VERTIV™

Power Insight

User Manual

The information contained in this document is subject to change without notice and may not be suitable for all applications. While every precaution has been taken to ensure the accuracy and completeness of this document, Vertiv assumes no responsibility and disclaims all liability for damages result from use of this information or for any errors or omissions.

Refer to local regulations and building codes relating to the application, installation, and operation of this product. The consulting engineer, installer, and/or end user is responsible for compliance with all applicable laws and regulations relation to the application, installation, and operation of this product.

The products covered by this instruction manual are manufactured and/or sold by Vertiv. This document is the property of Vertiv and contains confidential and proprietary information owned by Vertiv. Any copying, use, or disclosure of it without the written permission of Vertiv is strictly prohibited.

Names of companies and products are trademarks or registered trademarks of the respective companies. Any questions regarding usage of trademark names should be directed to the original manufacturer.

Technical Support Site

If you encounter any installation or operational issues with your product, check the pertinent section of this manual to see if the issue can be resolved by following outlined procedures.

Visit https://www.vertiv.com/en-us/support/ for additional assistance.

TABLE OF CONTENTS

This page intentionally left blank

1 Software Introduction

1.1 Overview

The Power Insight application is a web browser-based monitoring tool for your power infrastructure devices, and provides a central location to view power status, alarms and trends. It supports up to 100 critical power infrastructure devices.

1.2 Function

Power management applications 2.4 and later have the following features and benefits:

- Centralized power reading access
- Discovery and monitoring capabilities
- Alert triggered email and SMS notifications
- Protect the server in contingency situations
- Profile concept for easy reusability
- Default settings to get started quickly
- Shutdown script added
- Redundant shutdown

This page intentionally left blank

2 Installation of the software

2.1 Installation Requirements

2.1.1 Hardware

Power Insight Hardware Requirements:

Minimum Configuration

- CPU：4 core
- Memory: 8 GB
- Hard drive: 256 GB of free disk space

Recommended Configuration

- CPU: 8 core
- Memory: 8 GB
- Hard drive: 2TB free disk space

2.1.2 Software

Power Insight Supported 64-bit operating system:

- Microsoft Windows 7 and10
- Microsoft Windows Server 2012 R2 and 2016
- Red Hat Enterprise Linux 7.1 (With graphical user interface)

Power Insight Supported Browsers：

- Google Chrome 55 or above (desktop and tablet)
- Microsoft Edge 38 or above (desktop)
- Safari Mobile 9 or above (tablet)
- Internet Explorer 11 (Desktop)
- Firefox 51 or above (desktop)

Automation Agent Supported operating systems (for server shutdown)：

- Microsoft Windows 7, 8.1 and 10
- Microsoft Windows Server 2008 R2, 2012 R2 and 2016
- Microsoft Hyper-V Server 2012 R2 and 2016
- Red Hat Enterprise Linux 6.7, 6.9 and 7.1 - 7.4

NOTE: The shutdown function also supports virtual machines: VMWare ESXi 5.5, 6.0 and 6.5, but there is no need to install Automation Agent for virtual machines.

NOTE: x64 bit only support for Hyper-V and Red Hat systems.

