PowerApp - Your Energy Guard

PowerApp V5.8, 1. October 2024

iQSol
Security made in Austria.

Index

1 Components

The PowerApp solution consists of the following components:

- PowerApp (Hardware) or PowerApp VM (virtually based on VMware or Hyper-V)
  - Central Appliance for Management including database
  - Responsible for shutdown in headquarter
  - Cluster-capable
- PowerNode (Hardware) or PowerNode VM (virtually based on VMware or Hyper-V)
  - Appliance for shutdown in branches
  - Cluster-capable

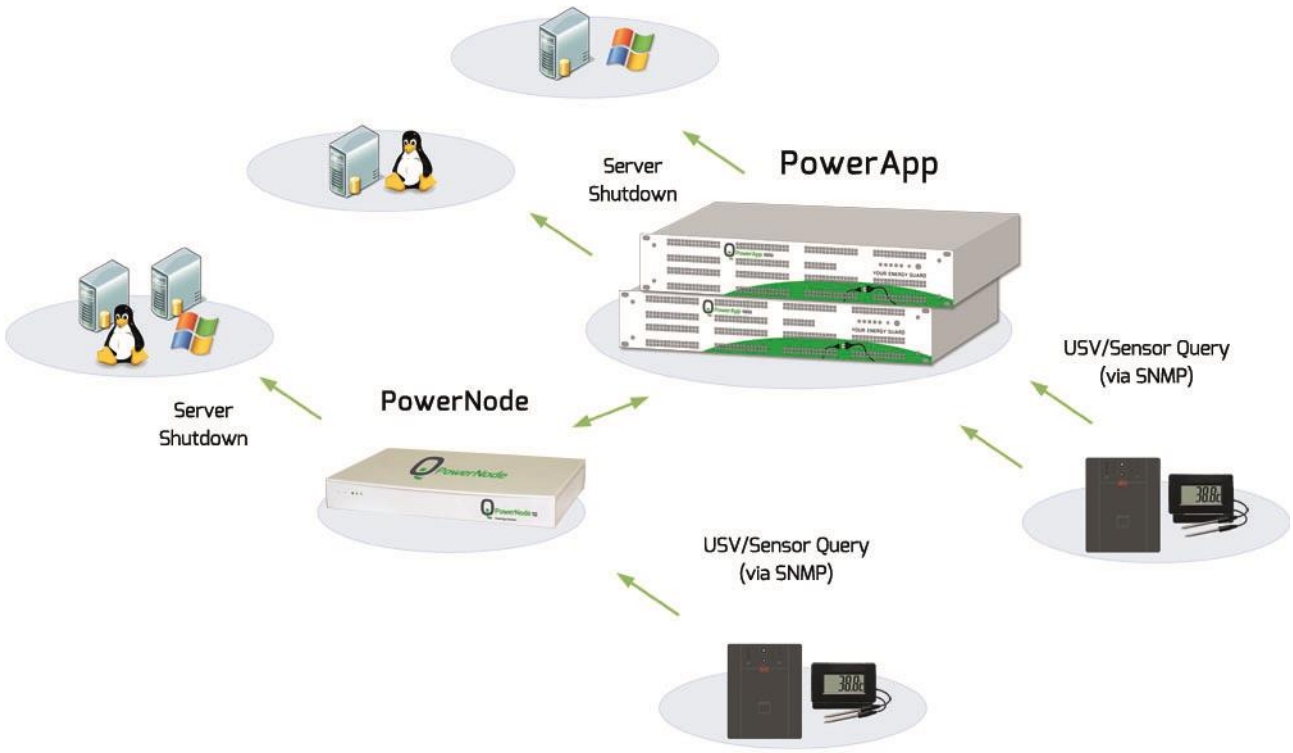


Figure 1: PowerApp Components

The PowerApp operates agentless, which means, that nothing needs to be installed on the systems (Windows/ Linux). The status of the UPS is determined by SNMP queries (using polling, not traps).

2 Installation

2.1 Requirements

2.1.1 Network Connectivity

The PowerApp operates using a network interface card. Interface bondDefault is used for management and provides the web interface. Due to agentless operation, it is necessary to guarantee access to all required systems on this interface by configuring appropriate firewall rules.

2.1.2 Required Ports

Following ports are required:

Function	Direction			Port
PowerApp/PowerNode outgoing communication				
SNMP-Queries	PowerApp/PowerNode	⇨	UPS/Sensor	161/UDP
Shutdown	PowerApp/PowerNode	⇨	Windows (legacy)	137-139 TCP/UDP 445/TCP
Shutdown	PowerApp/PowerNode	⇨	Windows (recommended)	5985/TCP 5986/TCP
Shutdown	PowerApp/PowerNode	⇨	Linux	22/TCP
Startup	PowerApp/PowerNode	⇨	MP	22/TCP
PowerApp incoming communication				
Synchronization	PowerNode	⇨	PowerApp	22/TCP 443/TCP 4444/TCP 4567/TCP 4568/TCP

Table 1: Required Ports

2.1.3 Optional Ports

Following ports are optional:

Function	Direction			Port
PowerApp outgoing communication				
Automatic update check	PowerApp	⇨	asf.anlx.cloud	443/TCP

Table 2: Optional Ports

2.2 Components

The central Shutdown-Appliance PowerApp and the PowerNode can both either operate as Hardware Appliance or as virtual machine. The operating modes can be combined as required.

In the case of an appliance, the software is already pre-installed; in the case of a VM installation, the software is delivered as an ISO image.

2.3 Powerapp Quick Start Guide

Figure 2: PowerApp Hardware

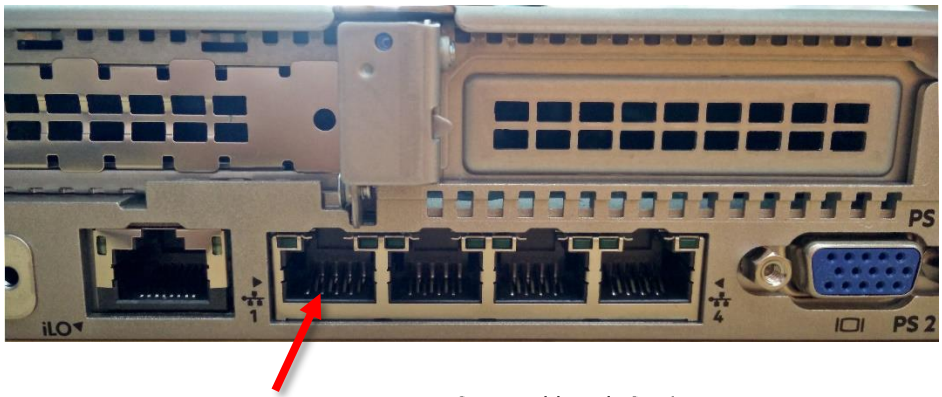
How to access the WebGUI:

Default IP/Netmask: 192.168.0.1/24
Default Gateway: 192.168.0.254
Default DNS: 192.168.0.254

Default user and password:
Superadmin

You can change the IP in System > System Settings.

On the CLI using a monitor and a USB keyboard or via the serial RS-232 port.
Enter:
ip bondDefault change



NIC Port 1 is configured by default.

Figure 3: PowerApp Port

2.4 ISO Image

The ISO is a hybrid ISO with UEFI and BIOS support. It can be booted in a VM in UEFI or BIOS mode. It also contains the required partition information for USB drives and can be copied directly to a USB flash drive.

An easy tool to copy the ISO to an USB disk is balenaEtcher.

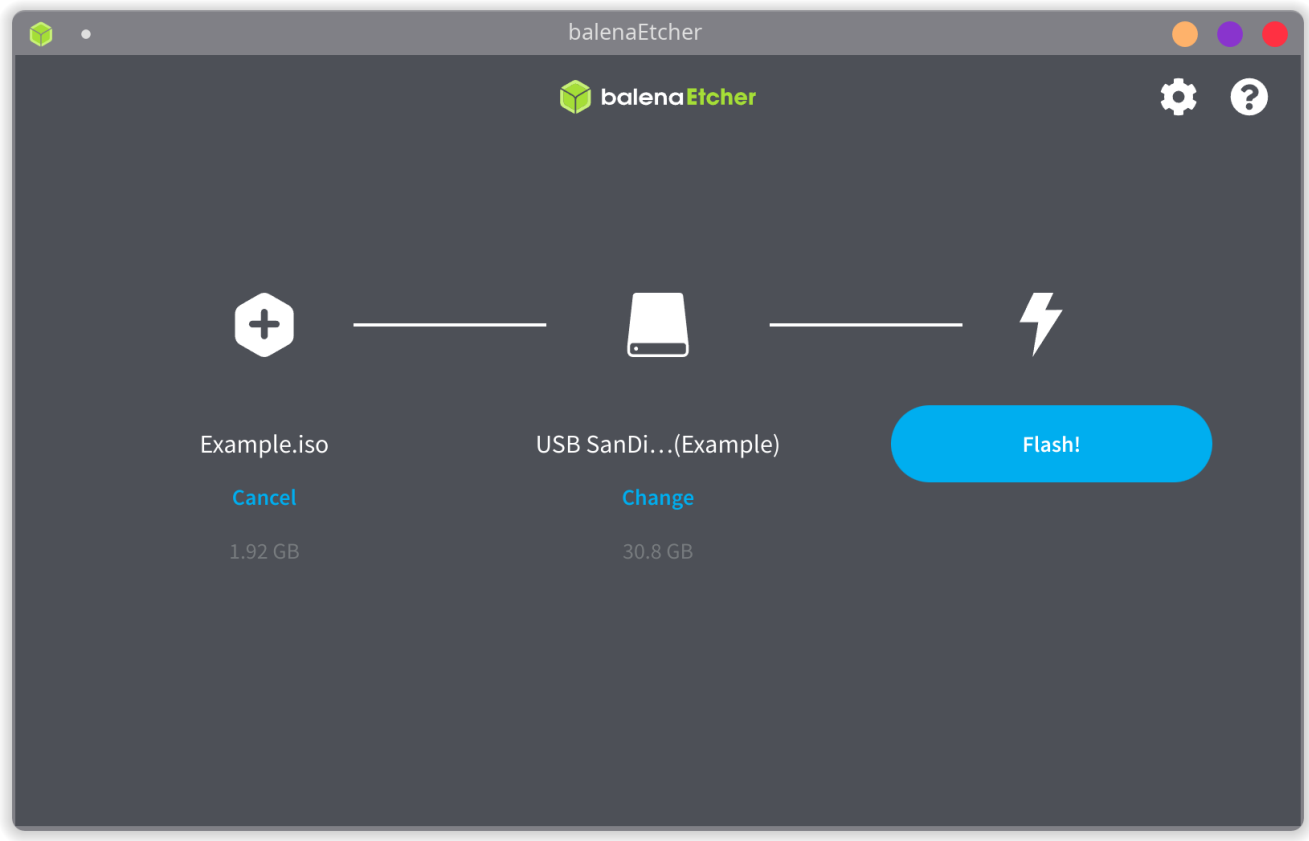


Figure 4: balenaEtcher

If you are familiar with the Linux CLI, you can also use a command like the following:

```
dd bs=4M if=path/to/example.iso of=/dev/sdx conv=fsync oflag=direct status=progress
```

Rufus is also suitable as an alternative GUI tool.

We recommend that you set your hardware to UEFI mode before the installation.

2.4.1 Requirements for virtual infrastructure

A virtual machine must be prepared with the following minimum requirements for this kind of installation:

- Dual Core CPU
- min. 4 GB RAM
- min. 60 GB HDD
- 1 Ethernet Interface

The accurate sizing (CPU, RAM, HDD) depends on the number of systems required for shutdown!

A static ip address must be assigned for the first network interface card during installation. The management interface is available on this ip address after installation is complete.

VMware Notes:

PowerApp is based on Ubuntu Server 64-Bit. This operating system needs to be assigned, while applying a new virtual machine in VMware.

We recommend setting the firmware to UEFI in the boot options.

2.5 Basic Installation

A menu for choosing the language is provided after installation is started. Choose a language for the installation process.

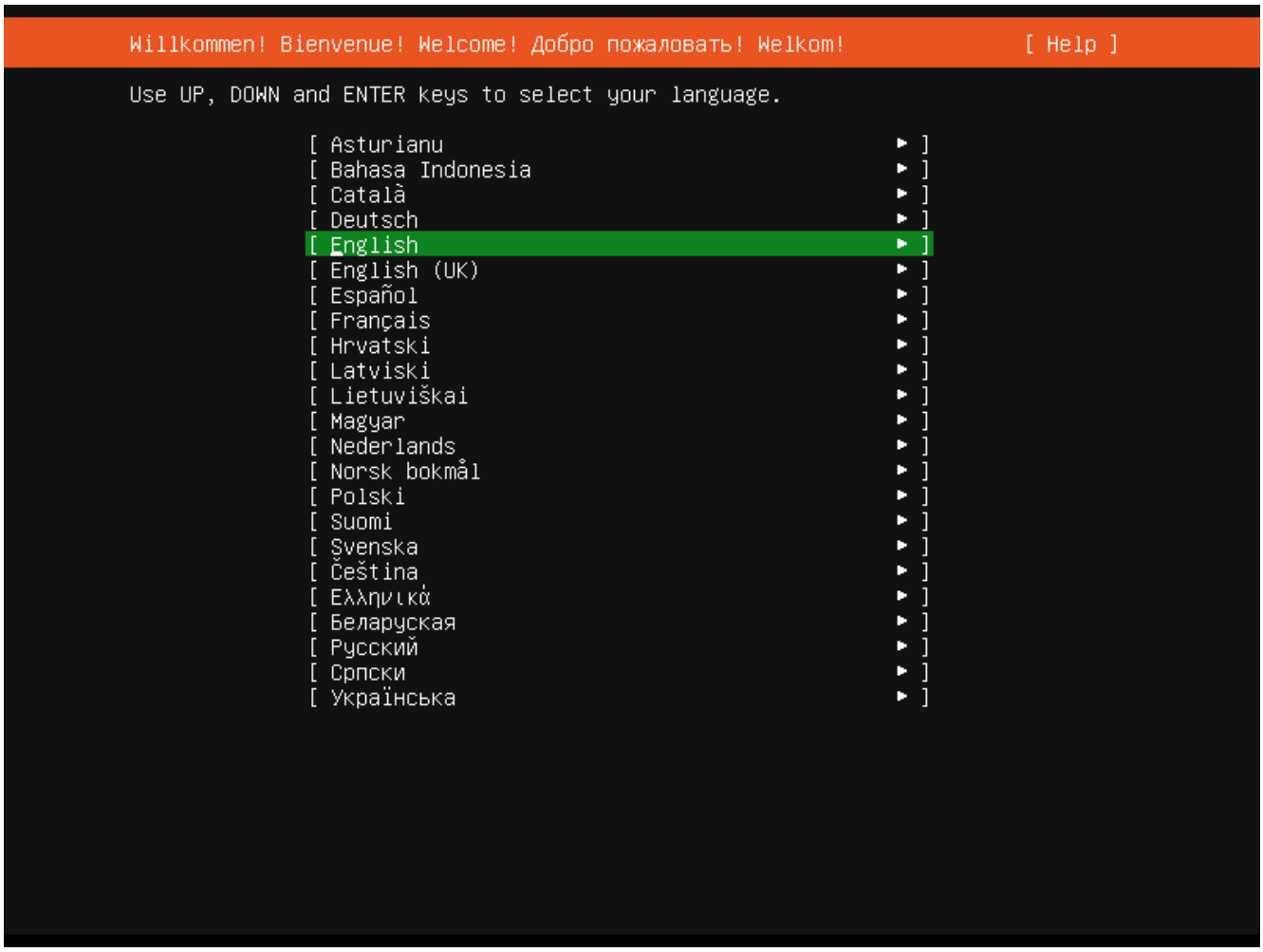


Figure 5: Language Selection

After the language selection a menu for keyboard configuration appears. Select your desired variant here and confirm with Enter.

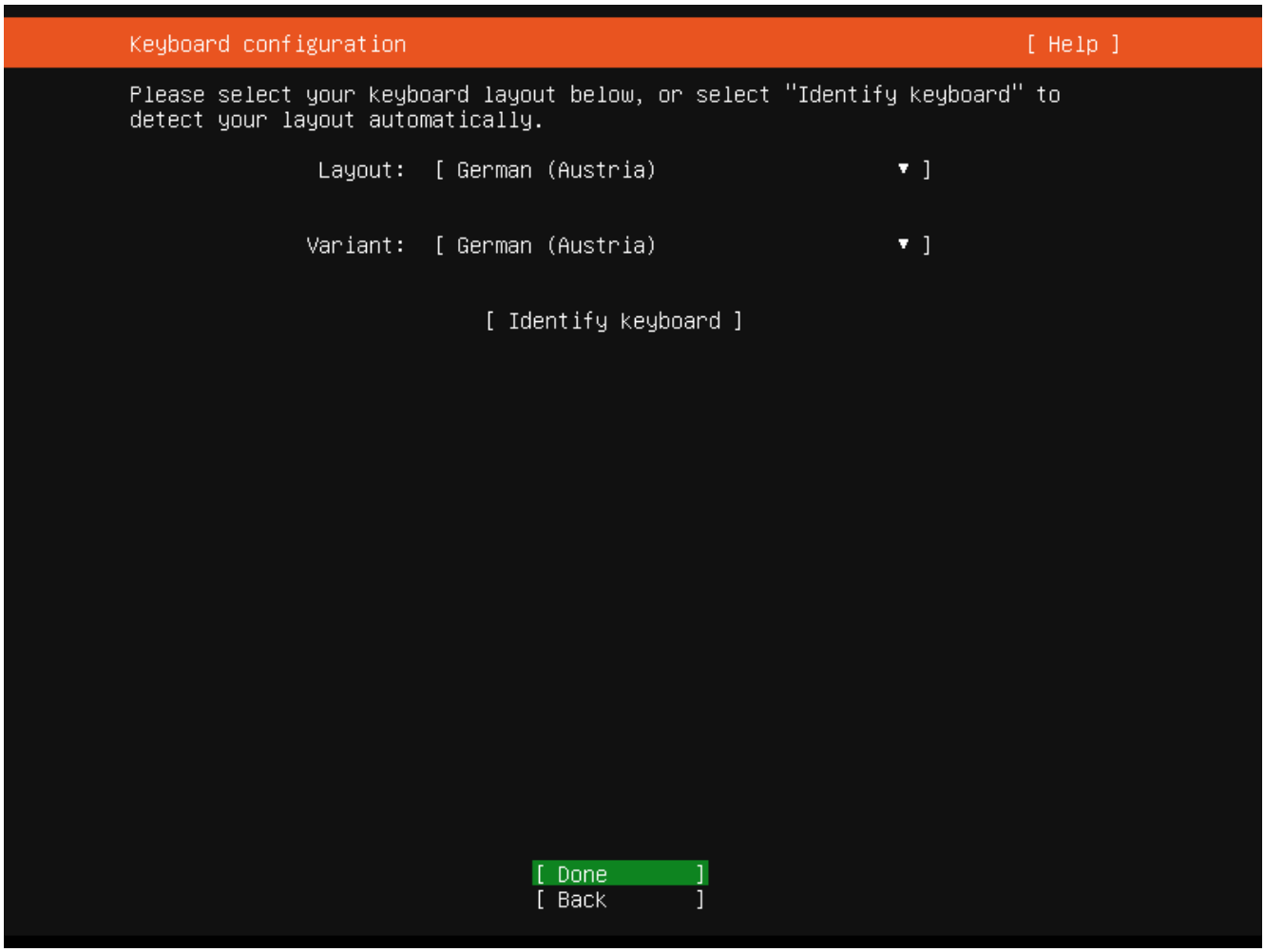


Figure 6: Keyboard Configuration

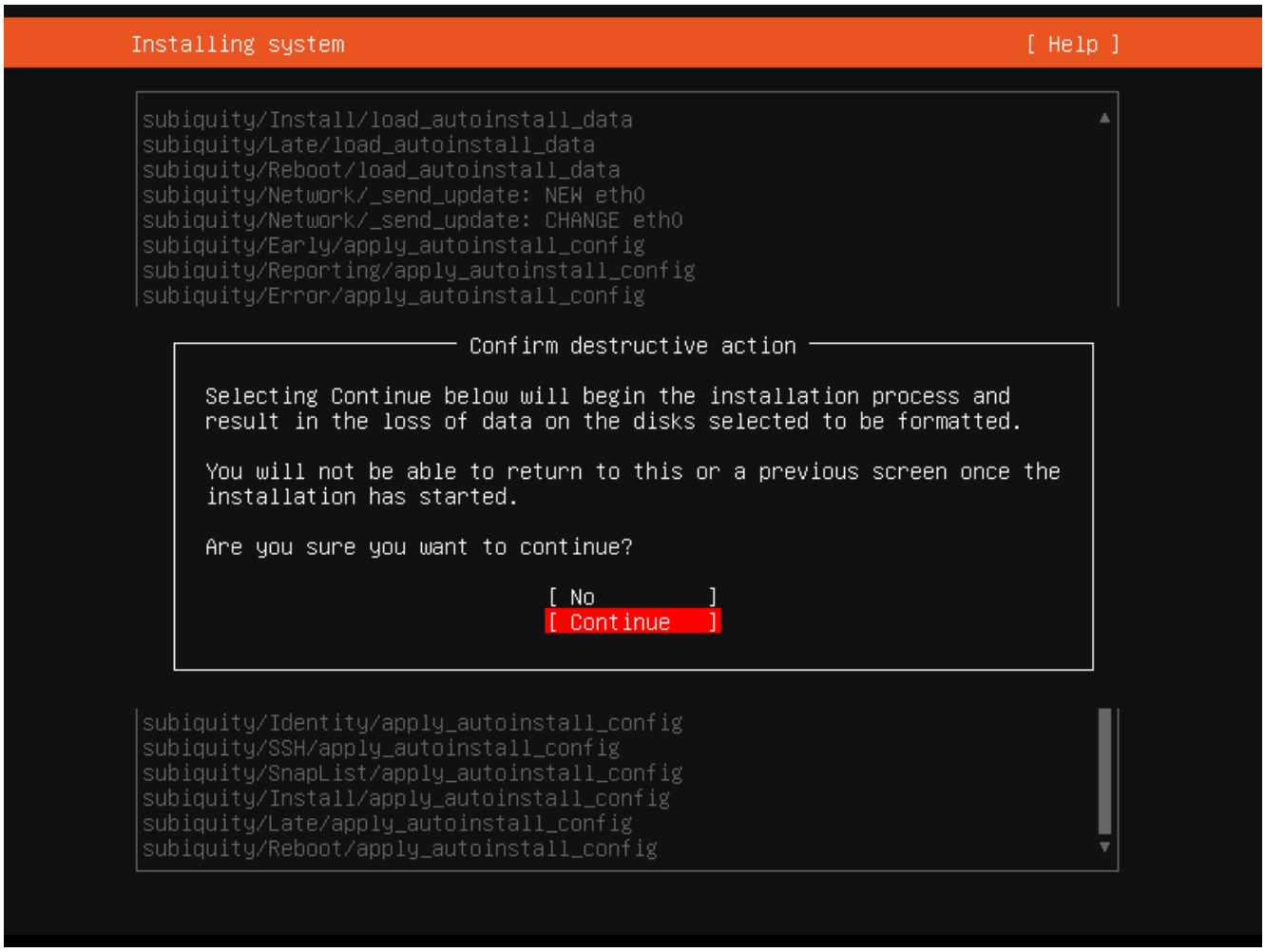


Figure 7: Continue installation

Select "Continue" to format the main hard disk and install the operating system.

After the installation process, you can login and configure the IP address.

Default user and password:
Superadmin

With the commad "ip bondDefault change" you can change the IP address, netmask and gateway.

Figure 8: Change IP

3 First Steps

3.1 Login

Login to the Management Interface with a web browser after installation is completed. Use the IP address, configured during the installation process. The request is automatically forwarded to a secure https connection. A certificate warning must be accepted on the first connection attempt.

The login mask prompts for username, password and client. The user „Superadmin“ was created during installation. Default Password: „Superadmin“. The client field stays empty at this time.

Two Login options are available:

- Login to the agentless central console with username „Superadmin“ and its password.
- Use username, password and client name to login to a configured client. When a new client is created, the user “Admin” with password “Admin” is automatically created for the first login.

Figure 9: PowerApp Login

3.2 Web Interface Structure

The dashboard is displayed after successful login. Different widgets provide an overview of the most important system information.

The menu is located on the left side of the PowerApp GUI. By clicking on a menu item, the sub-items appear, if available. Otherwise, the content is displayed in the right part of the window.

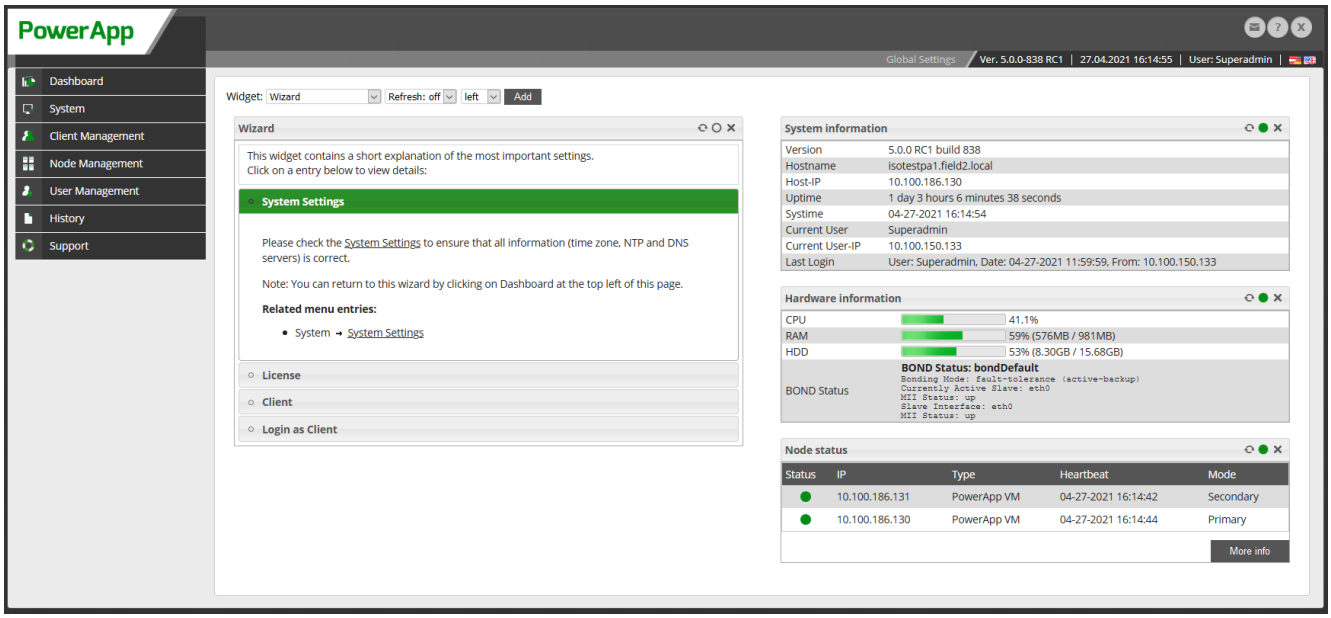


Figure 10: PowerApp Web GUI

Help texts are available for most pages of the web interface. These are displayed by clicking on "Info" at the bottom of the page.

3.2.1 Differences between superadmin and client

The web interface and the contents of the menu items differ depending on whether you are logged on as superadmin or client.

The superadmin environment is used to manage PowerApp. For example, the following administrative settings can be configured as Superadmin: Updates, licenses, IP address management etc. You can also create several superadmin users (see User).

As a Client the UPSs and servers that are to be included in the shutdown concept can then be managed.

3.2.2 Wizard widget

The contents of the wizard widget also differ depending on whether you are logged on as a superadmin or a client. The wizard widget guides you through the configuration process of the respective user and should be used during the initial configuration of PowerApp.

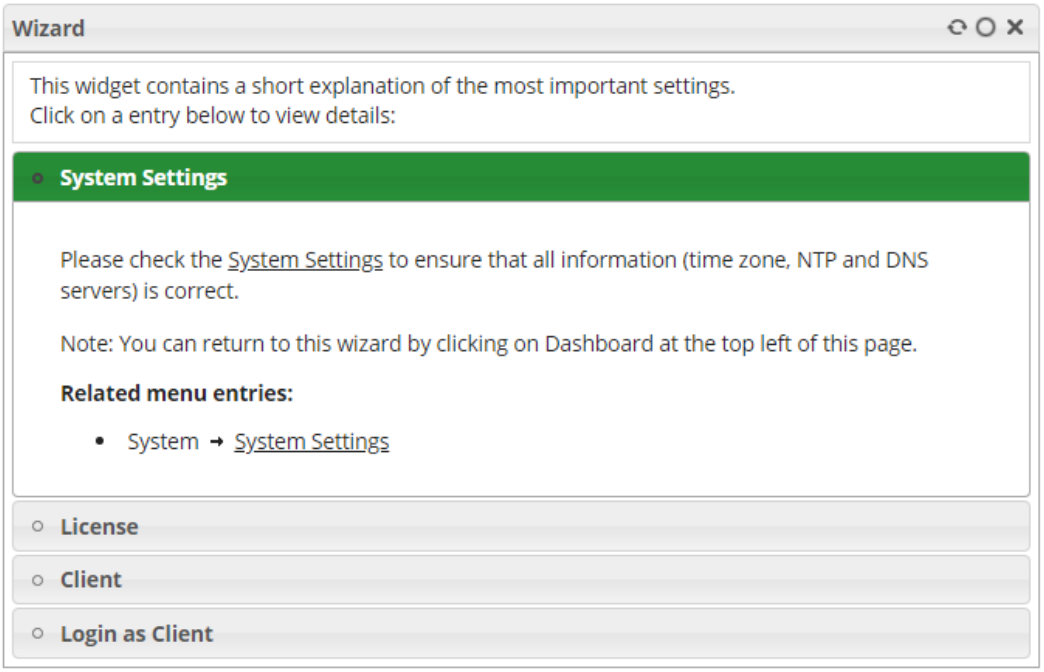


Figure 11: wizard widget as superadmin

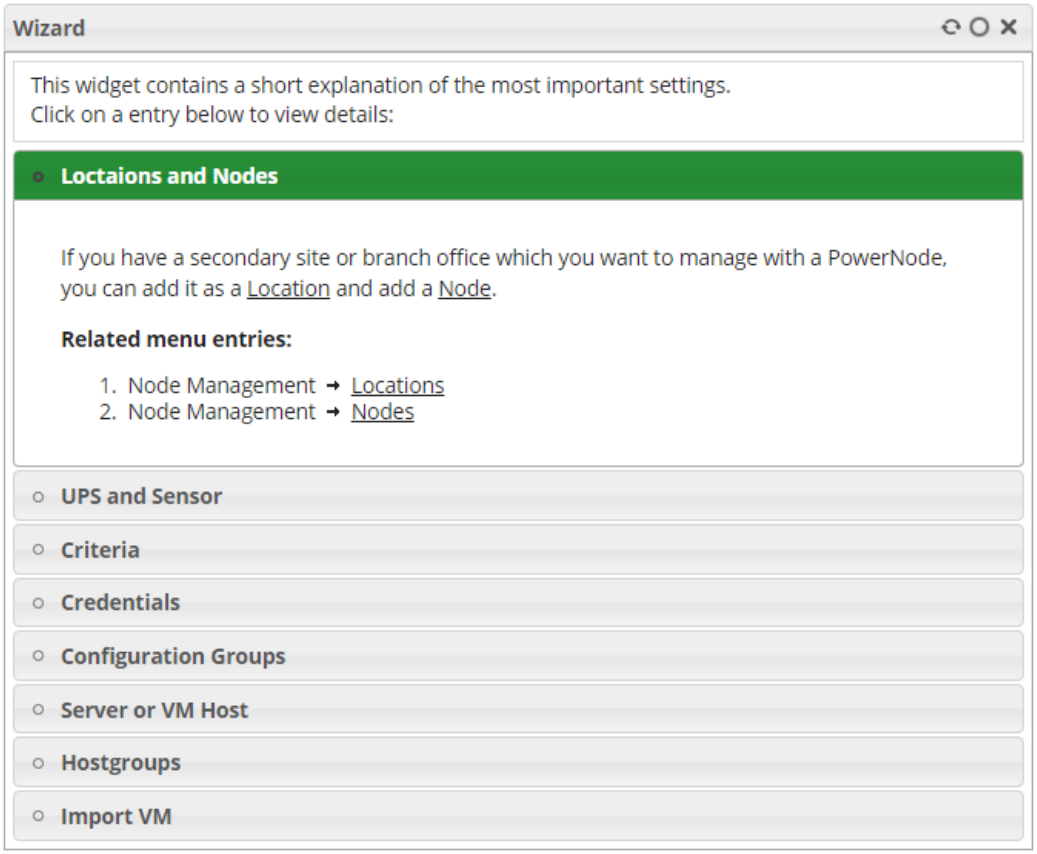


Figure 12: wizard widget as client

4 Configuration via wizard widget

4.1 Configuration of the Superadmin environment

4.1.1 System Settings

First, all system settings such as time, NTP and DNS servers must be checked and corrected if necessary. To do this, click on the underlined words System Settings in the wizard-widget-window.

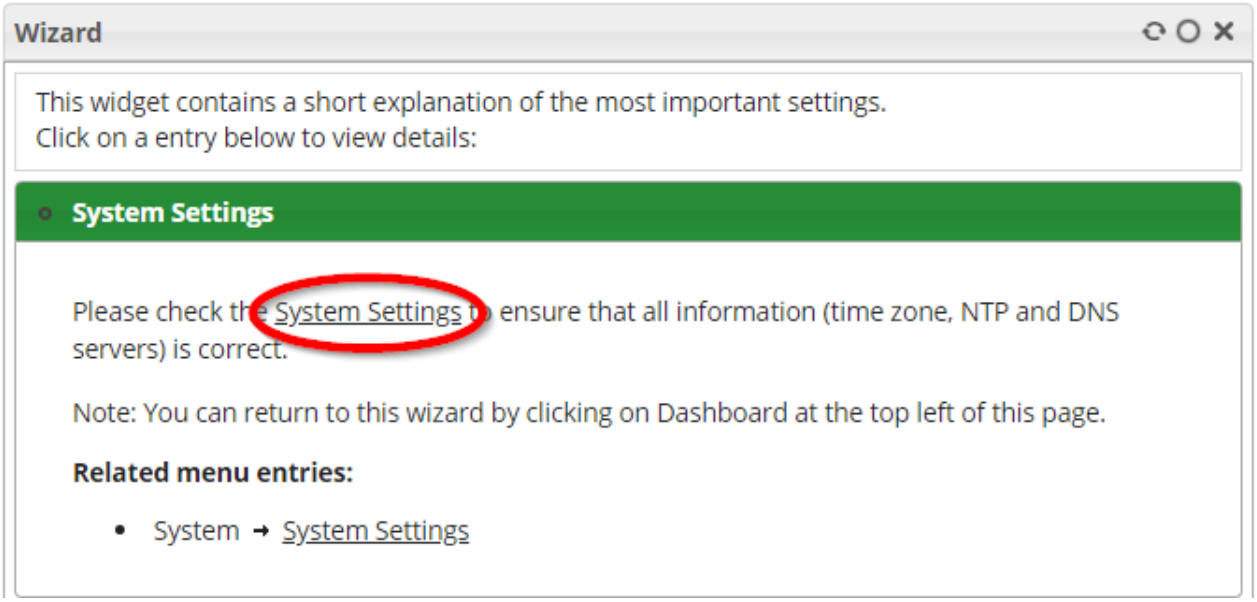


Figure 13: System Settings wizard-widget-window

1. Check all system settings and make any necessary corrections.
2. Apply the settings by clicking on the "Apply" button at the bottom right.
3. Then go back to the dashboard by clicking "Dashboard" in the left menu to continue with the wizard widget.

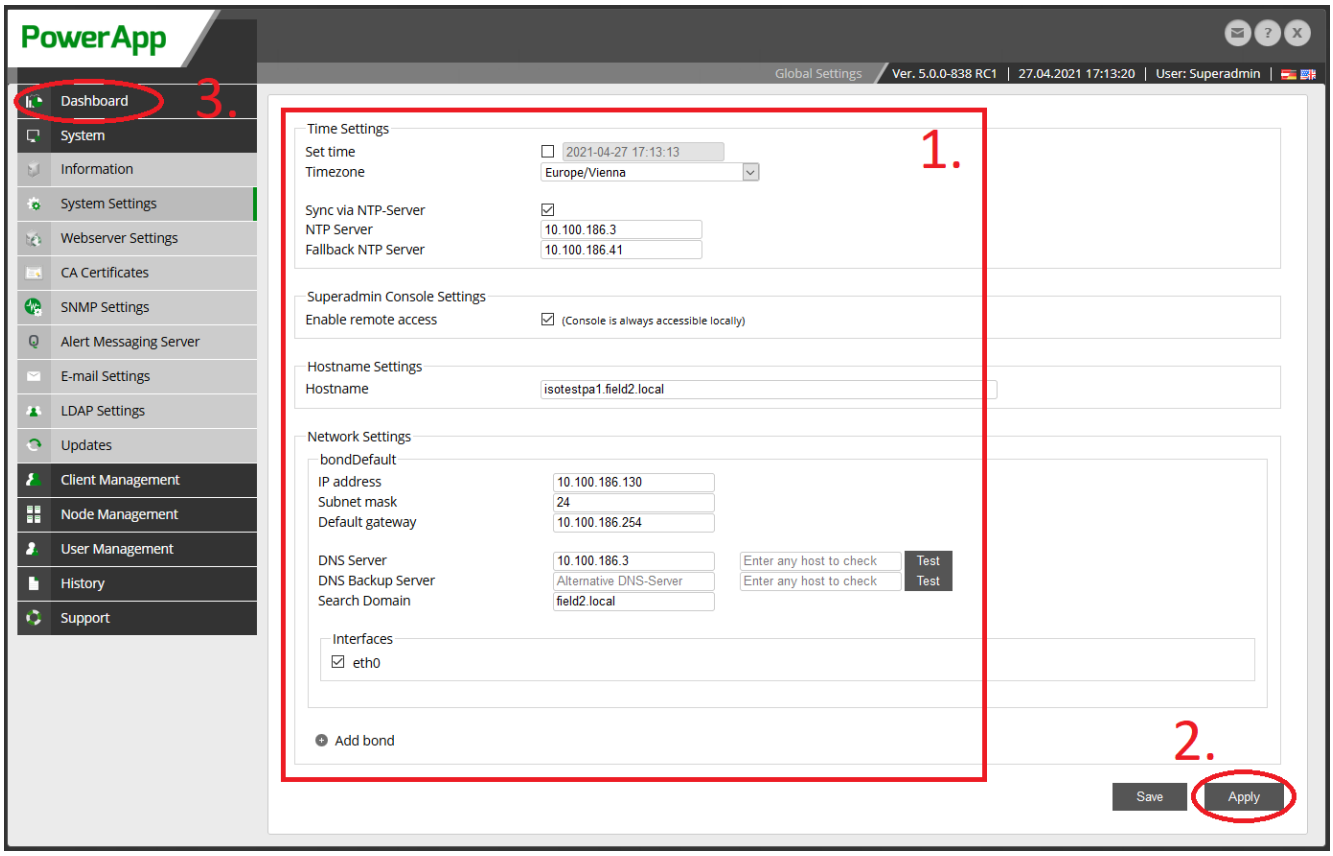


Figure 14: System settings menu

4.1.2 License

To proceed to the next entry for activating a license, click on the "License" entry in the wizard-widget-window.

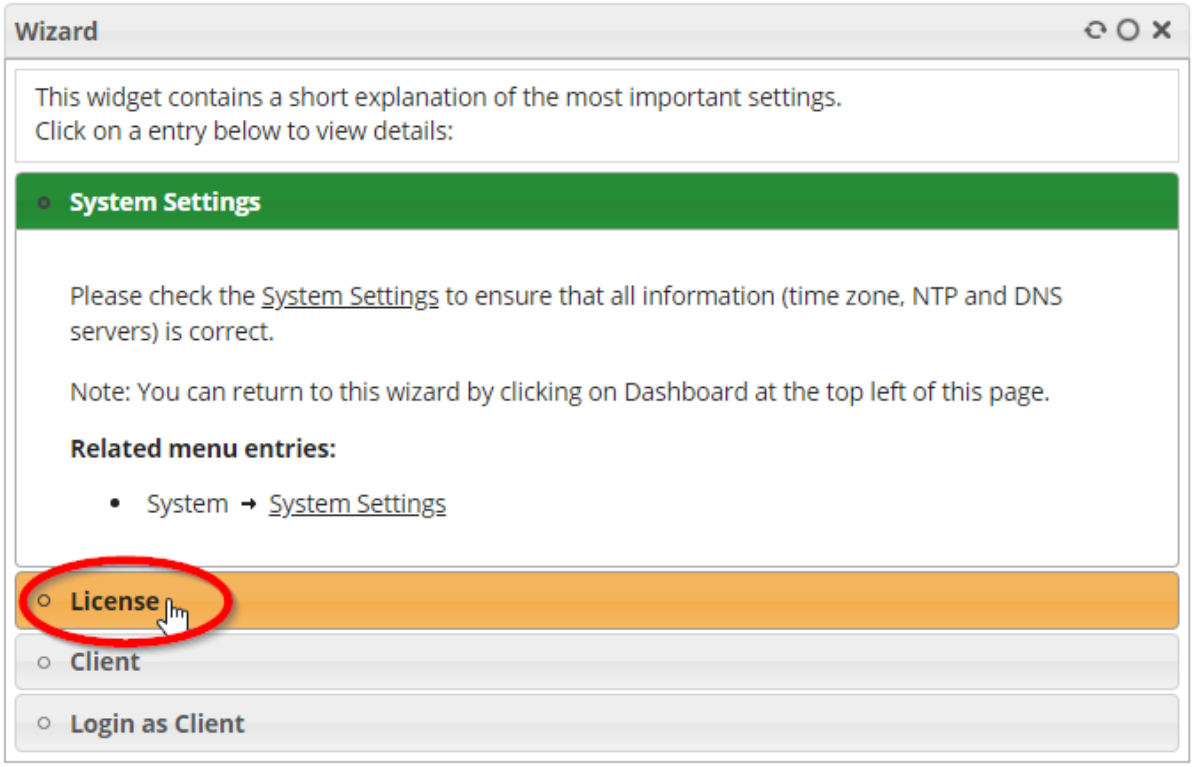


Figure 15: License entry wizard-widget-window

A 30-day trial license is active by default. If you have a license file, you can upload it by clicking on the underlined words Upload it here in the wizard-widget-window.

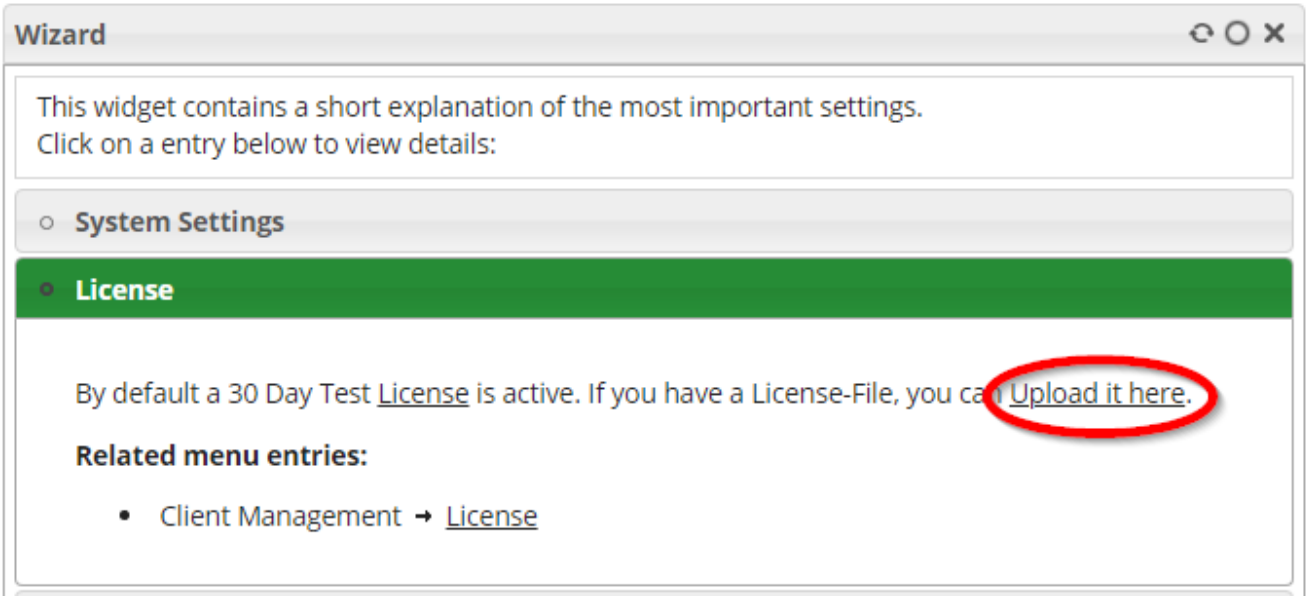


Figure 16: License wizard-widget-window

Then

1. Click on the "Select file" button.
2. Select the license file (file type: . pwrlic)
3. Open
4. Click on the "Upload" button.

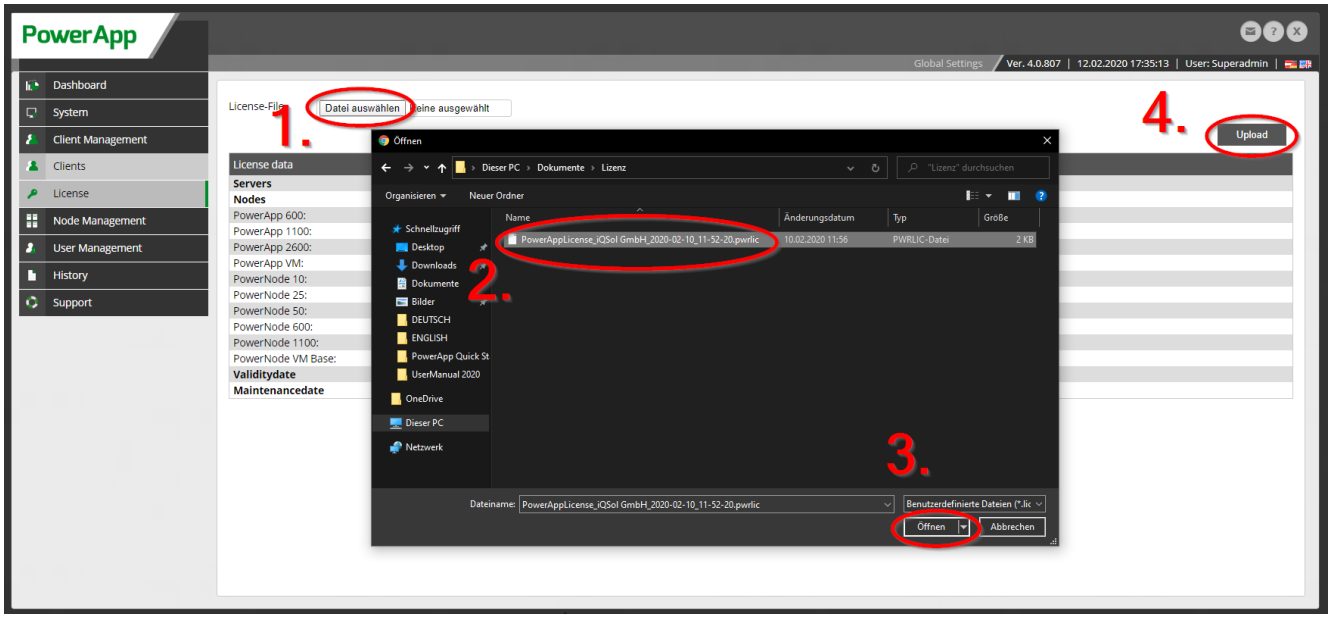


Figure 17: License menu

Base and maintenance licenses are valid for the entire product and do not have to be distributed to clients.

