 10.52 KB/s Errors 0%		
	Data storage 1 usage 2 % Total 62.87 GB Used 1.42 GB	Logs Download all the logs here Main	<u>tenance</u>	Logs

It provides you with application information and real-time metrics related to aplication 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
- andSystem 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.

		Datacenter LAB-A1-DEV	•	207 17:	•	admin administrator	
ations	Upgrade		ocal-Users		/	Account settings	>
					0 .	Change Password	
					€	Logout	
						Feedback	
					0	Legal Information	

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,

Account settings		×
Account details	Preferences	
Full Name DC Admin	Language English (US)	•
Email	Date format yyyy-mm-dd	•
Phone	Time format 24h	*
Organization	Temperature Celsius	~
		Save

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/STS

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%	
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.

Data Center Alarm Settings

For the Data Center alarm settings, you have the ability to set thresholds for both warning and critically high power usage alarms specific to your data center.

ttings										🖽 La	b A1-DEV	4 <mark>9</mark>	
count	Alarms	Connectors	Datacenter Layout	Date & Time	License	Moni	itoring	Network	Security Wallet	Notifications	Upgrade	Users	
	Data Center	UPS Row	Rack PDU	ATS/STS						14	l Alarms 1 Da	ta Center	
	DC-IPM2										14 1	hresholds	
IF	Parameter Temperature	e in datacenter Lab /	A01 DEV is critically low.	Value 14,0	С	THEN	Notify Send e-r	mail		~			
IF	Parameter Temperature	e in datacenter Lab <i>i</i>	A01 DEV is low.	Value 17,0	С	THEN	Notify None			~			
IF	Parameter Temperature	e in datacenter Lab /	A01 DEV is high.	Value 27,0	С	THEN	Notify			~			
IF	Parameter Temperature high.	e in datacenter Lab /	A01 DEV is critically	Value 30,0	С	THEN	Notify Send e-I	mail		~			
IF	_{Parameter} Humidity in	datacenter Lab A01	DEV is low.	Value 40	%	THEN	Notify None			~			
IF	Parameter Humidity in	datacenter Lab A01	DEV is critically low.	Value 30	%	THEN	Notify Send e-r	mail		~			
	Parameter			Value			Notify						

UPS Alarm Settings

On the UPS alarm settings page, you have the capability to set thresholds for UPS alarm management. These thresholds are set locally on the IPM instance.

The user can set certain thresholds at once for multiple UPSs.

To do so:

- Select the target devices,
- Click on Change UPS thresholds
- Enter the details in the text fields
- Click on the **Apply now to all UPS** button.

hange UPS thresholds	
Battery Level in UPS is low_warning	%
Battery Level in UPS is low_critical	9
Input voltage (1 phase) in UPS is low_critical	V
Input voltage (1 phase) in UPS is low_warning	V
Input voltage (1 phase) in UPS is high_warning	V
Input voltage (1 phase) in UPS is high_critical	V
Input voltage (3 phase) in UPS is low_critical	V
Input voltage (3 phase) in UPS is low_warning	V
Input voltage (3 phase) in UPS is high_warning	V
Input voltage (3 phase) in UPS is high_critical	V
Phase imbalance in UPS is high_critical	%
Phase imbalance in UPS is high_warning	%
Default load in UPS is low_critical	%
Default load in UPS is low_warning	%
Default load in UPS is high_warning	96
Default load in UPS is high_critical	96
Internal temperature in UPS is low_critical	C
Internal temperature in UPS is low_warning	C
Internal temperature in UPS is high_warning	C
Internal temperature in UPS is high_critical	C

Row Alarm Settings

On the Row alarm setting page, you have the capability of setting thresholds for alarm management for rows in your data center. The thresholds are set locally in the IPM application.

It is possible to change following thresholds:

- Temperature.
- Humidity.

You may set specific thresholds at once for multiple rows.

To do so:

- Select the target rows,
- Click on Change Row thresholds
- Enter the details in the text fields
- Click on the Apply now to all Rows button

Setting Views

Change Row thresholds	
Humidity in row is critically high	%
Humidity in row is high	
Humidity in row is critically low	5
Humidity in row is low	5
Temperature in row is critically high	C
Temperature in row is high	C
Temperature in row is critically low	C
Temperature in row is low	C
c	ancel Apply now to all Rows

Rack Alarm Settings

On the Rack alarm settings page, you have the capability of setting thresholds for rack level alarm management in your data center. The thresholds are set locally in the IPM application.