2.2 Software Download

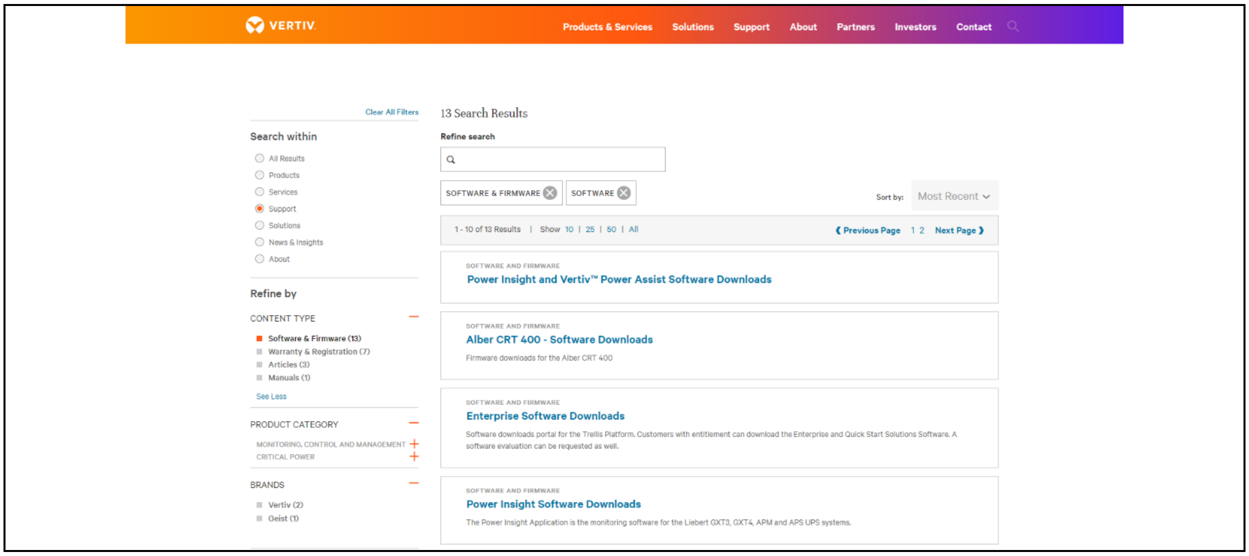
The following sections provide information on how to register an official account and download the Automation Agent and Power Insight software.

2.2.1 Account Registration

If you do not have a Vertiv™ account, register on the official website of Vertiv. The latest version of the software cannot be downloaded until registration is complete.

Sign-up Steps：