The following licenses are available:

Licenses	Description
Basic License	
PowerApp Basic License	Service life of the PowerApp in days
PowerApp Maintenance License	Maintenance duration for the PowerApp in days. Updates are only available during maintenance life.
PowerApp Licenses	
Server	Number of servers that can be included
Nodes	Number of Nodes (PowerApps and PowerNodes) that can be added

Table 3: Licenses

4.1.3 Client

Now a client must be added and the distribution of licenses must be performed. One or more clients can be created and managed. Clients can only be created as Superadmin. Each client can only access its own config to separate different organizations that share a PowerApp.

To add a client, click on the underlined words add a Client in the wizard-widget-window.

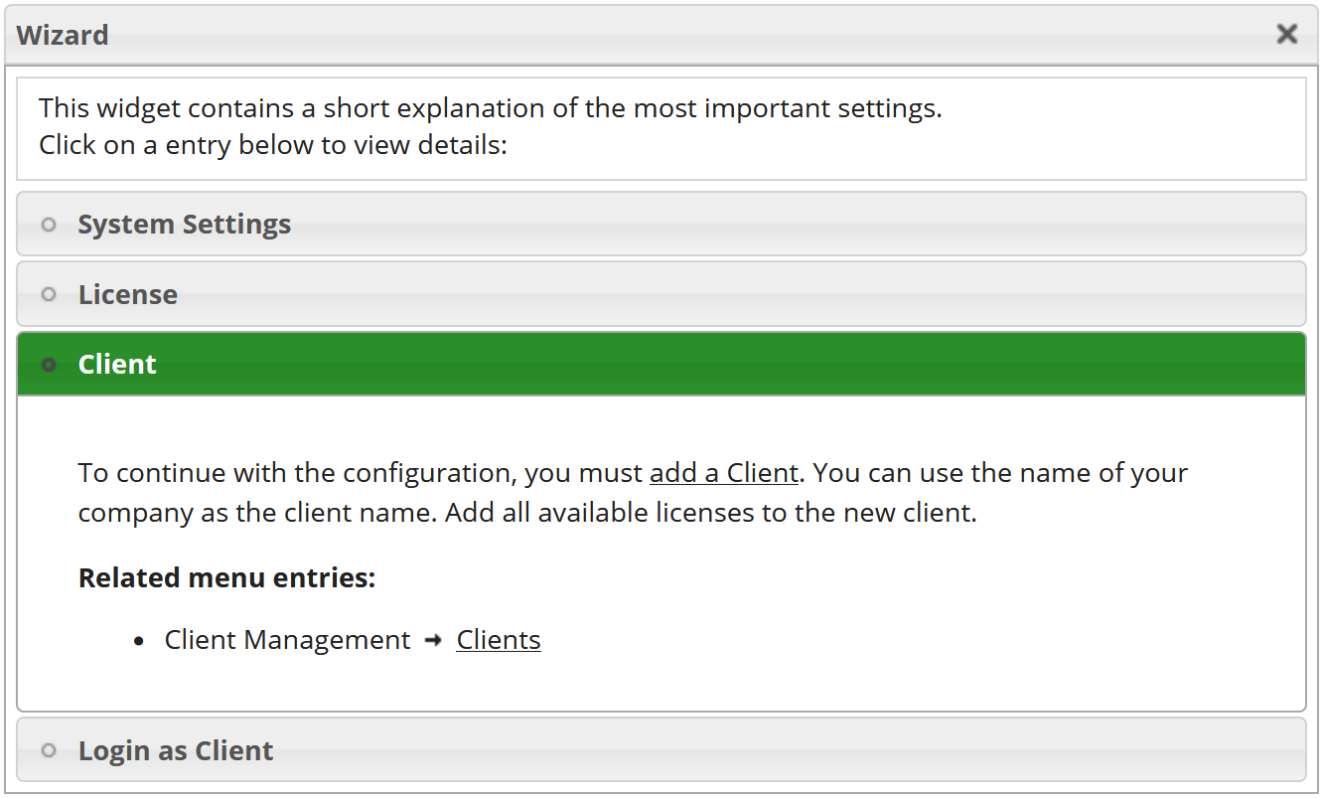


Figure 18: Client wizard-widget-window

Alternatively, you can also click on "Client management" -> "Client" in the menu. Then click on "Add Client".

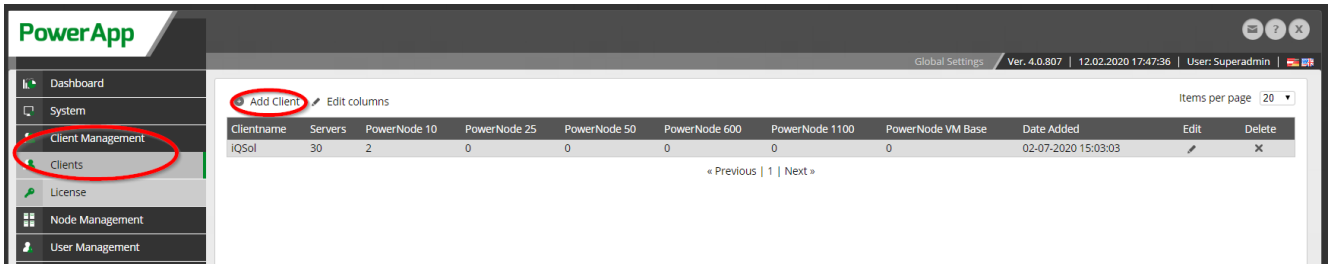


Figure 19: Client administration menu

Now enter a name for the client. The existing server licenses can be distributed to the individual clients as required.

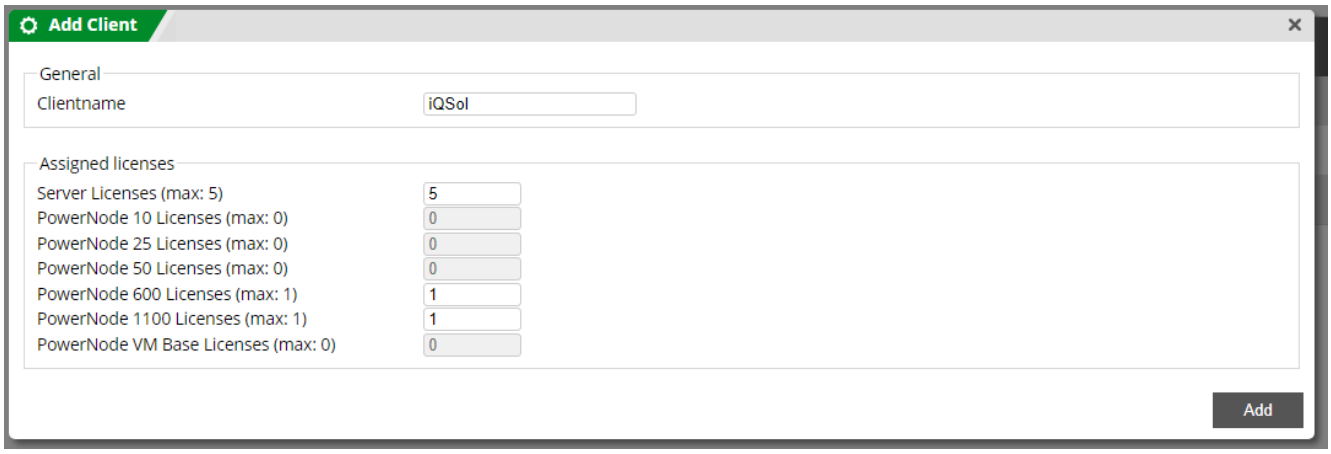


Figure 20: Add Client

4.1.4 Logging on as a client

After all important settings have been configured as superadmin, you must log on as client.

Log off as superadmin:

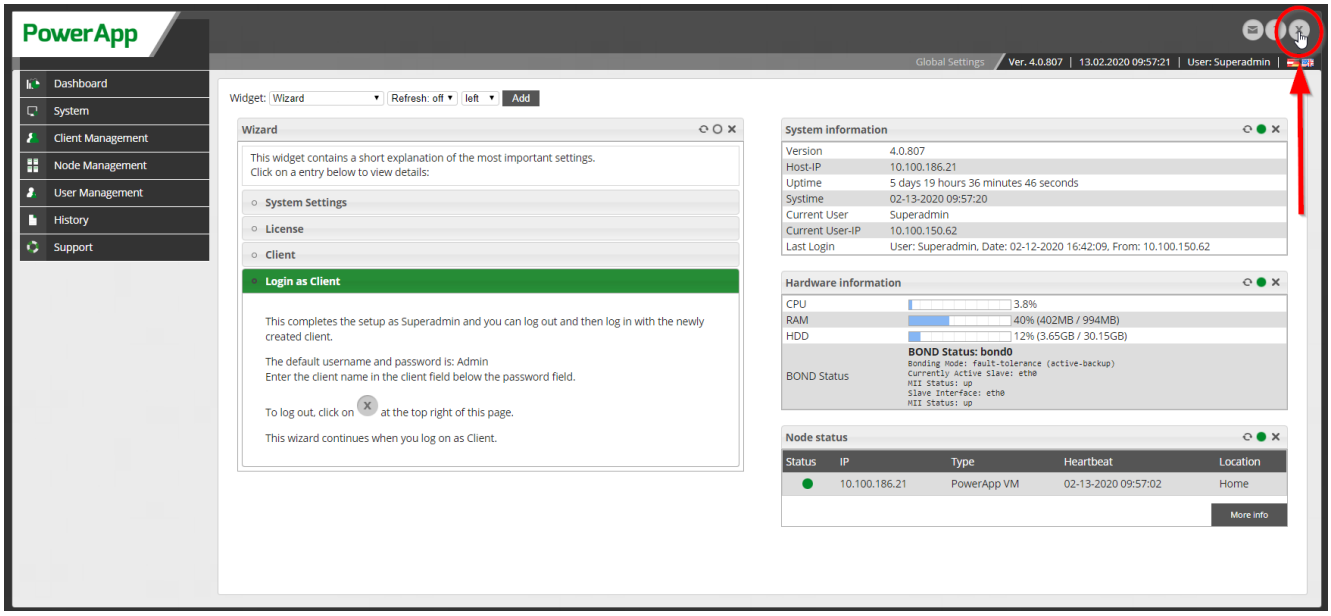


Figure 21: Logout button

Sign in as a client:

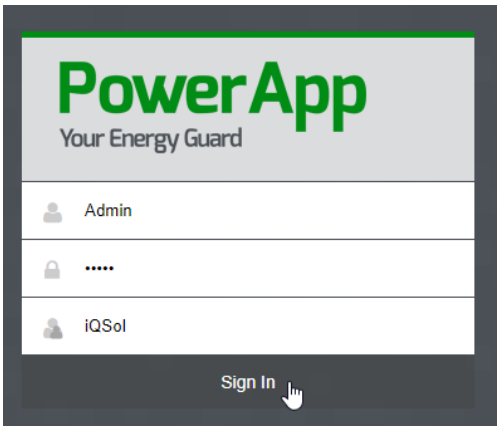


Figure 22: PowerApp Sign In

With user name, password and client name you can log on to a configured client. When a client is created, the user "Admin" is automatically generated with the password "Admin" for the first login.

4.2 Configuration of the client environment

4.2.1 Sites and nodes

To add a location, click on the underlined word Location in the wizard-widget-window.

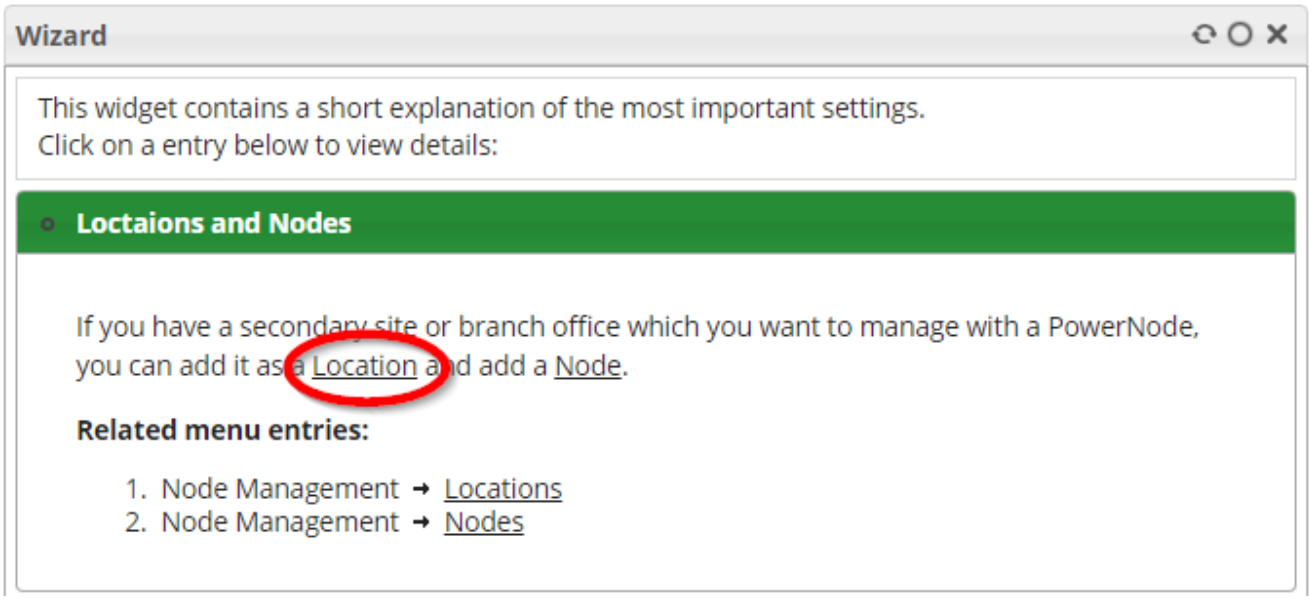


Figure 23: Locations and nodes wizard-widget-window

Then enter a location name and optionally a description and a position.

Figure 24: Add location

To add a node, click on the underlined word Node in the wizard-widget-window.

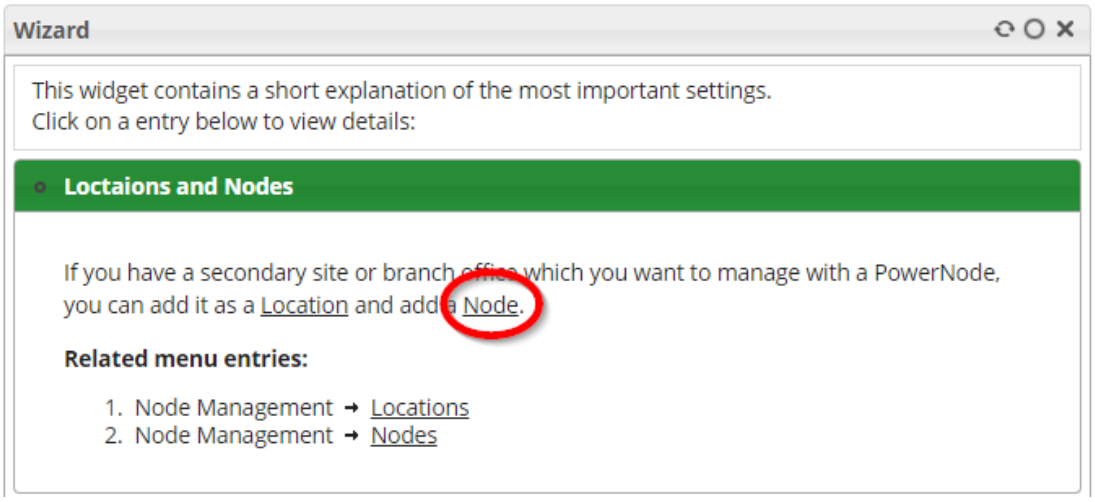


Figure 25: Locations and nodes wizard-widget-window 2

Then enter the IP of the node, select the node type and choose the location. You can optionally enter a description.

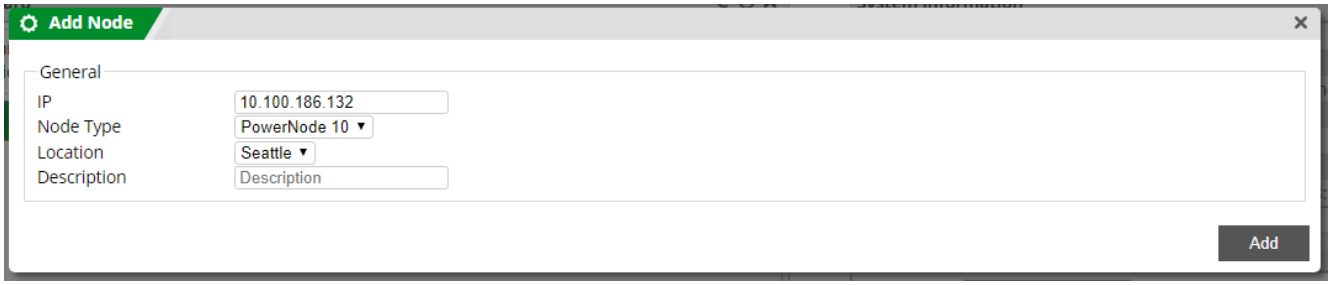


Figure 26: Add Node

For more information on adding sites and nodes, see Node Management

4.2.2 UPS and sensor

To go to the next entry for adding UPS and sensors, click on the "UPS and Sensor" entry in the wizard-widget-window.

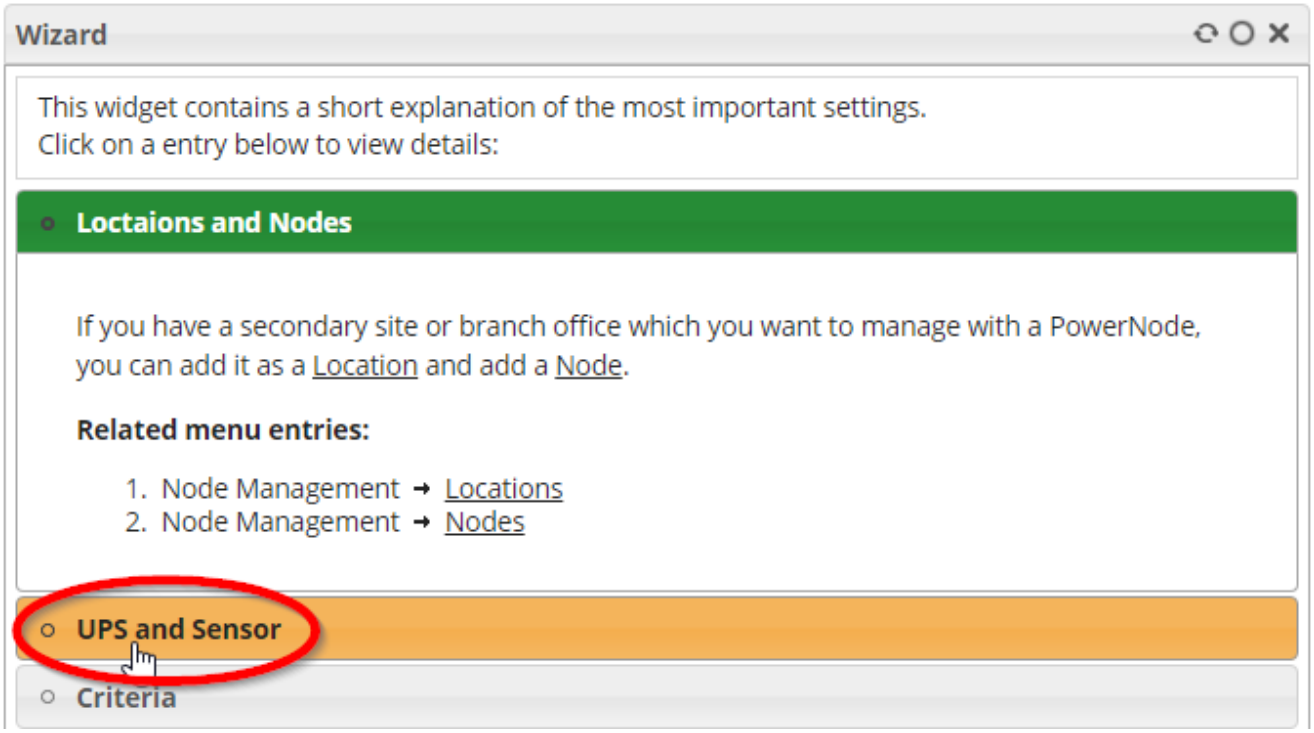


Figure 27: UPS and sensor entry wizard-widget-window

To add a UPS, click on the underlined word UPS in the wizard-widget-window.

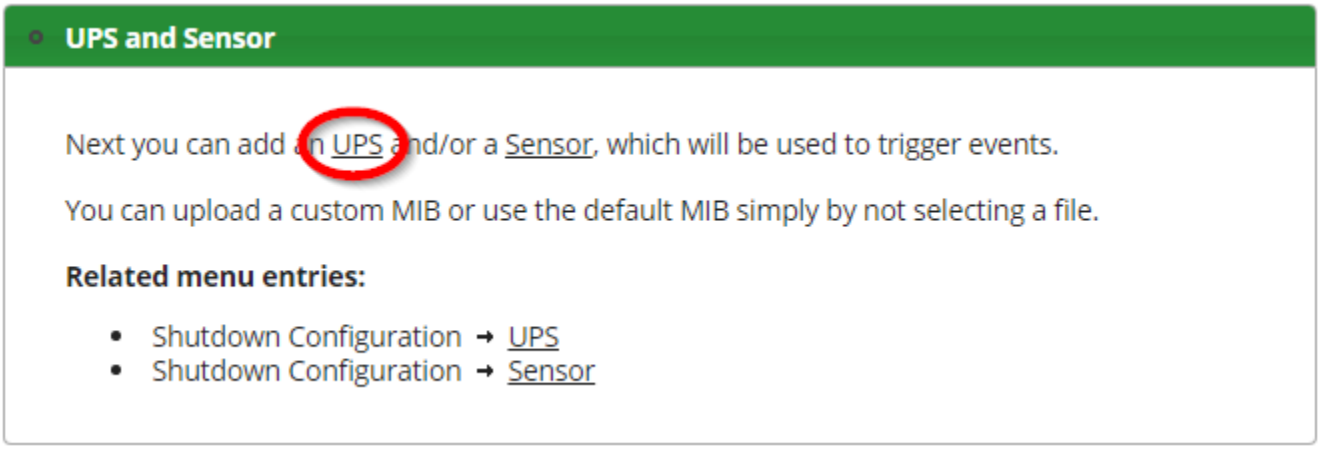


Figure 28: UPS and Sensor wizard-widget-window

Then enter the name of the UPS, enter the manufacturer and model name of the UPS and select the location of the UPS. For the connection to the UPS, enter the device IP and the Community / SecurityName. A MIB file can also be uploaded. Select the SNMP version for the connection settings.

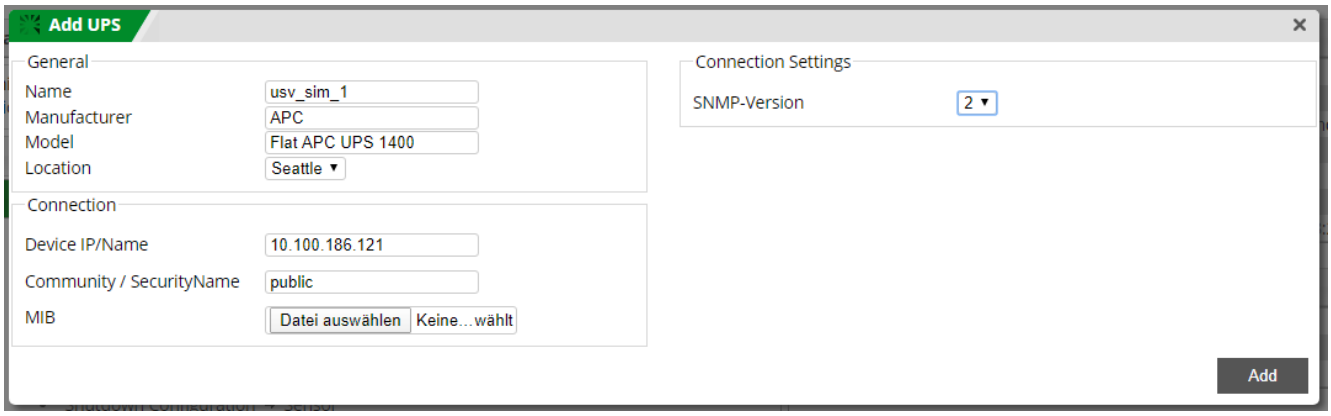


Figure 29: Add UPS

For more information on adding UPSs, see Uninterruptible Power Supply

4.2.3 Add sensor (optional)

To add a sensor, click on the underlined word Sensor in the wizard-widget-window.

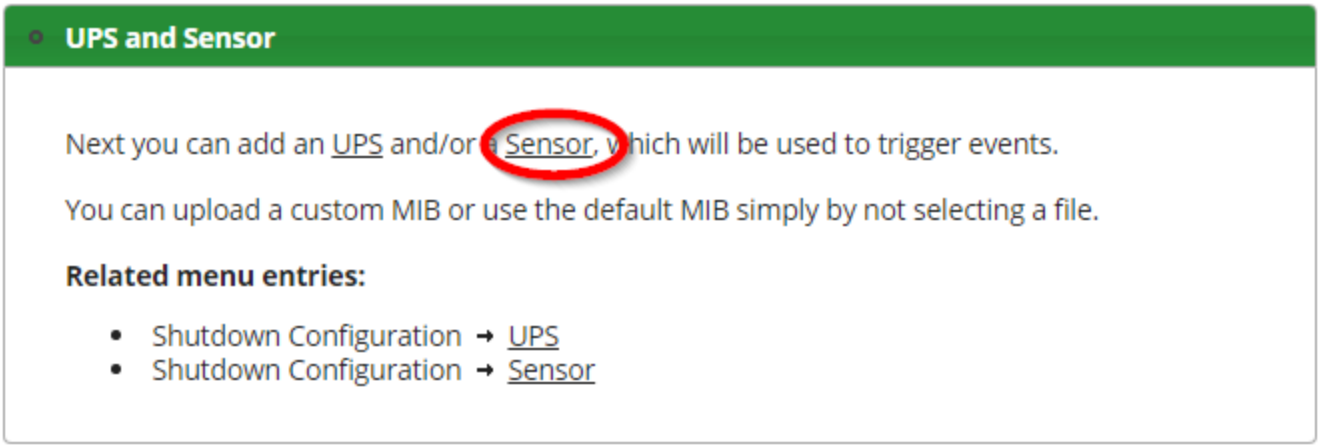


Figure 30: UPS and Sensor wizard-widget-window 2

Then enter the name of the sensor, enter the manufacturer, enter the model name of the sensor and select the location of the sensor. To connect to the sensor, select the connection type, enter the device IP and the Community / SecurityName. A MIB file can also be uploaded. Select the SNMP version for the connection setting.

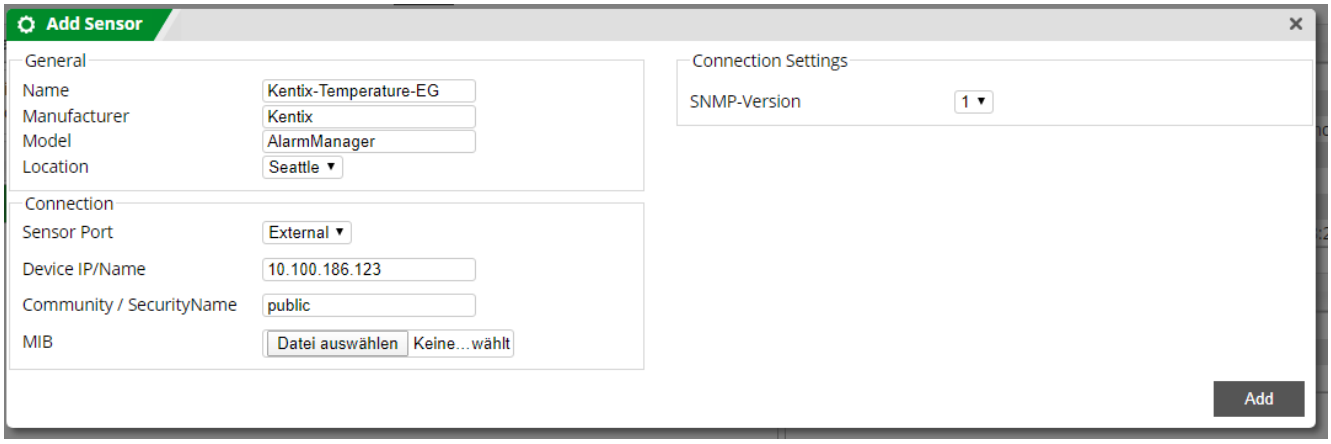


Figure 31: Add Sensor

For more information on adding sensors, see Sensor .

4.2.4 Criteria

To go to the next entry for adding criteria, click on the "Criteria" entry in the wizard-widget-window.

To add a criteria, click on the underlined word Criteria in the wizard-widget-window.

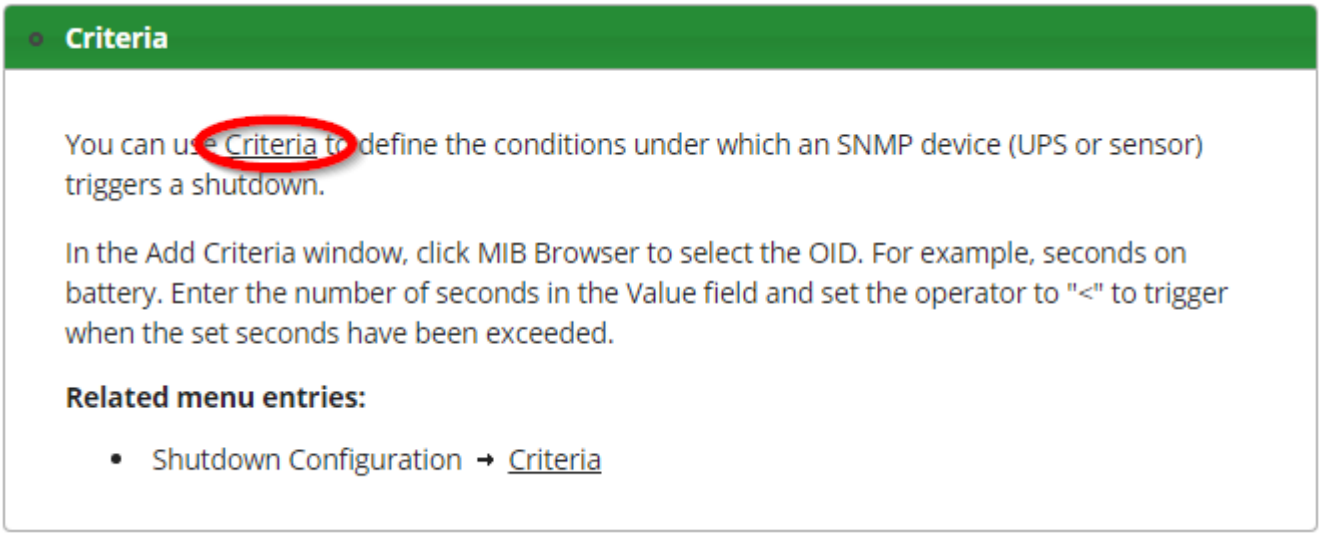


Figure 32: Criteria wizard-widget-window

Then click on "Add Criteria".

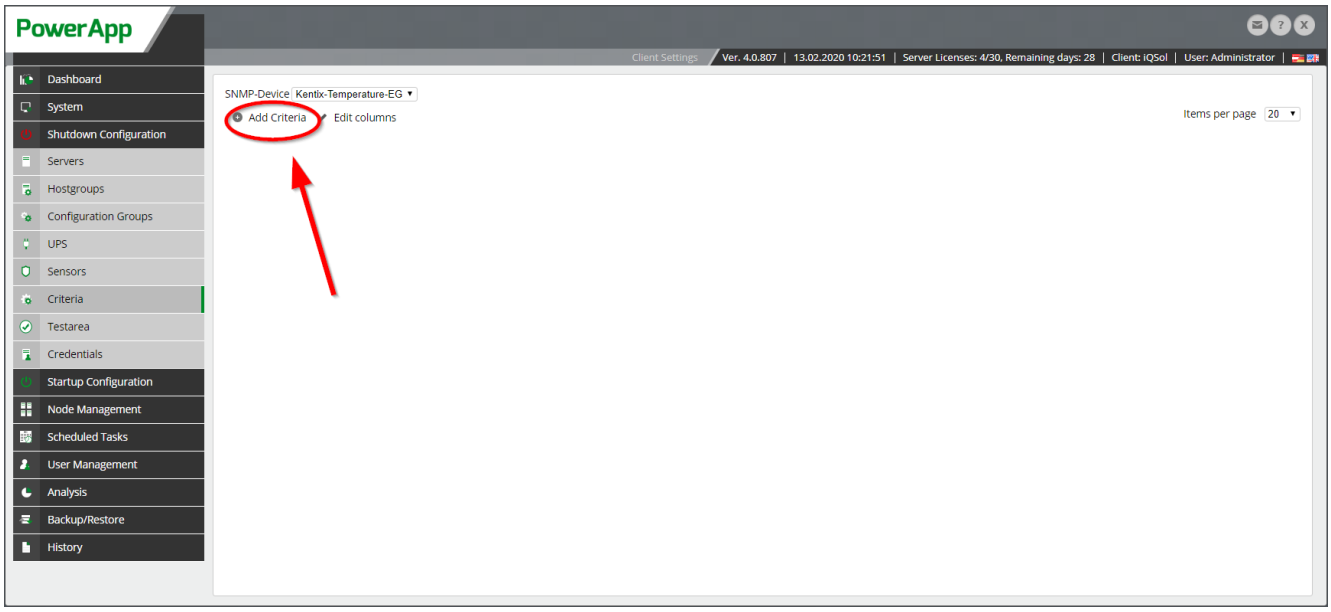


Figure 33: Criteria menu

Then enter the name of the criteria and select the SNMP device. Under Criteria Policy, specify the delay in minutes, enter the expected value and select the relational operator.

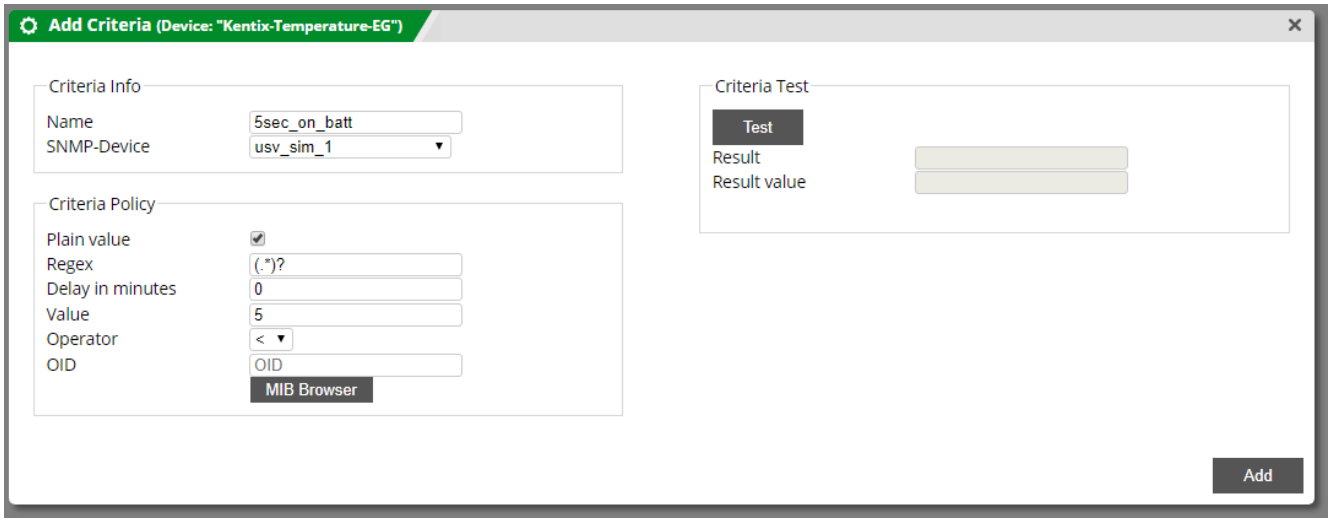


Figure 34: Add criteria

With the integrated MIB-Browser the desired SNMP objects can be selected, e.g. upsSecondsOnBattery. There are already some standard MIB objects available that should fit most UPSs.

For more information on adding criteria, see Shutdown Criteria or Startup Criteria.

4.2.5 Credentials

To move to the next entry for adding credentials, click on the "Credentials" entry in the wizard-widget-window.

To add credentials for the systems/servers, click on the underlined words add Credentials in the wizard-widget-window.

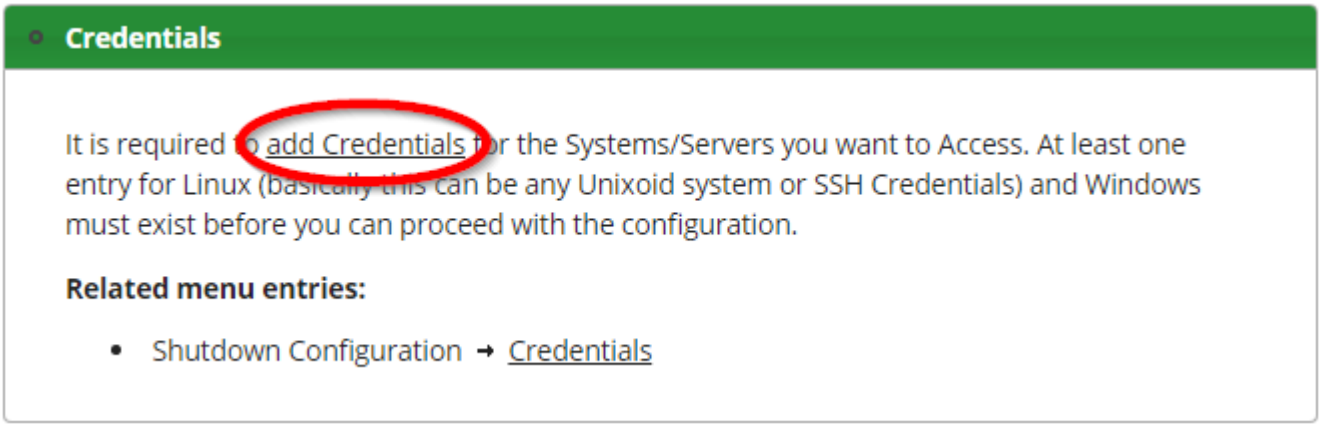


Figure 35: wizard-widget-window login details

Then enter a name, enter the username, enter the password and select the login type.

Figure 36: Add login data

For more information on adding credentials, see Credentials (Shutdown Configuration) or Credentials (Startup Configuration).

4.2.6 Configuration Groups

Configuration groups are used to define the time sequence of the shutdown. There are configuration groups for physical machine scheduling and groups for virtual machine scheduling.

To move on to the next entry for adding configuration groups, click on the "Configuration Groups" entry in the wizard-widget-window.

To add configuration groups, click the underlined words Configuration Groups in the wizard-widget-window.

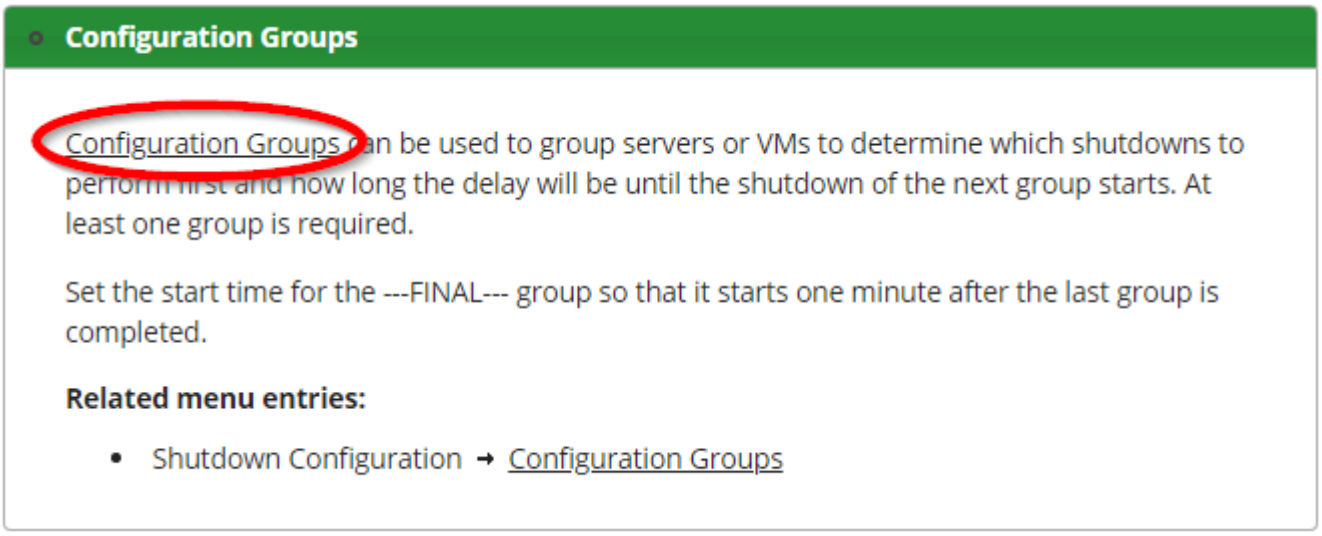


Figure 37: Configuration Groups wizard-widget-window

Then click on "Add Config Group".

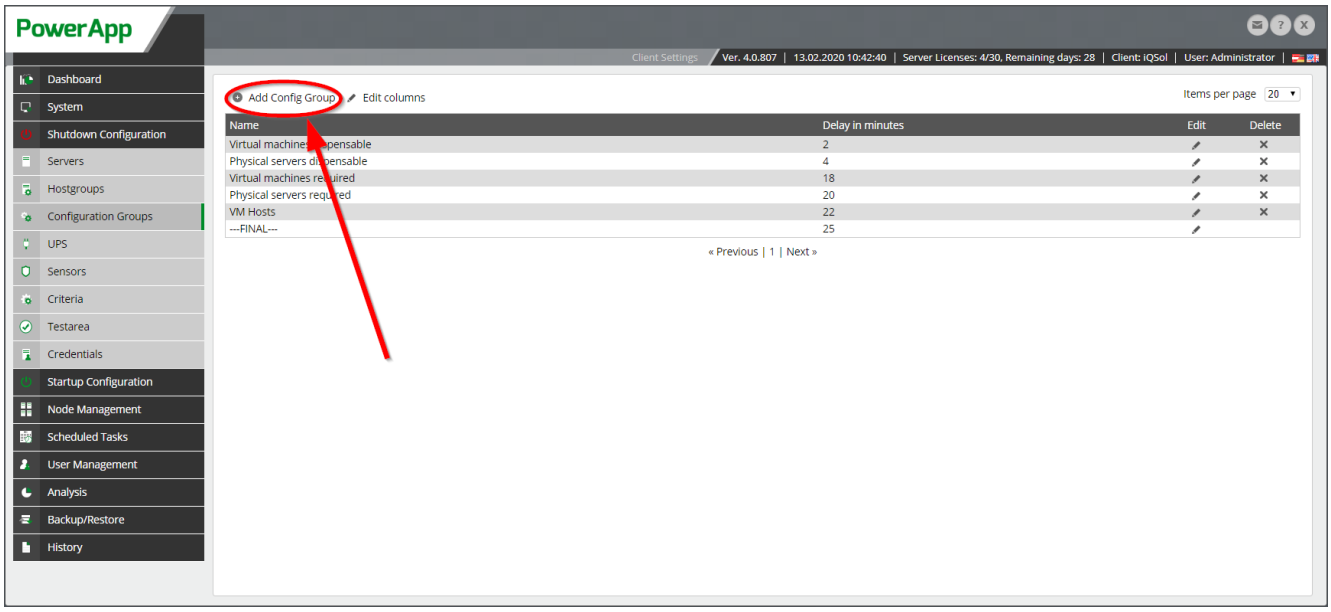


Figure 38: Configuration Groups Menu

Then enter a name for the configuration group and enter the delay time.

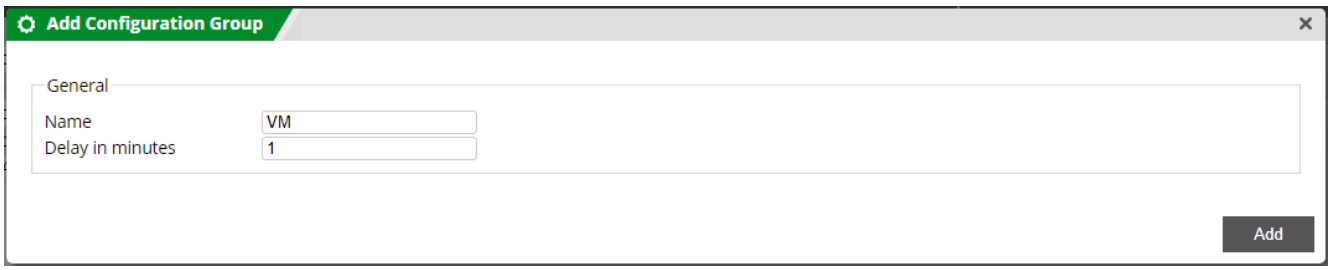


Figure 39: Add configuration groups

A sample configuration is shown here:

Add Config Group | Edit columns — Items per page 20

Name	Delay in minutes	Edit	Delete
Virtual machines dispensable	2		
Physical servers dispensable	4		
Virtual machines required	18		
Physical servers required	20		
VM Hosts	22		
---FINAL---	25		

Figure 40: Example configuration for configuration groups

The configuration group --FINAL-- is, so to speak, the deadline at which all servers/VMs have already been shut down (or booted up). Anything that has not been shut down (or booted) by then will not be taken into account and the shutdown (or startup) will be considered complete from that point on.

The delay time of configuration group --FINAL-- is always higher than the delay times of all other configuration groups.

For more information on adding configuration groups, see Configuration Groups (Shutdown Konfiguration) or Configuration Groups (Shutdown Konfiguration).

4.2.7 Server or VM Host

To move to the next entry for adding servers, VM host, or a device that is accessible via SSH, click the "Server or VM Host" entry in the wizard-widget-window.

To add a server or VM host, click on the underlined word add in the wizard-widget-window.