It is possible to change following thresholds:

- Temperature.
- Humidity
- Phase Imbalance
- Total Power in rack.

You may set specific thresholds at once for multiple racks.

To do so:

- Select the target racks,
- Click on Change Rack thresholds
- Enter the details in the text fields
- Click on the **Apply now to all Racks** button.

Humidity in rack is critically high	,
Humidity in rack is high	,
Humidity in rack is critically low	,
Humidity in rack is low	,
Phase imbalance in rack is critically high	,
Phase imbalance in rack is high	,
Temperature in rack is critically high	
Temperature in rack is high	
Temperature in rack is critically low	
Temperature in rack is low	
Total power in rack is critically high	V
Total power in rack is high	V
Total power in rack is critically low	V
Total power in rack is low	V

PDU Alarm Settings

On the PDU alarm setting page, you have the capability of setting thresholds for PDU level alarm management in your data center. The thresholds are set locally in the IPM application.

You may set specific thresholds at once for multiple target rack PDUs.

To do so:

- Select the target rack PDU,
- Click on Change PDU thresholds,
- Enter the details in the text fields,
- Click on the **Apply now to all selected PDUs** button.

ATS/STS 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 connectors:

- Virtualization:
 - VMware vCenter
 - VMware ESXi
 - Microsoft HyperV / Server
 - Microsoft SCVMM
 - Nutanix Prism Central / Cluster
 - Dell EMC VxRail
- Server:
 - Microsoft Windows Server
 - HPE OneView
- Storage:
 - NetAPP

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.

(i) Note

The virtualization connectors and IT actions supported per connector are detailled in the IPM Documentation section Automation / IT actions supported

Please note that some restrictions may apply with respect to your software licence and type of virtualisation connector configured as some actions are not avaiable on all connectors.

Add new connector

Click on ADD CONNECTOR and select the type of connector you want to configure : Virtualization, Storage or Server

Settings							
< Account	Alaı		Connectors	Data	acenter Layout	Date & Time	
➡+ ADD CONNECTOR	DELETE C	ONNECTOR	2				
Virtualization	►	VMware	vCenter				
Storage	►	VMware ESX/ESXI					
Server	►	Microsof	t Hyper-V / Server				
		Microsof	t SCVMM				
		Nutanix I	Prism Central / Cluster				
		Dell EMC	- VxRail				

Then enter valid credentials to finalize the connector configuration. Once a connection is established, the connector is added to the list:

Add a n	new 'V	Mware	ESX/E	SXi'	conne	ector	×				
Hostnam vesxi6	0-	ires *									
Passwor											
			CAN	CEL	ADD	CONN	ECTOR				
tings		Connec	ctor has been succe	ssfully created	GO TO VIRTUAI	L ASSETS				🗈 Lab A1-DEV	🗈 Lab A1-DEV
ount Alarms	Connectors	Datacenter Layout	Date & Time	License	Monitoring	Network	Security Wallet	Notifications	Notifications Upgrade	Notifications Upgrade Users	Notifications Upgrade Users
DD CONNECTOR	DELETE CONNECTO	DR I									

Delete connector

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

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

Acco	ount Alarms	Connectors	Datacenter Layout	Date & Time	License	Monitoring	Network	Security Wallet	Notification	s Up	ograde l	Jsers Sav	e & Restore
=+	ADD CONNECTOR	DELETE CONNECTO	R 🔋 2 items selected										
	Name			Type URI					Port	Login	Password	Status	Virtual Assets
	hpeoneview50.	ala ese com 443 🖌		http	<u>://hpeoneview</u>	1 <u>50</u>	AKI. Ə				•••••	0	Go to virtual assets
	vcenter-geonosis			http	os://vcenter-geo	onosis.	em.443. Ə				•••••	ø	Go to virtual assets
		1911 (all 1911 (com 141)		Delete cor	nnectors		× 🗇 Ə						
	vhyperv2019ws.	lat. etc. com 5585/wor	- 1	Are you su	re you want to	delete 2 connectors?	<u>(</u> 141)	Ð			•••••	ø	Go to virtual assets
			/		CANCEL	DELETE CONNECT	ORS						
				_									

2.13.4 Datacenter Layout

The **Data center layout settings** tab is accessible from the **Settings** 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.