1. From a web browser, navigate to www.vertiv.com and click *Support*.
2. Click *"Software/Firmware Updates" > click "Software Product Downloads"* > jump to a *new page*:



13 Search Results

1 - 10 of 13 Results | Show 10 | 25 | 50 | All

SOFTWARE AND FIRMWARE
Power Insight and Vertiv™ Power Assist Software Downloads

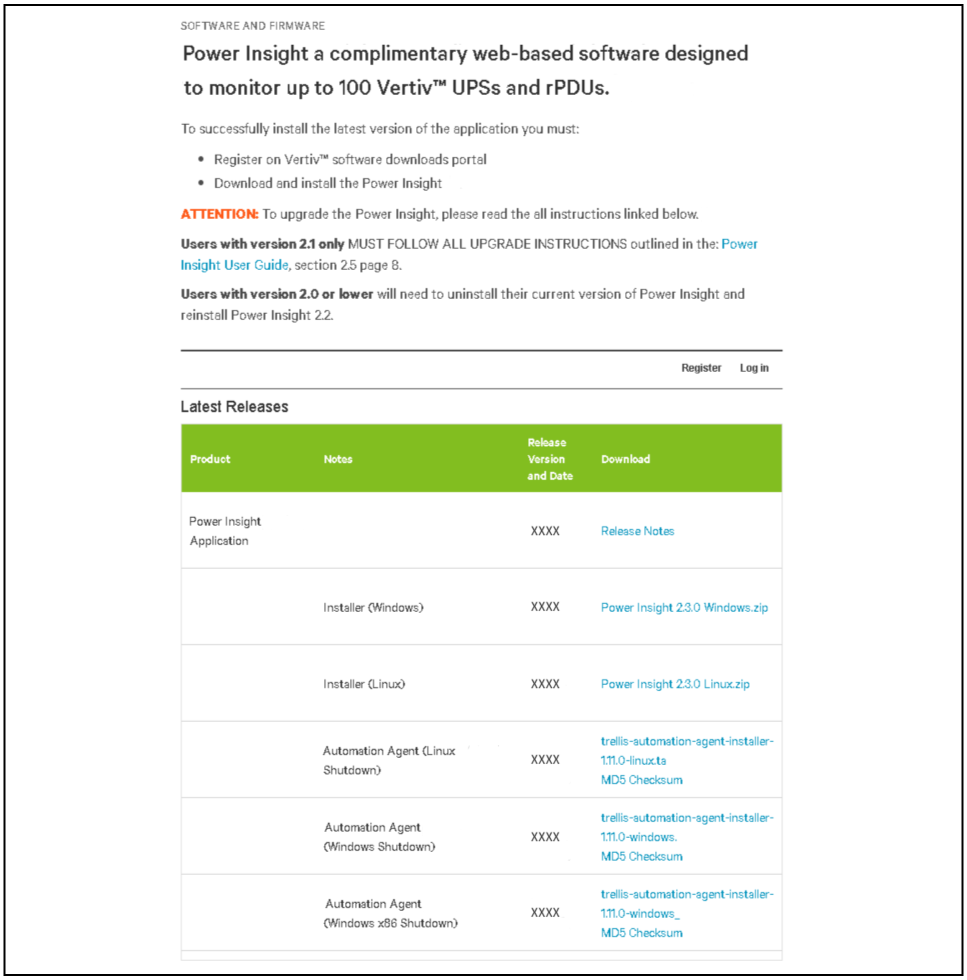
SOFTWARE AND FIRMWARE
Alber CRT 400 - Software Downloads
Firmware downloads for the Alber CRT 400