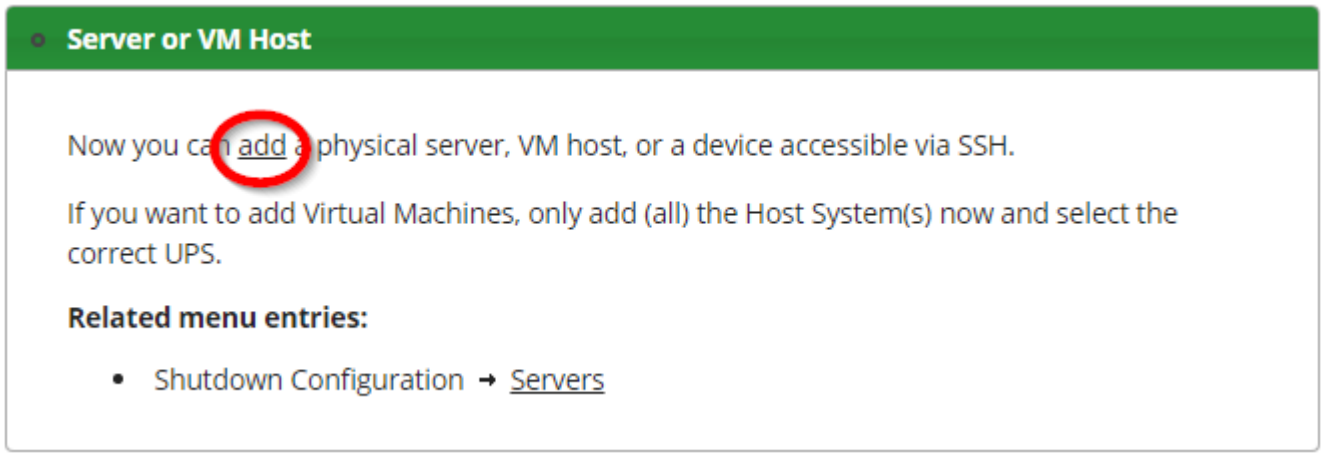


Figure 41: Server or VM host wizard-widget-window

Add a VM host. See this example:

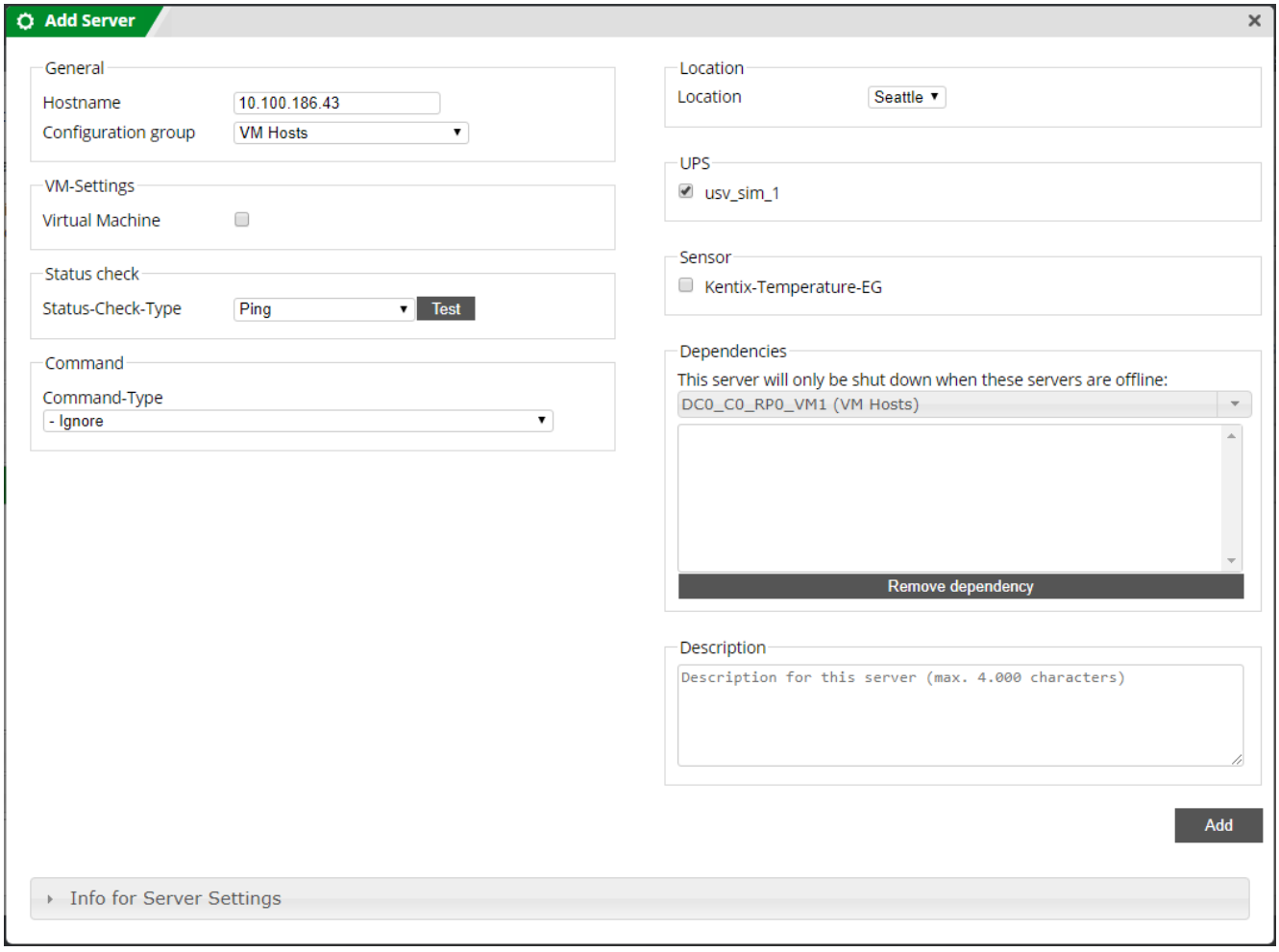


Figure 42: Add server Example

The VM host must be added before importing a VM.

For more information on adding servers, see Server.

4.2.8 Host Groups

To move to the next entry for adding host groups, click the Hostgroups entry in the wizard-widget-window

To add a host group, click the underlined word Hostgroups in the wizard-widget-window.

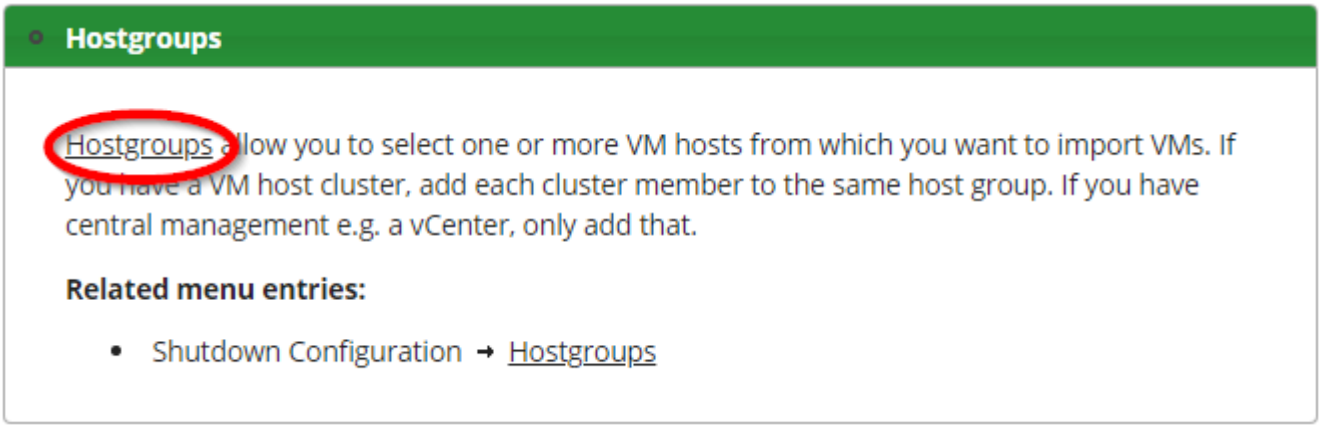


Figure 43: Hostgroups wizard-widget-window

Then enter the name of the host group, select the type of virtualization and choose the credentials. Then select the server on the right and use the "Test" button to verify that the login data is correct.

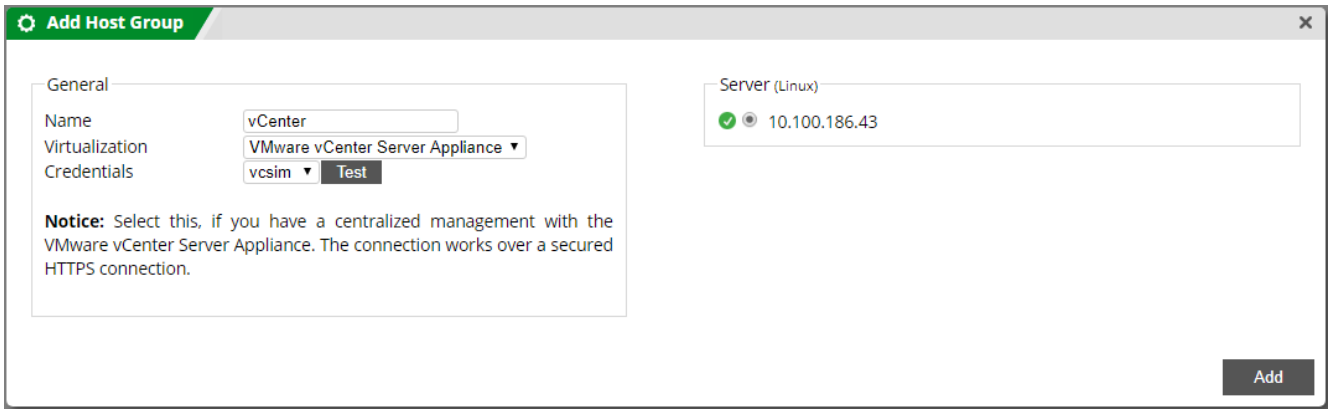


Figure 44: Add host group

For more information on adding host groups, see Host Groups .

4.2.9 VM Import

To move to the next entry for importing VMs, click the Import VM entry in the wizard-widget-window.

To import a VM, click the underlined words VM Import in the wizard-widget-window.

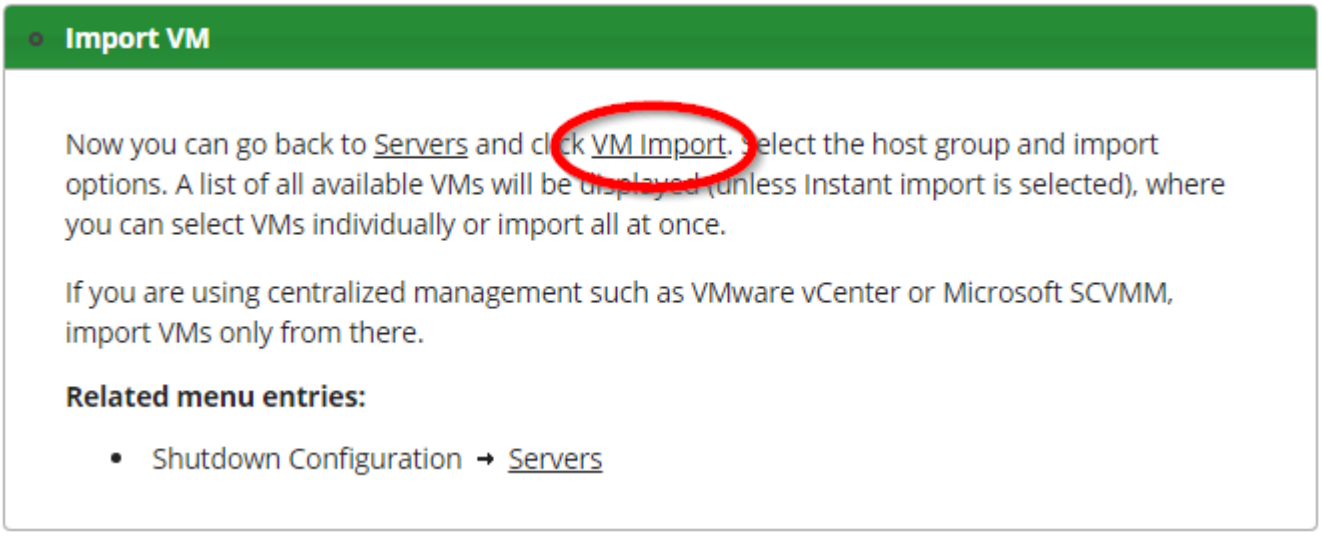


Figure 45: VM Import wizard-widget-window

Then select the host group type and host group name.

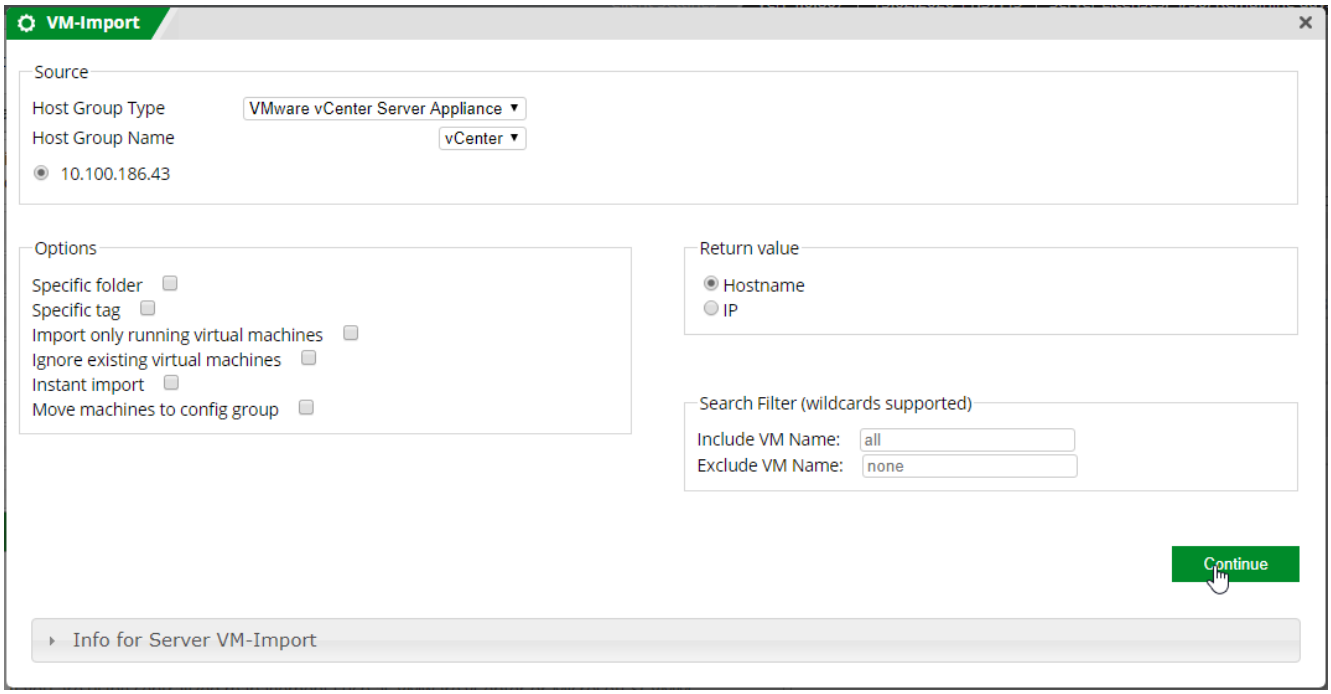


Figure 46: Import VM

Then import the VMs by clicking the "Add" button. In the example photo, "VM2" and "VM3" were imported. If you want to import all VMs, you have to click on the "Start import" button.

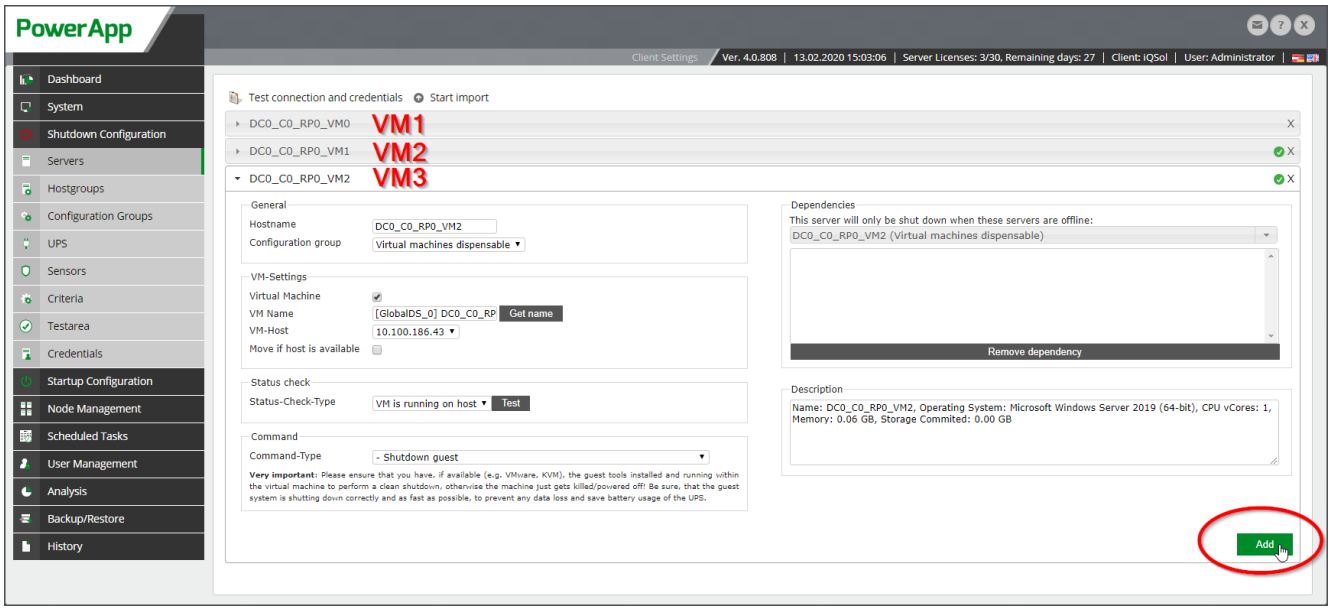


Figure 47: Import VM Example

4.3 Widgets

The first time you log in, the default configuration of the widgets is loaded. All widgets can be moved, removed or added by the user.

The individual widget windows have 3 menus in theupper right corner.

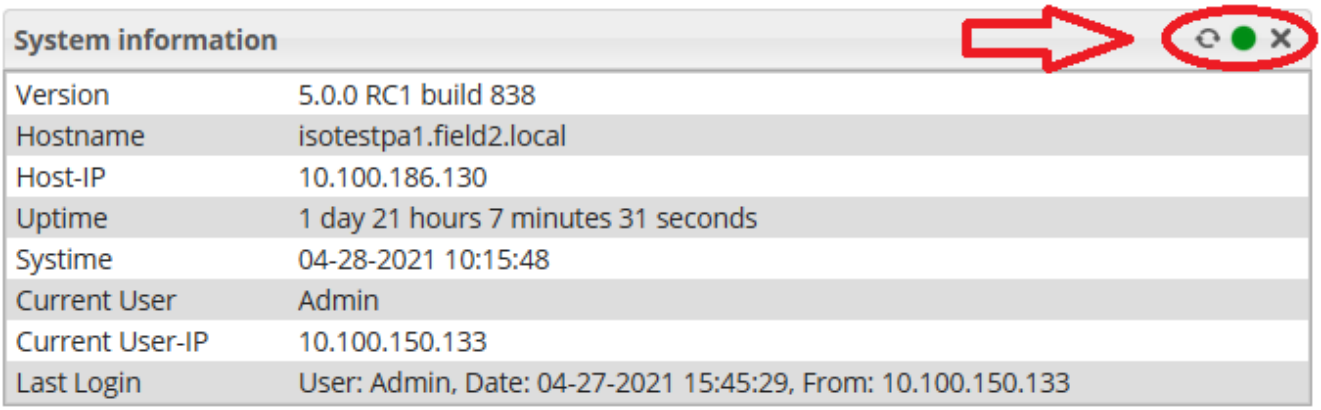


Figure 48: Widget window menu items

Update, Toggle Auto Update, Close

- Refresh: Refreshes the contents of the window.
- Toggle auto refresh: If the menu item is green, the contents of the window are automatically refreshed every 5 seconds. If it is grey, the contents of the window are not automatically refreshed.
- Close: Closes the window.

Adding a new widget:

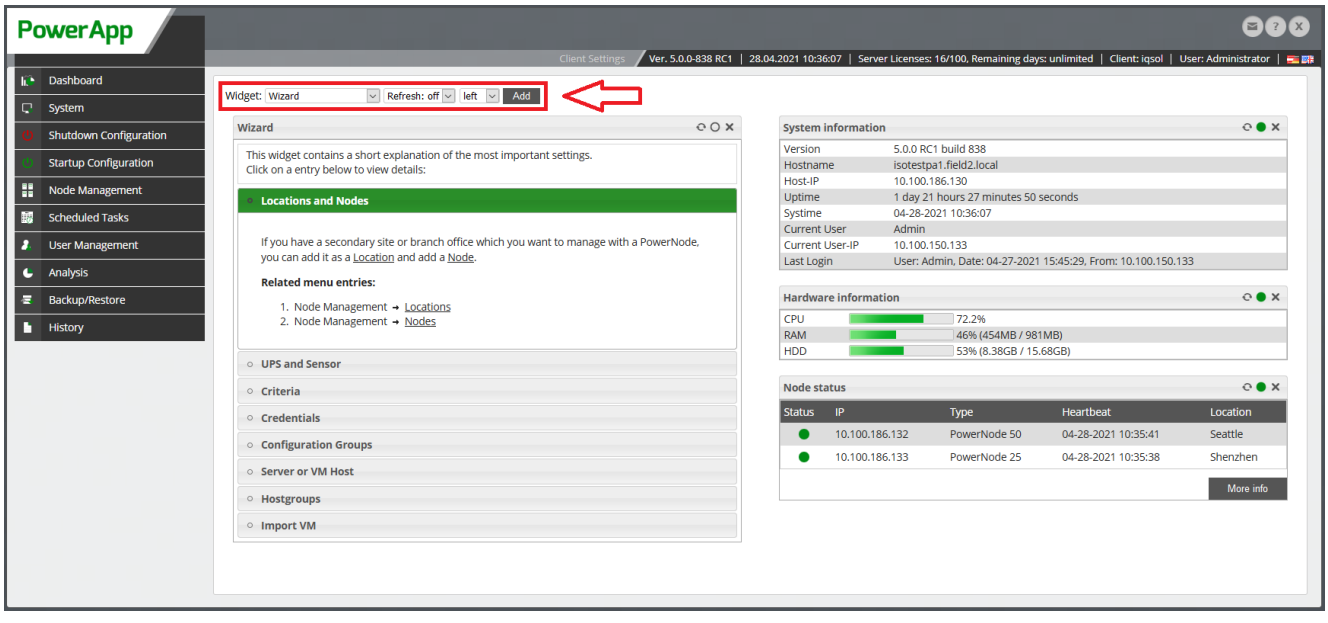


Figure 49: Add widget

In the center of the PowerApp GUI is the wizard widget. This widget contains a short explanation of the most important settings. On the right side of the PowerApp GUI are the System Information widget, the Hardware Information widget, and the Node Status widget.

The System Information widget displays the following information about the system:

- Version
- Host-IP
- Uptime
- Systime
- Current User
- Current User-IP
- Last login

The Hardware Information widget displays the following information about the hardware:

- CPU
- RAM
- HDD
- BOND status

The Node Status widget displays the status of the nodes.

PowerApp - Your Energy Guard

START OF SUPERADMIN SECTION

iQSol
Security made in Austria.

5 Configuration Settings Central Console

Add and manage clients and change settings in the central console (Superadmin), which affects all clients in the same way.

5.1 System

5.1.1 Information

Information about the system (e.g. PowerApp verison, uptime, host ip address, system utilization – CPU, RAM, Disk).

The PowerApp can be shutdown and rebooted, here.

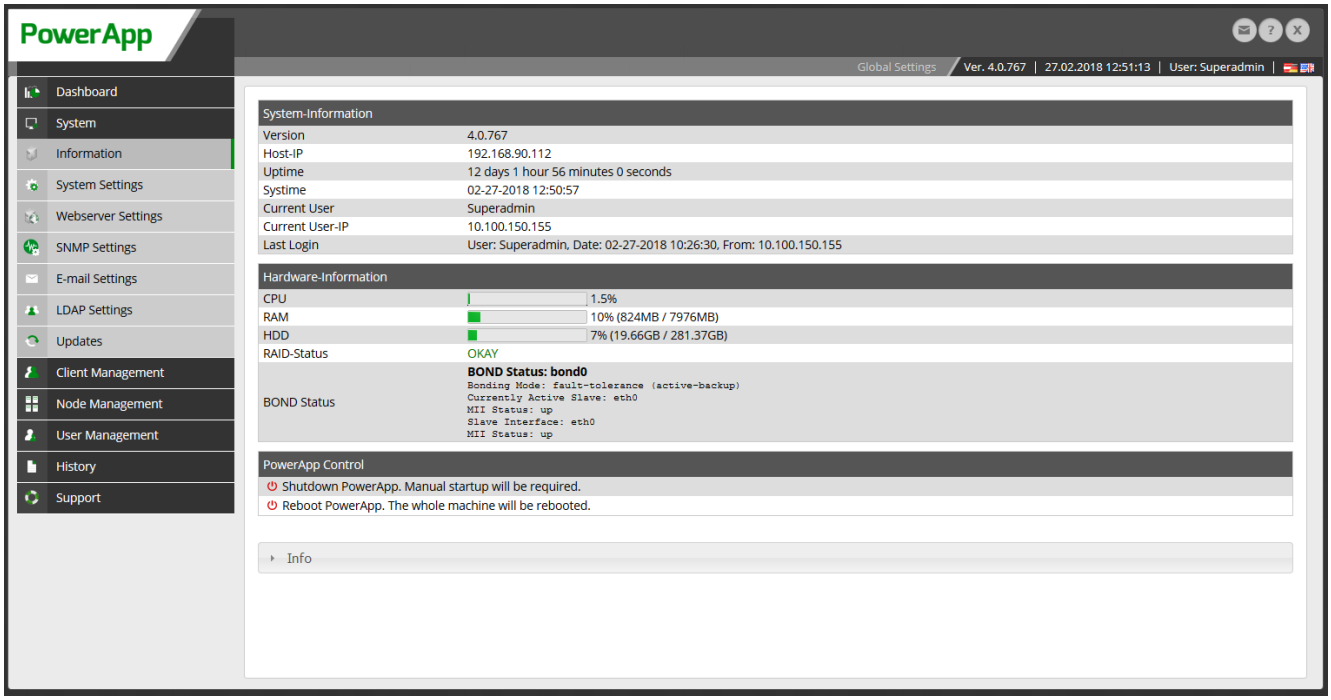


Figure 50: Information

5.1.2 System Settings

In "System Settings" it is possible to configure the time, time zone, NTP server for time synchronization, DNS server and bonding interfaces.

Bonding interfaces can bond physical network ports together to provide fail over functionality in an active-backup configuration. It is possible to only include one physical interface in a bond to assign a separate IP address to it.

The “bondDefault” interface is always there and can not be removed. It should be used to configure the main IP address of the system.

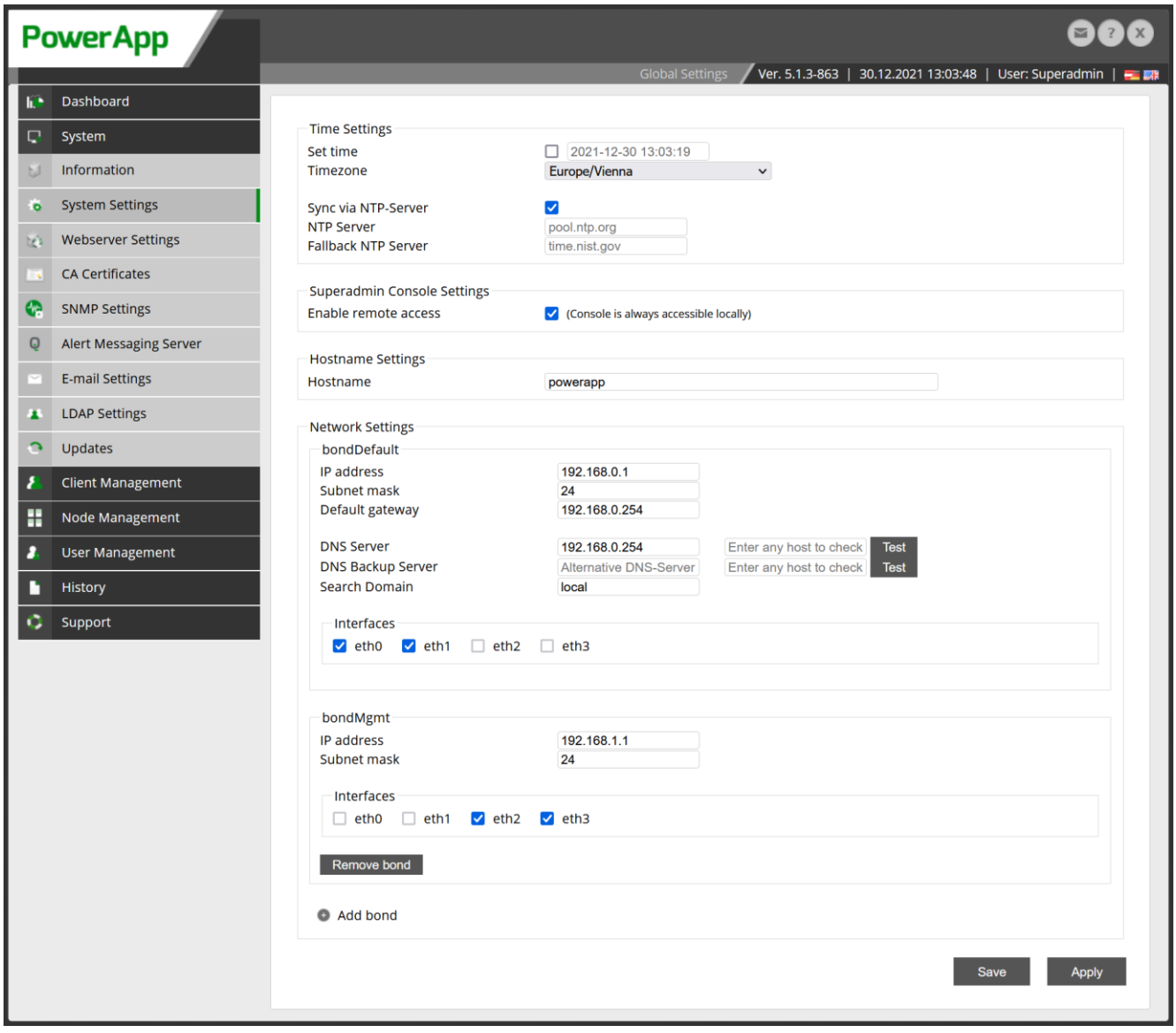


Figure 51: System Settings

5.1.3 Webserver Settings

In „Webserver Settings“ a new certificate for the WebGUI can be set. A certificate signing request can be created here.

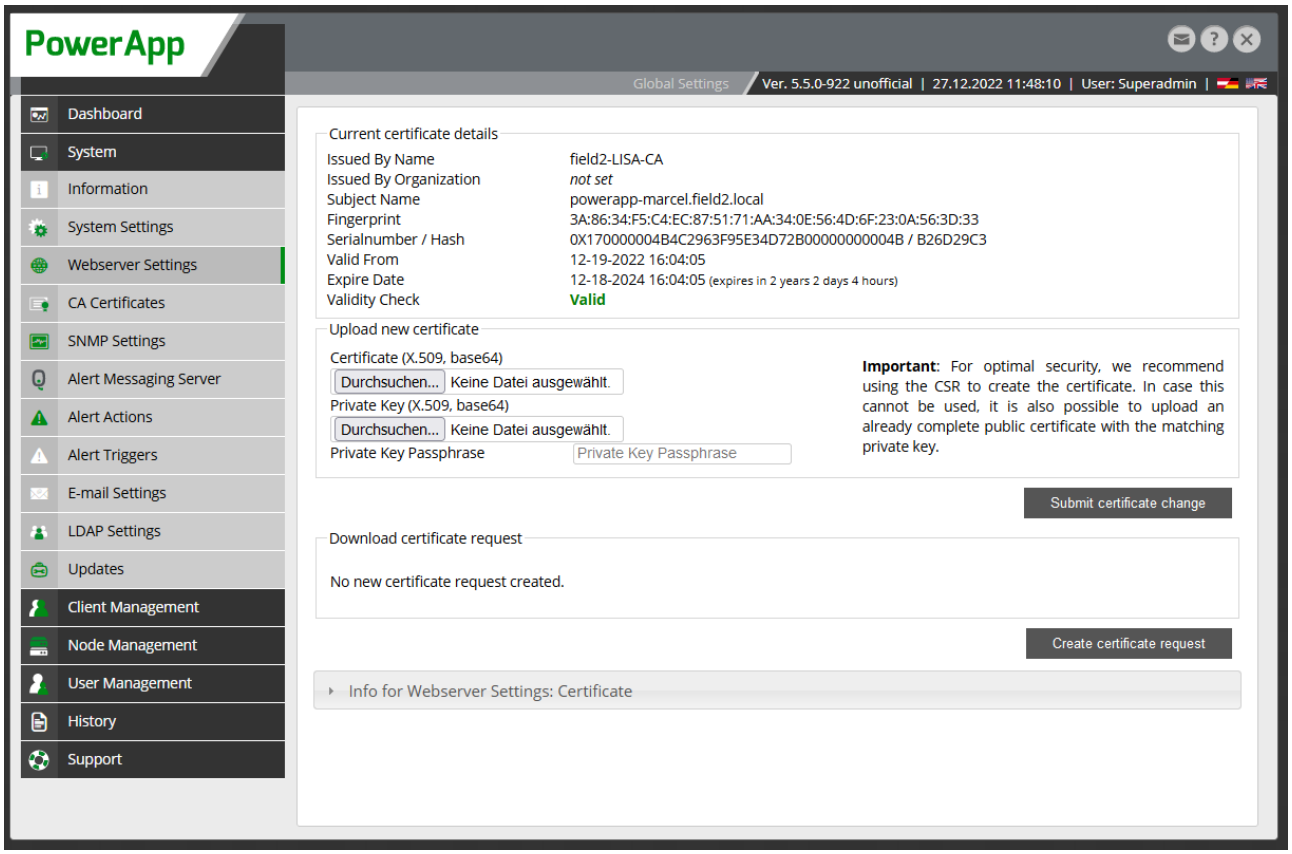


Figure 52: Webserver Settings

5.1.4 CA Certificates

Certificates which should be recognized system-wide can be uploaded here.

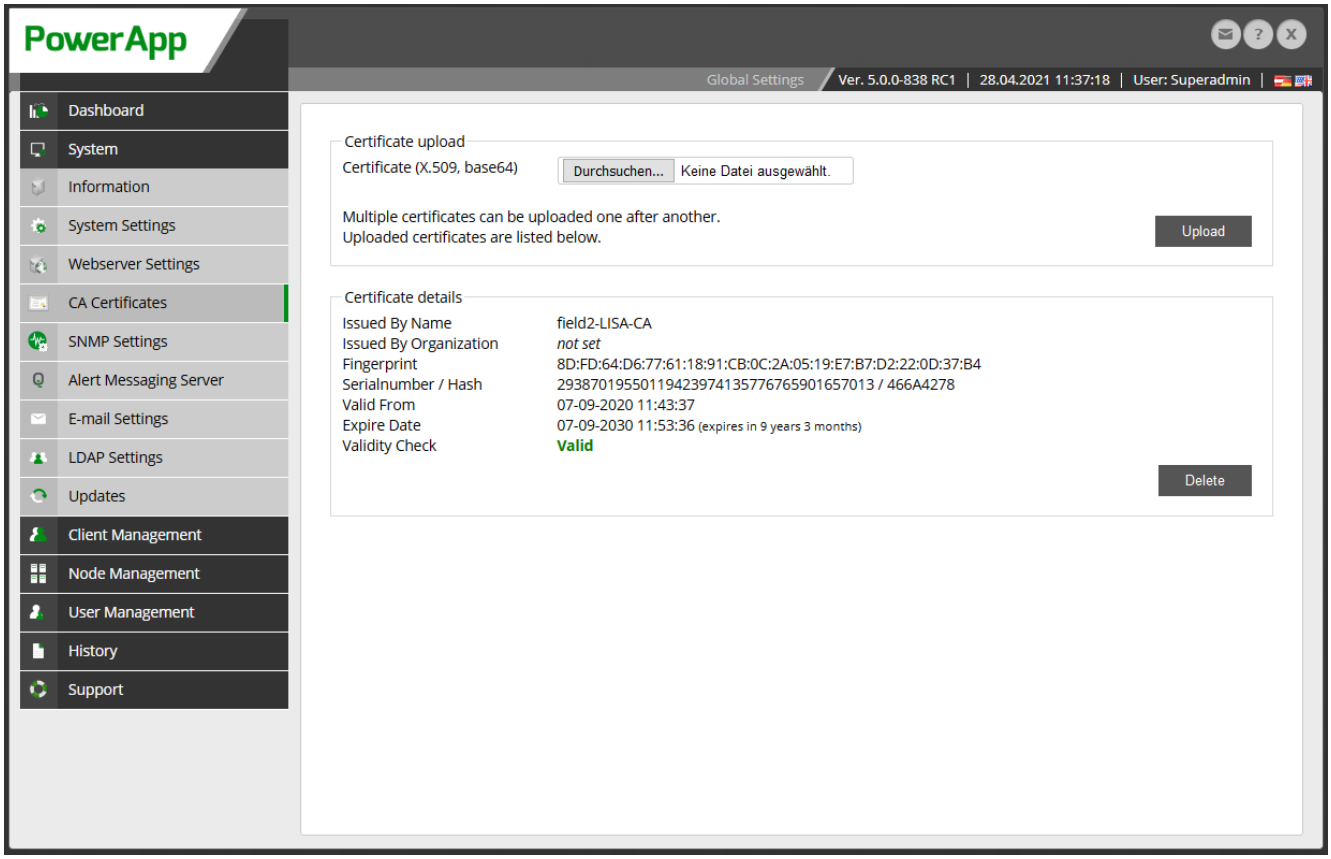


Figure 53: CA Certificates

5.1.5 SNMP Settings

In the „SNMP Settings“ menu are options to switch the whole SNMP daemon functionality on or off.

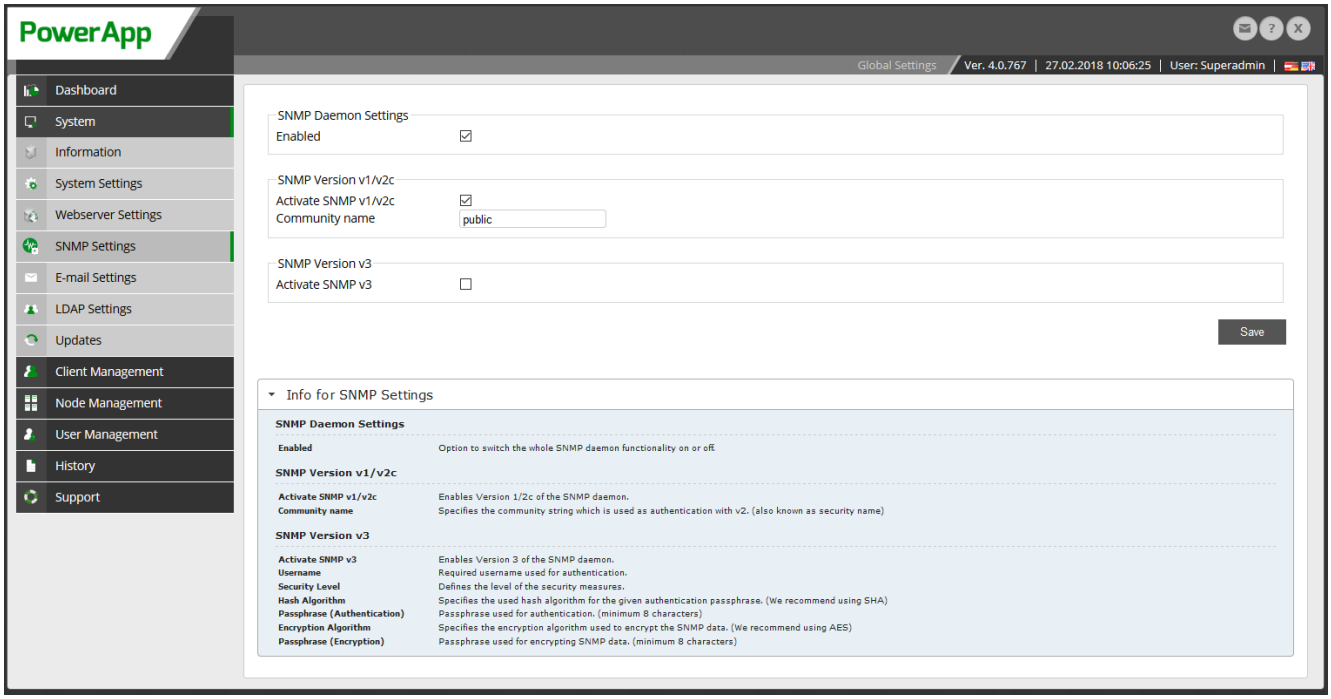


Figure 54: SNMP Settings

5.1.6 Alert Messaging Server

Look AMS (6.1.3)

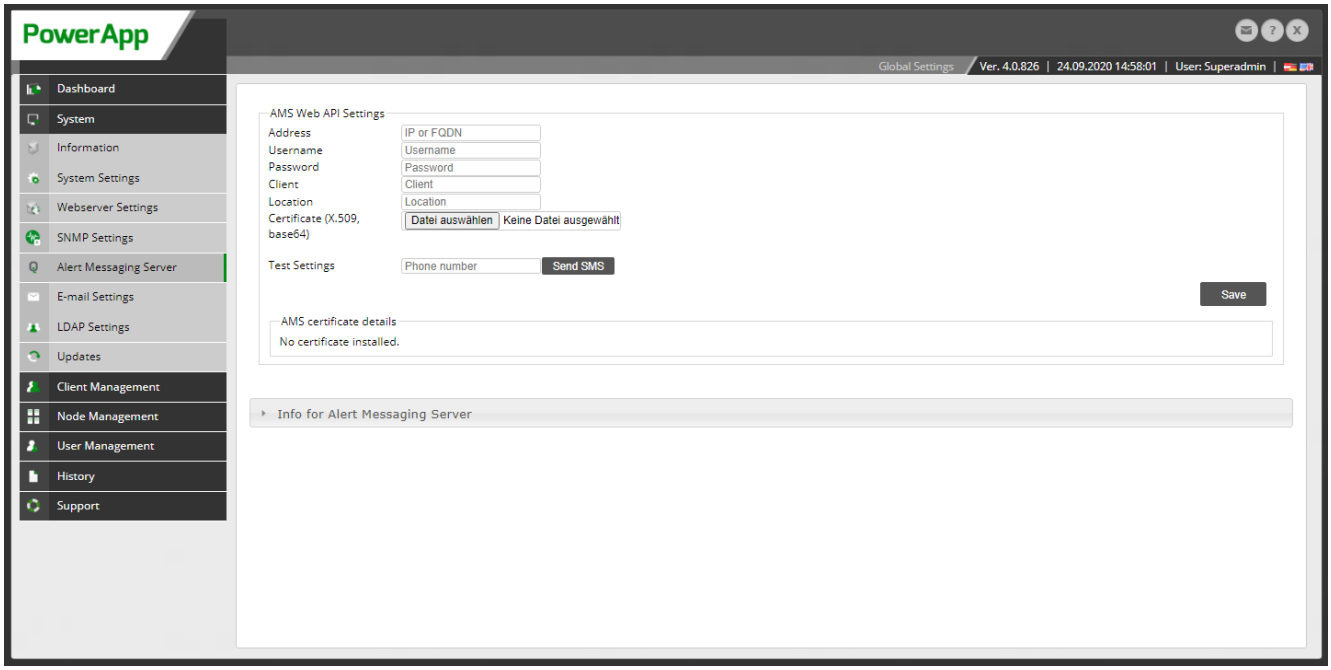


Figure 55: Alert Messaging Server

5.1.7 Alert Action

Configure action for execution on certain events (see chapter Alert Trigger). Sending emails and executing any command is supported by default. Additionally send sms or make phone calls by integrating the third party product „Alert-Messaging-Server“ (AMS) by iQSol.

5.1.8 Alert Trigger

Use Alert-Triggers to execute actions on certain events, e.g. sending emails (see chapter Alert Action).

Following Alert-Triggers are supported:

- New system update is available
- System boot complete
- Node is not reachable
- Node is reachable

5.1.9 E-mail Settings

The settings for email notifications can be set in the “E-mail Settings” menu.

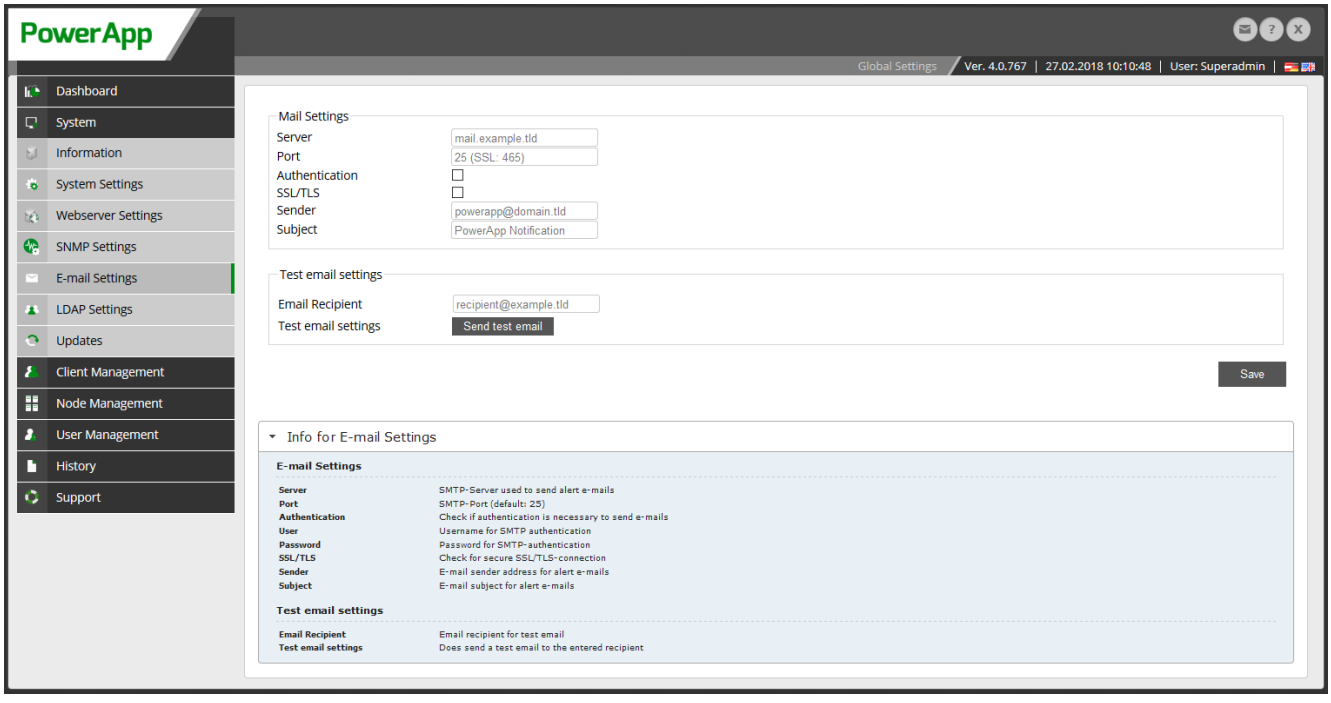


Figure 56: E-Mail Settings

5.1.10 LDAP Settings

Use the „LDAP-Settings“ menu for configuring LDAP servers for user authentication. Enter servername or IP address, port, authentication data and domain/organisation. Click save to automatically test the LDAP server connection. The LDAP tree is displayed, if the connection is successful.

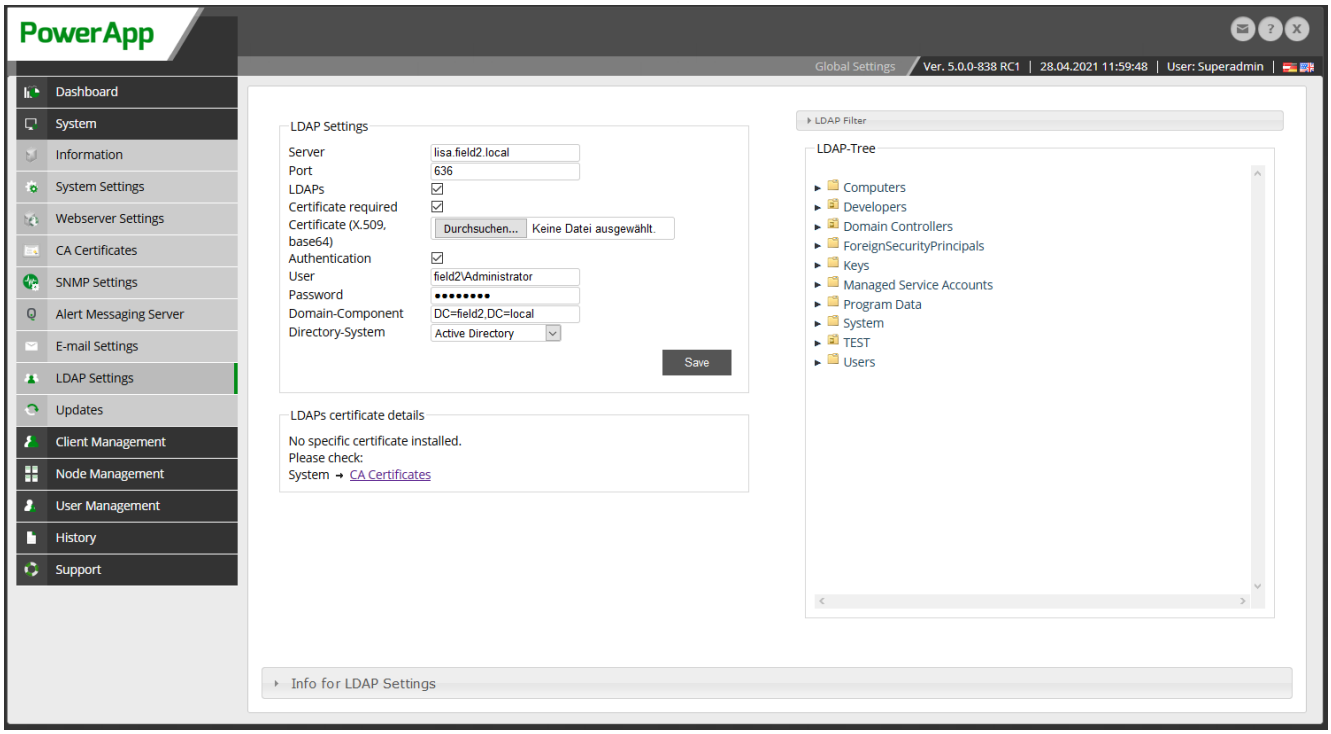


Figure 57: LDAP Settings

Import LDAP users to the „User-Management“ menu (see chapter User Management).