≡	Settings					Datacenter	2021-03-29 11:21:39	0 🔺 🛃
	< Alarms	Connectors	Datacenter Layout	Date & Time	License	Monitoring	Network	Security Wal 🔉
٠							_	
٥	IPM is currently in dev	vice centric mode. Click	here to exit device centric moo	de in order to manage ti	ne datacenter layout.	Enable datacenter lay	rout	
=								
\$₀								
0								
٠								

Once you have enabled Datacenter Layout, you can create data center layout topology : rooms, rows, racks.

Data center topology objects are currently also created and managed from the Asset Management page.

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

ettings									🛅 Lab A1-DEV		4 <mark>9</mark>	
count	Alarms	Connectors	Datacenter Layout	Date & Time	License	Monitoring	Network	Security Wallet	Notifications	Upgrade	Users	9
Lab A	A1-DEV										1 Rooms	
A F	Room1										1 Rows	5
F	Row1		Rack1 💼	Rack2	â	Rack3	â	+ Add Rack				
			Rack4									
	+ Add Row											
+ Add F	Room											
										ard Changes	Save	_

Any data center must have at minimum a room containing a row with a rack inside.

Additional rooms, rows and racks may be defined. None of the existing assets can be edited in this page, but only completely removed.

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

Once the full layout has been defined, simply click **Save**. All new assets are visible now in the Asset management page.

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)

2.13.5 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.

Ac				Date & Time	License	Monitoring	Network	Security Wallet	Notifications	Upgrade	
	Date &	Time		-							0
		ic (NTP) O N									
			lanual								
	NTP Server										
	n	om									
-						_					
						Save					

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.

2.13.6 License

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

The License settings displays the license status and details of your IPM application.

All information regarding the features that your instance of IPM application is entitled to use as well as relevent expiration dates are displayed here.

IPM Editions come with a one week initial trial License. Longer duration trial licenses are also available on 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.

License

You have to activate license in the following cases:

- When receiving your activation ID to perform an initial activation,
- After updating SW, to refresh your existing license.
- License for Optimize Edition Single Node Subscription is valid until 2022-03-20
 - Max node credits: 300
 - Remaining node credits: 273
- License for maintenance is valid until 2022-03-20

2.13.7 Monitoring

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

Details

Activate license

SNMP

You may add **SNMP v1** community names and/or **SNMP v3** credentials. See the **Security Wallet section** for more information on SNMP credential configuration.

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

< Alarms	Connectors	Datacenter Layout	Date & Time	License	Monitoring	Network	Security Wallet	Notifications	>
SNMP Polling Interval (seconds) 30	0								
				Save	Server IP Address * Server Port * 2003 Basename				
					Graphite Connector Not Connected				

Graphite connector (optional)

Please see the General information > Graphite / Graphana 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) * 30 Basename MyDatacenter	Server IP Address * 1.1.1.1 Activate	Server Port* 2003	
			Save
0 Not Connected			

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

Graphite Connector Status

Connected
2.13.8 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** to apply the changes.

< Alarms	Connectors	Datacenter Layout	Date & Time	License	Monitoring	Network	Security Wallet	Notifications	>
eth0									
DHCP O Static									
IP address									
Subnet mask									
Default gateway									
DNS									
Prefer these nameser	vers to DHCP nameser	vers							
Preferred DNS server				Alternat	te DNS server				
1				1					
HTTP proxy									
HTTP(S) proxy URL (e.g.	http://proxy.company.com	com:8080)							
									Save

2.13.9 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

tings									🛅 Lab	A1-DEV	4 ⁸	
ount	Alarms	Connectors	Datacenter Layout	Date & Time	License	Monitoring	Network	Security Wallet	Notifications	Upgrade	Users	
	TE NEW	📋 DELETE	Search Credendi	al								
	▼ Authen	tication type	Search Credena	Name			Tags	Usages				
	Snmpv1			Discovery p	ublic			Discovery And Monitori	ng			
	Http(s)			admin				Mass Device Manageme	ent			
	Http(s)			main admir	ı			Mass Device Manageme	ent			

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 SNMP v1 credential

- 1. Click on the **Create new** button. By default **Snmp v1** is selected
- 2. Enter a Credential name
- 3. Set the Usage field to Discovery and monitoring
- 4. You may set user specified tags. E.g. Management vlan 2
- 5. Enter the community name E.g. **public**
- 6. Click the **Save** button