SOFTWARE AND FIRMWARE
Enterprise Software Downloads
Software downloads portal for the Trellis Platform. Customers with entitlement can download the Enterprise and Quick Start Solutions Software. A software evaluation can be requested as well.

SOFTWARE AND FIRMWARE
Power Insight Software Downloads
The Power Insight Application is the monitoring software for the Liebert GXT3, GXT4, APM and APS UPS systems.

Figure 2.1

3. Find "*Power Insight Software Downloads on the page* and *click*. The following page is displayed.



SOFTWARE AND FIRMWARE

Power Insight a complimentary web-based software designed to monitor up to 100 Vertiv™ UPSs and rPDUs.

To successfully install the latest version of the application you must:

- Register on Vertiv™ software downloads portal
- Download and install the Power Insight

ATTENTION: To upgrade the Power Insight, please read the all instructions linked below.

Users with version 2.1 only MUST FOLLOW ALL UPGRADE INSTRUCTIONS outlined in the: Power Insight User Guide, section 2.5 page 8.

Users with version 2.0 or lower will need to uninstall their current version of Power Insight and reinstall Power Insight 2.2.

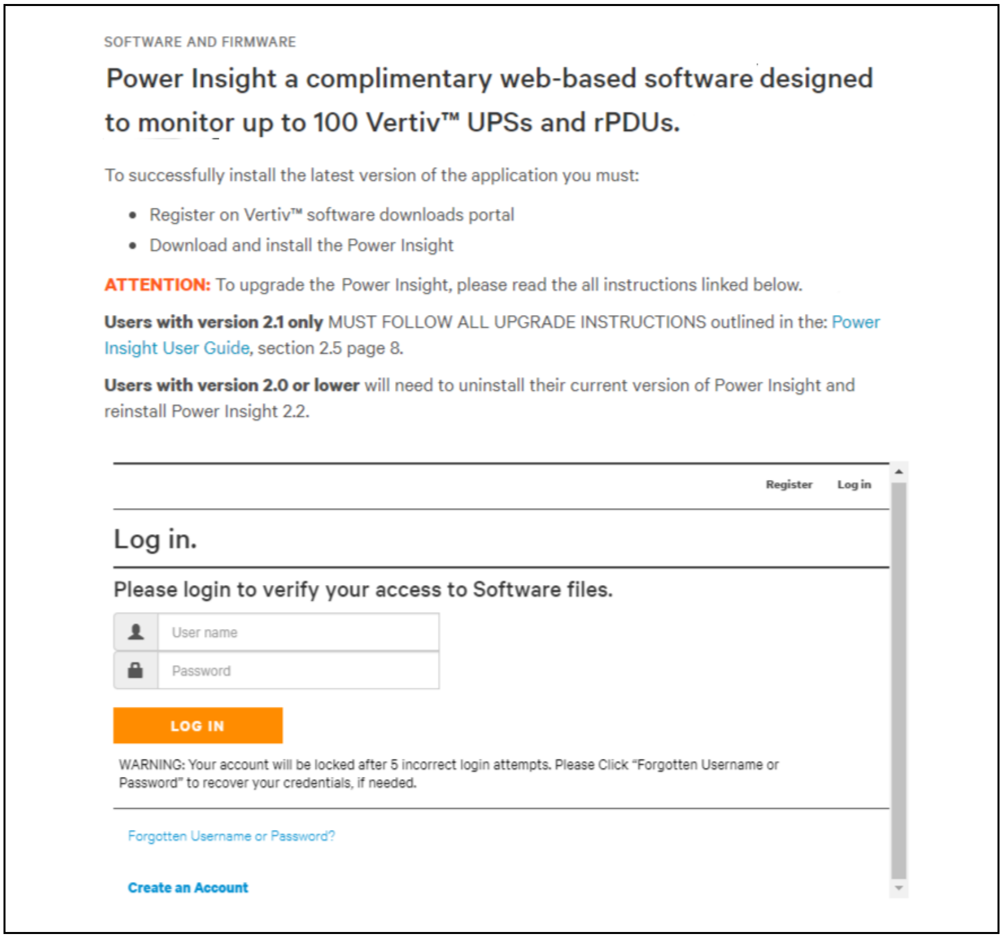
Register Log in

Latest Releases

Product	Notes	Release Version and Date	Download
Power Insight Application		XXXX	Release Notes
	Installer (Windows)	XXXX	Power Insight 2.3.0 Windows.zip
	Installer (Linux)	XXXX	Power Insight 2.3.0 Linux.zip
	Automation Agent (Linux Shutdown)	XXXX	trellis-automation-agent-installer-1.11.0-linux.ta MD5 Checksum
	Automation Agent (Windows Shutdown)	XXXX	trellis-automation-agent-installer-1.11.0-windows. MD5 Checksum
	Automation Agent (Windows x86 Shutdown)	XXXX	trellis-automation-agent-installer-1.11.0-windows_ MD5 Checksum

Figure 2.2

4. Click on *the object* and a pop-up window requesting for login details is displayed.



SOFTWARE AND FIRMWARE

Power Insight a complimentary web-based software designed to monitor up to 100 Vertiv™ UPSs and rPDUs.

To successfully install the latest version of the application you must:

- Register on Vertiv™ software downloads portal
- Download and install the Power Insight

ATTENTION: To upgrade the Power Insight, please read the all instructions linked below.

Users with version 2.1 only MUST FOLLOW ALL UPGRADE INSTRUCTIONS outlined in the: Power Insight User Guide, section 2.5 page 8.

Users with version 2.0 or lower will need to uninstall their current version of Power Insight and reinstall Power Insight 2.2.