The LDAP sesttings apply only to the central console and can be configured for every client individually.

5.1.11 Update

Use the „Update“ menu to upload and install update packages, which can be received from iQSol or an iQSol partner.

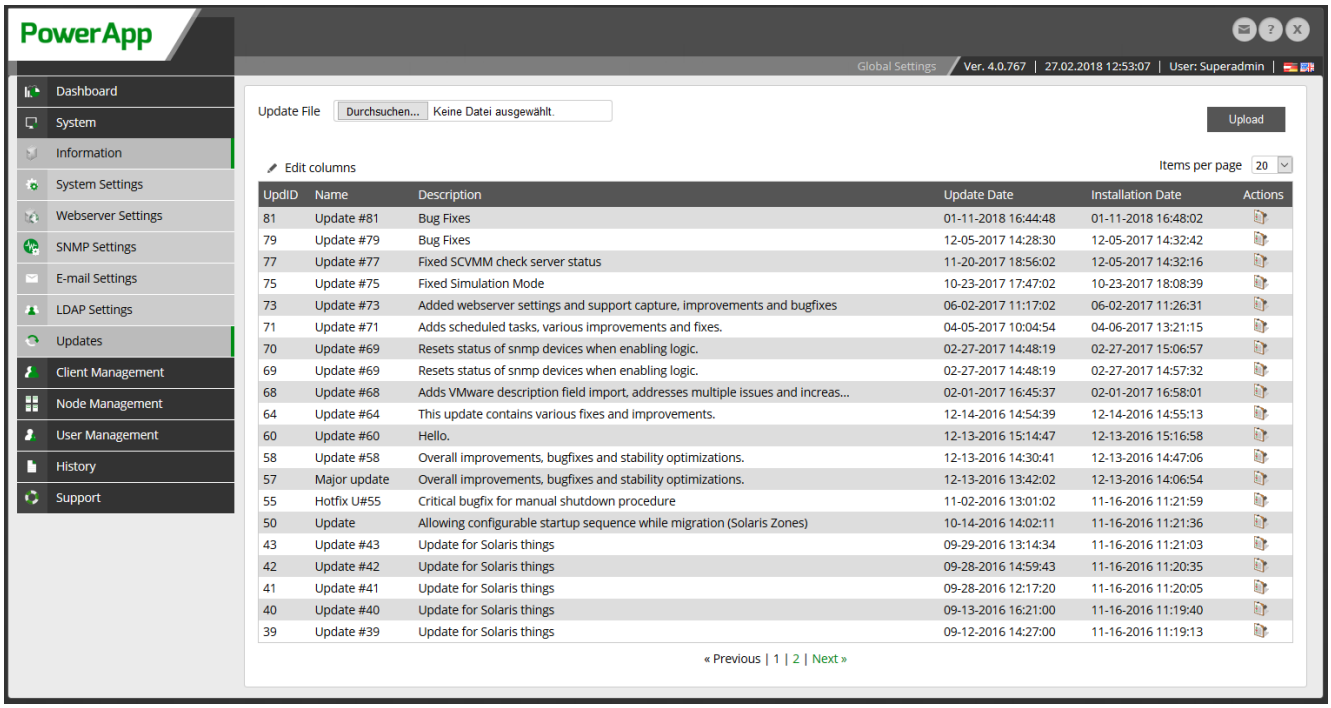


Figure 58: Update

Automatic Update Distribution

An update can also be distributed within a cluster so that the update is installed on all devices simultaneously. To do this, upload the update file to a PowerApp.

Then the automatic update distribution to all nodes will be started.

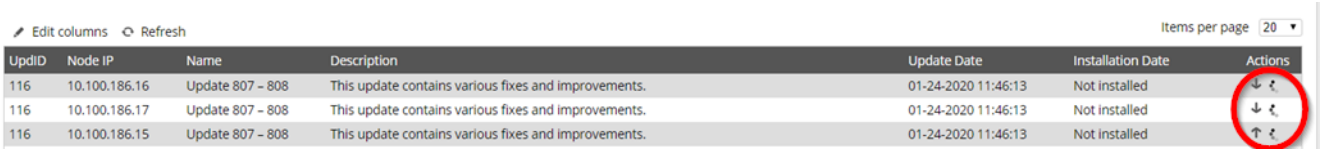


Figure 59: Update distribution

Then wait until the distribution is finished.

To install the update, click the following icon in the Actions column: 

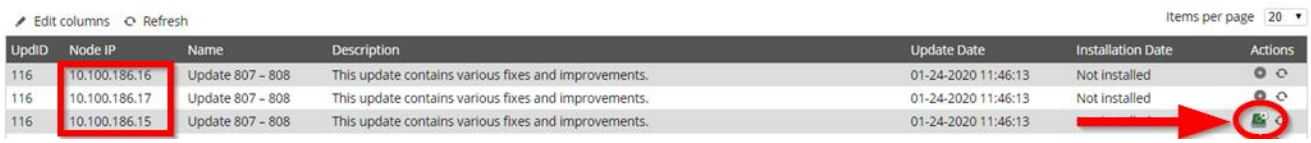


Figure 60: Update Distribution Installation

The nodes marked in the red frame are then updated simultaneously.

5.2 Client Management

5.2.1 Client

Use the menu „Client-Management“ -> „Client“ to add or edit clients and assign server licenses. Click „Add“ to create a new client.

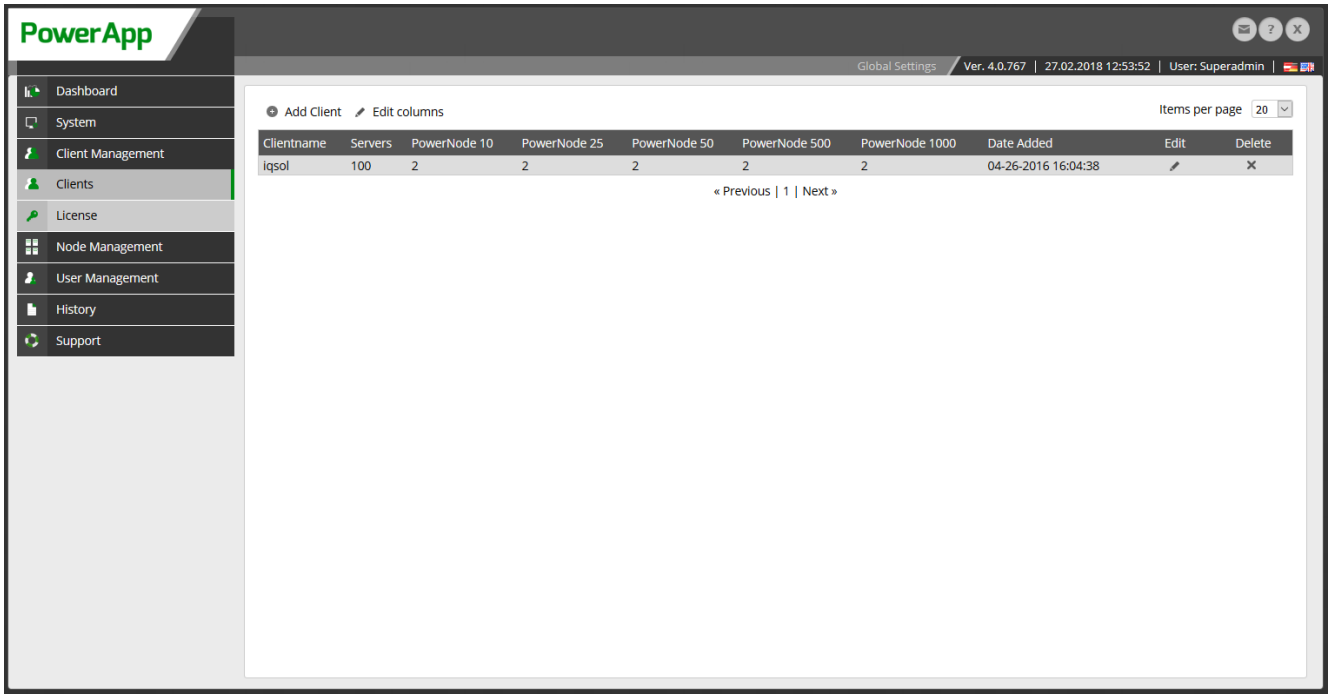


Figure 61: Show Clients

5.2.2 License

Upload license files in the „License“ menu. The validity date, maintenance date and the number of possible servers is included in the license file.

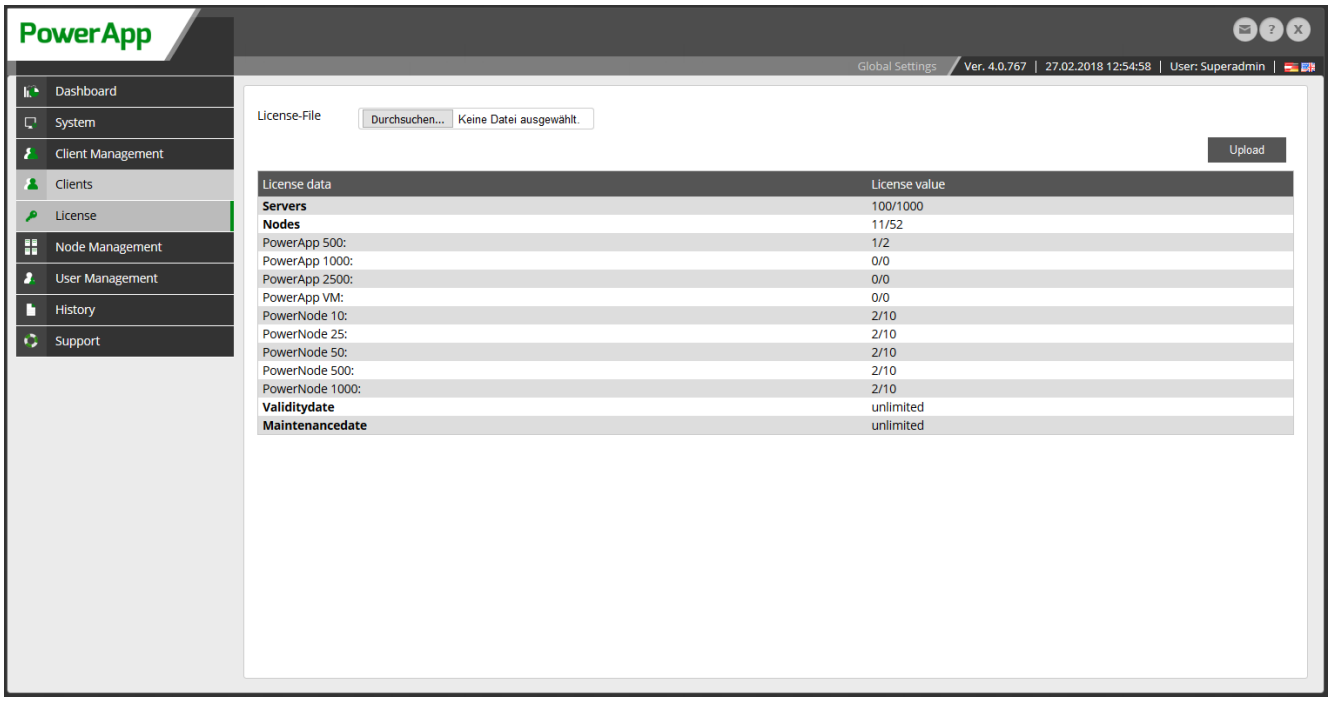


Figure 62: Upload License

5.3 Node Management

5.3.1 Locations

Here you can edit the name, description and position of your home location.

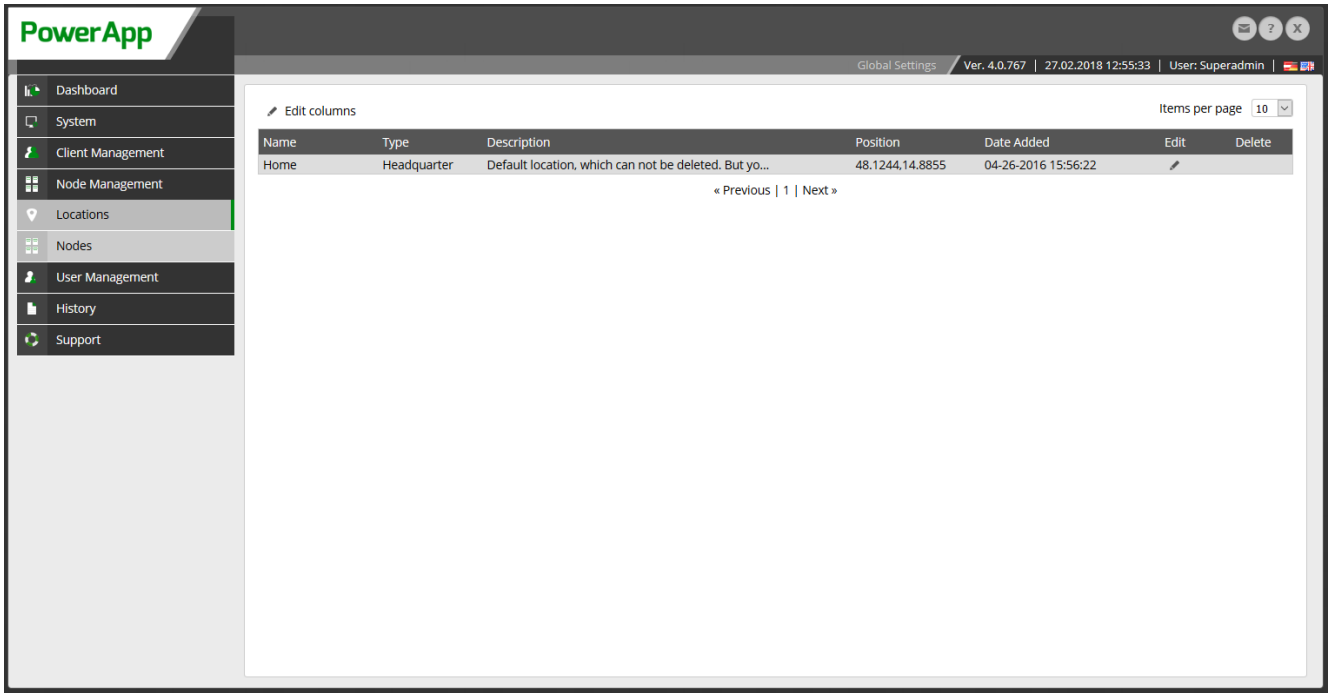


Figure 63: Locations

5.3.2 Nodes

Use this menu to add a second PowerApp for redundancy if your license enables it.

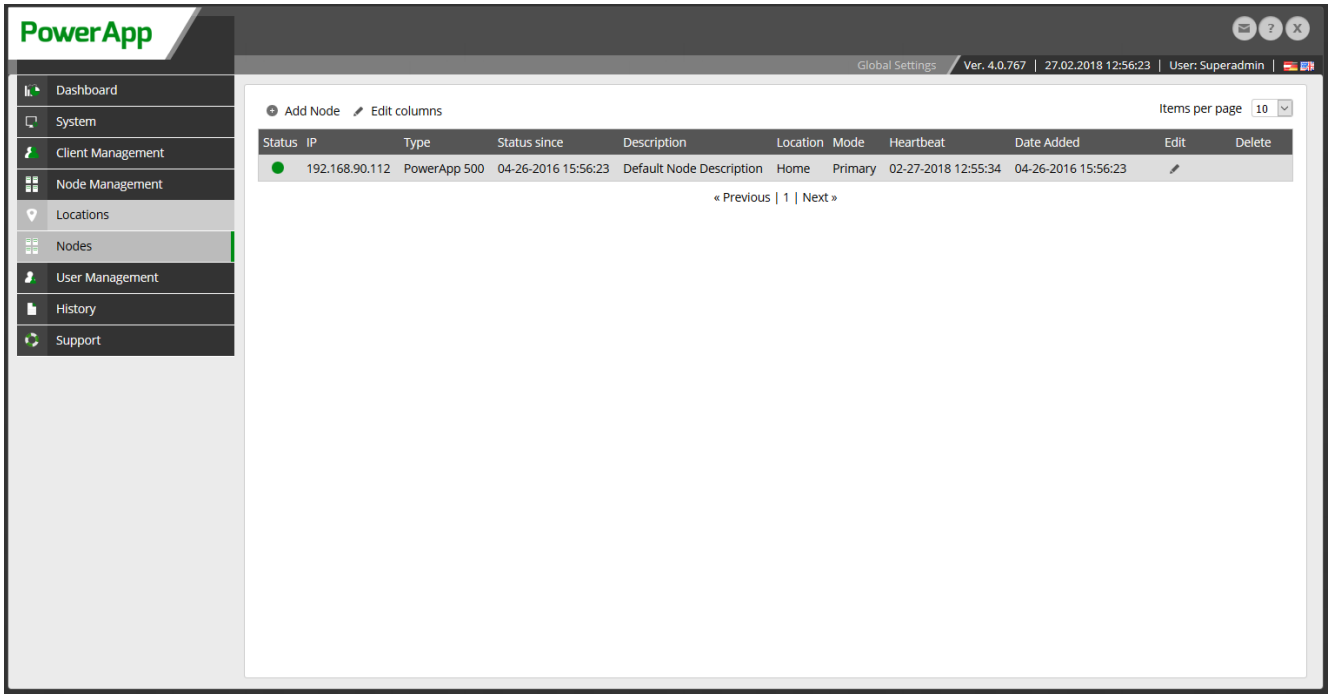


Figure 64: Nodes

Do not forget to add the access key of the second PowerApp to the first one. So that both trust each other.

5.3.3 Access

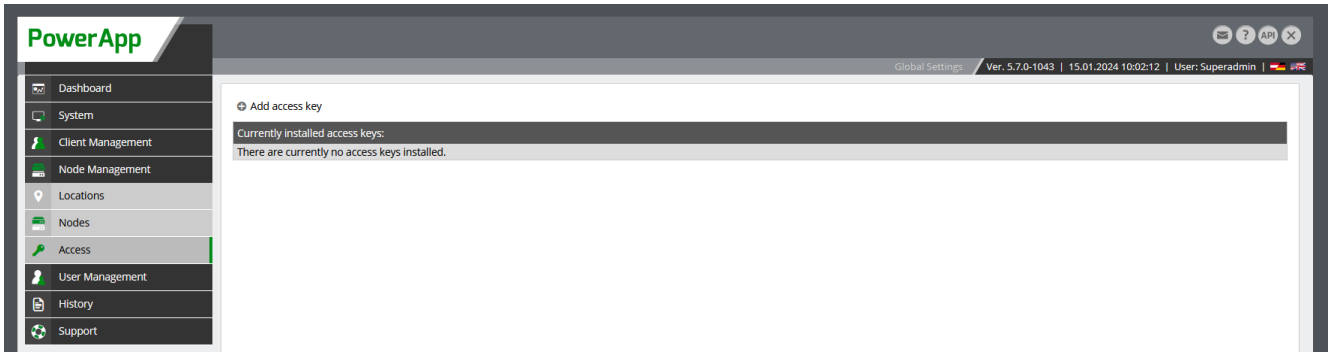


Figure 65: Access

The access keys are added here. Nodes only trust the main node if they know its access key and vice versa.

5.4 User Management

The PowerApp user configuration is accessible via the menu item "User Management". The permission structure is divided into users and groups.

A user object defines a user account that is allowed to log on to the PowerApp. Groups define the access rights.

After installation, only the user "Superadmin" is available, which is a member of the group "Superadmin". The "Superadmin" group has all available permissions by default.

5.4.1 MyUser

The MyUser page allows you to edit settings specific to your user account. This provides a centralized location for managing your personal preferences and account details.

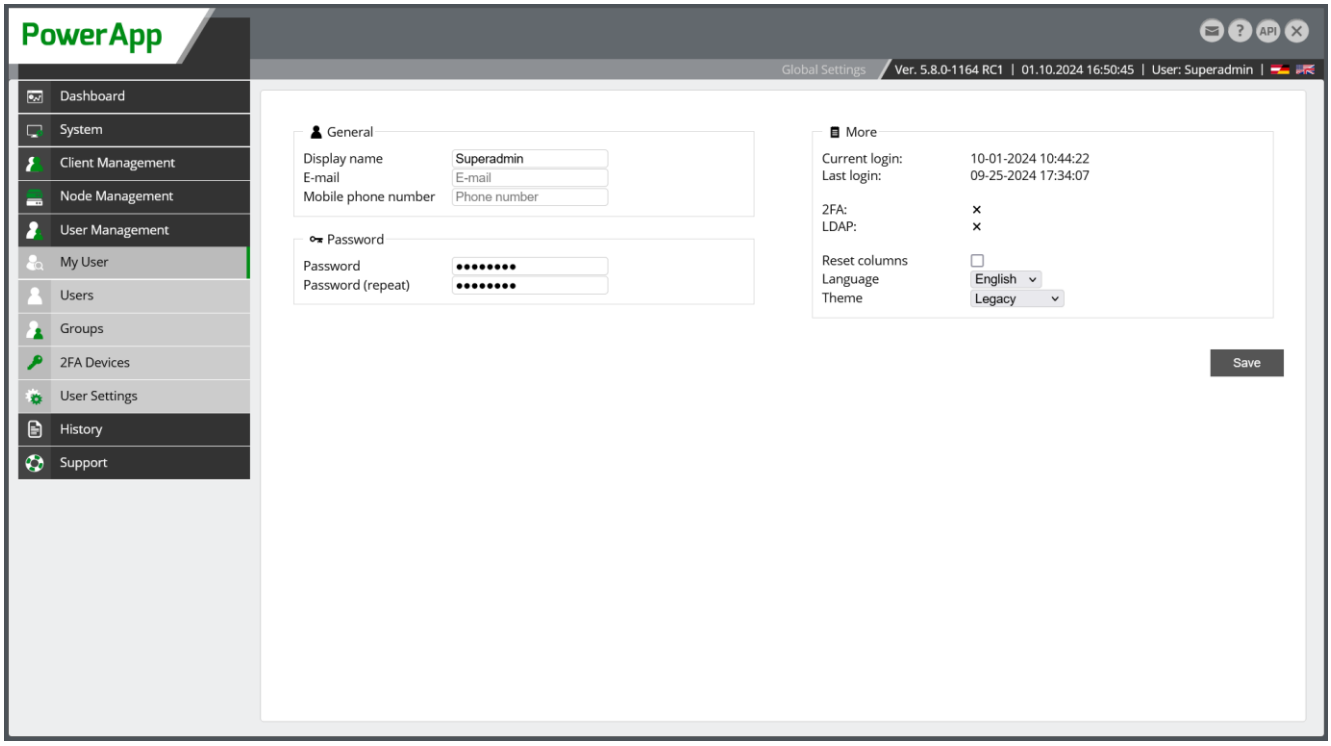


Figure 66: MyUser

5.4.2 User

Use the „user“ menu to view or edit existing or create new Superadmin-users.

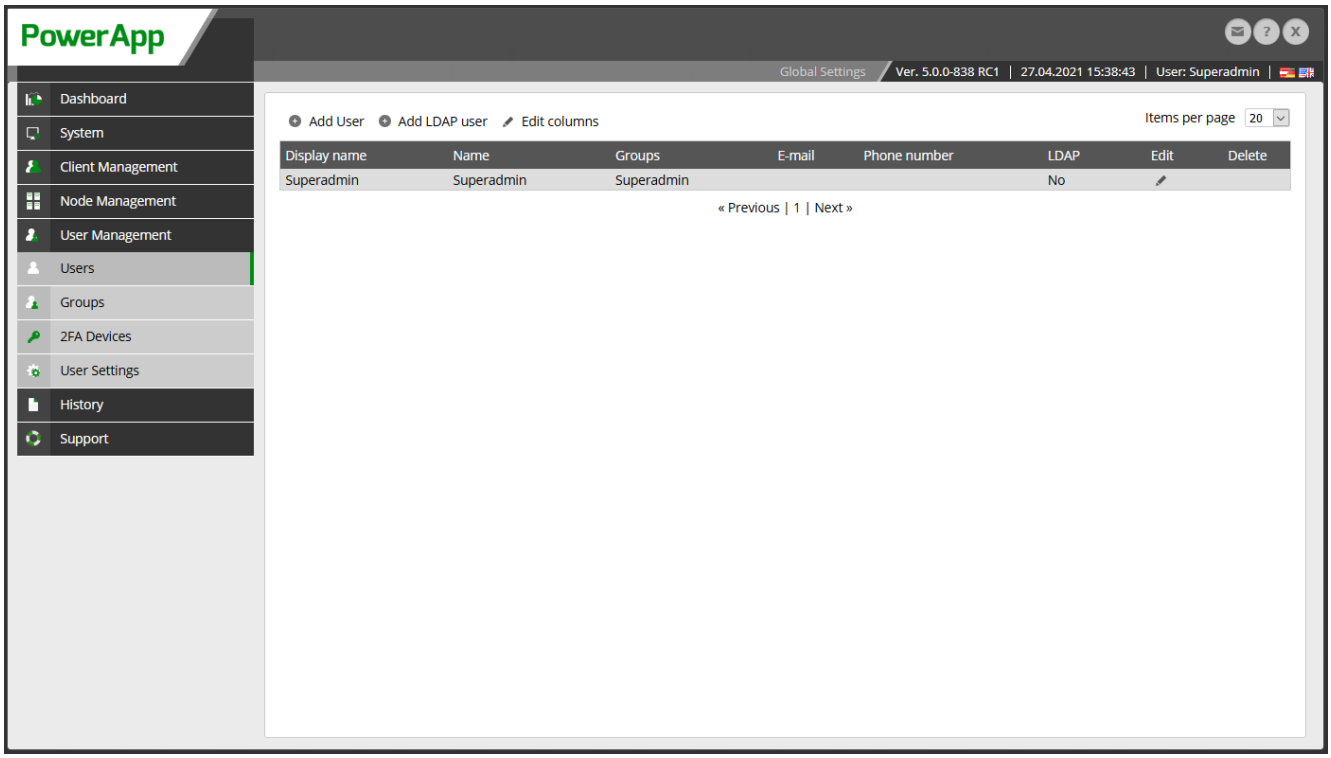


Figure 67: User Management

Existing users can be edited or delted in the list view.

The automatically generated superadmin user cannot be deactivated or deleted. It is recommended to change the default password immediately after the installation is finished.

New local users can be added with the „Add“ button. Display name, name, email address and password must be entered.

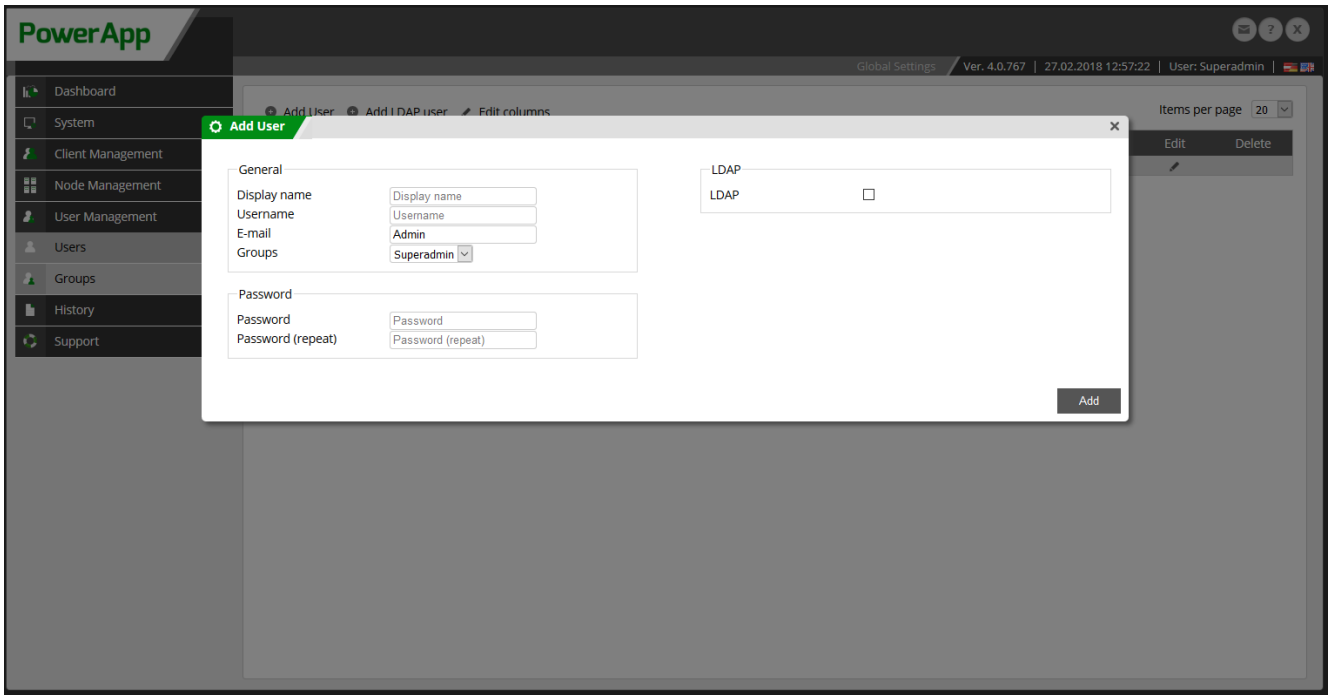


Figure 68: Add User

Use the „Add LDAP user“ button to import users from an existing LDAP server (see chapter Webserver Settings). Choose the user for PowerApp login, from the LDAP tree.

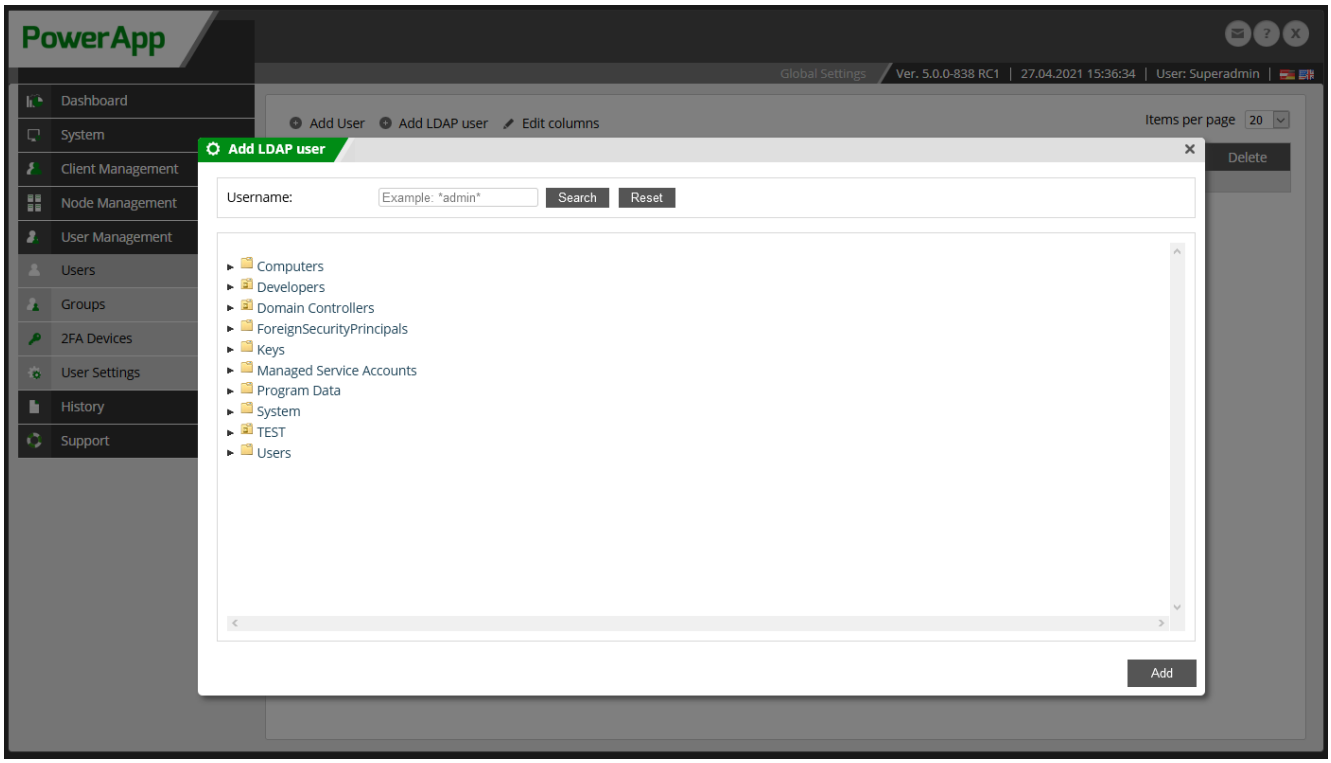


Figure 69: Add LDAP User

5.4.3 Groups

Use the menu „Group“ to view and edit existing groups and add new groups. All PowerApp users, in the central and client console, must be member of a group, to receive any right. Group memberships are the basis of alerting the the client console

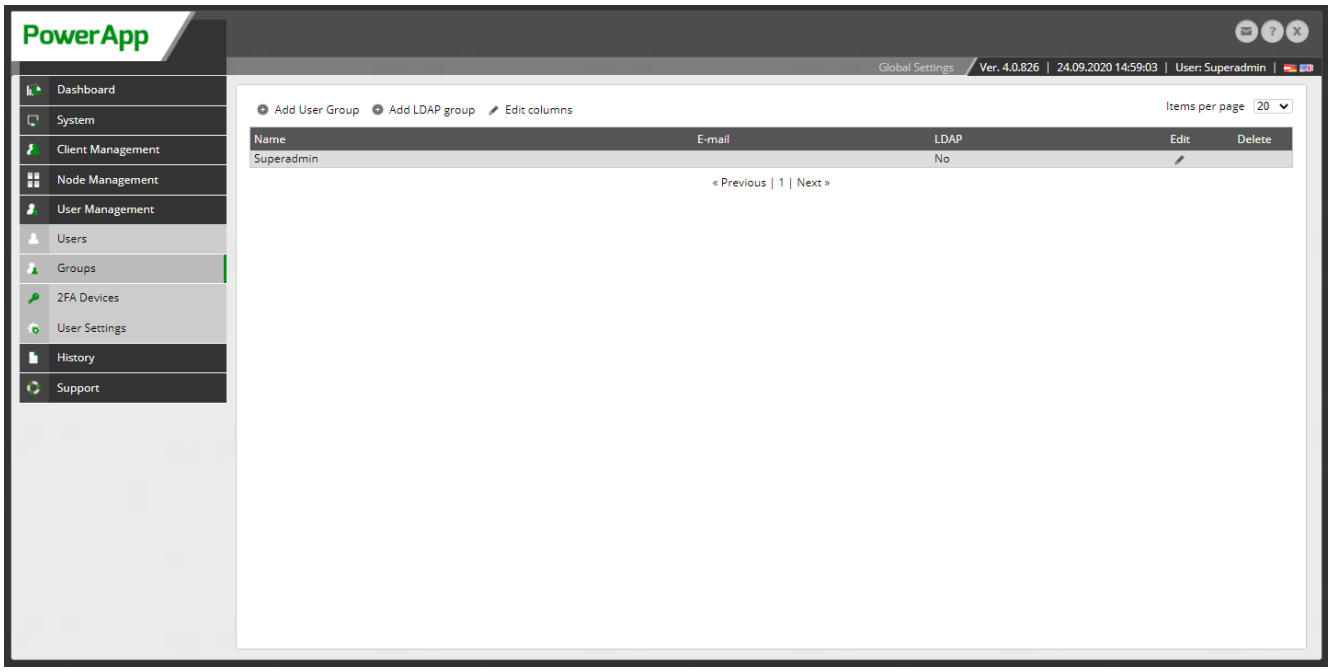


Figure 70: Group Management Superadmin

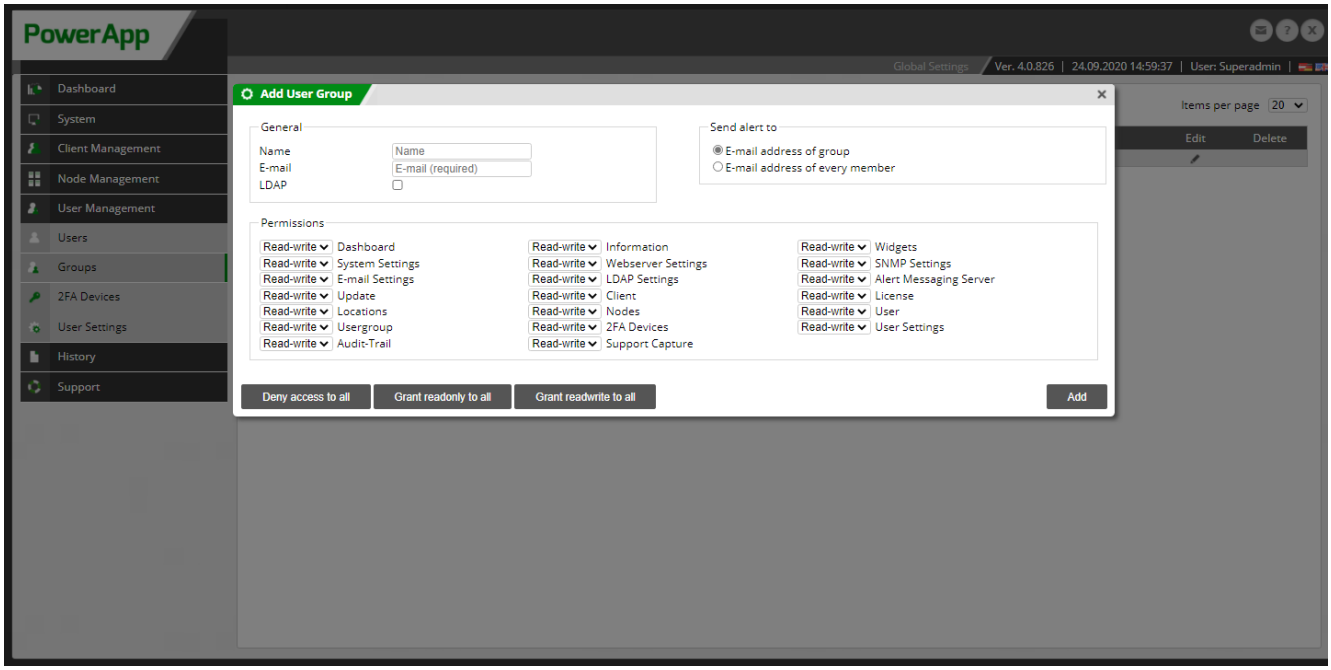


Figure 71: Add Group

Refer to VM Import.

5.4.4 Two-factor-authentication

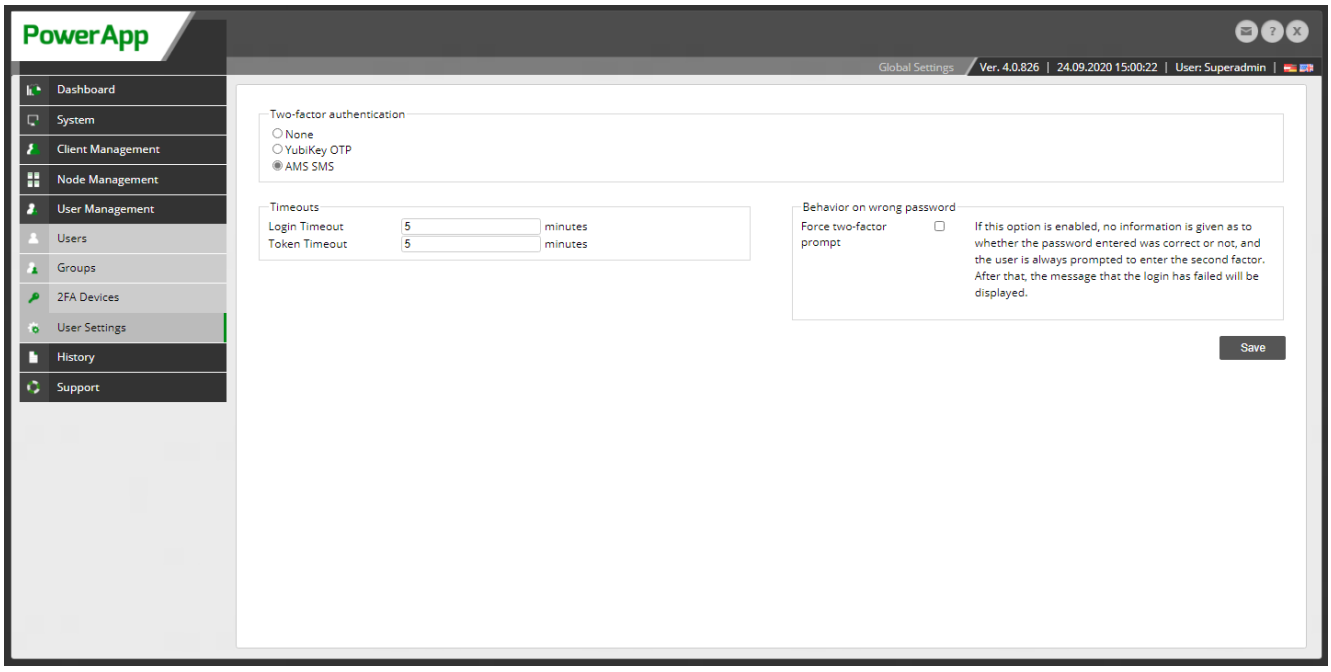


Figure 72: Two-factor-authentication

Refer to Two-factor-authentication for detailed instructions.

5.5 History

5.5.1 Audit-Trail

Use the menu „History“ -> „Audit-Trail“ to view all actions of the Superadmin-users. Therefore every change is completely traceable. Filter for different criteria and export the log into CSV-format.

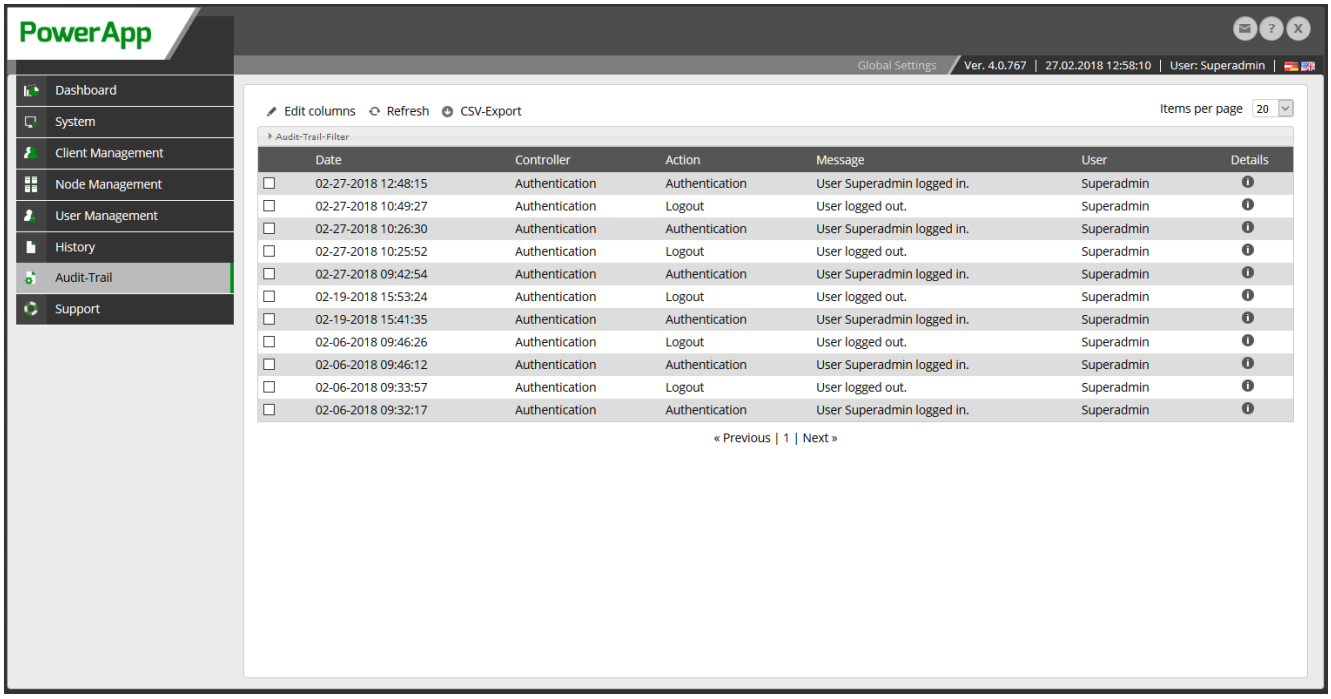


Figure 73: Audit-Trail

5.6 Support

5.6.1 Support Capture

In case of any issues or strange behaviors it may end up in a quite long conversation until our support team will get all kind of helpful information to be able to offer the best possible level of support. This may be time-consuming. To make this even easier for both customers and our skilled team, this support capture functionality is for.

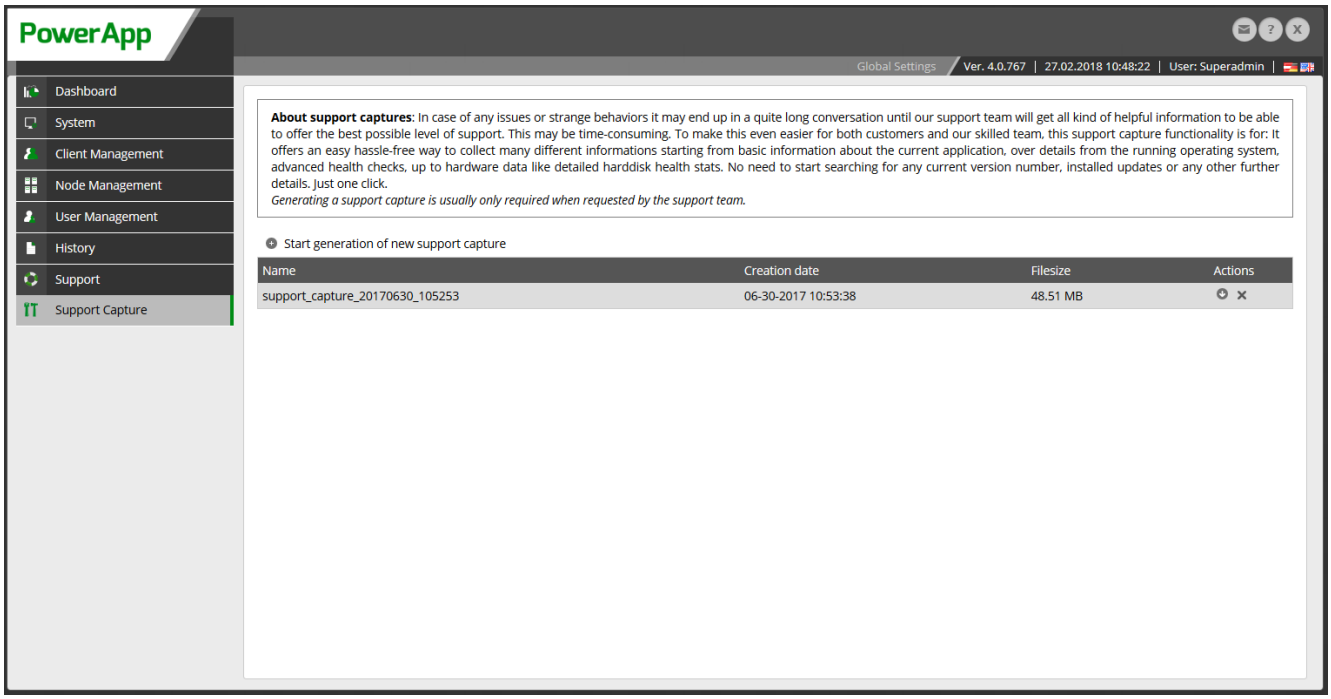


Figure 74: Support Capture

5.7 CLI

5.7.1 Display help

The "help" command shows you all the commands that can help you. Use "help [command]" to get more information about the command you have specified.

```
PowerApp # help
help                        Print this help message
help <command|list>         Print detailed help message of given command
support capture             Creates a Support Capture and provides a download link.
...
```

```
PowerApp # help htop
>> Help of command 'htop':

 Description:
  htop provides you a overview of all running processes on the
  appliance. This is must helpful to take a clooser look, which applications
  needs how much ressources.
PowerApp #
```

5.7.2 Changing the IP address

The “ip [Interface] change" command can be used to change the IP address of the specified interface.

```
PowerApp # ip bondDefault change
>> Network Configuration Setup
################################### WARNING! ###################################
> If you are connected from remote over SSH you may loose the connection to
> the appliance after submitting the settings. Wrong settings may result in a
> completely unavailbility. If this happens, use the Superadmin Console locally!
################################### WARNING! ###################################

> Please provide the following network information to continue.
Address:
...
```

5.7.3 Changing routes

The "route" command opens the "Route Manager", which can be used to easily add new routes or view or delete existing routes.