							Security Wallet
(+) CRE	ATE NEW	PEDIT É	Ĵ DELETE				
			Create Credent	ial			
	Authenticati	on type	Snmp v1 Snr	mp v3 Basic o	redential		
	Snmpv1	-	Credential Name				
		_	Usages *				•
			Add a tag and tap enter				
			Community Name				
						CANCEL	SAVE

Create a new SNMP v3 credential

- 1. Click on the Create new button
- 2. Select the **Snmp v3** tab
- 3. Enter a Credential name
- 4. Set the Usage field to Discovery and monitoring
- 5. You may set user specified tags. E.g. Management vlan 2
- 6. Enter the **Username**
- 7. 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
- 8. Depending on the security level you have selected, you will be prompted to add more information
- 9. Select the **Authentication security** algorithm (if applicable)
 - a. MD5
 - b. SHA-1
- 10. Select the Privacy security algorithm (if applicable)
 - a. DES
 - b. AES
- 11. Click the **Save** button

	Create Credential
_	Snmp v1 Snmp v3 Basic credential
Authentication type	Credential Name
Snmpv1	Usages *
	Add a tag and tap enter
	Username Username is required Protocol Security* AUTH_PRIV
	Authentication Security* MDS Authentication Password
	Privacy Security* DES Privacy Password
	CANCEL SAVE

Create a new Basic credential

- 1. Click on the **Create new** button
- 2. Select the **Basic credential** tab
- 3. Enter a Credential name
- 4. Set the Usage field to Mass Device Management
- 5. You may set user specified tags. E.g. ePDUs
- 6. Enter the **Username**
- 7. Enter the **Password**
- 8. Click the Save button

Account Alarms Connectors		Security Wallet
	n delete	
	Create Credential	
Authentication type	Snmp v1 Snmp v3 Basic credential	
Snmpv1	Credential Name	
	Usages *	•
	Add a tag and tap enter	
	Username	
	Password	
	CAN	EL SAVE

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**

Account	Alarms	Connectors	Datacenter Layout	Date & Time	License	Monitoring	Network	Security Wallet
⊕ CRE	ATE NEW	✓ EDIT	Ĵ DELETE					
			Search	Credential				
	Authenticat	ion type		Name		Tags	Use	ages
	Snmpv1			SNMP PUBLIC			Dis	covery And Monitoring
		CN					Disserv	
Auth	enticat	te to delet	e selected c	redential(5)			
Please	enter voi	ur own nassw	ord to confirm					
	, enter you	ar onn passw						

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" "passwd"

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" \$(secwcmd -u "My credential") \$(secwcmd -p "My credential")

"secwcmd" stands for "Security Wallet Command" and gives access to the login and password detail of a credential stored in the scurity wallet of IPM Edition by just mentionning 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.

2.13.10 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.

Account Alarms Connectors	Datacenter Layout	Date & Time		Monitoring	Network	Security Wallet	Notifications	Upgrade	
SMTP				SMS Gate	eway 🛛				8
Server m om Port 25	SMTP Server Au User Password	uthentication							Save
Sender Email joe.doe@mail.example.com No Encryption STARTTLS TLS Verify Certificate Authority									
Test Email email@something.com		Test Con	nection Save						

 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

2.13.11 Upgrade view

Overview

The **Upgrade settings** 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 **communication card firmware versions**.

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

int Alarms Connectors Datacenter Layout	Date & Time Lie	cense Monitoring	Network	Security Wallet	Notifications	Upgrade	Users	
grade Software								
IMPORT 🛱 DELETE 🗘 ACTIVATE								
firmware in the repository								
grade Devices								Quota Available : 126 392
grade Devices JIMPORT To DELETE OUPGRADE PROGRES	i5							Quota Available : 126 392
-	iS Version	Vendor	Туре	Product		Eligi	ible	Quota Available : 126 392 Progress

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.

When it is downloaded, it can be added to the system by clicking on "Import" and browsing to the dowloaded 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:

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

Upgrade Software	e 🗘 activate				1 items
Status	Version	Release date	Upload date	Activation date	File size
Active	2.3.0	2021-03-29	2021-03-29	2021-03-29	434.25 MB

Warning

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

Once a firmware package has been dowloaded, it maybe imported into the system by clicking on the **Import** button, then selecting the package with the file browser.