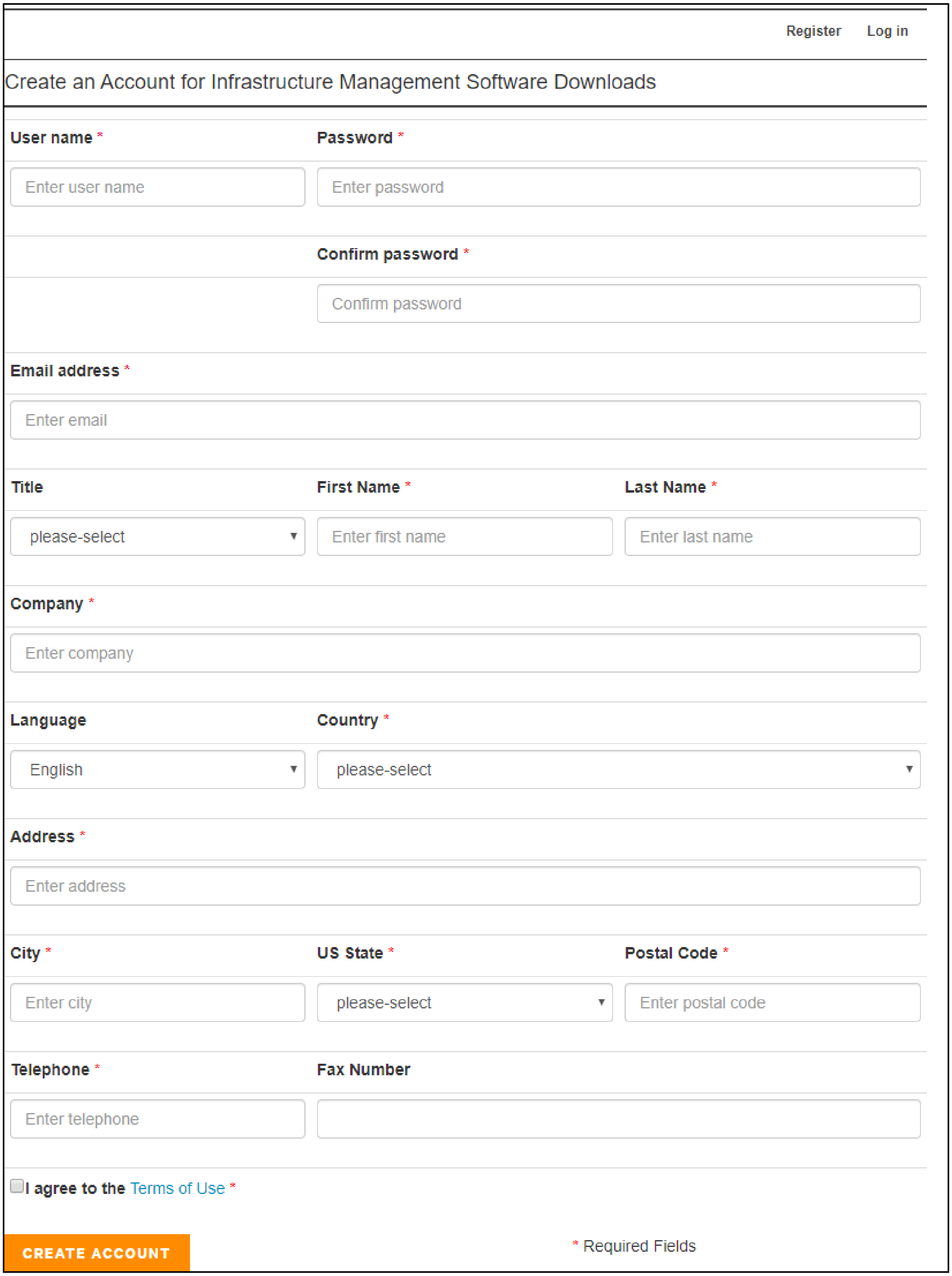
Log in.

Please login to verify your access to Software files.

WARNING: Your account will be locked after 5 incorrect login attempts. Please Click "Forgotten Username or Password" to recover your credentials, if needed.

Figure 2.3

5. Click *Register* in the upper right corner. The browser pops up a new window named as "Register" as shown below:



Create an Account for Infrastructure Management Software Downloads

User name *	**Password** *	
Enter user name	Enter password	
	Confirm password *	
	Confirm password	
Email address *		
Enter email		
Title	**First Name** *	**Last Name** *
please-select ▾	Enter first name	Enter last name
Company *		
Enter company		
Language	**Country** *	
English ▾	please-select ▾	
Address *		
Enter address		
City *	**US State** *	**Postal Code** *
Enter city	please-select ▾	Enter postal code
Telephone *	**Fax Number**	
Enter telephone		