5.7.4 Verbose mode

To activate or deactivate verbose mode, use the "verbose true"/"verbose false" command.

```
PowerApp # verbose true
Activating verbose mode...
PowerApp # verbose false
Deactivating verbose mode...
```

PowerApp - Your Energy Guard

START OF CLIENT SECTION

iQSol
Security made in Austria.

6 Configuration Settings Client Console

6.1 System

6.1.1 Information

The „Information“ menu shows general system information and hardware utilization (CPU, RAM, Disk).

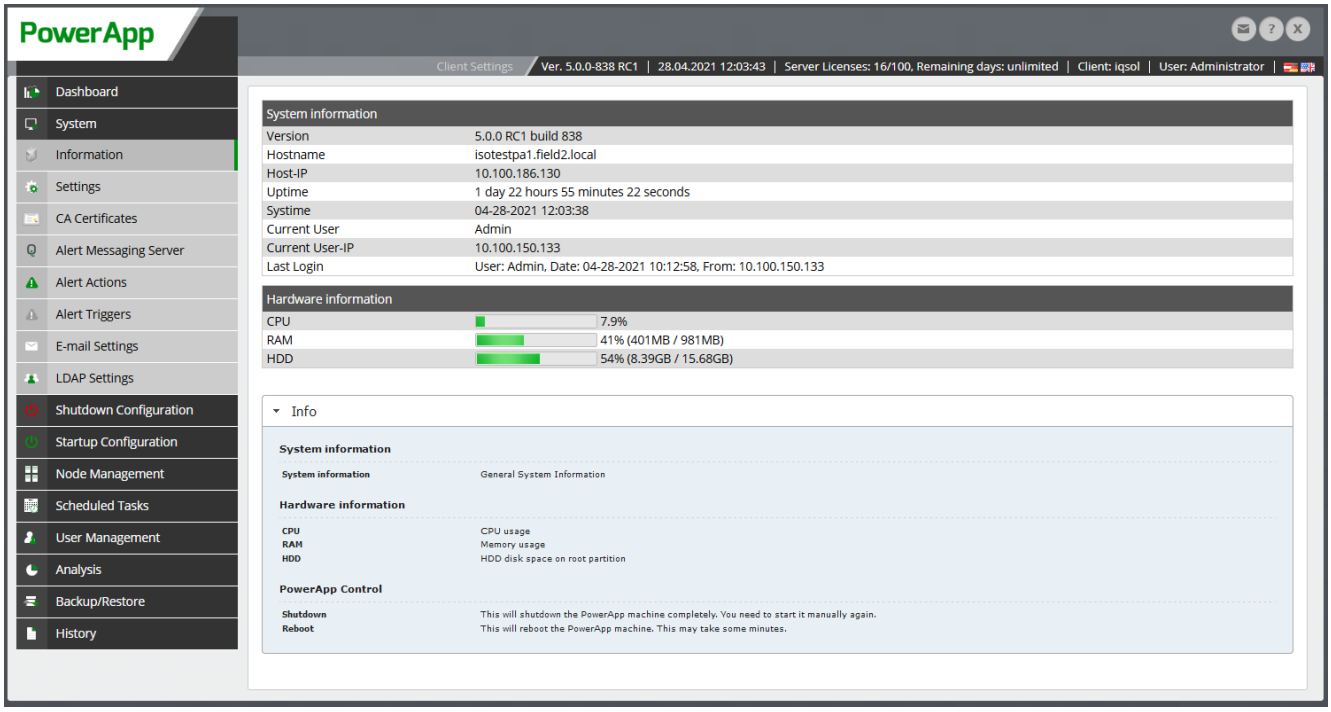


Figure 75: System Information

6.1.2 Settings

Following options can be configured in the basic settings of the client console:

Option	Description
General Settings	
Interval between UPS-checks in seconds	This interval specifies how often the UPS is going to be checked.
Automatically adjust check interval	Automatically optimize check interval for UPS checks. (Recommended)
Move VM command timeout in minutes	This specifies the time how long a VM move can take before the operation is aborted.
Shutdown Settings	
Activate PowerApp-Shutdown-logic	If unchecked, the complete PowerApp logic will be disabled (useful for UPS maintenances)
Startup Settings	
Activate PowerApp-Startup-logic	If unchecked, the complete PowerApp Startup logic will be disabled (if manual startup is planned)
Startup Trigger Level	Change startup trigger level to initiate a startup sequence in certain states
Timer before startup logic will be triggered	Timer before startup logic will be triggered, when all UPS was online the entered time (in minutes)
Move VMs back to origin host	If checked, VMs are moved back to the origin host where they were located before shutdown.
Datastream Collector Settings	
Activate datastream collector globally	Decide if the datastream collector should run. Unchecking completely disables the data collection, independently of the status of each datastream.
Task Scheduler Settings	
Activate task scheduler globally	Decide if the task scheduler should run. Unchecking completely disables the task scheduler, independently of the status of each task.
Credential Settings	
Daily credential check	Automatically check credentials of all servers every day. An alert will be triggered if no connection could be established.
Time of daily credential check	Time of the daily credential check.
Standard-Credentials Windows	When a new Windows-Server is added, automatically assign this credentials.
Standard-Credentials Linux	When a new Linux-Server is added, automatically assign this credentials.
Standard-Credentials Management Port	When a new Management interface is added, automatically assign this credentials.

Purge Settings	
Offline time until e-mail alert (Server, days)	After how many days a server needs to be offline, before the users will be alerted. (0 for never)
Offline time until deletion (Server, days)	Amount of time in days, a server has to be offline until it will be deleted. (0 for never)
Offline time until e-mail alert (Management ports, days)	After how many days a management needs to be offline, before the users will be alerted. (0 for never)
Offline time until deletion (Management ports, days)	Amount of time in days, a management port has to be offline until it will be deleted. (0 for never)
Purge log entries older than (days)	Amount of time in days to keep logs. (0 for forever)

Table 4: Settings Client Console

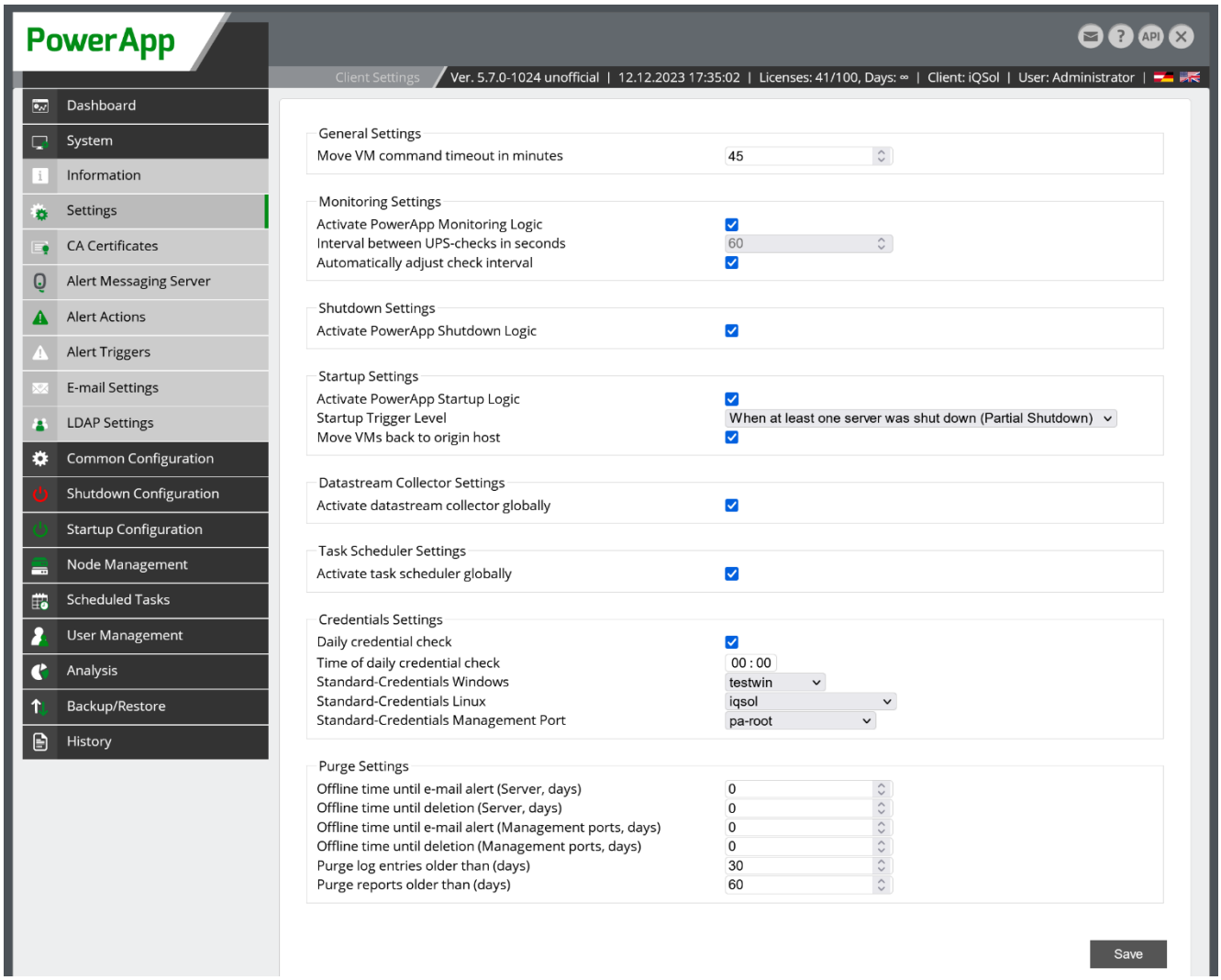


Figure 76: Settings

6.1.3 CA Certificates

Certificates which should be recognized system-wide can be uploaded here.

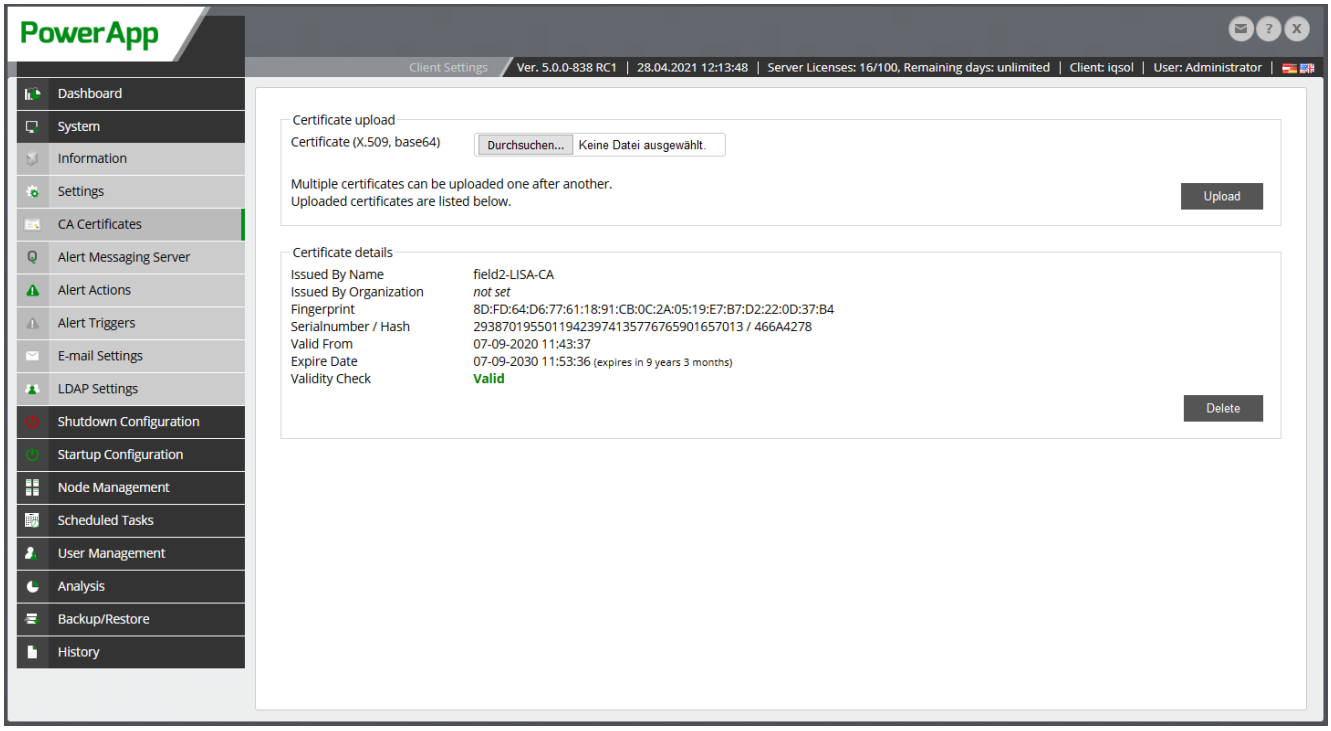


Figure 77: CA Certificates

6.1.4 Alert Messaging Server

In the AMS settings, the IQSol Alert Messaging Server can be connected for further alerting via SMS or voice. Either via the console client or via the web application.

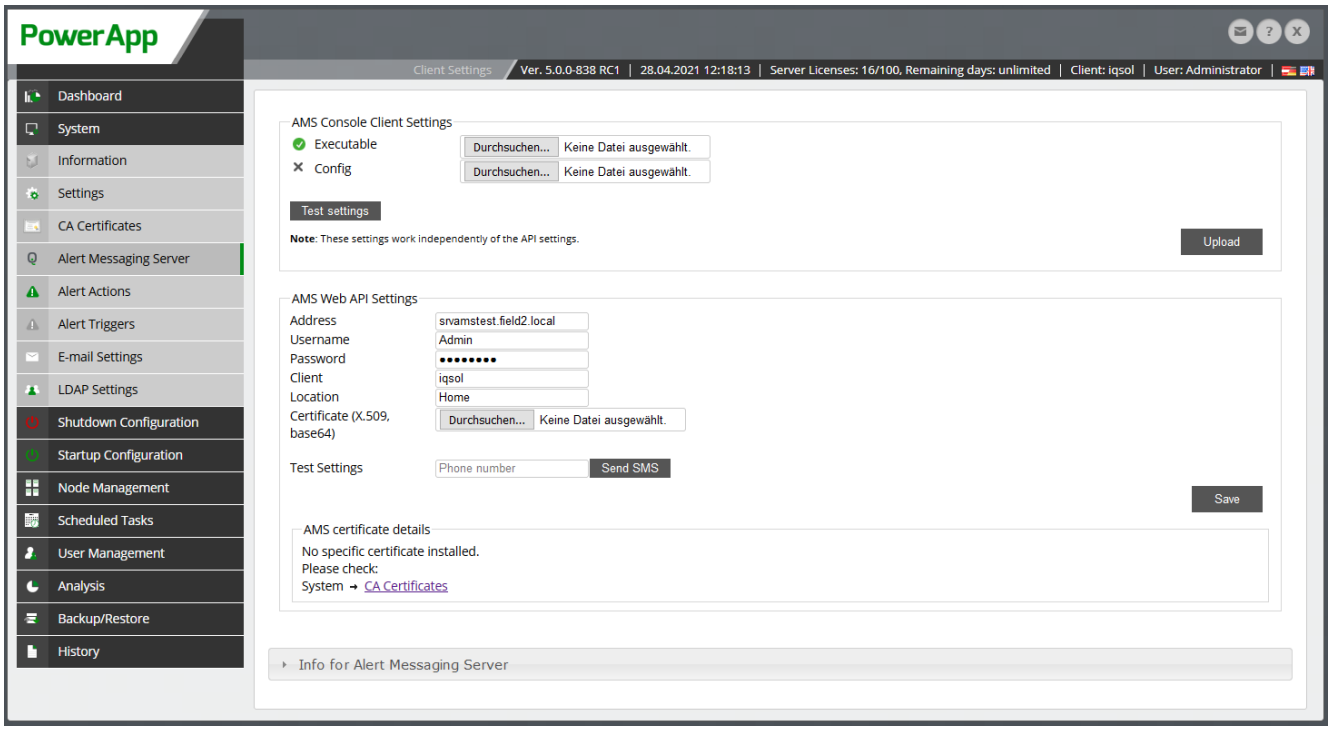


Figure 78: Alert Messaging Server Settings

Console Client

To connect the AMS, the AMS client in use and the config file created for the PowerApp must be saved. Both files can be obtained from the AMS Management Interface.

Note: These settings work independently of the API settings.

Web API

The following information must be entered:

- Adresse (IP or FDQN)
- User name
- Password
- Mandate
- Location
- The associated certificate

These settings can be tested by entering a telephone number

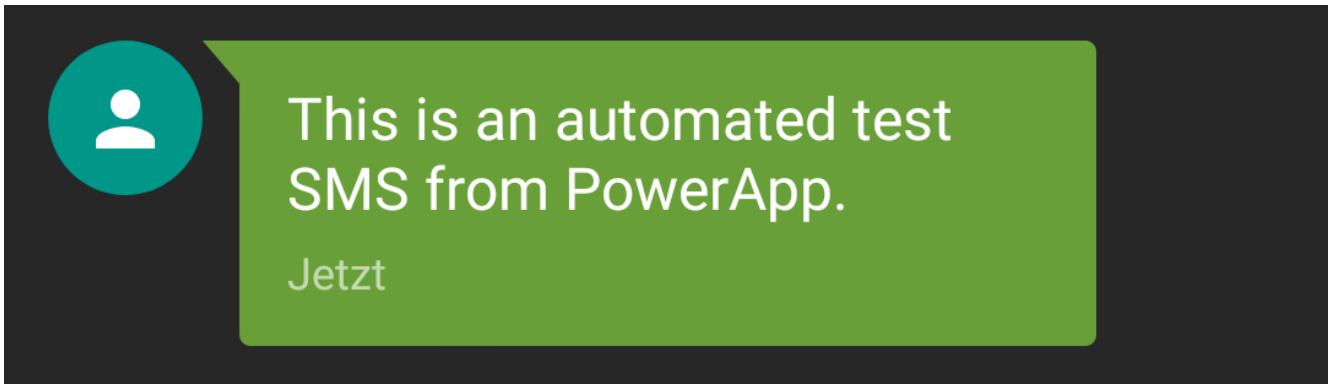


Figure 79: TEST SMS

6.1.5 Alert Action

Configure action for execution on certain events (see chapter Alert Trigger). Sending emails and executing any command is supported by default. Additionally send sms or make phone calls by integrating the third party product „Alert-Messaging-Server“ (AMS) by iQSol.

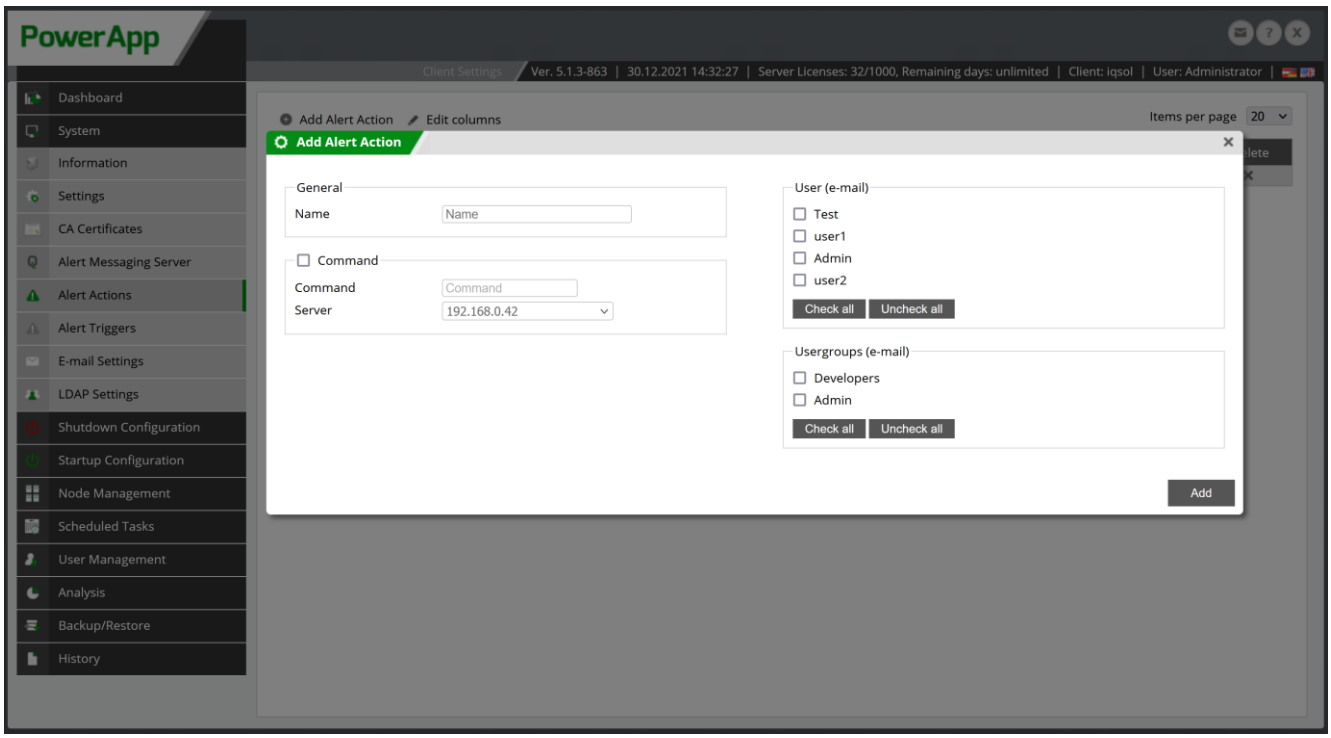


Figure 80: Alert Action

6.1.6 Alert Trigger

Use Alert-Triggers to execute actions on certain events, e.g. sending emails (see chapter Alert Action).

Following Alert-Triggers are supported:

- Shutdown Logic started
- Startup Logic started
- Daily credential check failed
- Report data collection started
- Report data collection ended
- Server is starting up
- Server is shutting down
- Server is offline a long time/will be deleted.
- ESXi enter/exit maintenance mode
- vCenter DRS change
- Node is not reachable
- Node is reachable
- SNMP device criteria matched
- SNMP device status changed
- Error while retreiving SNMP-Data
- Scheduled Task - VM import result
- Scheduled Task - CSV import/export result

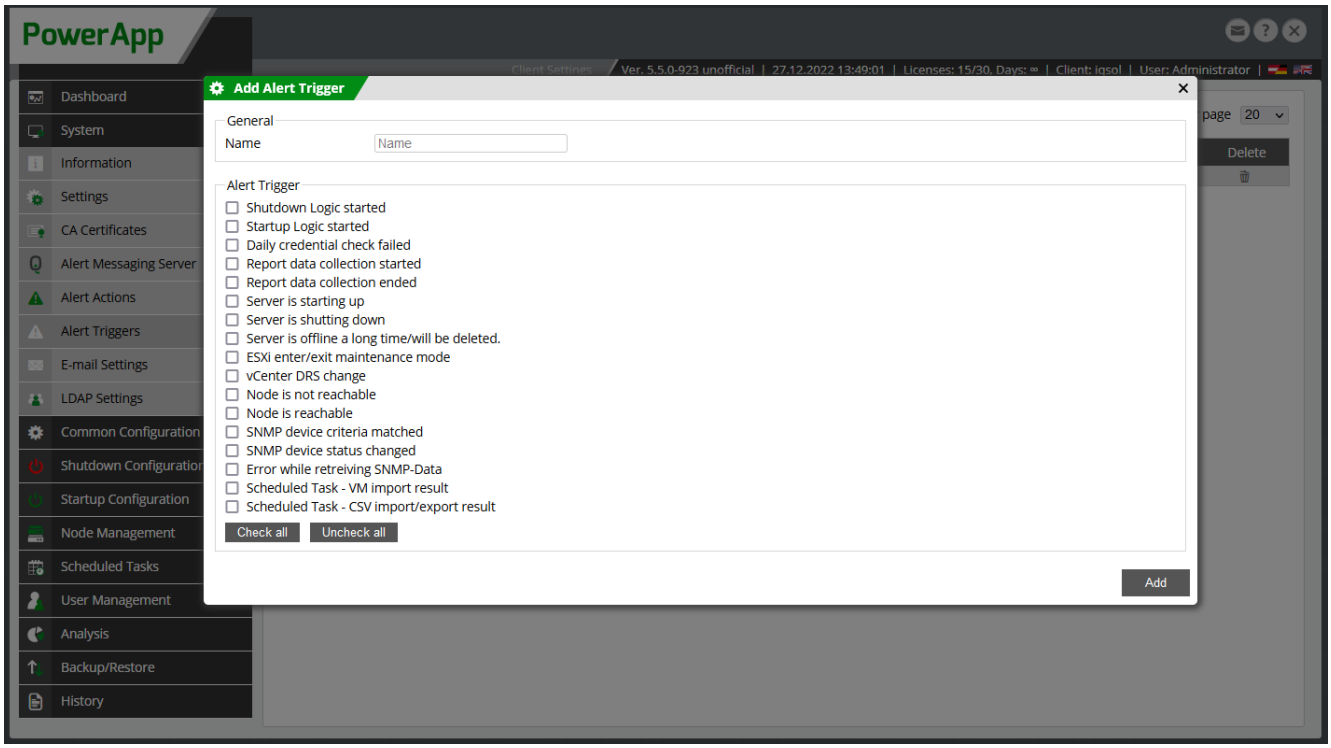


Figure 81: Alert Trigger

6.1.7 E-Mail Settings

Configure the SMTP server for alerting in the „E-Mail Settings“. The user group itself, or all users of a user group are alerted via email, if an alert is triggered, and alert actions and alert triggers are active.

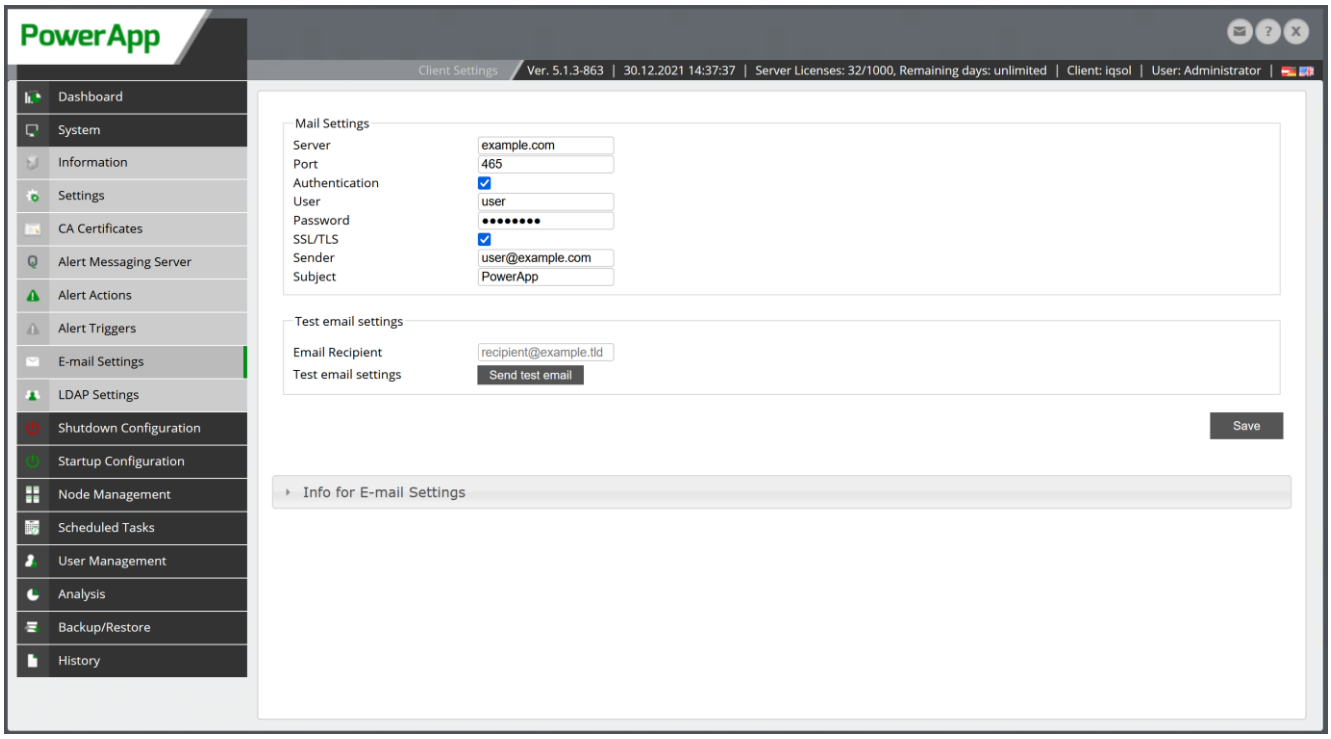


Figure 82: E-Mail Settings

6.1.8 LDAP Settings

Use the „LDAP-Settings“ menu for configuring LDAP servers for user authentication. Enter servername or IP address, port, authentication data and domain/organisation. Click “Save” to automatically test the LDAP server connection. The LDAP tree is displayed, if the connection is successful.

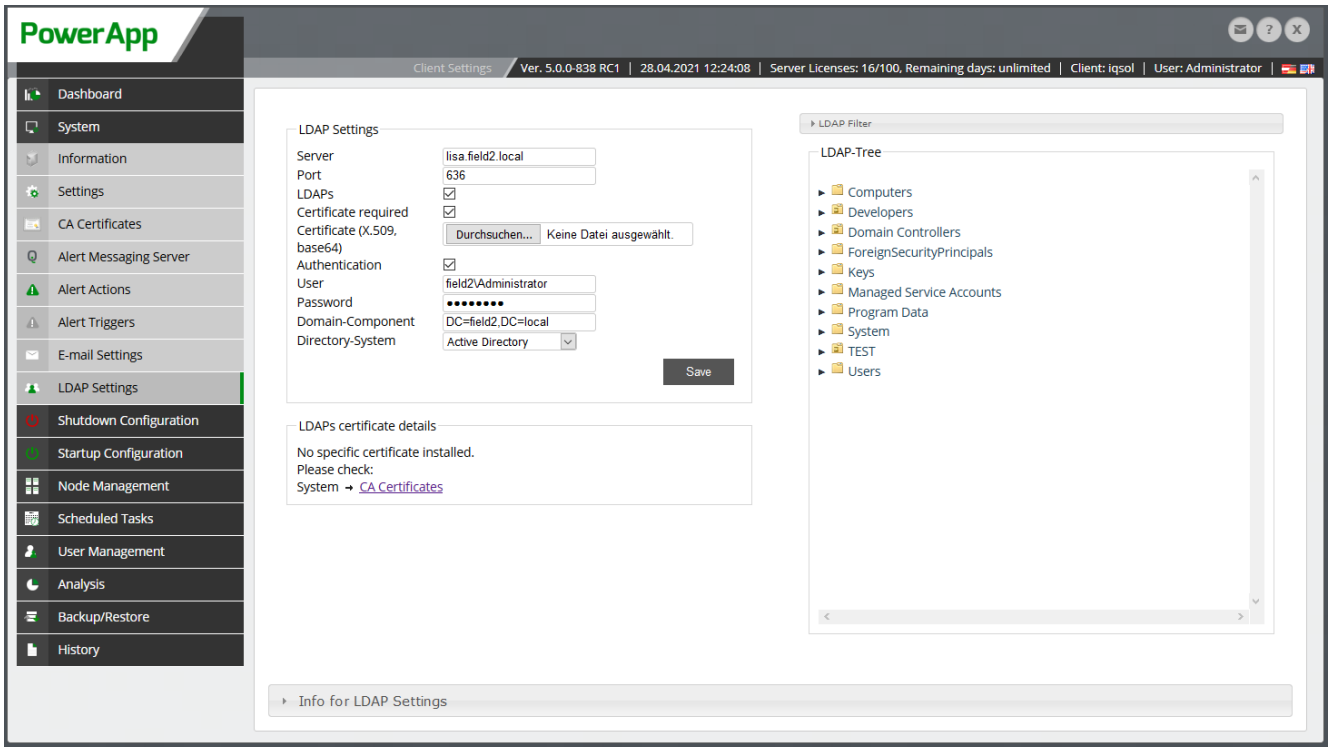


Figure 83: LDAP Settings

Import LDAP users to the „User-Management“ menu (see chapter Scheduled Tasks).

6.2 Common Configuration

The settings made in common configurations affect both the shutdown configuration and the startup configuration.

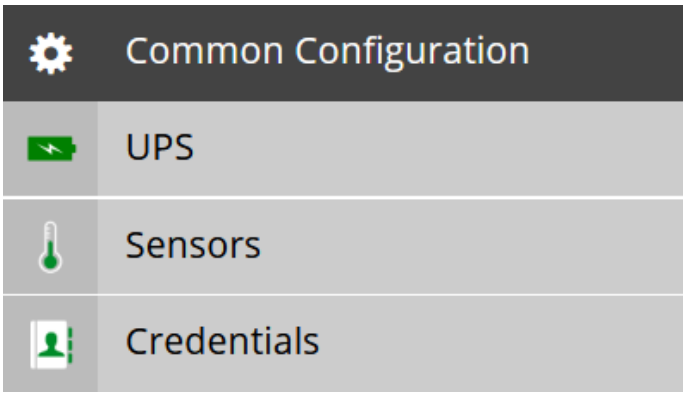


Figure 84: Common Configuration

6.2.1 Uninterruptible Power Supply

Use this menu to add UPSs. All models are supported, as far as they are supporting SNMP queries. Version 1, 2 and 3 is supported. The PowerApp does not trust SNMP traps, but queries the status actively via SNMP polling using SNMP-Get. Define the interval of the UPS queries in the menu „System“->„Settings“. The vendor specific MIB defines, which object needs tob e queried via SNMP. The MIB can be imported while adding a UPS. A shutdown or startup action is triggered, if all defined criteria (e.g. UPS on battery) matches (see chapter Criteria or Shutdown Criteria & Startup Criteria).

When the Maintenance Mode checkbox is selected, the device is completely ignored by all tasks.

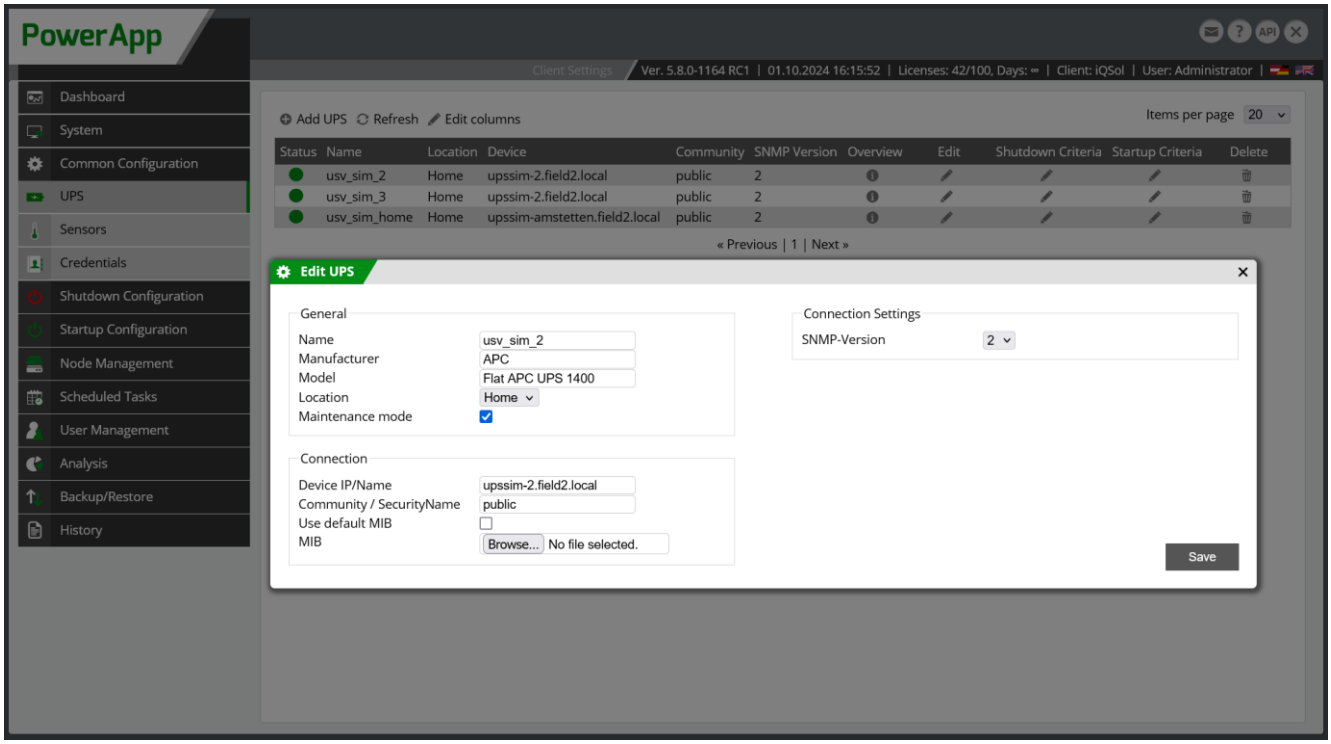


Figure 85: Uninterruptible Power Supply

6.2.2 Sensor

Sensors are added as SNMP devices – as well as UPSs- and are able to trigger a shutdown action as well. Fire detectors and temperature sensors are also integrateable here. Define the trigger condition under „Criteria“ (see chapter Criteria or Shutdown Criteria & Startup Criteria) e.g. if the temperateure is higher than 30° Celsius.

When the Maintenance Mode checkbox is selected, the device is completely ignored by all tasks.

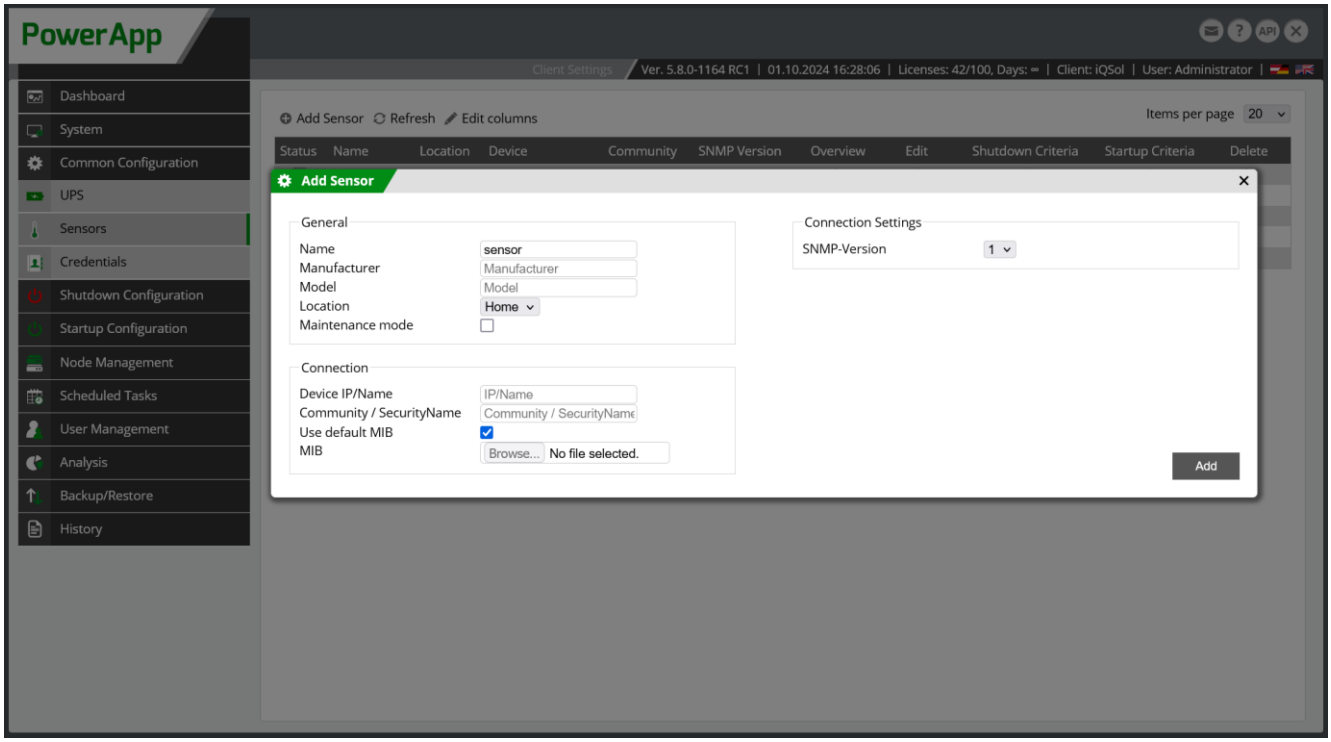


Figure 86: Sensor

6.2.3 Credentials

Define login credentials for accessing Windows and Linux systems and executing commands for shutdown. Username/password as well as authentication via SSH key is supported.

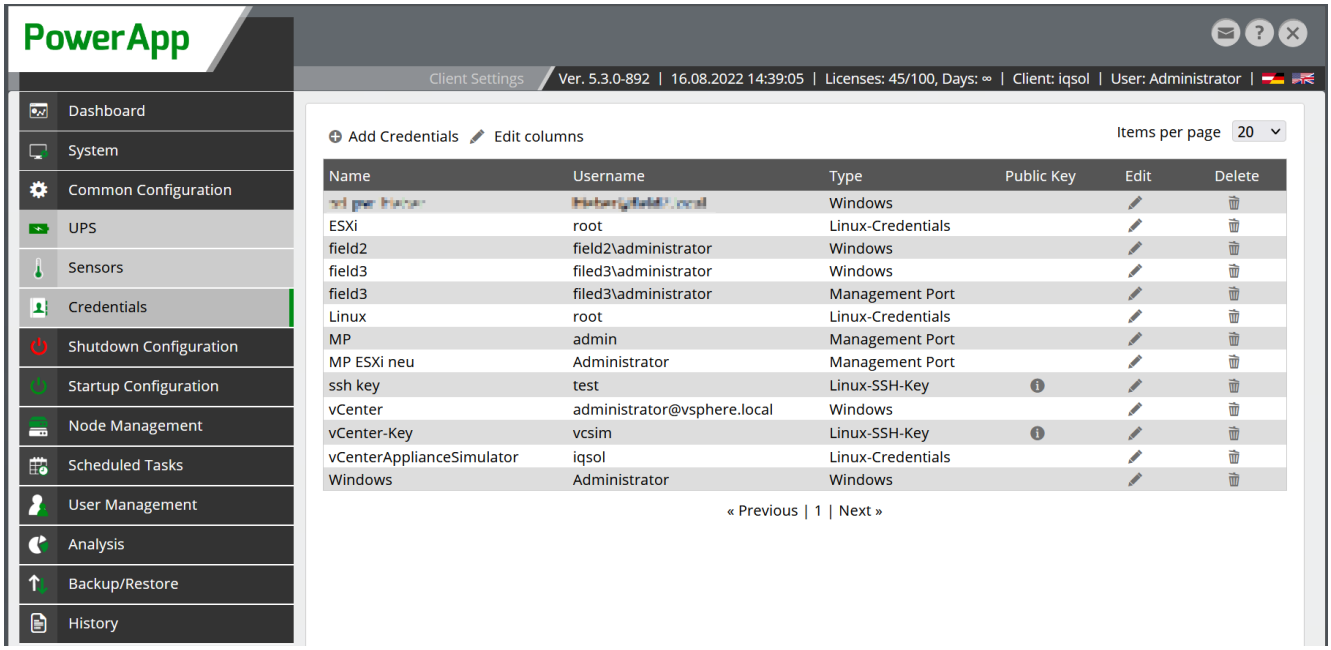


Figure 87: Credentials

6.3 Shutdown Configuration

6.3.1 Server

Use the menu „Server“ to view and edit existing servers or add new ones. Existing servers can be edited or removed with the buttons in the listview and entered commands can be executed on the servers. Filter for different criteria and export or import entries in CSV-format. Use button „VM-Host-Import“ to import virutal machines directly from the host or vCenter or SCVMM. All available machines are listed under „Host Groups“ (see chapter Host Groups or Host Groups). The listview can be adapted using „Edit columns“.

The „Submit“ button below the table is used for executing operations on multiple servers. Select the servers marking the checkbox, choose the command (e.g. „Check Credentials“) and click „Submit“.

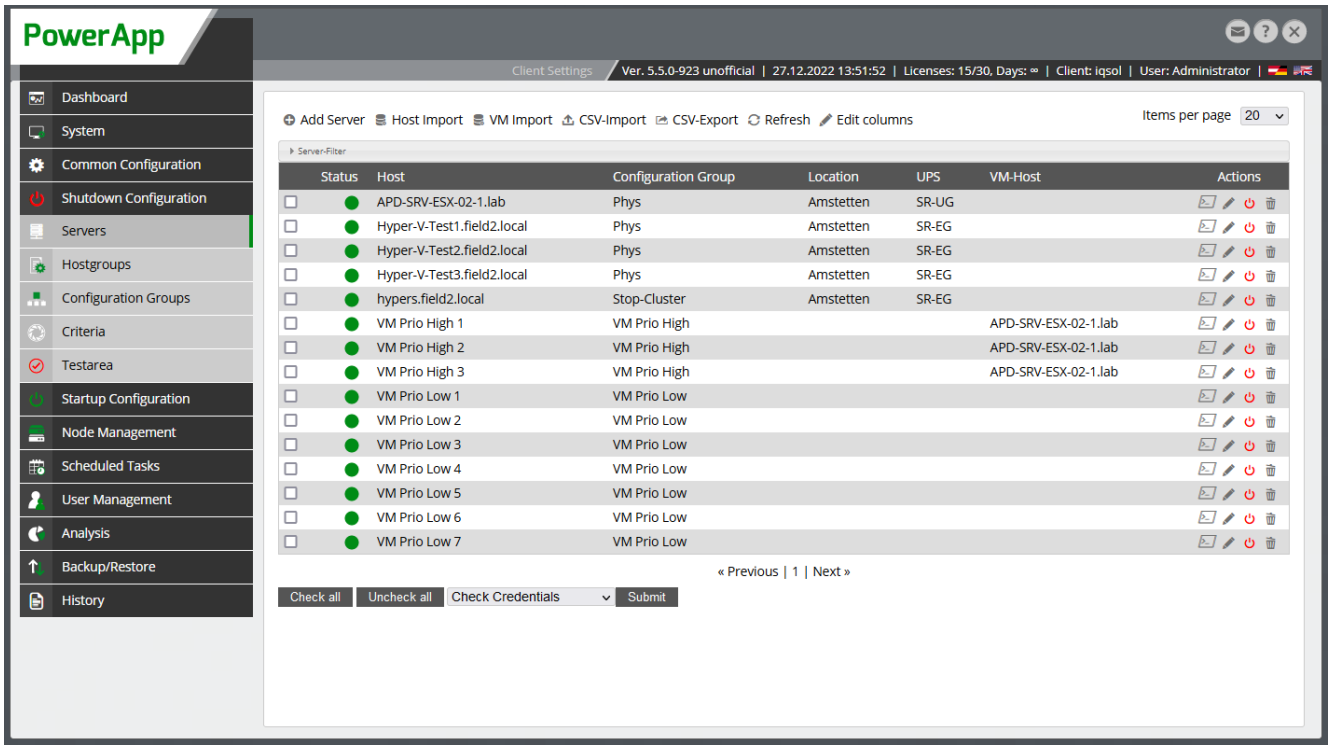


Figure 88: Server

If you click in the Actions column on this you can execute a one-time command.