Once imported into the system, it appears in the firmware repository list and it may be selected.

At this point, click on the **Upgrade** button to start the firmware upgrade process.

TAGE Devices						Quota Available : 126 392 Kl
Name	Version	Vendor	Туре	Product	Eligible	Progress
eaton_network_m2_1.6.6.tar	1.6.6	EATON	UPS	Gigabit Network Card	0	

2.13.12 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.

i	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.
(i)	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

l	license	Monitoring	Network	Security Wallet	Notifications	Upgrade	Local-Users	Remote-Users	Save & Restore
LOCAL USER	RS								
🚭 Globa	al Settings	🕀 New	lete						
		Username	Email			Profile	Status		
	1	admin				Administrator	Active		
	1	monitor				Viewer	Passwo	ord expired	
	1	jo				Administrator	Active		
	1	jerome	je	:@ com		Administrator	Active		

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.

New user		
User details	Reset password	
Active	Generate randomly 🕖 Enter manually	
Yes		
	OUje6Pk	
Profile * Administrator	User will be enforced to change the password at next login	
	Please enter your own password to confirm	
Username *	Confirm password *	
new user		
	Lock account	
Full name		
	User account never blocks 💡	
Email	Password expiration	
	User password never expires 😮	
Phone		
Organization		
-		
		_
		Save

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 has to reauthenticate by entering his/her own password. The **Save** button will be activated only after this has been completed. 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

③ 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.

2.13.13 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.

LDAP configuration	×
Primary server	Secondary server
Name * Primary	Name Secondary
Hostname * 10.130.35.9	Hostname
Port 389	Port
ጬ Request parameters	Or Credentials
User base DN *	Anonymous search bind
ou=soft,dc=support,dc=mbt,dc=lab,dc=etn,dc=com	Search user DN *
User name attribute *	
uid	Password
Group base DN * ou=soft,dc=support,dc=mbt,dc=lab,dc=etn,dc=com	
Group name attribute *	
cn	
	Save

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

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

〈 Vlonitoring	Network	Security Wallet	Notifications	Upgrade	Local-Users	Remote-Users	Save & Restore
LDAP							
Activate Ldap					🔾 Configure 🔵	Profile mapping	2 User preferences
Name		Address	Port	Security	Certificate	Status	
Primary		10.1	389	9		ОК	

Profile mapping

The feature is about mapping remote groups to local profiles.

Profile mapping	×
Remote group	Local profile
Sales	Viewer
SupportTeam	Viewer
Engineering	Administrator
	Viewer
	~

Save

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.

Setting Views

Remote Users Preferences X Global Settings Language English (US) Temperature °F Date format Time format 24h



1. Press Users preferences to define preferences that will apply to all LDAP users

- Language
- Temperature
- Date format
- Time format

2. Click Save.

2.13.14 Save & Restore view

Overview

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

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.

Save

(De)select all	
Assets management	~
Auto discovery settings	~
Mass management settings	~
SNMP settings	~
Network settings	~
Notification settings	~
User session settings	~

Passphrase Description *		
Passphrase Confirm *		
		Save

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.

Setting Views

Save	
De)select all	
Assets management	^
Security Wallet	
Physical assets	
Virtual assets	
Alert settings	
Automation settings	
Automations	
Auto discovery settings	~
Mass management settings	~
SNMP settings	~
Network settings	~
Notification settings	~
User session settings	~
Dacenhraca Nacerintion *	
	Cancel Save

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.

Restore

This action is not recoverable The system will reboot and may have a different address Choose File restorelpm2Config (3).json						
	(De)select all					
	Assets management	~				
	Auto discovery settings	~				
	Mass management settings	~				
	SNMP settings	~				
	Network settings	~				
	Notification settings	~				
	User session settings	~				

Passphrase *

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.

Cancel Restore ...

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.