□ **I agree to the** Terms of Use *

* Required Fields

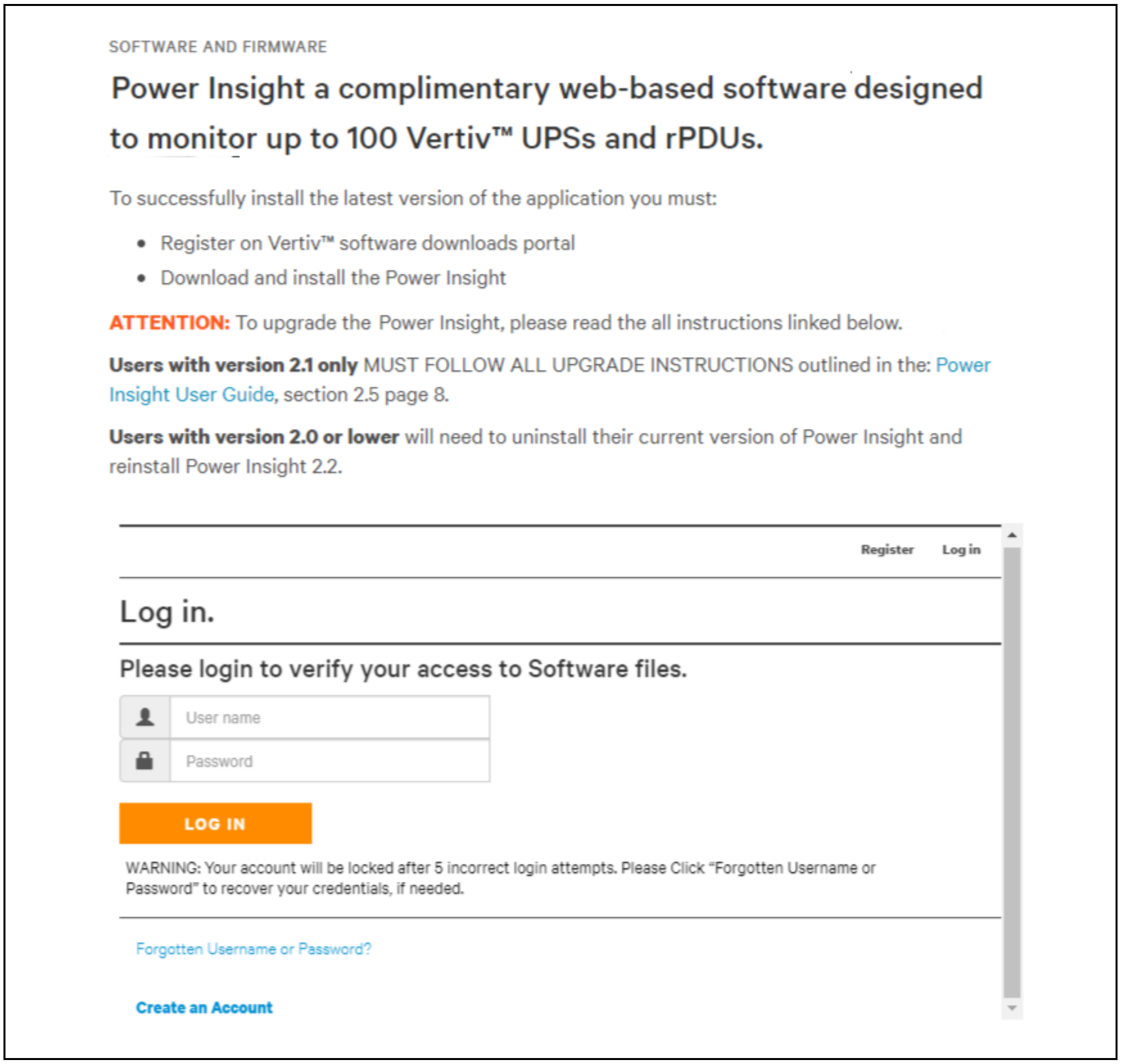
Figure 2.4

Fill in the required fields (fields marked by red asterisk are mandatory) and click *I agree to the Terms of Use* and then click *Create Account*. The mailbox verification page is displayed.

6. Access *the email address* provided during the registration process and obtain *the activation code* from the "Welcome to Vertiv™ Software Downloads" email.
7. Enter *the activation code* in the Code field and click *Submit*. Registration is complete.

2.2.2 Download

1. Access the page of Add UPS, rPDU on page 27 by following the registration process mentioned in Account Registration on page 4 .



SOFTWARE AND FIRMWARE

Power Insight a complimentary web-based software designed to monitor up to 100 Vertiv™ UPSs and rPDUs.

To successfully install the latest version of the application you must:

- Register on Vertiv™ software downloads portal
- Download and install the Power Insight

ATTENTION: To upgrade the Power Insight, please read the all instructions linked below.

Users with version 2.1 only MUST FOLLOW ALL UPGRADE INSTRUCTIONS outlined in the: Power Insight User Guide, section 2.5 page 8.

Users with version 2.0 or lower will need to uninstall their current version of Power Insight and reinstall Power Insight 2.2.