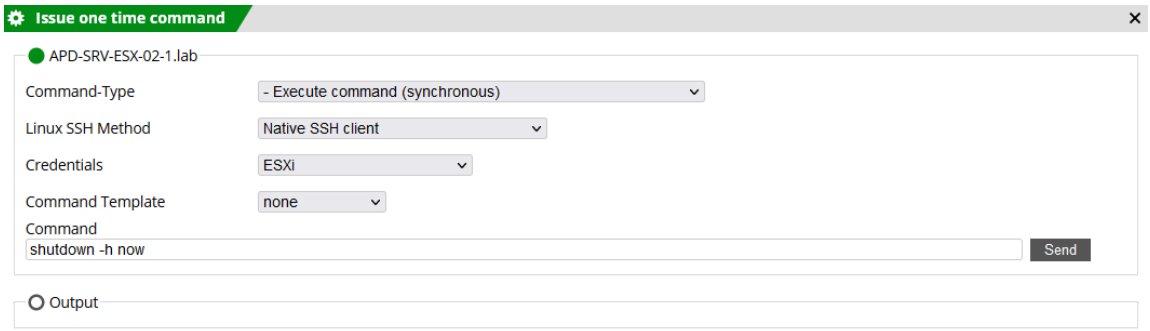


Figure 89: One time command

New servers can be added manually with the „Add server“ button.

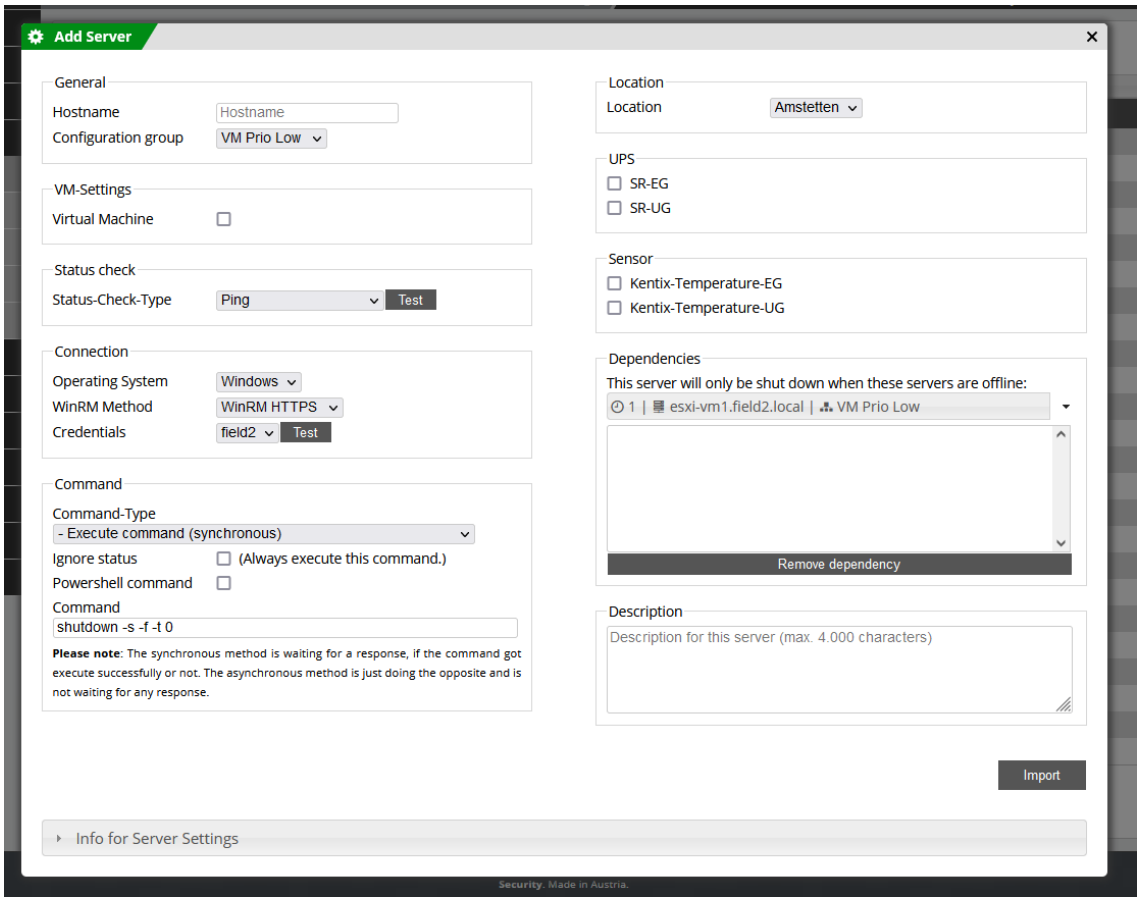


Figure 90: Add server

WinRM Methods

This short section is about the WinRM methods used to connect to Windows systems.

WinRM HTTPS	Requires access to the Windows host on port 5986 and the CA's certificate. https://learn.microsoft.com/en-us/windows/win32/winrm/installation-and-configuration-for-windows-remote-management
WinRM HTTP	Requires access to the Windows host on port 5985.
winexe (legacy)	Is no longer recommended for use.

Linux SSH Methods

This short section is about the SSH methods used to connect to Linux systems.

Native SSH client	The recommended SSH method.
Embedded SSH client	Alternative option if native has compatibility problems.
Python SSH client	Better compatibility to older SSH clients.

6.3.2 Host Groups

Add VMware and Hyper-V hosts and enter login credentials in the „Host Groups“ menu (see chapter Credentials or Credentials (Shutdown Configuration)). Establish a connection to the vCenter or SCVMM here. Migration of virtual machines via vMotion or Quick/Live-Migration is supported as well.

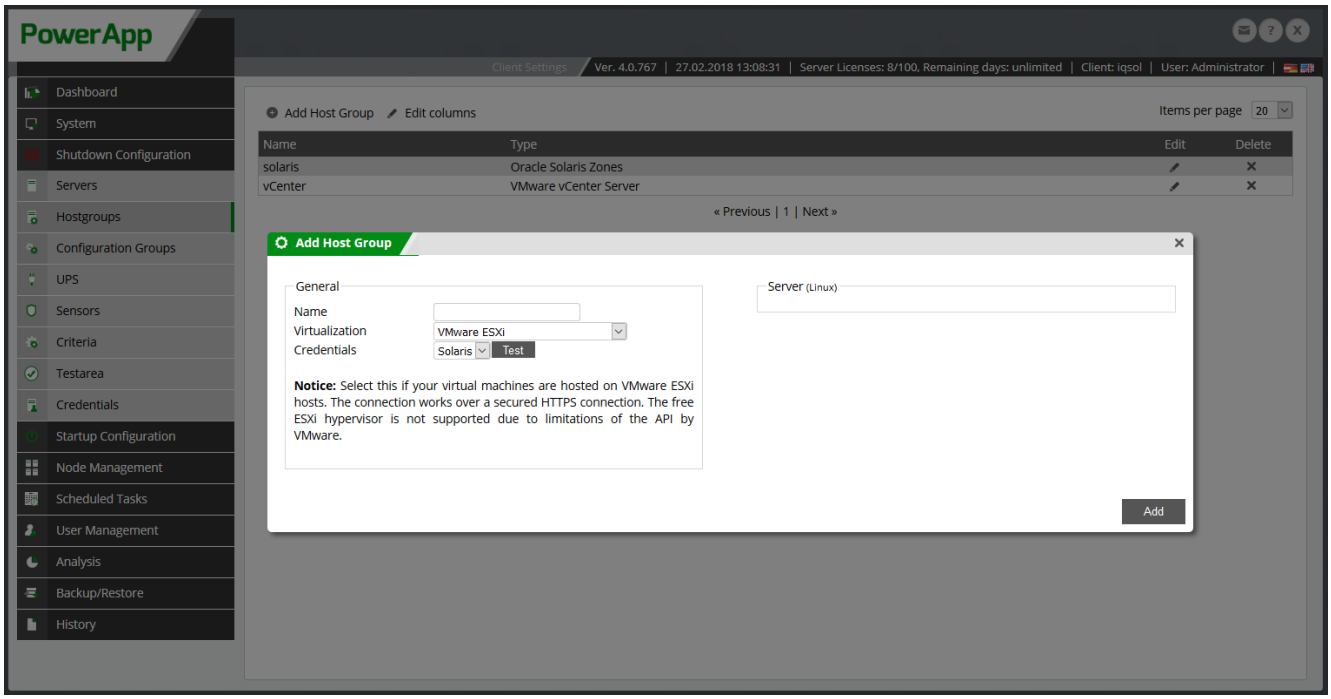


Figure 91: Host Groups

6.3.3 Configuration Groups (Shutdown Configuration)

Use „Configuration Groups“ to define the time sequence for the shutdown. While adding a configuration group a name and the delay in minutes must be entered. Every server needs a configuration group assignment, so that the PowerApp is able to arrange the shutdown process in time.

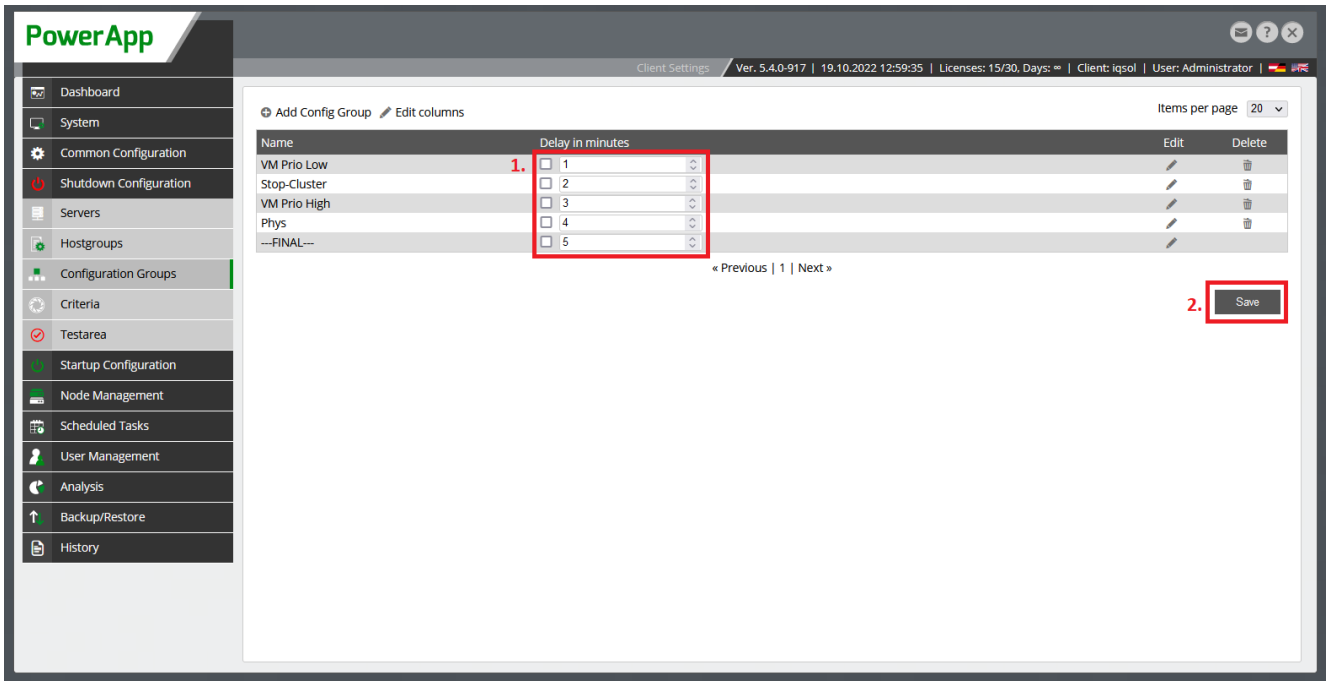


Figure 92: Configuration Groups

1. Here it is possible to set the delay without opening the configuration group editing window. With a check mark in the small boxes you can count up or balance the delay for several configuration groups at the same time.
2. In order to apply these changes, it is necessary to click on "Save".

6.3.4 Shutdown Criteria

Criteria keep track of individual values of an SNMP device and record whether and since when a condition matches.

In the Add Criteria window, click MIB Browser to select the OID. For example, seconds on battery. Enter the number of seconds in the Value field and set the operator to "<" to match when the set seconds have been exceeded.

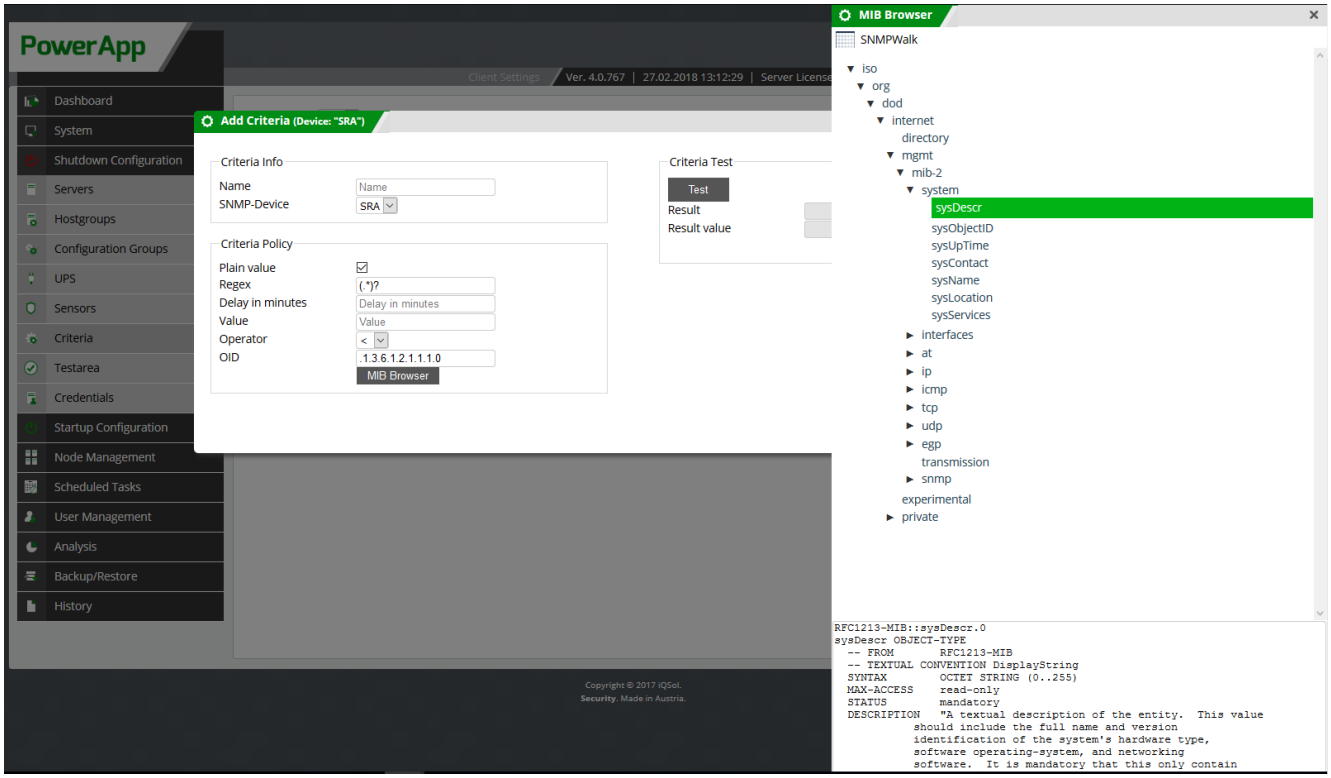


Figure 93: Criteria

6.3.5 Shutdown Trigger

Logic Triggers are used to define the conditions under which a shutdown should be initiated.

To achieve this, SNMP devices and criteria (organized into groups) are assigned to the trigger. For the trigger to activate, all assigned criteria in at least one group must match.

You can create new criteria groups (organized in tabs) and drag criteria into each group.

To remove a criterion, simply drag it back to the available criteria pool.

For the trigger to activate, all assigned criteria in at least one group must match.

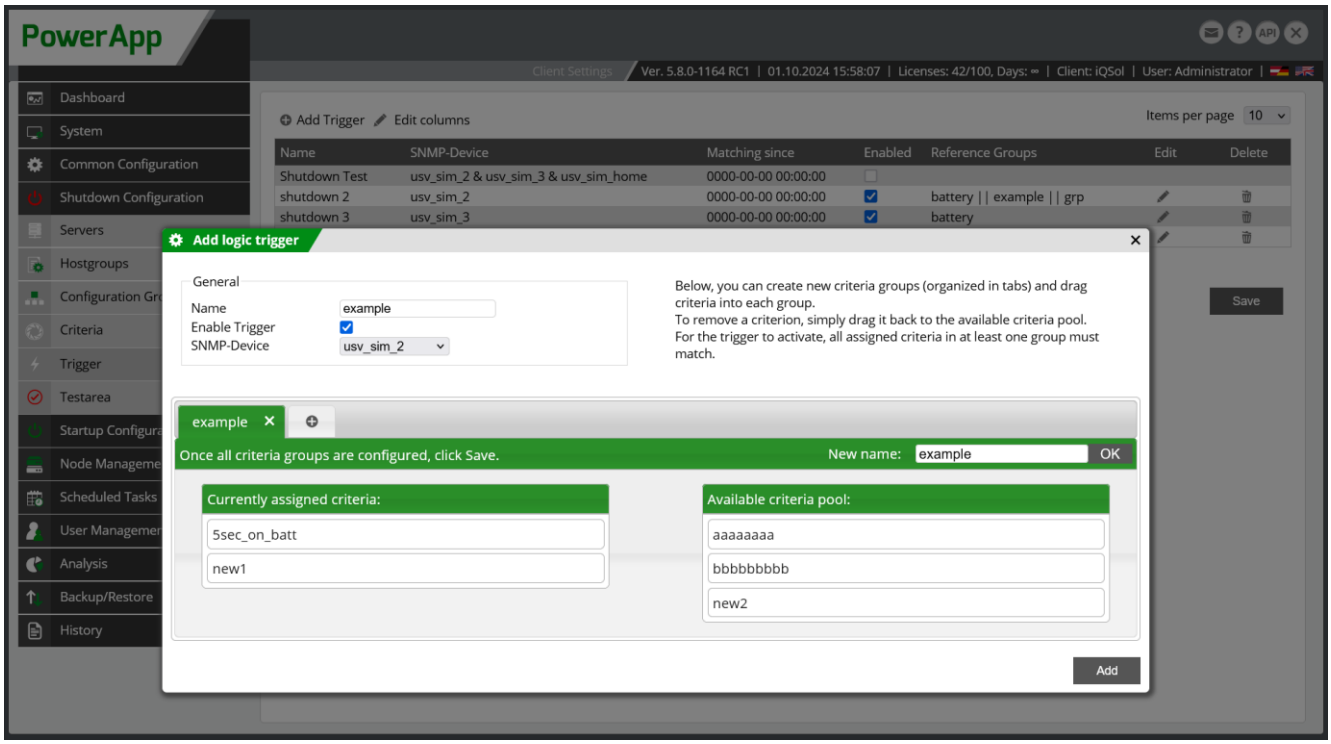


Figure 94: Shutdown Trigger

6.3.6 Test Area (Shutdown Configuration)

Overview

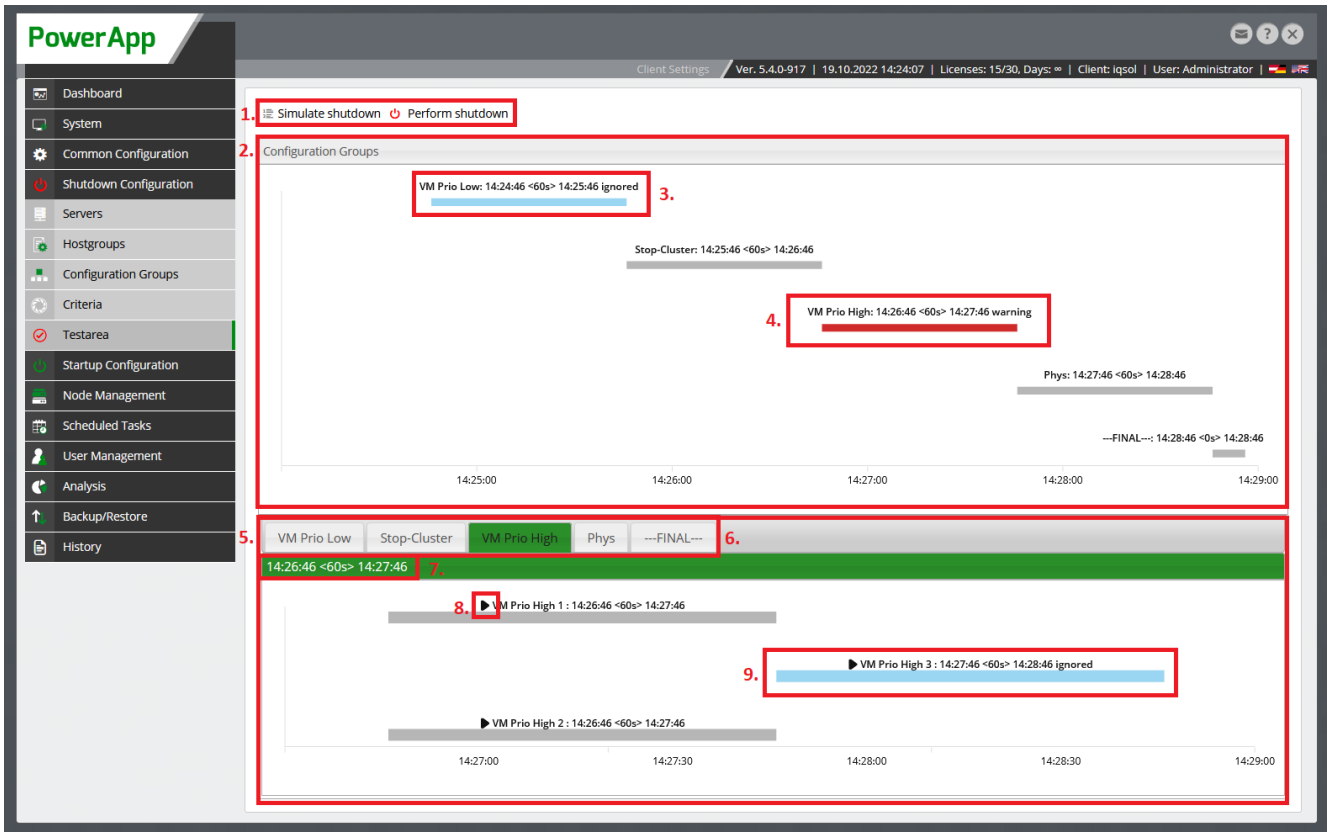


Figure 95: Shutdown simulation

1. Use the button „Simulate Shutdown“ to display all systems and their planned shutdown. No real shutdown is executed. This is only for succesfull configuration check.

   Use „Perform Shutdown“ button to configure the shutdown process manually. If all UPSs are chosen, an overall shutdown is executed. In the other case a part shutdown is executed, and only those servers are shutdown, which are connected to the affected UPS. The same logic is used for the automated shutdown. The systems are shutdown on basis of a temporal sequence, depending on configuration group assignment and dependencies.

   NOTE: A real shutdown of the systems **IS** executed!

2. The configuration groups are displayed here.
3. A configuration group turns blue when it is ignored. Configuration groups are ignored if they do not contain any servers or if all servers in a configuration group are ignored.
4. A configuration group turns red if the servers take longer than the configuration group.
5. The servers of the individual configuration groups are displayed here. If you click on a server bar, you can configure it directly. In addition, if you move the mouse over a bar, you can get more and better readable information.
6. Here you can select which configuration group is displayed.
7. If you click on the gray area (it can also be green if you click on the respective configuration group bar at the top), you can configure the configuration group directly.
8. This small sign indicates the status of the server. If it shows the "Play" sign, the server is on, if it shows the "Pause" sign, the server is off.
9. A server turns blue when it is ignored (The command type is set to "Ignore").

Note: Also, the text of a configuration group or server may turn yellow/orange if there is a problem with the dependencies.

Shutdown (live view)

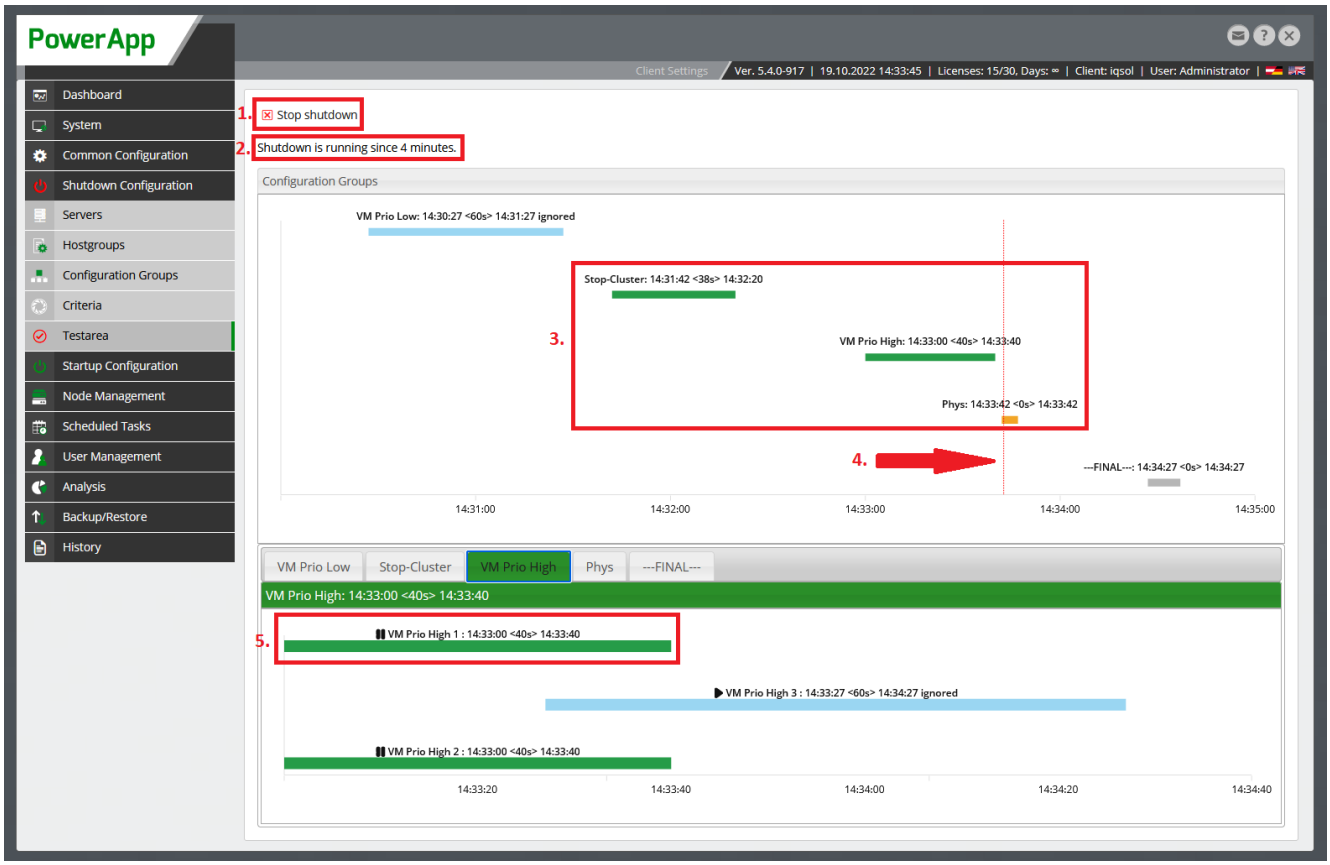


Figure 96: Shutdown live view

1. Here you can stop the shutdown. This button is not available for an automated shutdown.
2. Shows how long the shutdown has been running
3. Configuration groups turn green if something was done with all servers that were not ignored. If the configuration group is yellow/orange, something was not done with all servers in the group.
4. The red line indicates the current time.
5. Servers turn green when the result is successful.

NOTE: Servers turn yellow/orange if the result is unknown. Servers turn red if the result is not successful.

6.4 Startup Configuration

6.4.1 Management Ports

Physical machines can be rebooted via management ports. The PowerApp connects via SSH to the IP of the management port using the entered login credentials (see chapter Credentials or Credentials (Startup Configuration)) and executes the reboot command (e.g. start /system1). The configuration group assignment defines the reboot process (see chapter Configuration Groups (Startup Configuration)) and a random order can be defines within a configuration group. The physical server, which is rebooted via the management port, should be assigned here for better overview. The status

of the management port and the server is displayed. Filter for different criteria and export or import the entries in CSV format. Adjust the listview using „Edit columns“.

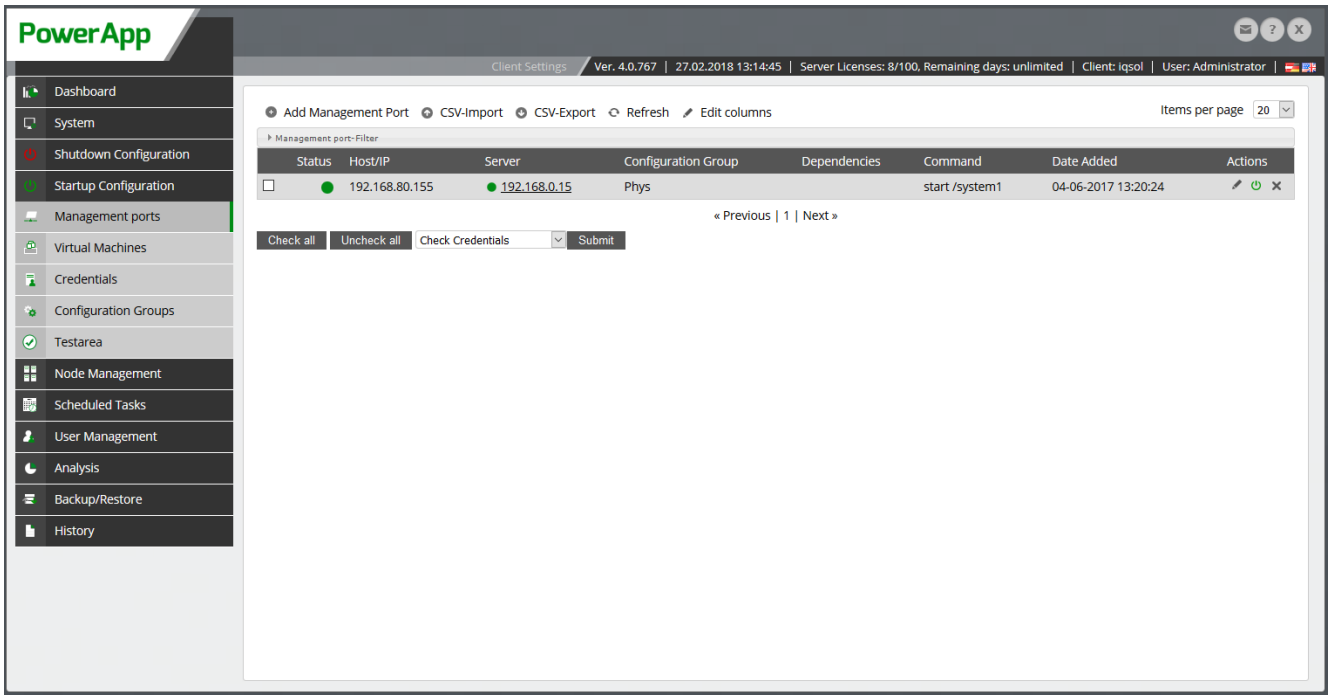


Figure 97: Management Ports

Following Management Ports are supported:

Management Port Type	Startup Command
Standalone	
HP (iLO)	start
Dell (DRAC)	start
IBM (IMM)	power on
Oracle (ILOM)	start /SYS
Oracle (ALOM)	poweron
Oracle (ELOM)	set /SP/SYS/CtrlInfo PowerCtrl=on
Unspecific (IPMI)	power on
Bladeserver	
HP Bladeserver	poweron server <ServerID>
IBM Bladeserver	power -on <ServerID>
Dell Bladeserver	racadm serveraction powerup

Table 5: Supported Management Ports

6.4.2 Virtual Machines

All machines declared as VM are listed in this menu. Define for every VM, if it should be started or not (status activated or deactivated), when start should take place, configuration group assignment (see chapter Configuration Groups (Startup Configuration)) and VM dependencies.

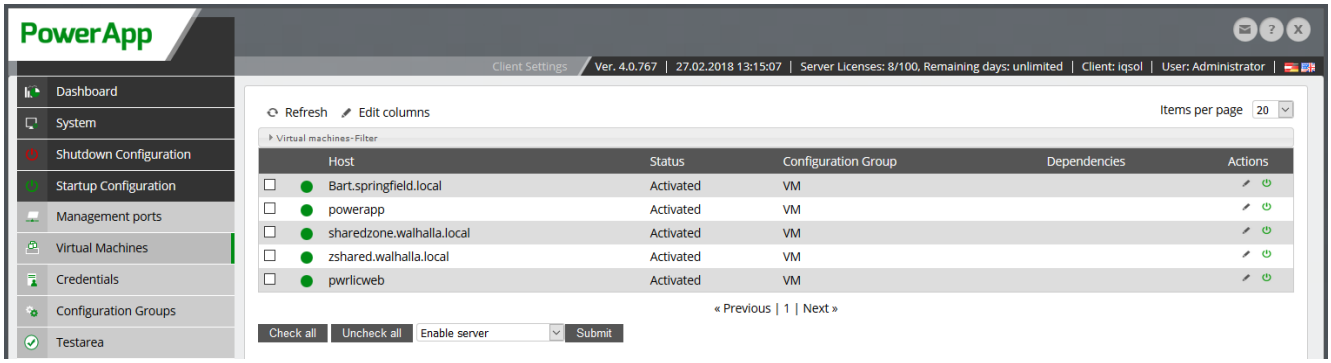


Figure 98: Virtual Machines

6.4.3 Configuration Groups (Startup Configuration)

Use „Configuration Groups“ to define the time sequence for the Startup. VMs are not able to start before the physical host is started.

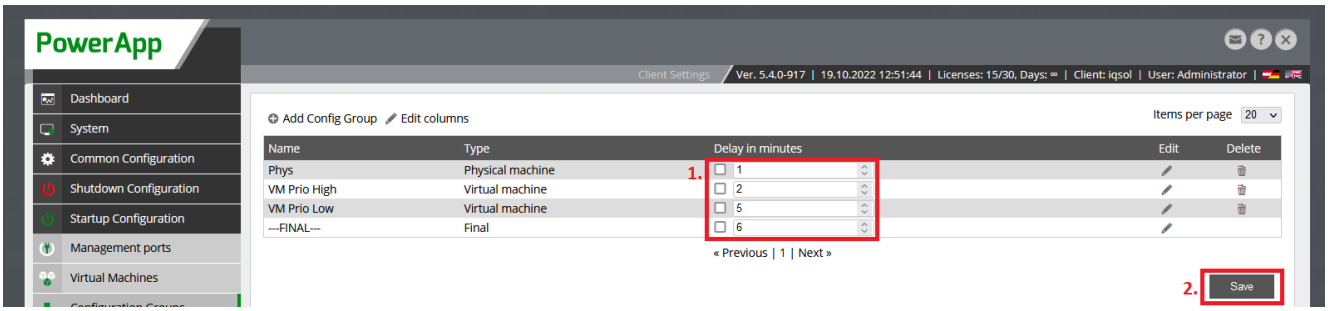


Figure 99: Configuration Groups

1. Here it is possible to set the delay without opening the configuration group editing window. With a check mark in the small boxes you can count up or balance the delay for several configuration groups at the same time.
2. In order to apply these changes, it is necessary to click on "Save".

6.4.4 Startup Criteria

Criteria keep track of individual values of an SNMP device and record whether and since when a condition matches.

In the Add Criteria window, click MIB Browser to select the OID. For example, seconds on battery. Enter 0 seconds in the Value field and set the operator to "=" to match when the value is 0.

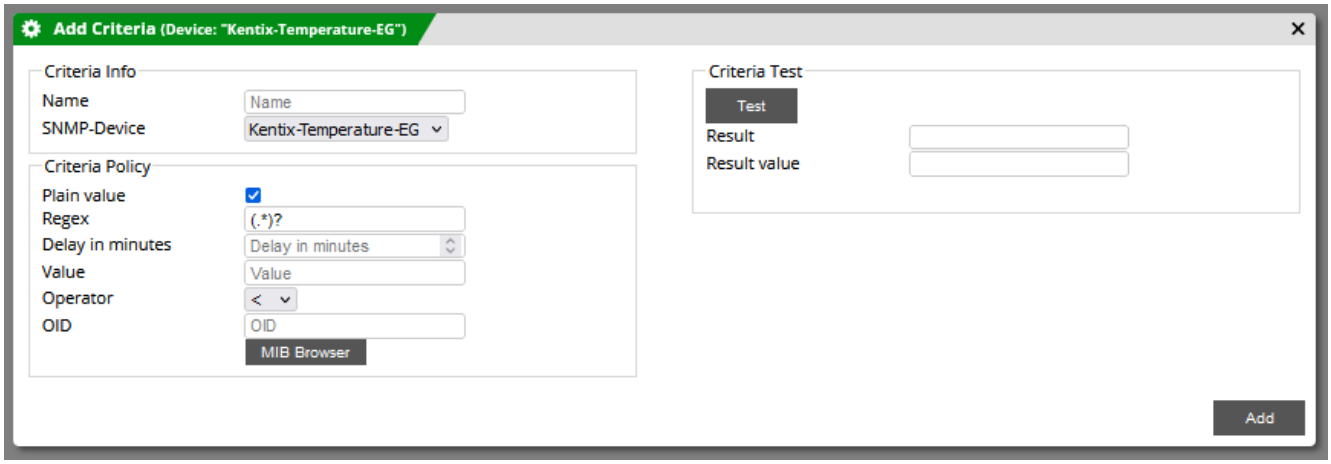


Abbildung 100: Startup Criteria

6.4.5 Startup Trigger

Logic Triggers are used to define the conditions under which a startup should be initiated.

To achieve this, SNMP devices and criteria (organized into groups) are assigned to the trigger. For the trigger to activate, all assigned criteria in at least one group must match.

You can create new criteria groups (organized in tabs) and drag criteria into each group.

To remove a criterion, simply drag it back to the available criteria pool.

For the trigger to activate, all assigned criteria in at least one group must match.

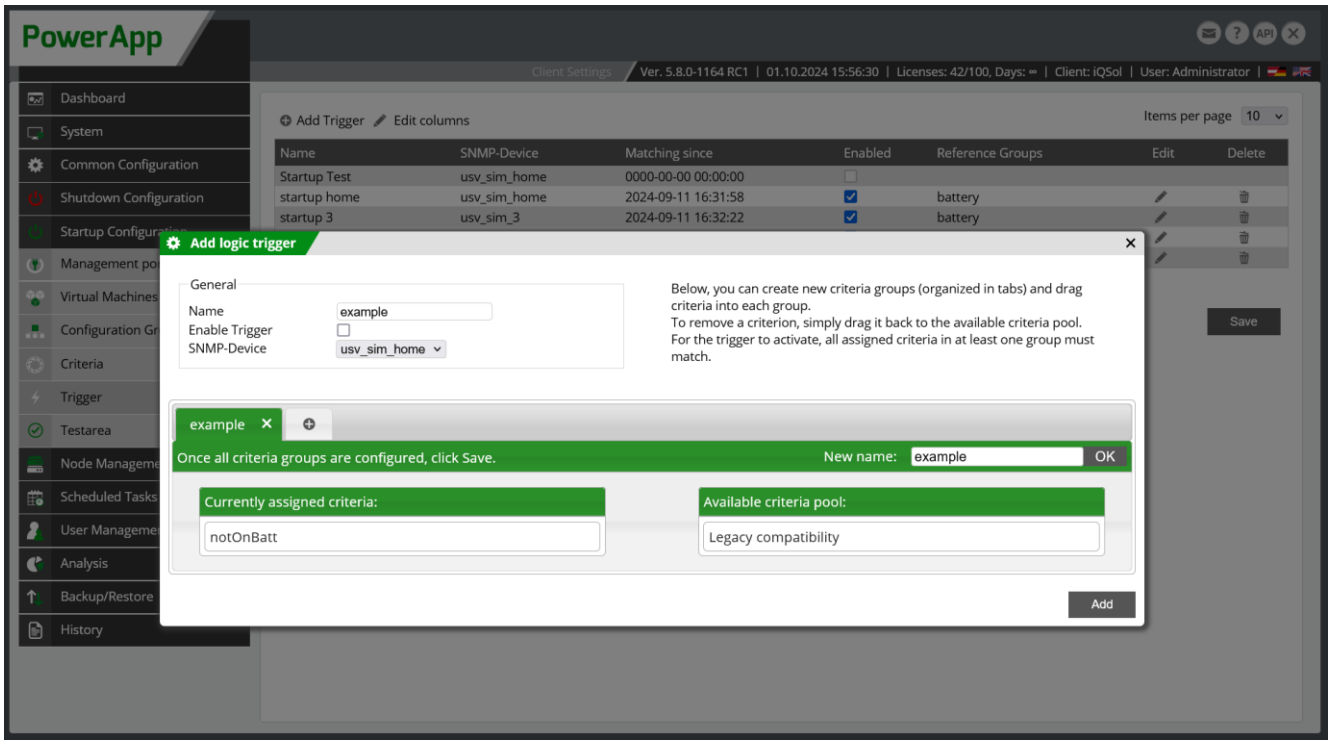


Figure 101: Startup Trigger

6.4.6 Test Area (Startup Configuration)

As with a shutdown, the startup is also performed according to a time sequence that depends on the configuration groups and the dependencies. The visualization of the startup is structured the same as for a shutdown. Explanations to the visualization are to be found here: Test Area (Shutdown Configuration)

6.5 Node Management

6.5.1 Locations

Here you can edit the name, description and position of the headquarter (Superadmin) and create further locations for your branche offices.

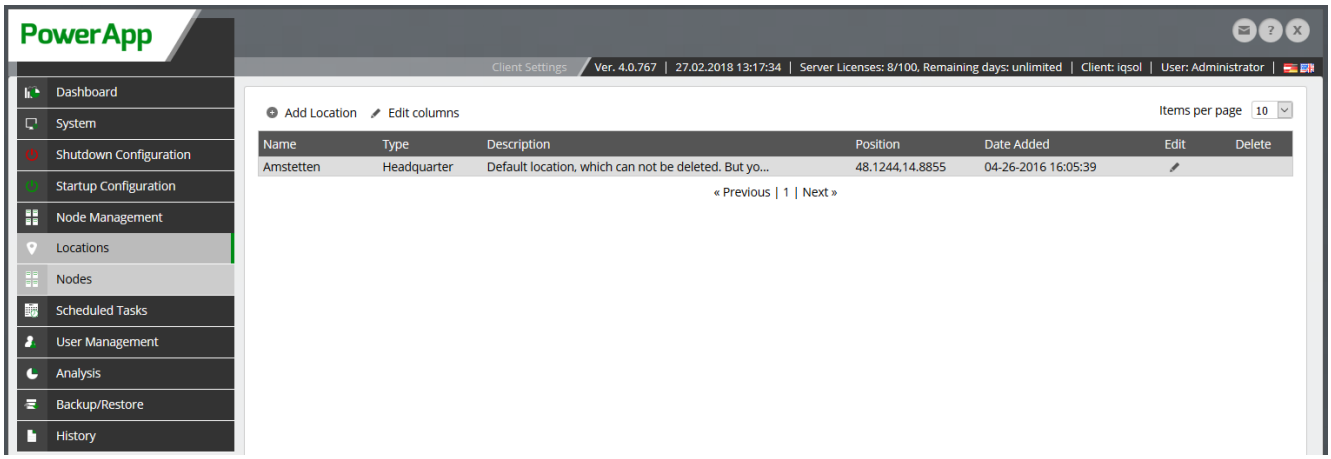


Figure 102: Locations

6.5.2 Nodes

Use this menu to add PowerNodes to your branch offices if your license enables it.

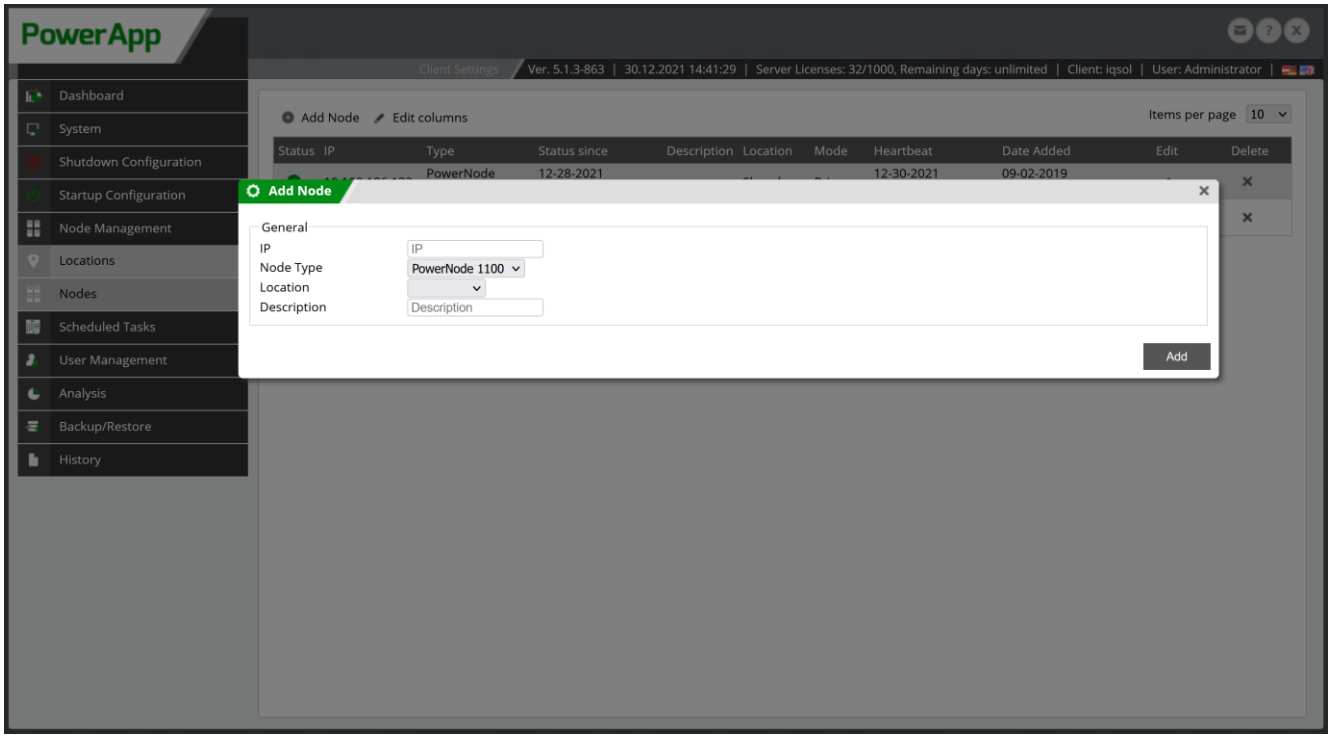


Figure 103: Nodes

Do not forget to copy the access keys from both PowerApps (if available) to all PowerNodes.