	Alarms	🖿 Lab A1-DEV 🏾 🧳 🚦
Admin 1 Account ~	Asset Type Severity Status Priority Name All • All • All •	7 Active 0 Acknowledged
DASHBOARD	Today Alarm details	
POWER	Active	Humidity in row Row1 is critically low.
	▲ 10:46 Humidity in datacenter Lab A1-DEV is critically low.	
ASSETS 1	os46 Humidity in rack <u>Rack4</u> is low. Active Name Row1	Status Active
automation	19-07-2019 priority P1	Location Room1
STATUS	Active	
SETTINGS	18-07-2019 0 09:27 Total power is high in rack Rack3. Active Active Active 	
	05-07-2019	
	11:06 Total power in datacenter Lab A1-DEV is critically high. Active	
	▲ 11.06 Total power is critically high in rack <u>Rack2</u> . Active ▼	
FAT-N Powering Basenas Vizabolite		
Intelligent Power Manager 2.0		

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. Asset Type
- 2. Severity
- 3. Status
- 4. Priority
- 5. Name

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

2.15 Feedback Tool

i 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.

	Send us some feedback!
	Found a bug? Have a suggestion?
	$\ensuremath{{ \bullet }}$ About the application in general $\ensuremath{{ \circ }}$ About this page
	Comment
	Enter you comment here!
	Reply Email
- 1	reply@mail.com
	Choose file No file chosen
- 1	
	I'm willing to participate in the product improvement program.
- 1	
- 1	
- 1	Send
	CONS

- 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

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.

Se	ttings								DC		• ?	A 8
<	Alarms	Connectors	Datace	enter Layout	Date & Time	License		Monitoring	Network		Security Wallet	Notificati 🔉
=	ADD CONNECTOR	DELETE CONNECTO	R Î									
												Ш
	Name		Туре	URI			Port	Login	Password	Status	Virtual Assets	
	myvcenter.my.lab:443	1		https://myvce	enter.my.lab:443 €				•••••	•	<u>Go to virtual asset</u>	<u>ts</u>

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).

Procedure to collect all required data to get some support

=	Intelligent Power Manager 2.3.0	Status	· • • • • • • • • • • • • • • • • • • •
	Dashboard	System Information	Metrics
٠	Power	Serial number	Uptime 36d 15h
٥	Environment	Software Version IPM_Editions-va-2.3.0 Installation date	Memory 32% Total 7.79 GB
≡	Assets	Product IPM Editions VA Name	Used 2.47 GB
۰,	 Automation Status 	Clock Legal_Information	CPU Usage 3% CPU Temp Unknown
•		Update	· · · · · · · · · · · · · · · · · · ·
۵	Settings	Storage	Network Information eth0 Received 46.99 KB/s Errors 0% Transmitted 679.47
		System storage usage 9 % Total 62.87 GB Used 5.42 GB	KB/S Errors 0%
		Data storage 1 usage 4 % Total 62.87 GB Used 2.2 GB	Logs Download all the logs here Maintenance Logs
	Powering Business Worldwide		

- 2. Save your configuration and share it
 - Open the settings page
 - Get to the Save & Restore tab
 - Click on the Save button

≡	Intelligent Power Manager 2.3.0	Settir	ıgs				• 0 📌 😫
5	Dashboard	< g		Security Wallet	Upgrade		Save & Restore
	Power	Sav	/e and Restore				
٥	Environment		ose an action to perform				
=	Assets			Save Restore			
¢.	Automation						
0	Status						
¢ (Settings						
	Powering Business Worldwede	v					

- 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	\sim
~	Auto discovery settings	\sim
~	Mass management settings	\sim
~	SNMP settings	\sim
~	Network settings	\sim
~	Notification settings	\sim
~	Users and sessions settings	\sim



Cancel Save...

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

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

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

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

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

- Introduction
- File global structure
- List of groups and features
- "Asset management" (group-assets)
 - Customize Physical Assets
 - Customize Automations
 - Customize Connectors in a file saved by IPM Editions

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 apply only to save files generated with version 2.3.0 of IPM Editions

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"
},
]
}

Each file have a mandatory fields:

- checksum It ensure that the file can be restore on IPM Editions. it cannot be modified otherwise, the file will never be accepted again.
- 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 this version:

- 1. group-assets "Asset management"
 - security-wallet "Security Wallet"
 - asset-agent "Physicals assets"
 - automatic-groups "Automatic groups"
 - virtual-assets "Virtual assets"
 - alert-agent "Alert settings "
 - automation-settings "Automation settings"
 - automations "Automations"
- 2. group-discovery "Auto discovery settings"
 - discovery "Auto discovery settings"
- 3. group-mass-management "Mass management settings"
 - etn-mass-management "Mass management settings"
- 4. group-monitoring-feature-name "SNMP Settings"
 - monitoring "SNMP Settings"
- 5. group-network "Network settings"network "Network settings"
- 6. group-monitoring-feature-name "Notification settings"notification "Email settings"
- 7. group-user-session-management "Users and sessions settings"
 - user-session-management "Users and sessions 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

Phisical assets (ups, epdu, ...) are saved into the feature called "asset-agent".