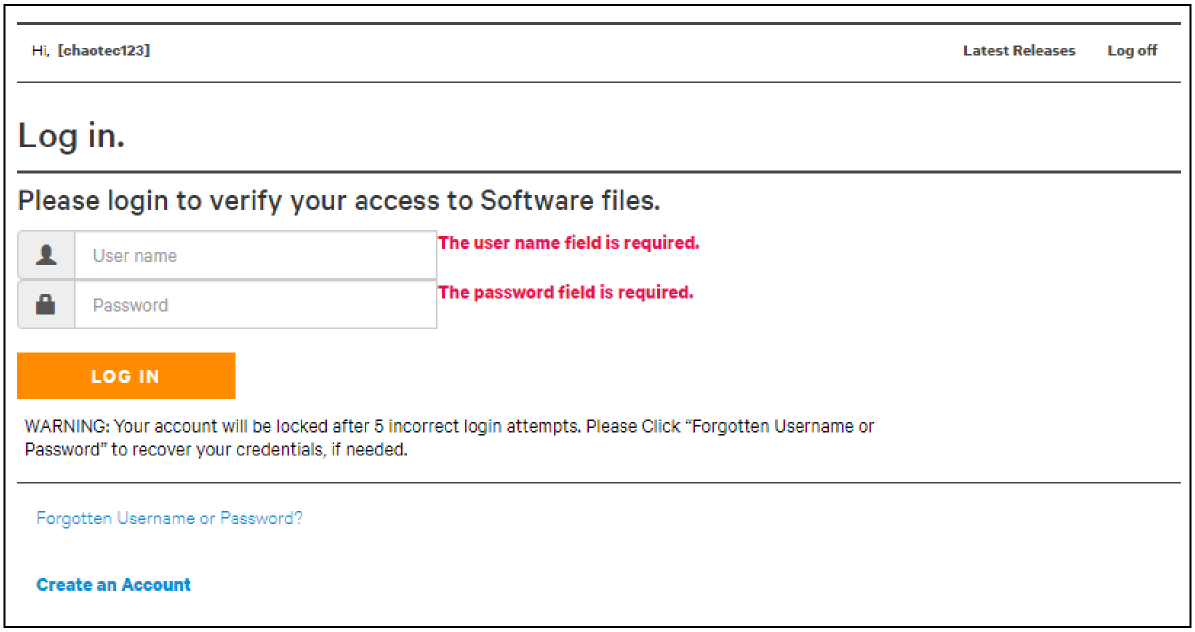
Log in.

Please login to verify your access to Software files.

WARNING: Your account will be locked after 5 incorrect login attempts. Please Click "Forgotten Username or Password" to recover your credentials, if needed.

Figure 2.5

2. Click *Log in* in the upper right corner. A new window will pop up in the browser as shown below:



Hi, [chaotec123]　Latest Releases　Log off

Log in.

Please login to verify your access to Software files.

User name　The user name field is required.

Password　The password field is required.

LOG IN

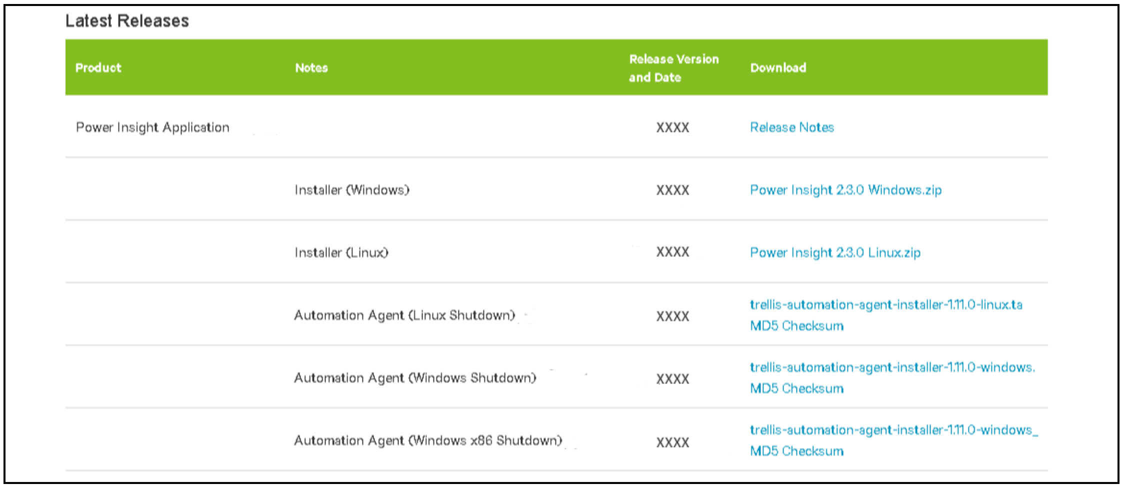
WARNING: Your account will be locked after 5 incorrect login attempts. Please Click "Forgotten Username or Password" to recover your credentials, if needed.