6.6 Scheduled Tasks

6.6.1 File Import/Export

Use „File Import/Export“ to periodically import/export servers from/to a CSV file.

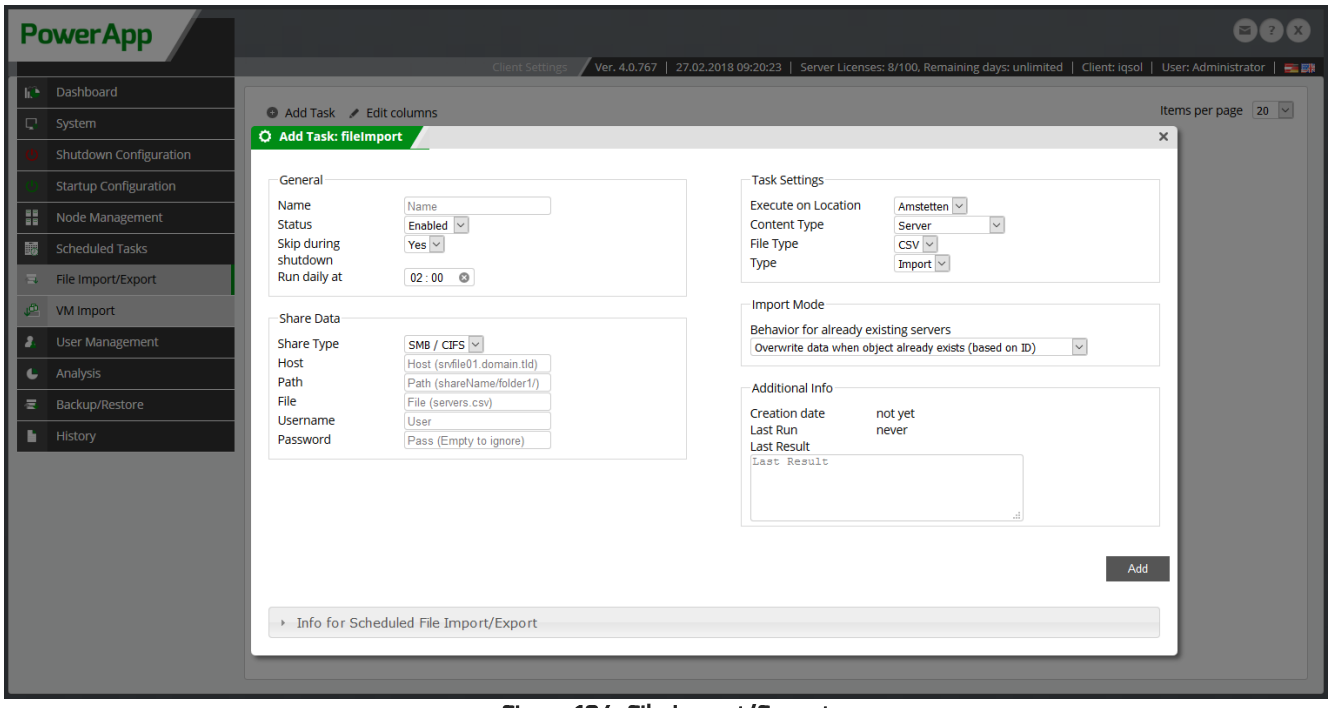


Figure 104: File Import/Export

6.6.2 VM Import

Use „VM Import“ to periodically import/export VMs from Hosts.

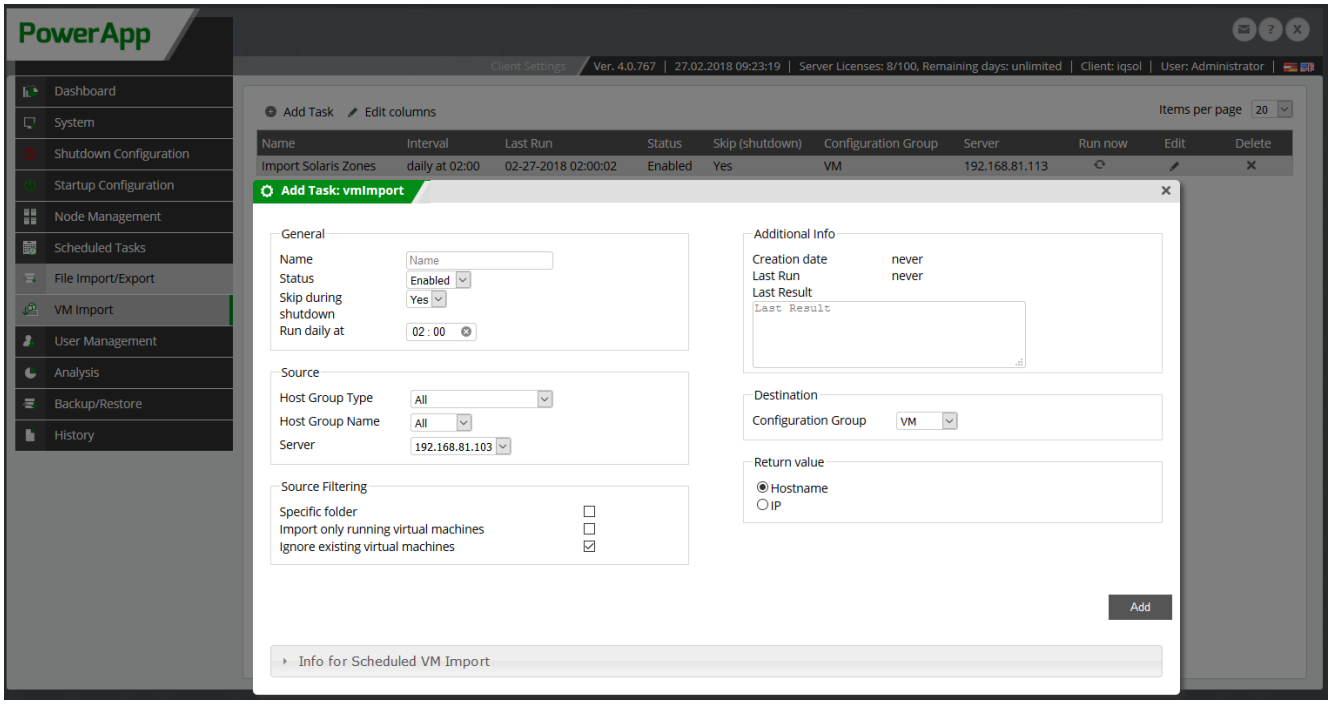


Figure 105: VM Import

6.7 User Management

The PowerApp user configuration is accessible via the menu item "User Management". The permission structure is divided into users and groups.

A user object defines a user account that is allowed to log on to the PowerApp. Groups define the access rights.

After installation, only the user "Admin" is available, which is a member of the group "Admin". The "Admin" group has all available permissions by default.

6.7.1 MyUser

The MyUser page allows you to edit settings specific to your user account. This provides a centralized location for managing your personal preferences and account details.

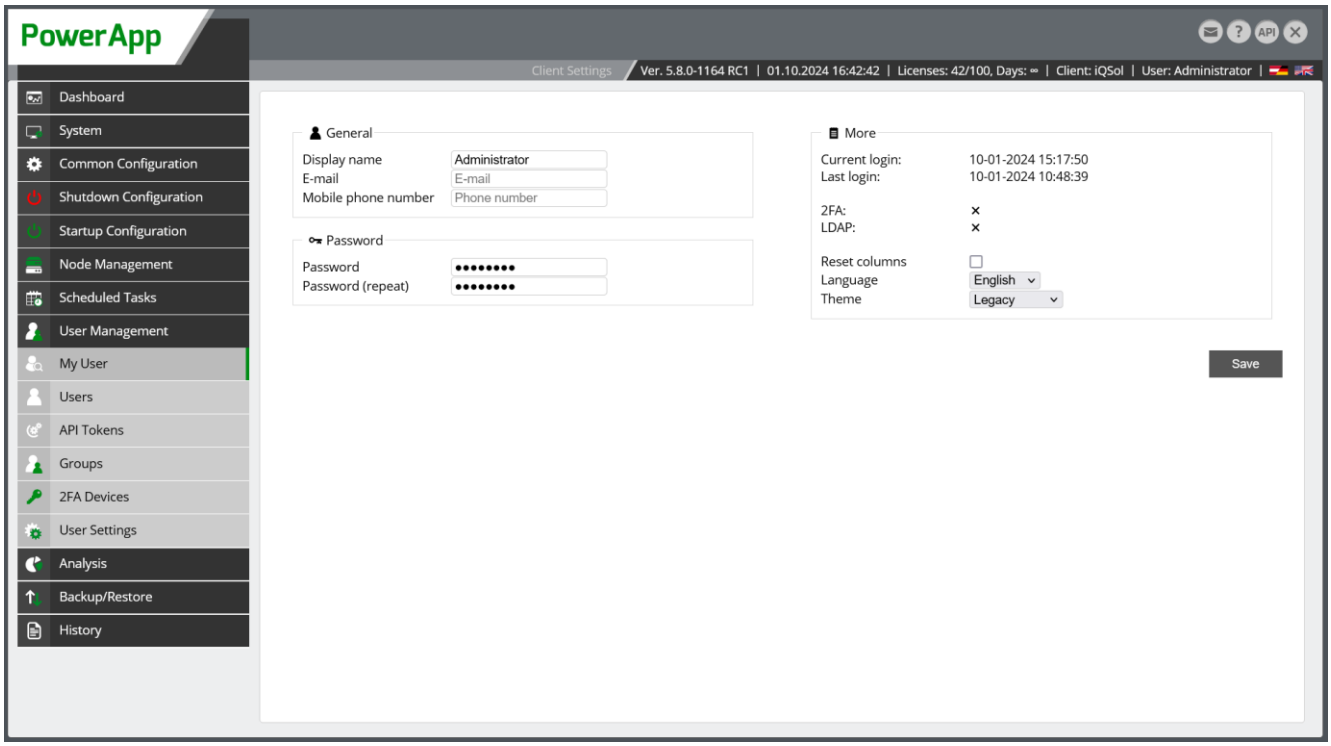


Figure 106: MyUser

6.7.2 User

Use the „user“ menu to view or edit existing or create new users..

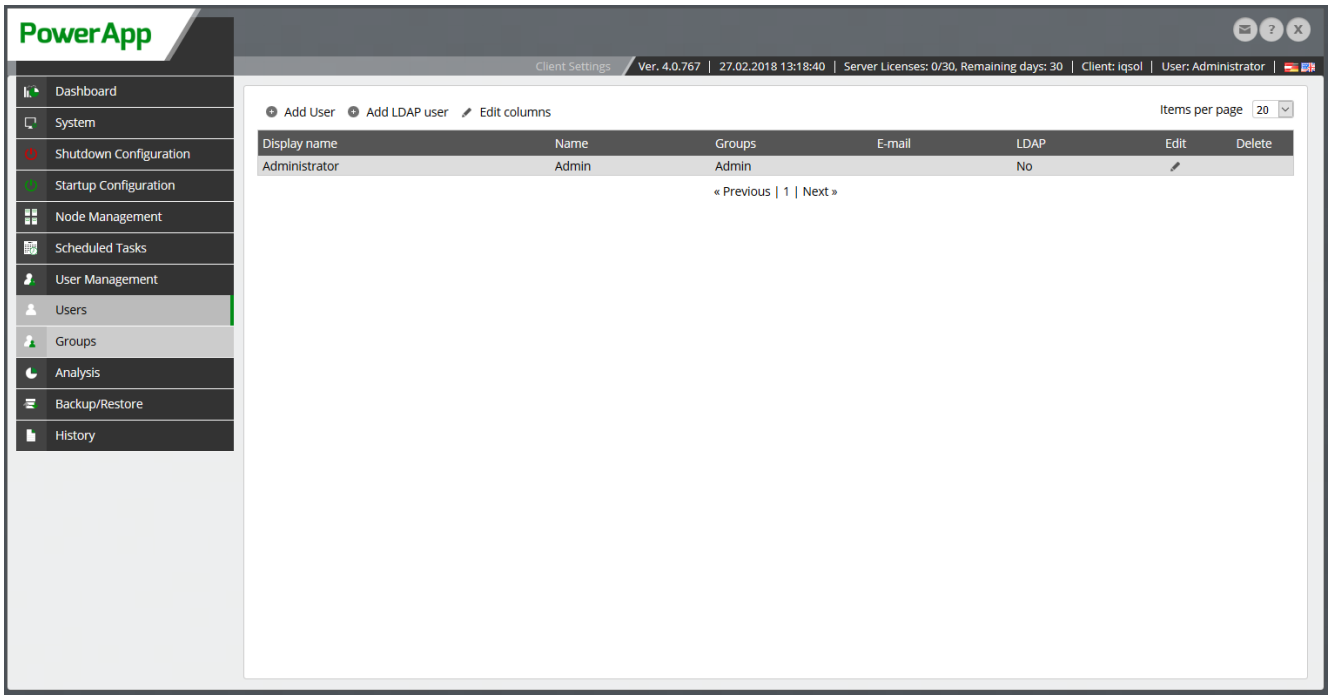


Figure 107: User Management

Existing users can be edited or delted in the list view.

The automatically generated Admin user cannot be deactivated or deleted. It is recommended to change the default password immediately after the first logon.

New local users can be added with the „Add“ button. Display name, name, email address and password must be entered.

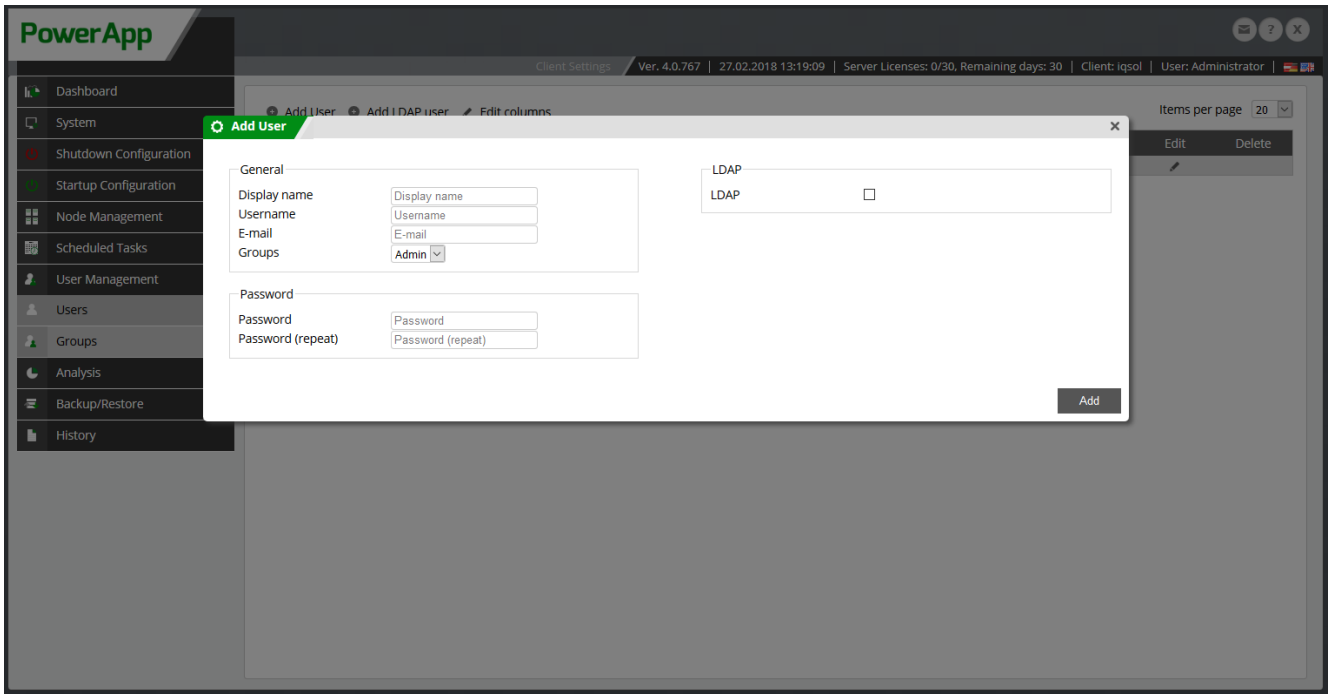


Figure 108: Add User

Use the „Add LDAP user“ button to import users from an existing LDAP server (see chapter 6.1.8). Choose the user for PowerApp login, from the LDAP tree.

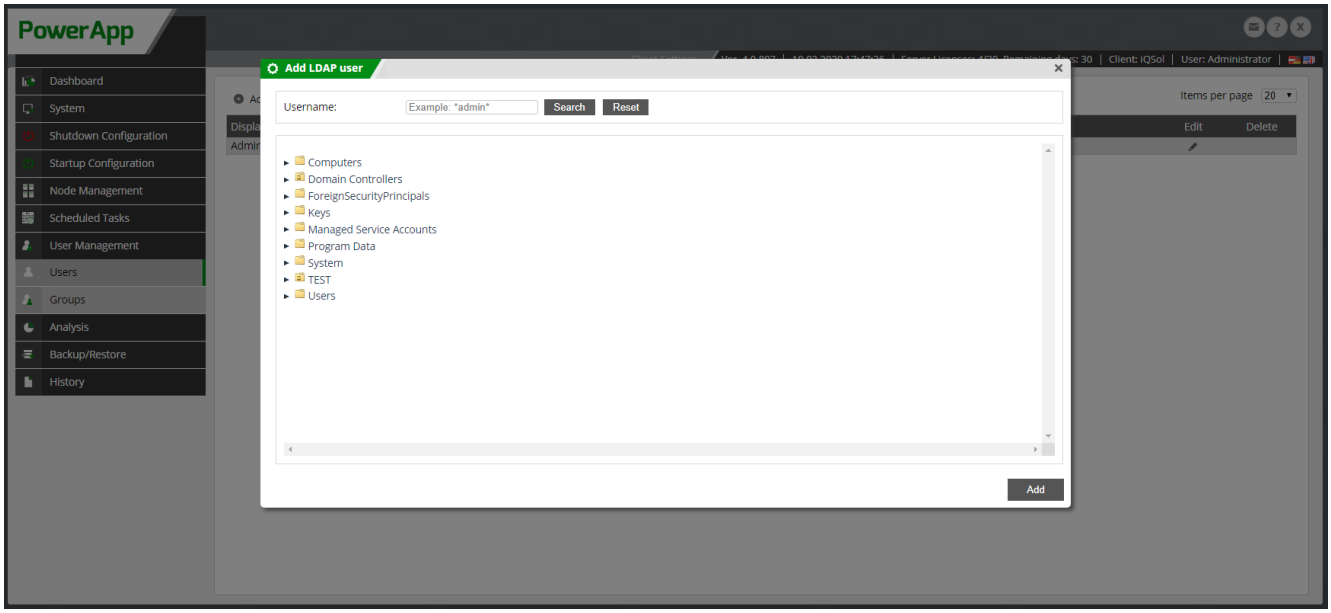


Figure 109: Add LDAP User

6.7.3 API Tokens

Use the menu "API Tokens" to create, view and delete API tokens.

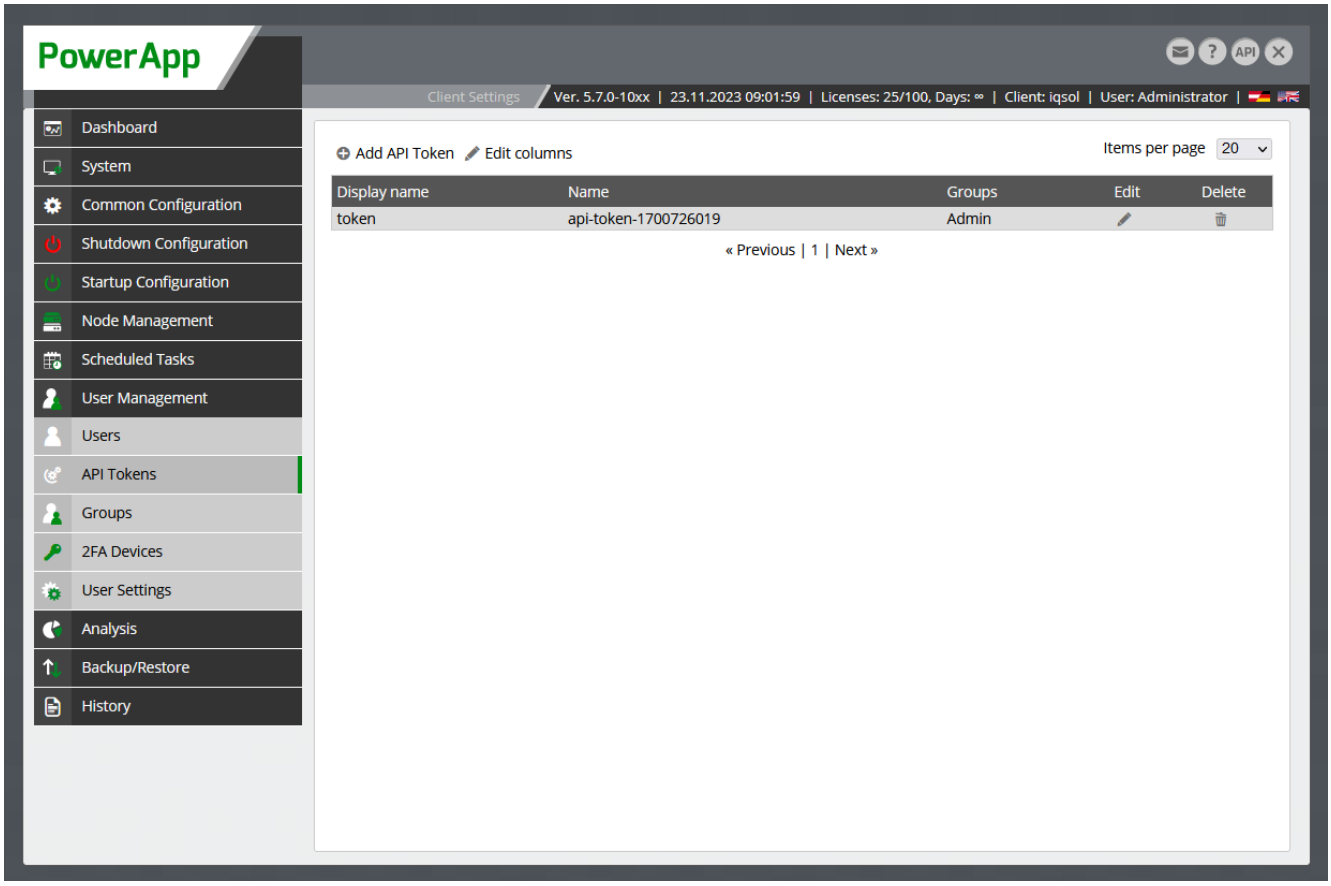


Figure 110: API Tokens

If you click on "Add API Token" following window opens. Here you can input the display name of the API token and to which group the API token will be assigned.

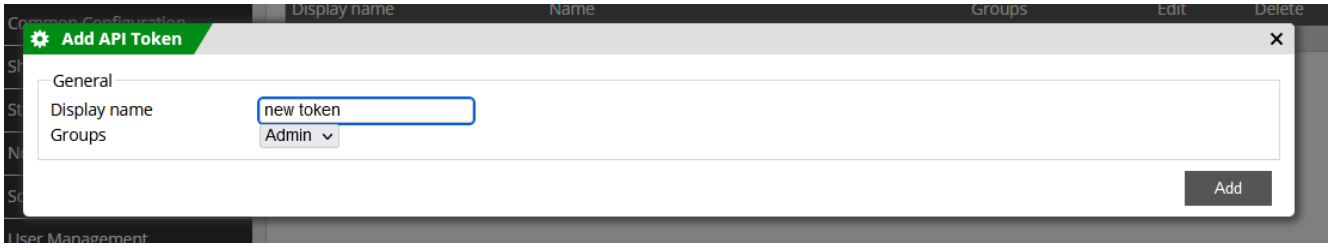


Figure 111: Add API Token

After you click on "Add" another window will appear that will prompt the API token. The API token is needed to make API calls. For more information about the API look here.

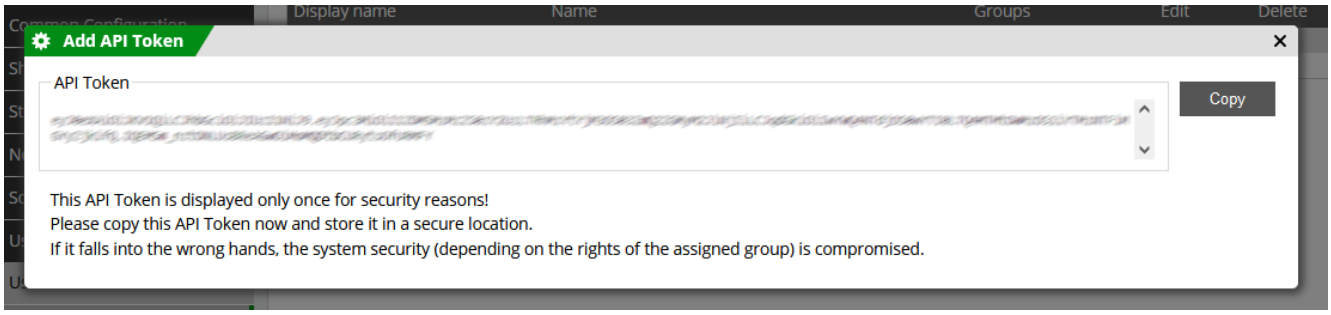


Figure 112: API Token prompted

6.7.4 Groups

Use the menu „Group“ to view and edit existing groups and add new groups. All PowerApp users, in the central and client console, must be member of a group, to receive any right. Group memberships are the basis of alerting the the client console.

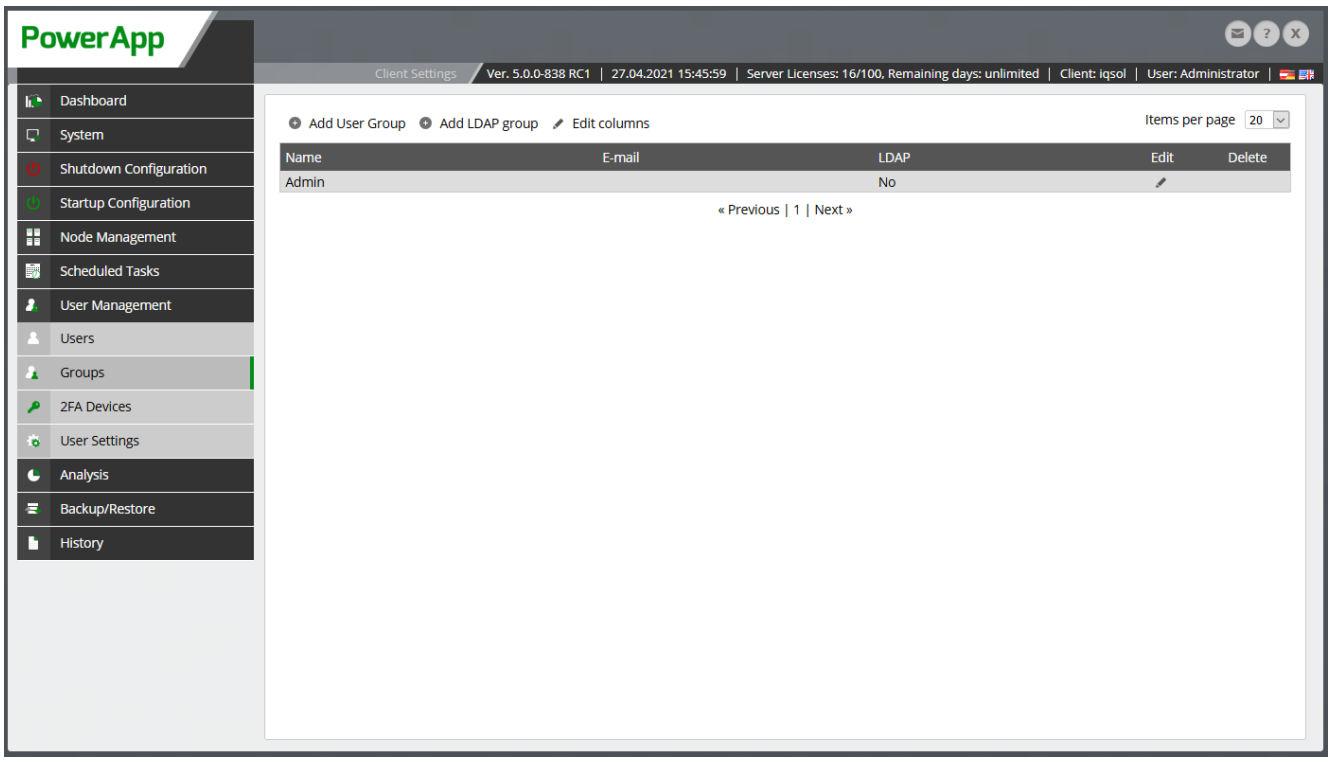


Figure 113: Group Management

Use „Add usergroup“ button to add new local groups. Existing roups can be edited in the listview.

Change groupname and email address using „edit“. Remove groups with the „remove“ button. The „Admin“ group is automatically generated while creating a new client, and cannot be deleted.

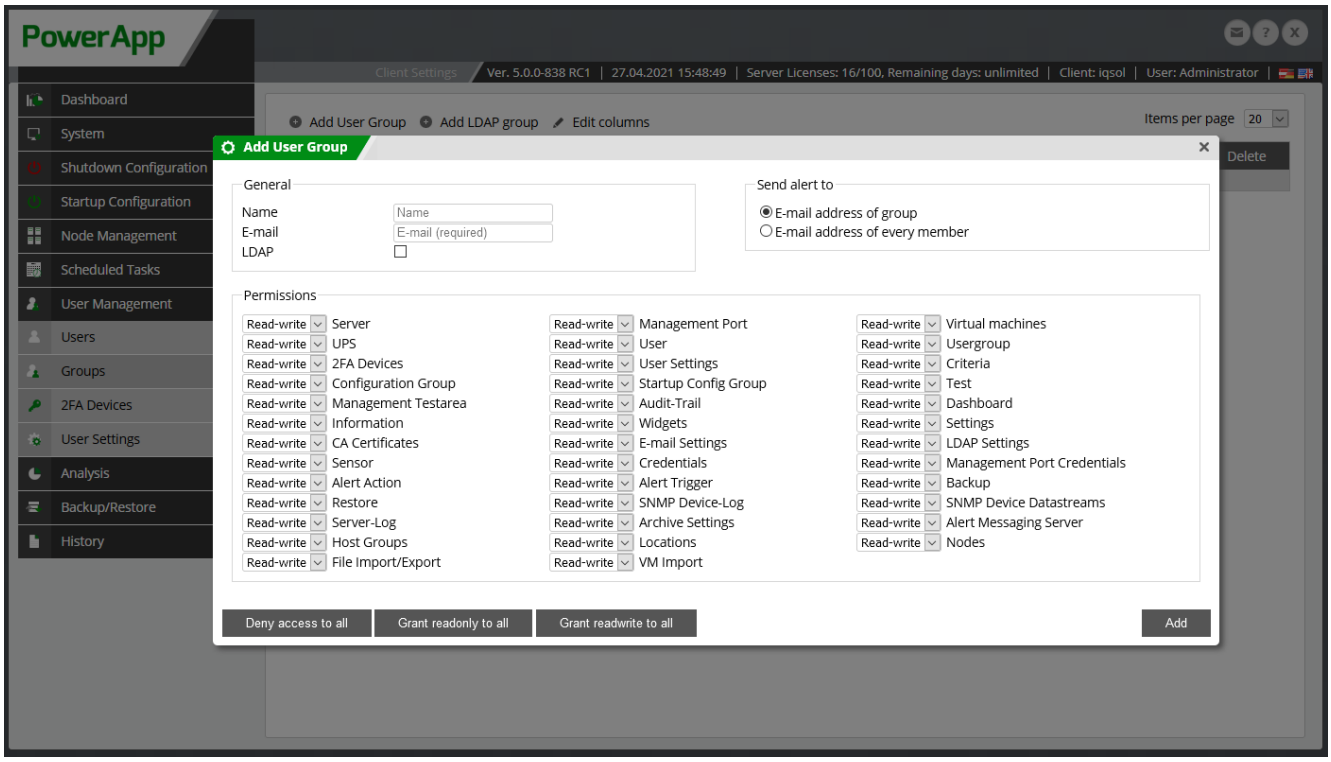


Figure 114: Add Group

Use „Add LDAP group“ to import groups from an entered LDAP server (see chapter LDAP Settings). Choose the group from the LDAP tree, which users are able to logon to the PowerApp.

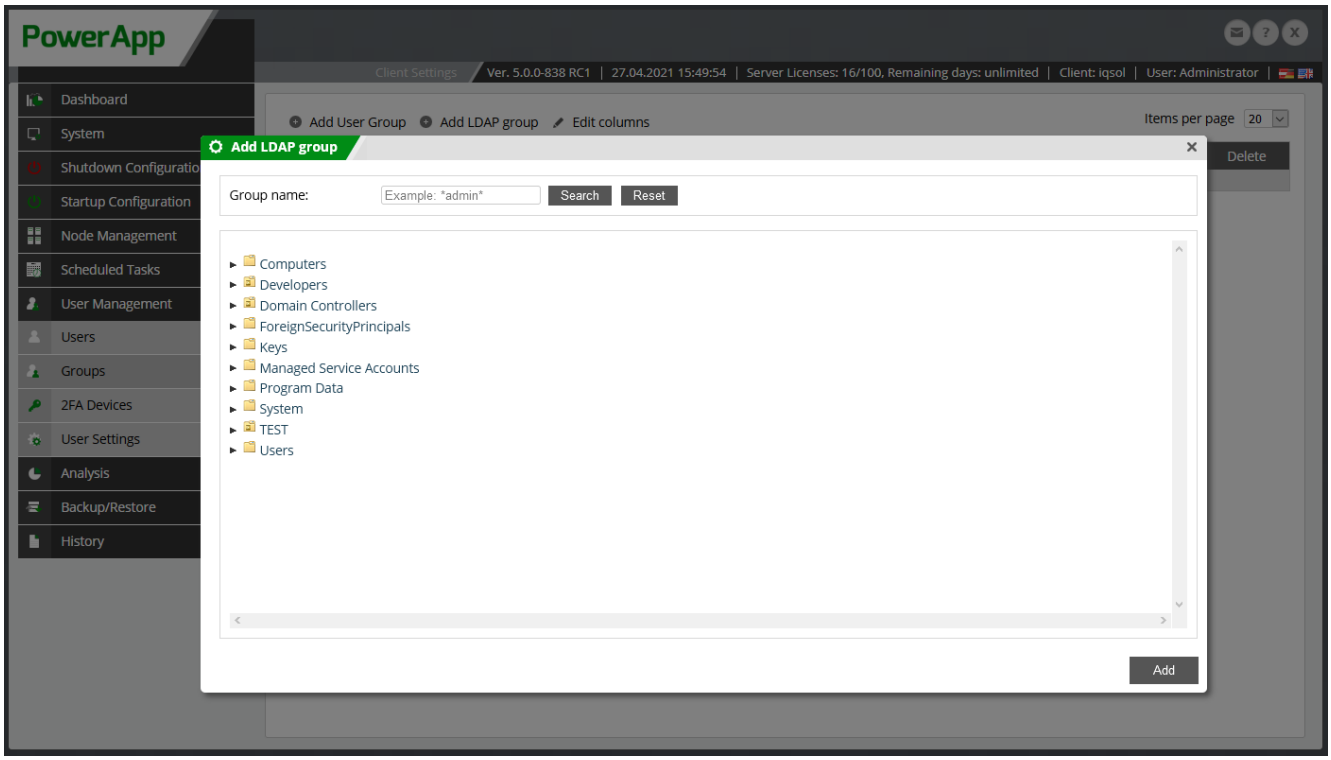


Figure 115: Add LDAP Group

6.7.5 Two-factor-authentication

Two-factor-authentication can be created under the menu item “User Settings”. Either through the AMS or a YubiKey.

For the users "Superadmin" and "Admin", the two-factor authentication cannot be activated in order to prevent accidental locking out of the system.

After activating 2FA, it is recommended not to use the default users any more and to secure them with a very long password that is kept in a safe place.

Deactivation of the 2FA mode is only possible via these users.

All other settings should only be made via newly created users (for which 2FA is active) where the rights have been assigned accordingly via the groups.

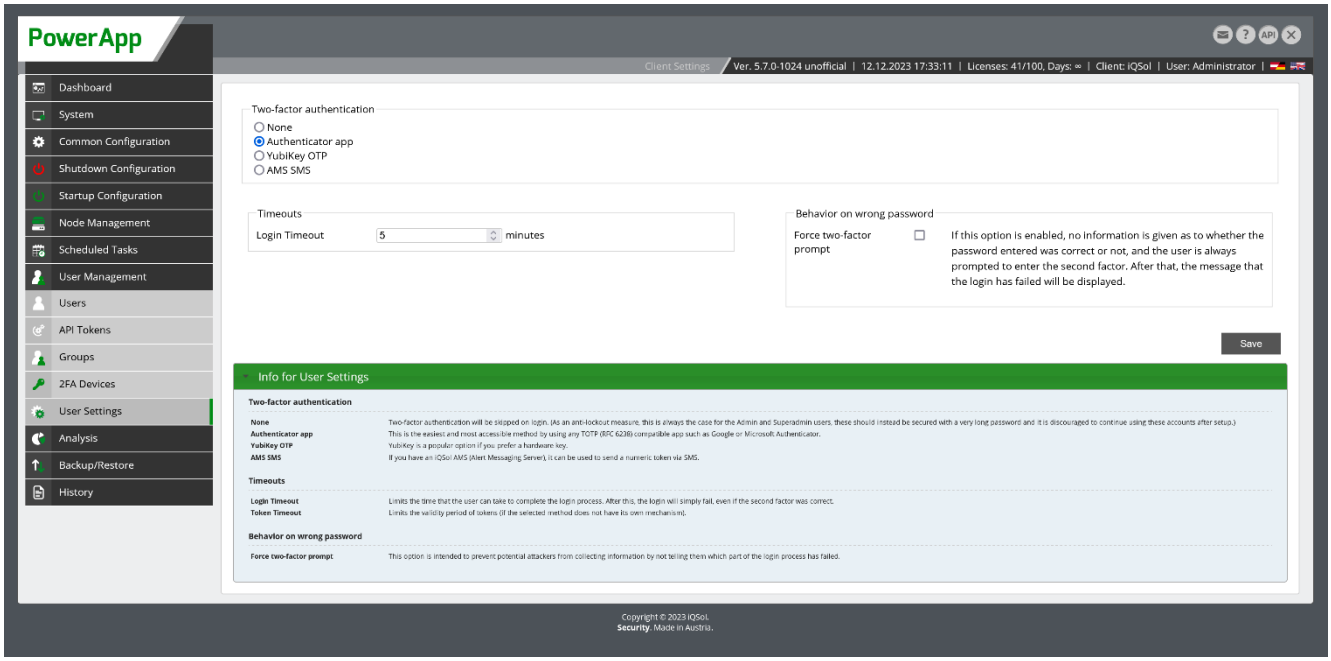


Figure 116: Two-factor-authentication

Authenticator app TOTP RFC 6238

Enables the use of Authenticator apps such as Microsoft or Google Authenticator for two factor authentication. When logging in for the first time, the user receives a QR code, which needs to be scanned via the Authenticator app.

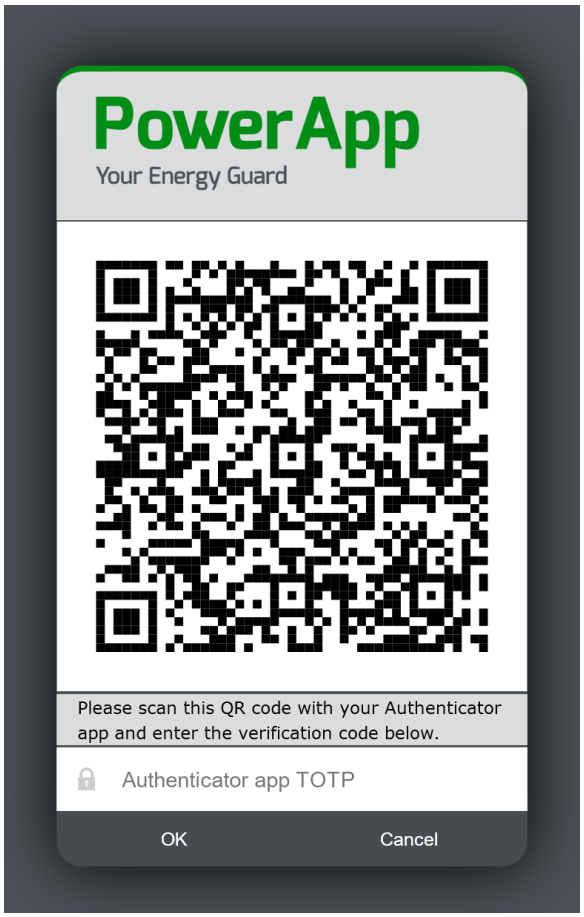


Figure 117: QR – Code to scan

For verification the code from the app must be entered to proceed. All subsequent logins require the code from the Authenticator app.

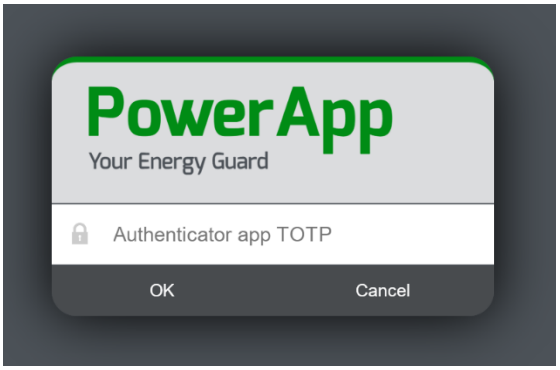


Figure 118: Subsequent logins

AMS SMS

The configuration for the AMS server can be carried out as described under Alert Messaging Server.

To log in, the user then receives an SMS in the following format:

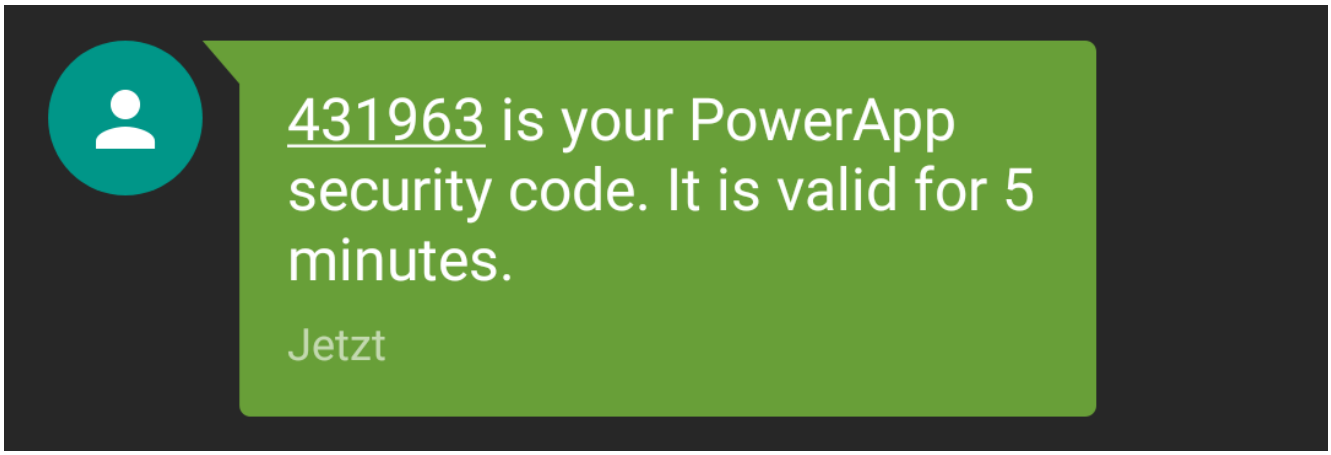


Figure 119: SMS Security code

YubiKey authentication

A YubiKey can be added under the menu item "2FA devices". The serial number, public name, internal name and AES key must be specified (without spaces).