"Asset management" (group-assets)

High level asset-agent payload			
"asset-agent": {			
"status": "success",			
"version": "1.0",			
"error": "",			
"data": {			
"version": "1.0",			
"data": [
{},			
<i>{}</i>			
]			
}			

```
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": "",
```

Partial example of one asset		
"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,	"priority": 5,			
"tag": "",	"tag": "",			
"ext": {	"ext":{			
"name": {	"name": {			
"readOnly": false,	"readOnly": false,			
"value": "My name"	"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,	"priority": 5,		
"tag": "",	"tag": "",		
"ext": {	"ext": {		
"endpoint.1.protocol": {	"endpoint.1.protocol": {		
"readOnly": false,	"readOnly": false,		
"value": "nut_snmp"	"value": "nut_snmp"		
},	},		
"endpoint.1.nut_snmp.secw_credential_id": {	"endpoint.1.nut_snmp.secw_credential_id": {		
"readOnly": false,	"readOnly": false,		
"value": "b4e60d7e- dd0c-4515-94cc-791242dd51ae"	"value": "ace584855-47847485-477854ew-58844-447778544"		
},	},		
"endpoint.1.port": {	"endpoint.1.port": {		
"readOnly": false,	"readOnly": false,		
"value": "161"	"value": "8161"		
},	},		
"ip.1": {	"ip.1": {		
"readOnly": false,	"readOnly": false,		
"value": "192.168.0.1"	"value": "myups.mynetwork.com"		
},	},		
},	},		
"id_secondary": "",	"id_secondary": "",		
"linked": [],	"linked": [],		
"status": 2,	"status": 2,		
"subtype": "ups",	"subtype": "ups",		
"parent": "",	"parent": "",		

Payload without modification	Updated payload
"id": "ups-89890588",	"id": "ups-89890588",
"type": "device"	"type": "device"
}	}

5.4.2 Customize Automations

Introduction

Automations are saved into the feature called "automations".

All configured automations are described into automationList in json format.

High level automations payload

```
{
    "automations": {
        "version": "1.0",
        "status": "success",
        "error": "",
        "data": {
        "bundleVersion": "2.3.14",
        "automationList": [
        {...},
        {...}
        ]
      }
}
```

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",

ample of one automation		
"value": ["10"]		
}],		
"timeout": 3600,		
"onSuccess": null,		
"onFailure": null		
],		
'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",	"name": "My new automation name",
"comments": "",	"comments": "New automation comment!",
"createdBy": "admin",	"createdBy": "admin",
"active": false,	"active": false,
"schedule": "",	"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",	"name": "My automation name",		
"comments": "",	"comments": "",		
"createdBy": "admin",	"createdBy": "admin",		
"active": false,	"active": false,		
"schedule": "",	"schedule": "",		
"initialTrigger": "{0}",	"initialTrigger": "{0}",		
"triggerType": "CAT_OTHER",	"triggerType": "CAT_OTHER",		
"triggers": { },	"triggers": { },		
"tasks": [{	"tasks": [{		
"index": 0,	"index": 0,		
"name": "Wait 10 seconds",	"name": "Task waiting for 10 seconds",		
"group": "WAIT",	"group": "WAIT",		
"subgroup": "DELAY",	"subgroup": "DELAY",		
"properties": [{	"properties": [{		
"key": "duration",	"key": "duration",		
"value": ["10"]	"value": ["10"]		
}],	}],		
"timeout": 3600,	"timeout": 3600,		
"onSuccess": null,	"onSuccess": null,		
"onFailure": null	"onFailure": null		
}],	}],		
"notification": {	"notification": {		
"notifyOnFailure": false,	"notifyOnFailure": false,		
"emails": []	"emails": []		
}	}		
}	}		