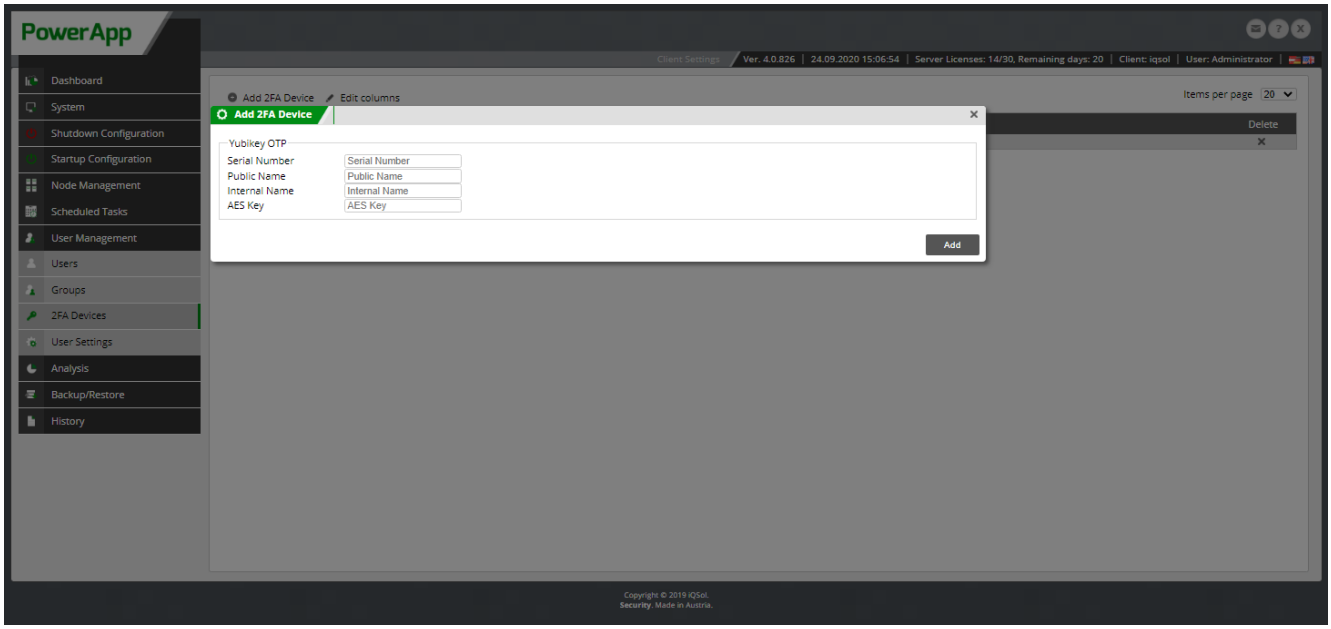


Figure 120: Add YubiKey

The download link for the YubiKey Manager:

https://www.yubico.com/support/download/yubikey-manager/

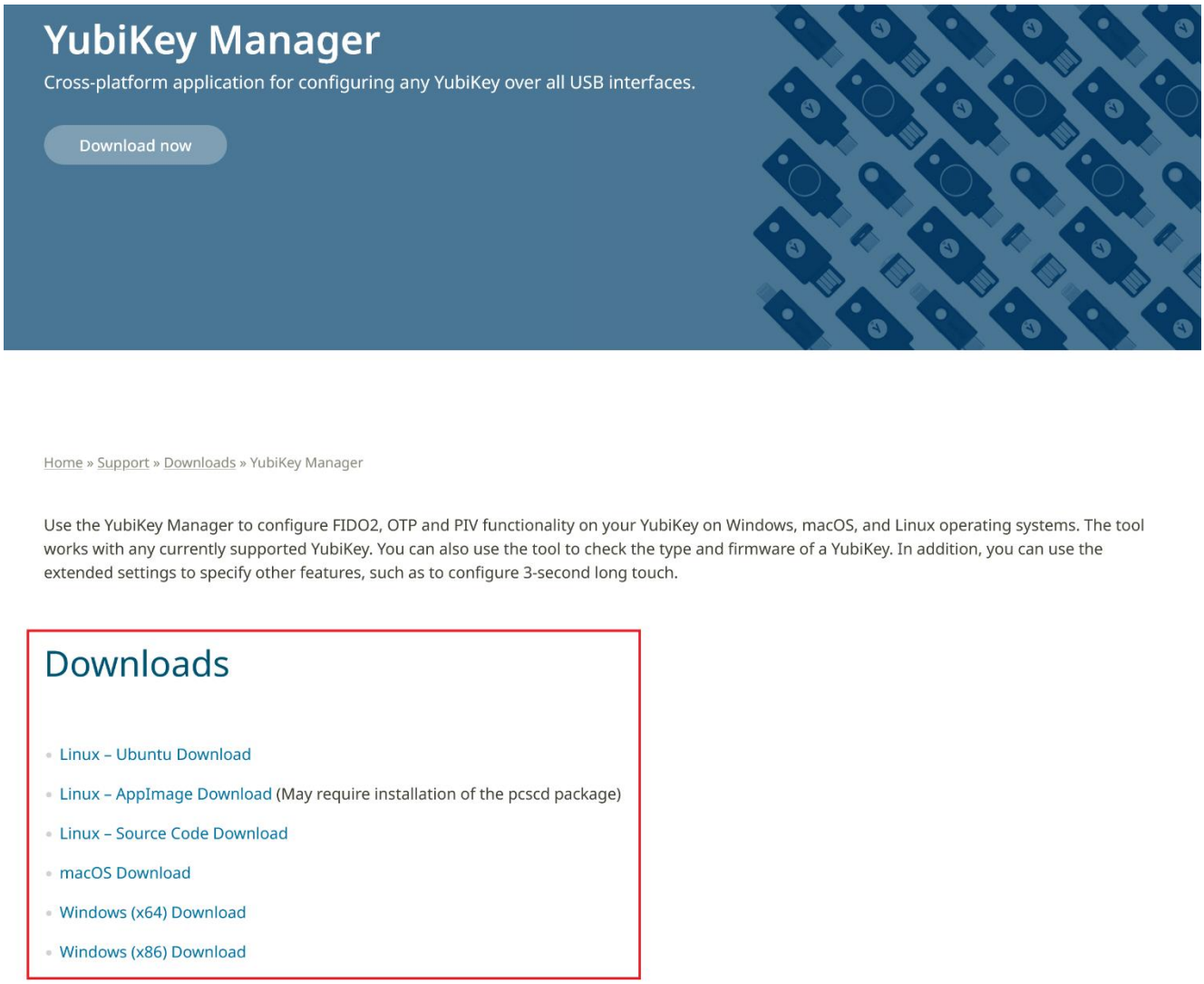


Figure 121: Download YubiKey Manager

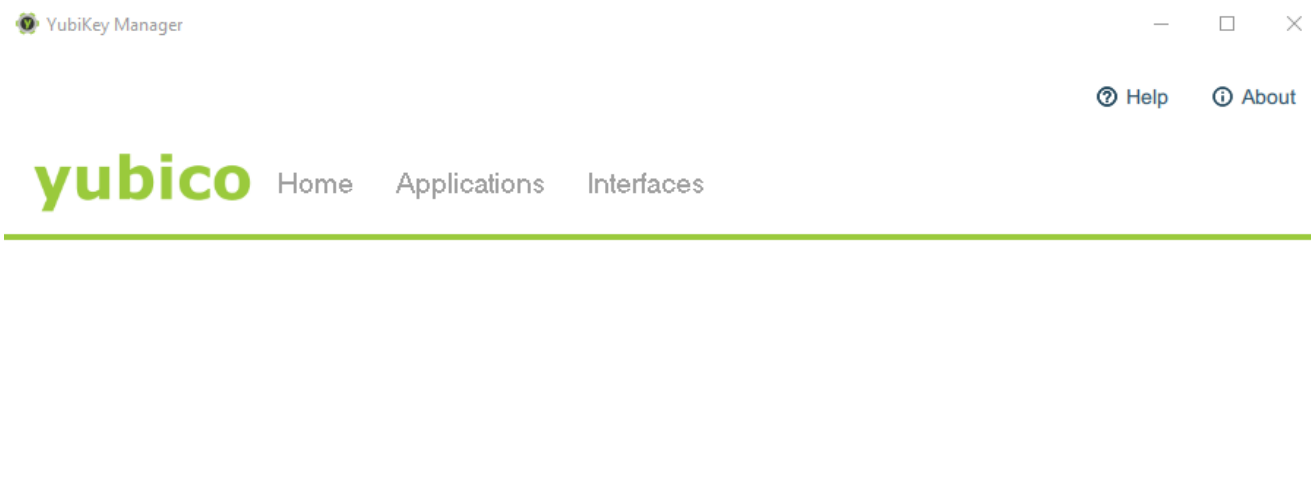


Figure 122: YubiKey Manager

The YubiKey must now be inserted and you navigate to "Applications" → "OTP". Now select a free slot. Then select "Yubico OTP" as the "Credential Type". The serial number is displayed at the top left next to "Help". "Use serial" is selected as the "Public ID". The "Private ID" and the "Secret key" must be generated. These 4 parameters should be inserted one after the other in the PowerApp window "Add 2FA device".

As soon as you click on "Finish", if you have selected a slot that is not free, it will be overwritten and can no longer be restored.

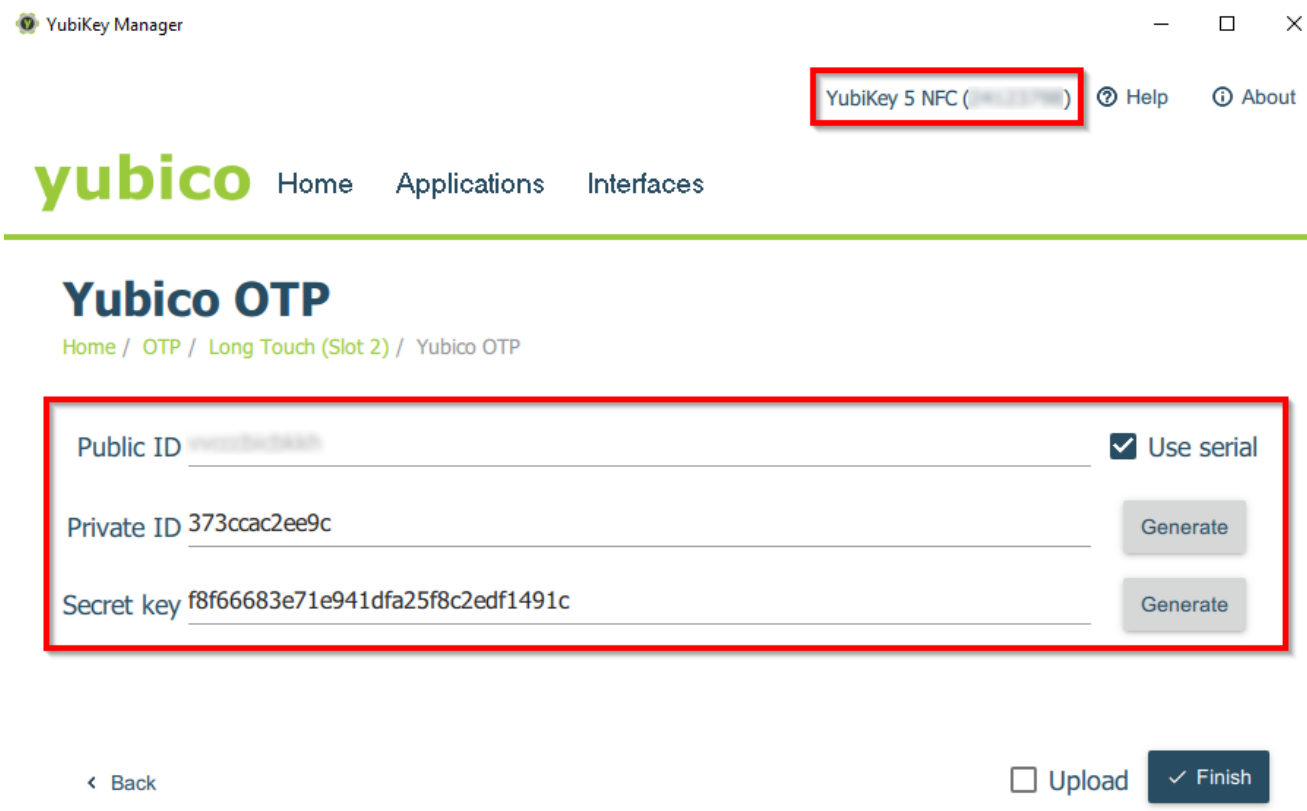


Figure 123: YubiKey parameter

The YubiKey is linked to the user the first time he logs in. It is therefore recommended that a new user should log in immediately after receiving a YubiKey.

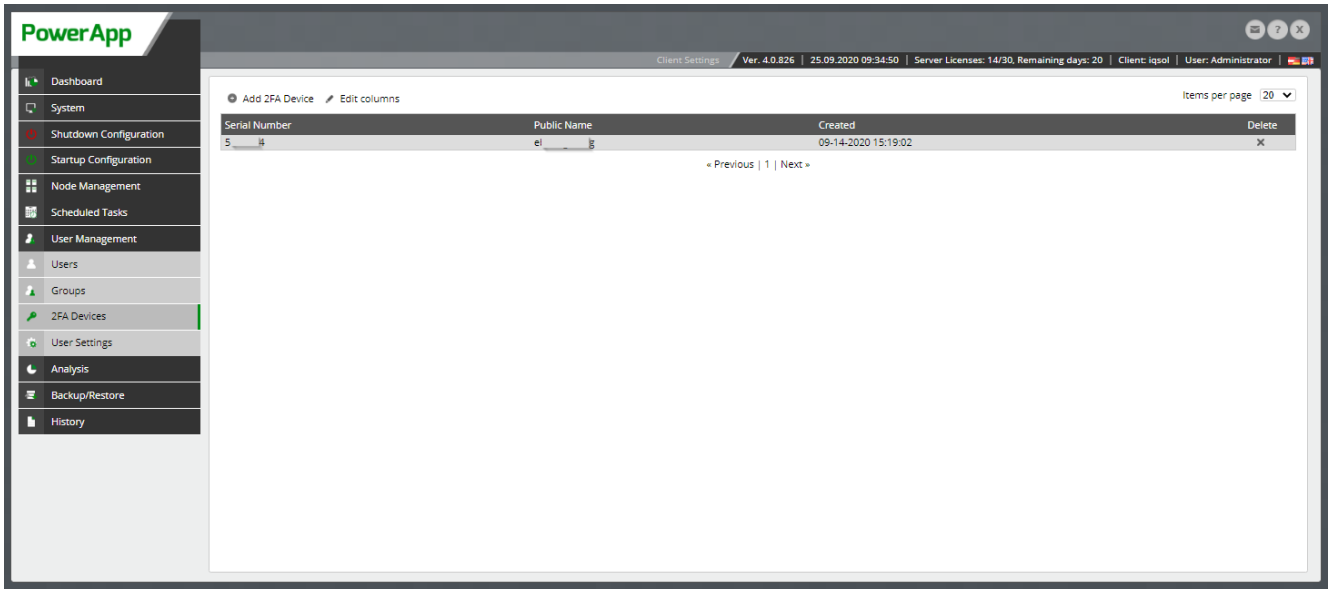


Figure 124: Saved YubiKey

6.8 Analysis

6.8.1 SNMP Device Datastreams

Use the menu „SNMP Device Datastreams“ to add Datastreams for SNMP Devices.

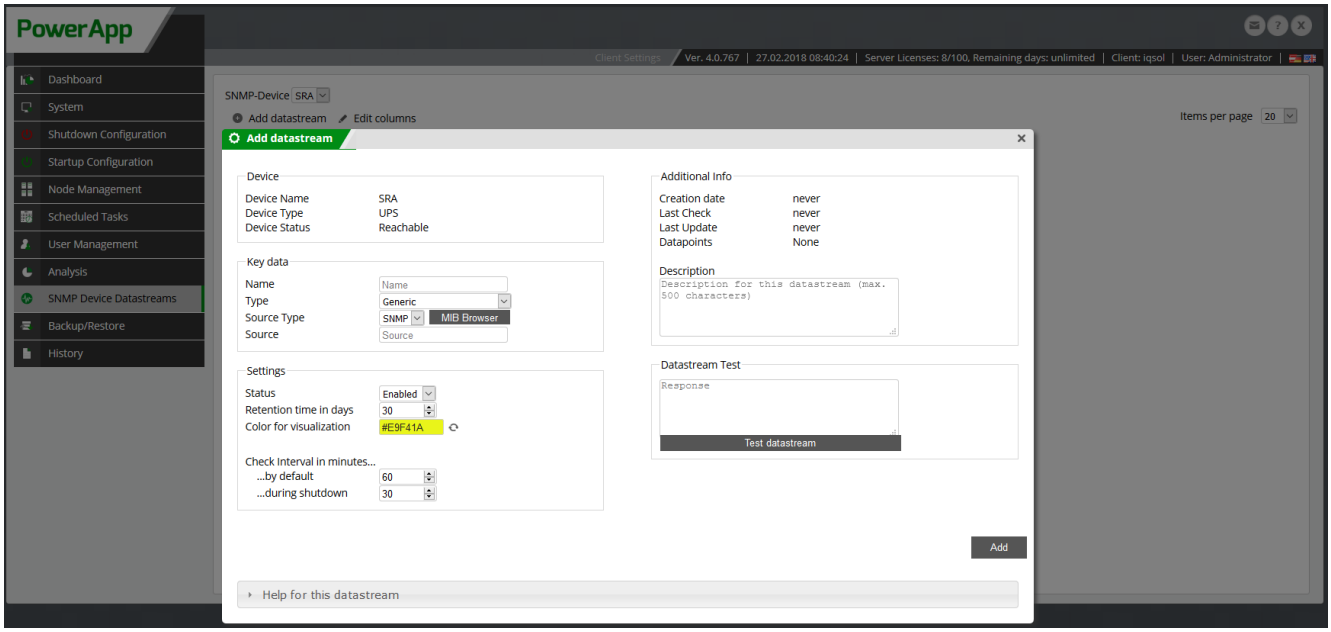


Figure 125: Add a Datastream

Choose a SNMP-Device from the Dropdown Menu and click on „Add datastream“.

6.8.2 Show overview/statistics

You can show the collected data in the menu „Shutdown Configuration“ „UPS“ by clicking on „Open overview“. To get usable data the datastream should run for some time.

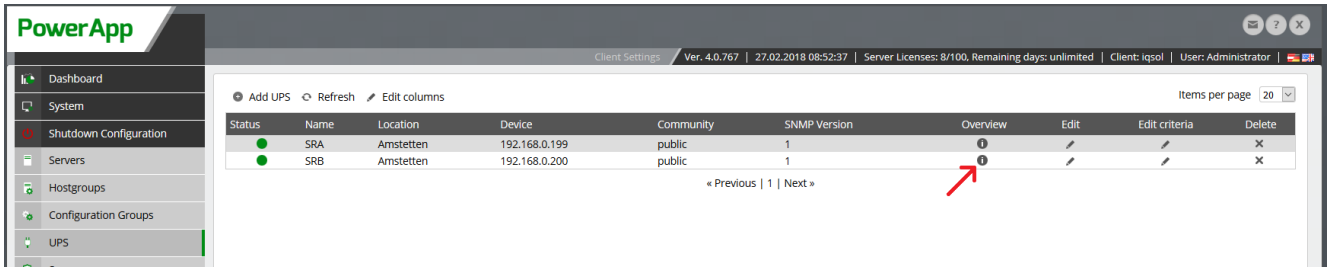


Figure 126: Open overview

Figure 127: overview/statistics from a UPS

6.9 Backup/Restore

6.9.1 Archive Settings

Click „Start backup now“ to create a new backup or to create scheduled backups. The backup files can be saved locally or can be exported to SMB, NFS or SFTP shares. Choose the backup content under „Archive content“.

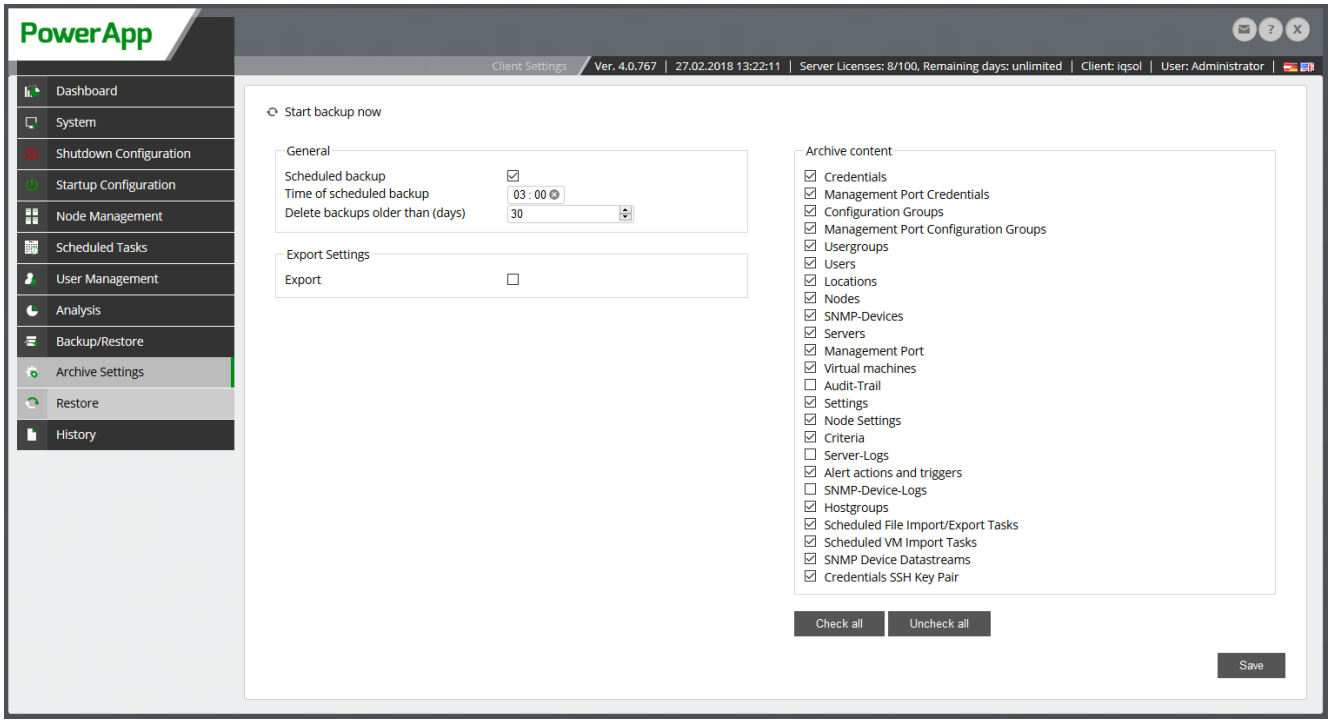


Figure 128: Archive Settings

6.9.2 Restore

Local PowerApp backups as well as backups saved on CIFS shares can be restored, downloaded or deleted.

NOTE: All data is overwritten by restoring a backup! It is possible to restore only individual content and not the whole backup (object level recovery).

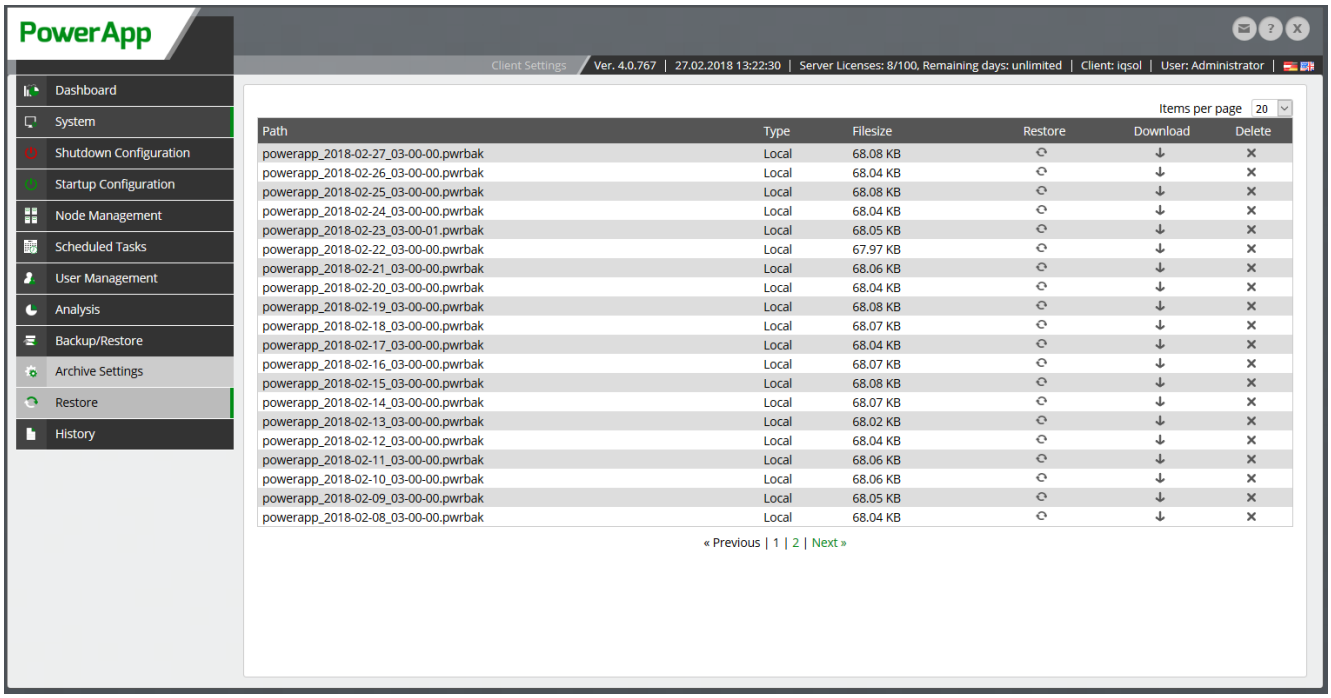


Figure 129: Restore

6.10 History

6.10.1 Audit-Trail

Use the menu „History“ -> „Audit-Trail“ to view all actions of the Superadmin-users. Therefore every change is completely traceable. It is possible to filter for different criteria and export the log into CSV-format.

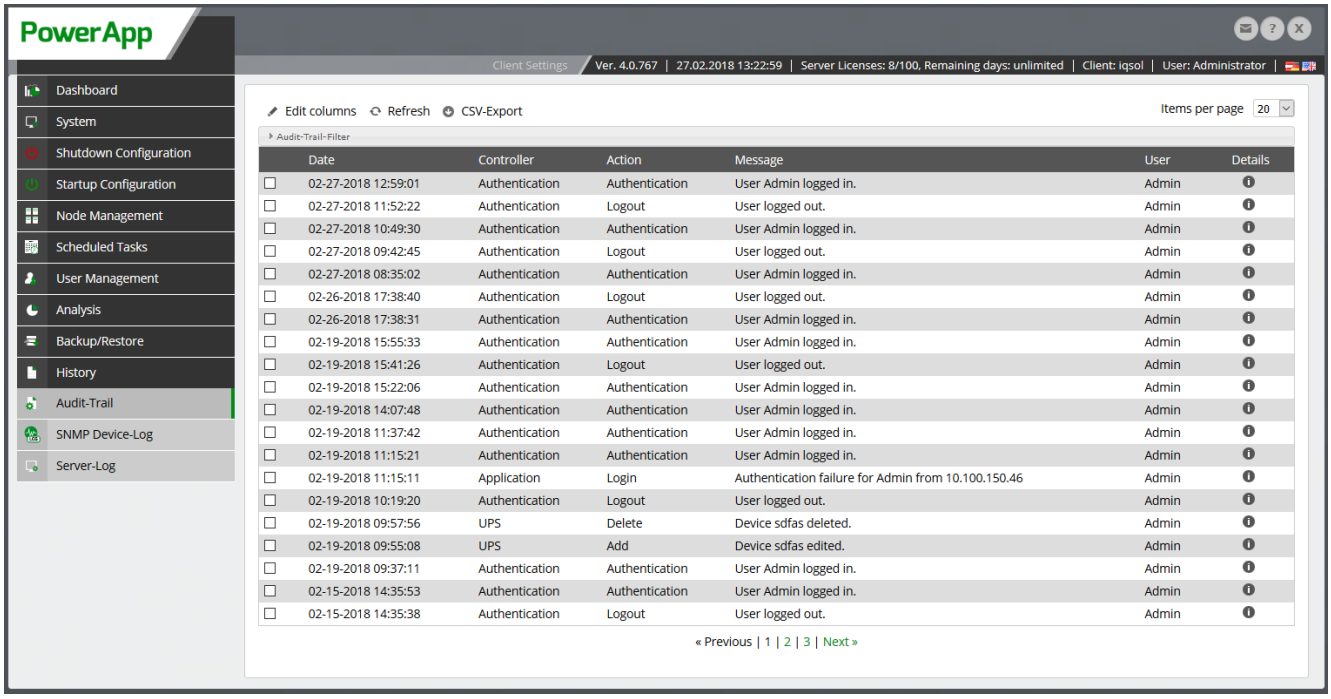


Figure 130: Audit-Trail

6.10.2 SNMP Device-Log

The menu „SNMP Device-Log“ displays the log of all SNMP devices, including status information of all UPS devices and sensors. It is possible to filter for different criteria and export to CSV format.

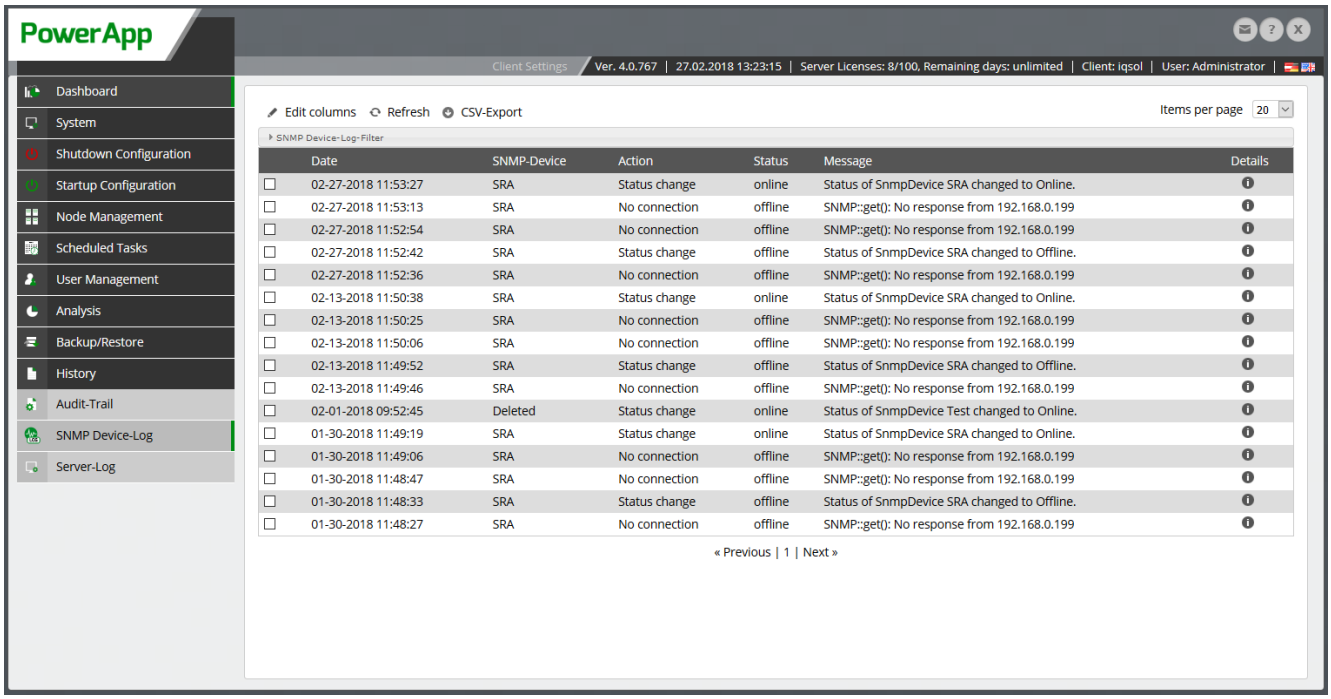


Figure 131: SNMP Device-Log

6.10.3 Server-Log

Use the menu „ Server-Log“ to display all status information about servers. It is possible to filter for different criteria and export logs into CSV format.

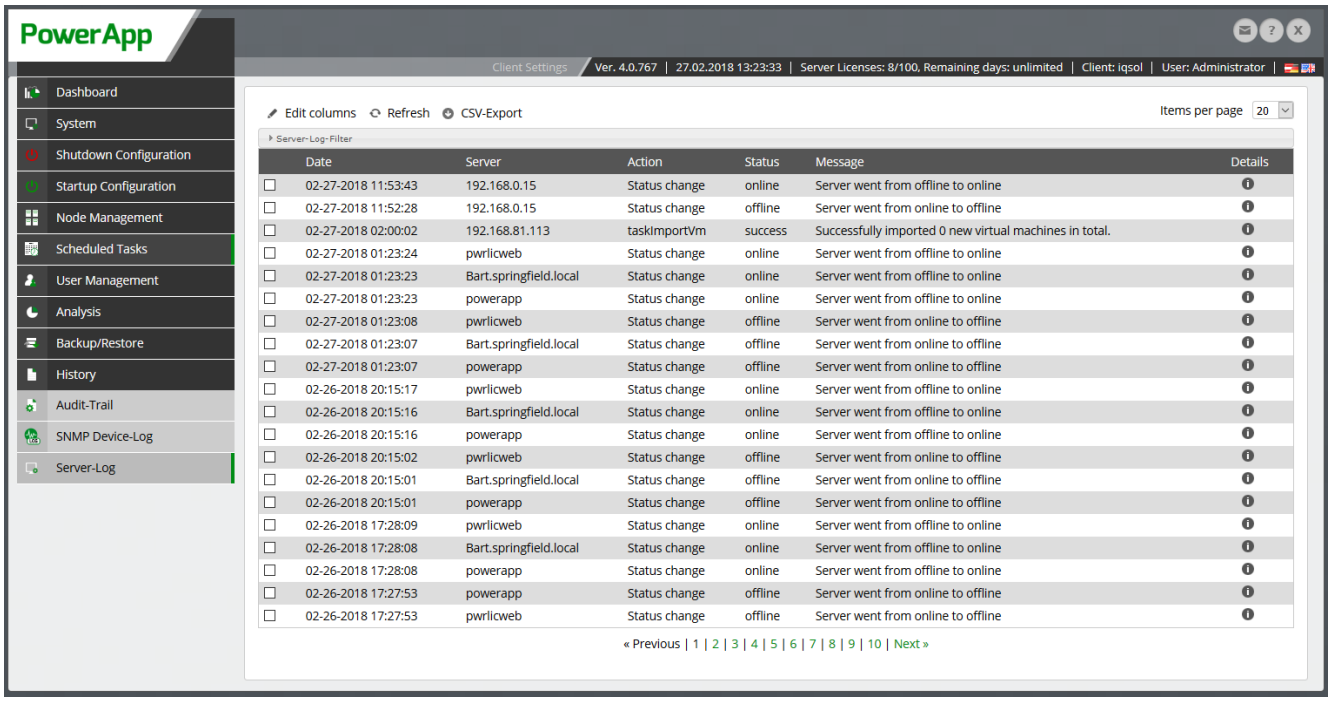


Figure 132: Server-Log

6.10.4 Reports

For each shutdown, all activities are recorded as events, which can be analyzed via the "Reports" menu. After clicking PDF or YAML, a new report will be generated based on the existing event data.

The YAML format represents the internal array of the report to allow external processing. By clicking the PDF button, a readable PDF report based on this array gets created.

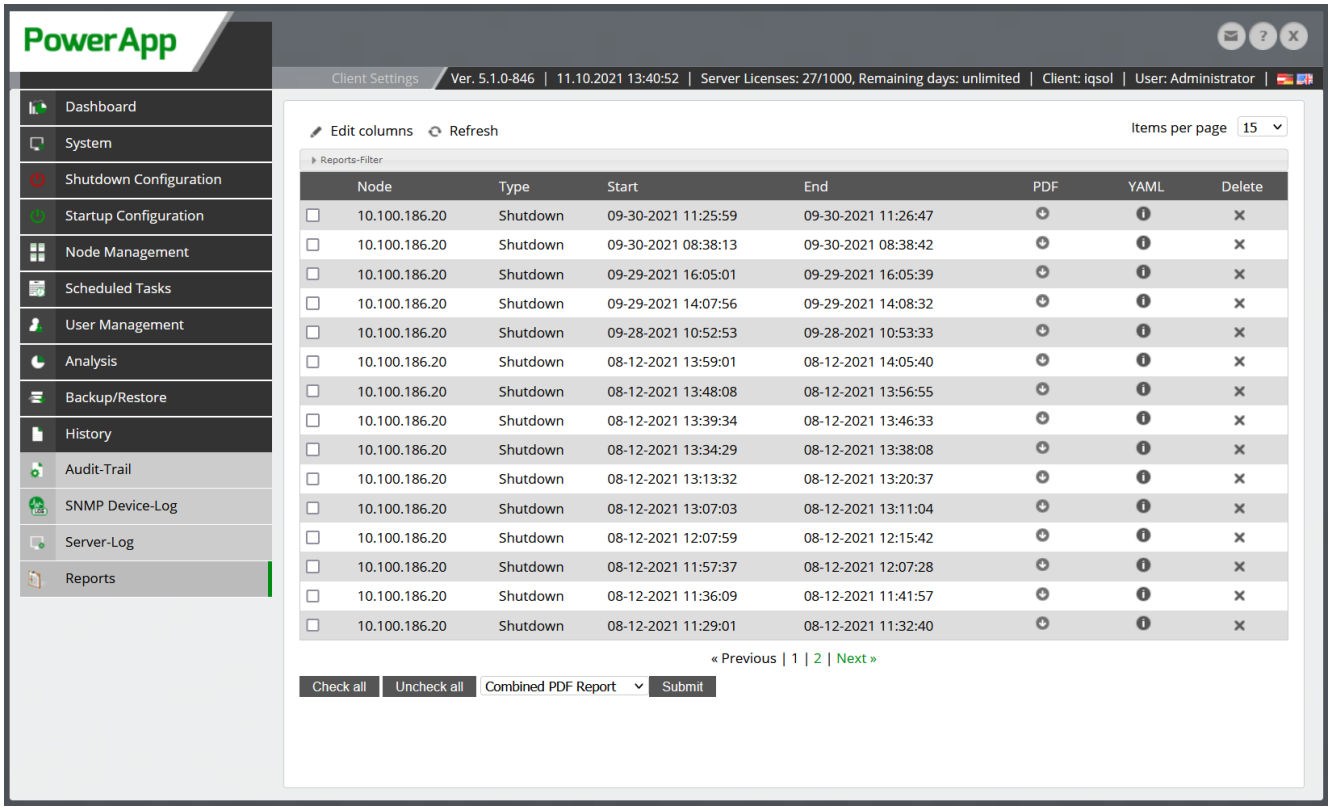


Figure 133: Reports

6.11 API

The API allows you to access data and/or perform automated actions on the PowerApp from another system. This chapter explains how to use the API.

6.11.1 How to use the API

API GET

```
curl -X GET 'https://192.168.0.1/api/system-information' --header 'Accept:
application/json' --header 'Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiI4MjgyNTdiYi04YzUwLTRmZGMtYjMwYi1lNzM5
MDFlNDE1MDIiLCJqdGkiOiIyMzQwMmM1YS0xMTIwLTQ4MWEtODUzYi01M2ZiOWM5YzU2ZmYifQ.OzVycCezoR
y5jrPhs7erM3kA2yRuW6PGSGAtazcXxQU' -k
```

-k ignores the certificate (should not be used productively)
--header 'Authorization: Bearer < here the token should be inserted>'
--header 'Accept: application/json' defines the format to be used
-X GET/POST '<URL that you see in Swagger>'

URL filter

Here are some examples of URL filters.

https://192.168.0.1/api/server?format=names&orderBy=SID&order=DESC

format=names	Output only names and IDs.
orderBy=<column>	Order by defined column.
order=ASC/DESC	Order ascending/decending.

https://192.168.0.1/api/server?operatingSystem=windows&isVm=1
You can filter the output by columns. Like in the example above only get servers where the operating system is Windows and the server is a virtual machine.
The full list of available options is below.

API POST

```
curl -X POST --header 'Content-Type: application/json' --header 'Accept:
application/json' --header 'Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiI4MjgyNTdiYi04YzUwLTRmZGMtYjMwYi1lNzM5
MDFlNDE1MDIiLCJqdGkiOiIyMzQwMmM1YS0xMTIwLTQ4MWEtODUzYi01M2ZiOWM5YzU2ZmYifQ.OzVycCezoR
y5jrPhs7erM3kA2yRuW6PGSGAtazcXxQU' -d '{"runCommandNow": true, "customCommand": "echo
API TEST"}' 'https://192.168.0.1/api/server-command/a483eec8-a9c7-4187-aa92-
58c803e0c702' -k
```

-d <json> POST the following json.

6.11.2 API documentation

To view the API documentation, click on the API button in the top right hand corner.

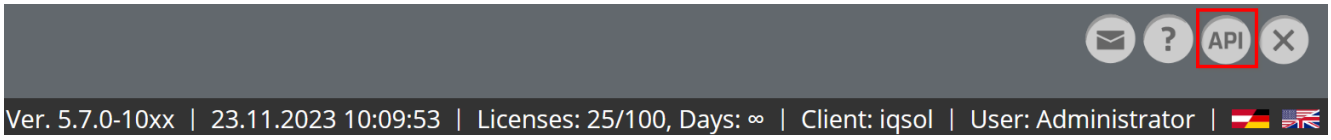


Figure 134: Open API documentation

A new window will open that looks like this. It shows all the options for API calls.

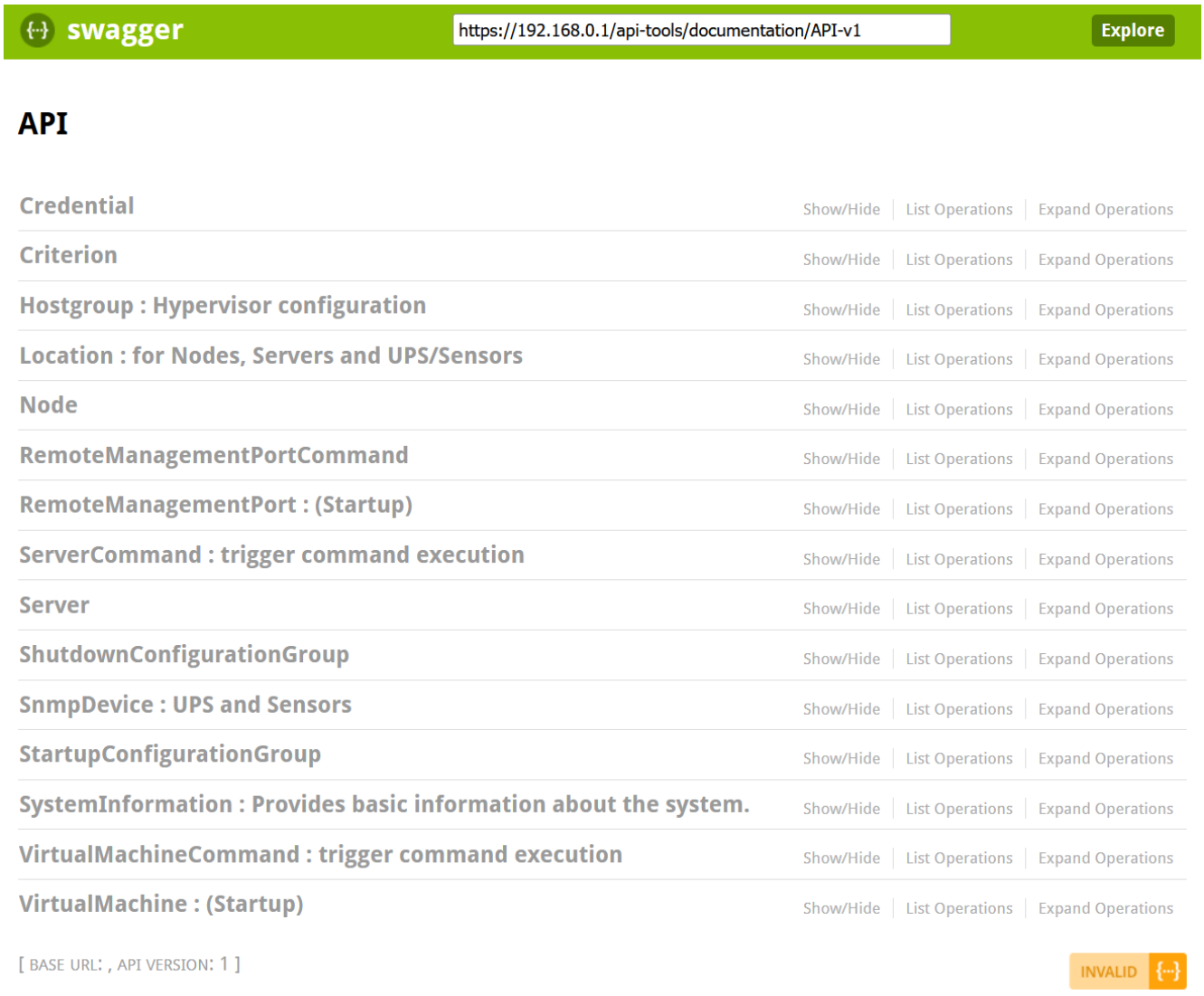


Figure 135: API documentation

6.11.3 All available URL filters

REST service (https://<host>/api/<service>)	Available URL filters
system-information	-
server	SID, hostname, port, LID, status, ignoreStatus, CGID, operatingSystem, remoteAccessMethod, CREID, commandType, isVm, HGID, vmHost, physicalHost, originHost, targetHost, moveIfHostAvailable
server-command	-
hostgroup	HGID, hostGroupName, vmType, CREID
shutdown-configuration-group	CGID, groupname, delay, enabled
startup-configuration-group	CGID, groupname, type, delay, enabled
snmp-device	SDID, type, name, LID, host, manufacturer, model, status
criterion	CrID, SDID, type, threshold, operator, oid, name, delay, matching
remote-management-port	MID, SID, hostname, status, ignoreStatus, CGID, remoteAccessMethod, CREID
remote-management-port-command	-
virtual-machine	SID, enabled, CGID
virtual-machine-command	-
location	LID, name, type, position
node	NID, LID, type, status, mode
credential	CREID, name, username, pubicKey, type

Table 6: Available URL filters

6.11.4 Practical example with PRTG

Examples of using the PowerApp API in conjunction with PRTG monitoring software are listed below. Other monitoring software that supports REST API should work similarly.

PRTG Sensor

After you have added and selected the PowerApp as a device in PRTG, add a sensor. The sensor must be a REST custom sensor.

The following settings should now be made on the sensor.

REST Specific

Request method	GET
Request protocol	HTTPS
Authentication Method	Token
Token	API-Token der PowerApp einfügen
HTTP headers	Send custom HTTP headers
Custom HTTP Headers	Accept: application/json
REST Query	A request URL can be created from the API documentation and everything from "/api/" to the end of the URL should be copied. In this example, "/api/system-information" is used as the request query.

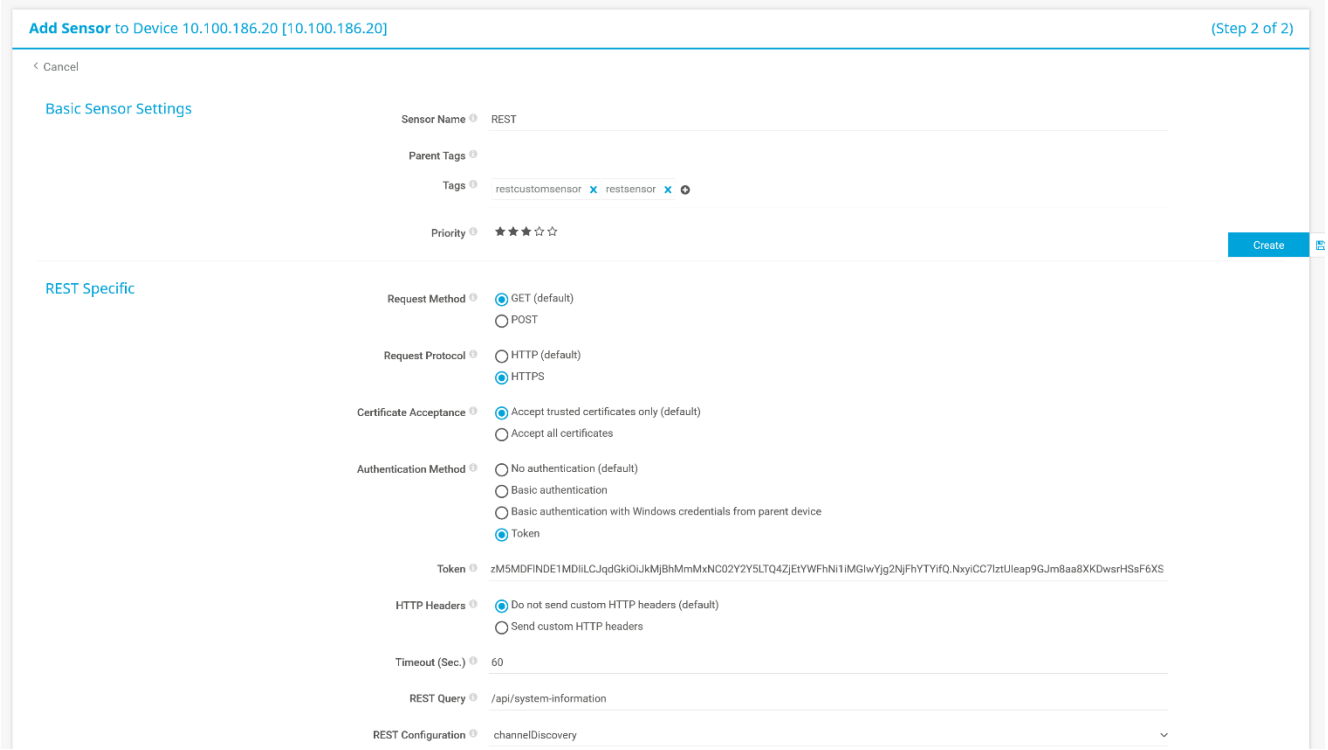


Figure 136: Create PRTG REST Sensor

The sensor can now be created.

After a short time, the sensor is scanned. In this example, the channels $["monitoringLogicEnabled"], $["monitoringLogicEnabled"], $["shutdownLogicEnabled"], $["startupLogicEnabled"] and $["updateFound"] are created in addition to the channel downtime and response time.

For the following channels, the Lookup parameter should be changed as follows

$["monitoringLogicEnabled"]	prtg.standardlookups.boolean.statetrueok
$["startupLogicEnabled"]	prtg.standardlookups.boolean.statetrueok
$["shutdownLogicEnabled"]	prtg.standardlookups.boolean.statetrueok
$["updateFound"]	prtg.standardlookups.boolean.statefalseok

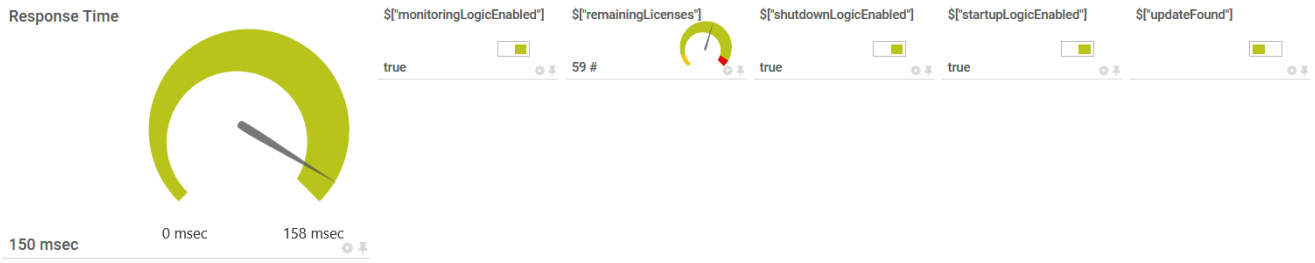


Figure 137: Result of the channel configuration

Table of Figures

Tables