Payload without modification	Updated payload

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

, ampre		
{	{	{
"name": "new-automation",	"name": "new-automation2",	"name": "new-automation3",
"active": false,	"active": false,	"active": false,
"comments": "",	"comments": "",	"comments": "",
"notification": {	"notification": {	"notification": {
"notifyOnFailure": false,	"notifyOnFailure": false,	"notifyOnFailure": false,
"emails": []	"emails": []	"emails": []
},	},	},
"schedule": null,	"schedule": null,	"schedule": null,
"initialTrigger": "",	"initialTrigger": "",	"initialTrigger": "",
"triggerType": "Manual	"triggerType": "Manual Override",	"triggerType": "Manual Override",
Override",	"triggers": {	"triggers": {
"triggers": {	"ipmInfraEvent": [],	"ipmInfraEvent": [],
"ipmInfraEvent": [],	"ipmItEvent": null,	"ipmItEvent": null,
"ipmItEvent": null,	"metricEvents": []	"metricEvents": []
"metricEvents": []	},	},
},	"tasks": [{	"tasks": [{
"tasks": [{	"index": 0,	"index": 0,
"index": 0,	"timeout": 3600,	"timeout": 3600,
"timeout": 3600,	"name": "It Action powerOff",	"name": "It Action powerOff",
"name": "It Action powerOff",	"group": "ACTION",	"group": "ACTION",
"group": "ACTION",	"subgroup": "IT",	"subgroup": "IT",
"subgroup": "IT",	"properties": [{	"properties": [{
"properties": [{	"key": "group",	"key": "group",
"key": "group",	"value": ["vms"]	"value": ["vms"]
"value": ["vms"]	},{	},{
}, { "key": "command",	"key": "command",	"key": "command",
	"value": ["powerOff"]	"value": ["powerOff"]
		., .

"value": ["powerOff"]	}, {	},{
}, {	"key": "asset",	"key": "asset",
"key": "asset",	"value": []	"value": [
"value": []	}, {	"vm-125075b",
}, {	"key": "groupIds",	"vm-127075b"
"key": "groupIds",	"value": ["2"]]
"value": ["5"]	}],	}, {
}],	"onSuccess": null,	"key": "groupIds",
"onSuccess": null,	"onFailure": null	"value": []
"onFailure": null	}]	}],
}]	}}	"onSuccess": null,
}}		"onFailure": null
		}]
		}}

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

{	{
"name": "My automation name",	"name": "My automation name",
"comments": "",	"comments": "",
"createdBy": "admin",	"createdBy": "admin",
"active": false,	"active": false,
"schedule": "",	"schedule": "",
"initialTrigger": "{0}",	"initialTrigger": "{0}",
"triggerType": "CAT_OTHER",	"triggerType": "CAT_OTHER",
"triggers": {	"triggers": {
"ipmInfraEvent": [{	"ipmInfraEvent": [{
"index": 0,	"index": 0,
"operator": "and",	"operator": "and",
"templateName": "input_voltage_low@namerule",	"templateName": "input_voltage_low@namerule",
"assets": ["assets": [
"ups-23"	"ups-42"
],],
}	}

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.

{	{
"name": "Utility return",	"name": " Utility return ",
"comments": "",	"comments": "",
"createdBy": "admin",	"createdBy": "admin",
"active": false,	"active": false,
"schedule": "",	"schedule": "",
"initialTrigger": "{0}",	"initialTrigger": "{0}",
"triggerType": "CAT_OTHER",	"triggerType": "CAT_OTHER",
"triggers": {	"triggers": {
"ipmInfraEvent": [],	"ipmInfraEvent": [],
"metricEvents": ["metricEvents": [
{	{
"index": 0,	"index": 0,
"assets": ["assets": [
"ups-59489058"	"ups-2256789"
],],
"operator": "OR",	"operator": "OR",
}	}

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.

```
{
    "virtual-assets": {
    "version": "2.3.13",
    "status": "success",
    "error": "",
    "data": {
        "assetList": [...],
        "assetList": [...],
        "assetLinkList": [...],
        "assetLinkList": [...],
    }
}
```

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": [
     {...},
     ł
       "id": 420,
       "asset": {
         "id": 31,
         "name": "connector-31"
       λ.
       "key": "URI",
       "value": "https://192.168.100.200:8443"
    <u>}</u>,
    {...}
  ],
  "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.

"Asset management" (group-assets)

Example



6 Appendix III - Using the command line interface (CLI)

- Introduction
- List of available commands
 - license-agreement.sh
 - license-activation.sh
 - fty-srr-cmd

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 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/myrestore.json