Forgotten Username or Password?

Create an Account

Figure 2.6

3. After entering the previously registered username and password, click the *LOG IN* button. Go to the *download page*, see **Figure 2.7** below



Latest Releases

Product	Notes	Release Version and Date	Download
Power Insight Application		XXXX	Release Notes
	Installer (Windows)	XXXX	Power Insight 2.3.0 Windows.zip
	Installer (Linux)	XXXX	Power Insight 2.3.0 Linux.zip
	Automation Agent (Linux Shutdown)	XXXX	trellis-automation-agent-installer-1.11.0-linux.ta MD5 Checksum
	Automation Agent (Windows Shutdown)	XXXX	trellis-automation-agent-installer-1.11.0-windows. MD5 Checksum
	Automation Agent (Windows x86 Shutdown)	XXXX	trellis-automation-agent-installer-1.11.0-windows_ MD5 Checksum

Figure 2.7

4. Depending on the operating system, click the link to *download* the corresponding software versions. Wait *until the download is completed.*

Software Name	Operating System	System Installation Package
Power Insight	Windows	Power Insight 2.4.0 Windows.zip
	Linux	Power Insight 2.4.0 Linux.zip
Automation Agent	Windows 32 bit operating system	trellis-automation-agent-installer-1.11.0-windows_x86.zip
	Windows 64 bit operating system	trellis-automation-agent-installer-1.11.0-windows.zip
	Linux	trellis-automation-agent-installer-1.10.0-linux.tar.gz

NOTE: For the specific operating system version, refer to Software on page 3 for a list of supported software versions.

5. Wait *until the download is completed.*

2.3 Software Installation

2.3.1 Power Insight Installation

Steps to install the application on the Windows operating system

NOTE: You must be logged in as a local administrator.

1. Go *to the folder where Power Insight 2.4.0 Windows.zip is located.*
2. Double-click *on the Trellispowerinsightinstaller.exe file in the compressed file.*
3. Select *the preferred language from the drop-down list and click OK.*

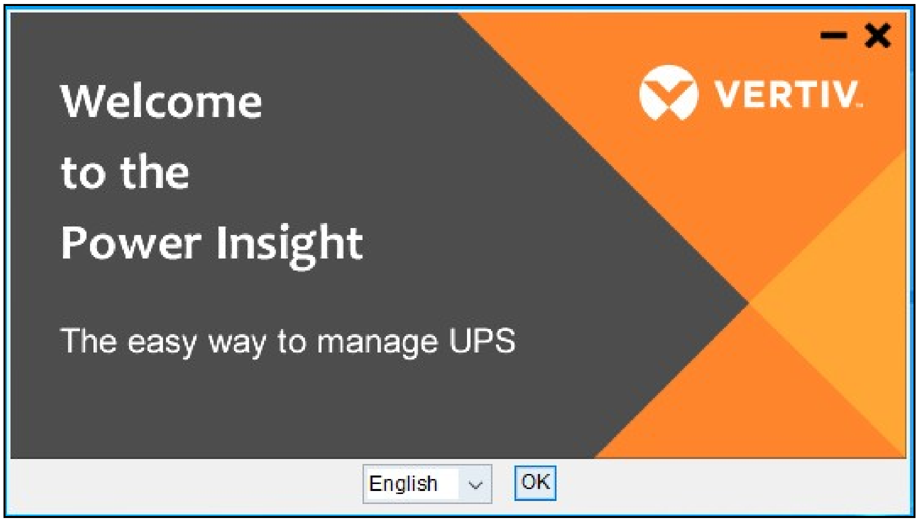
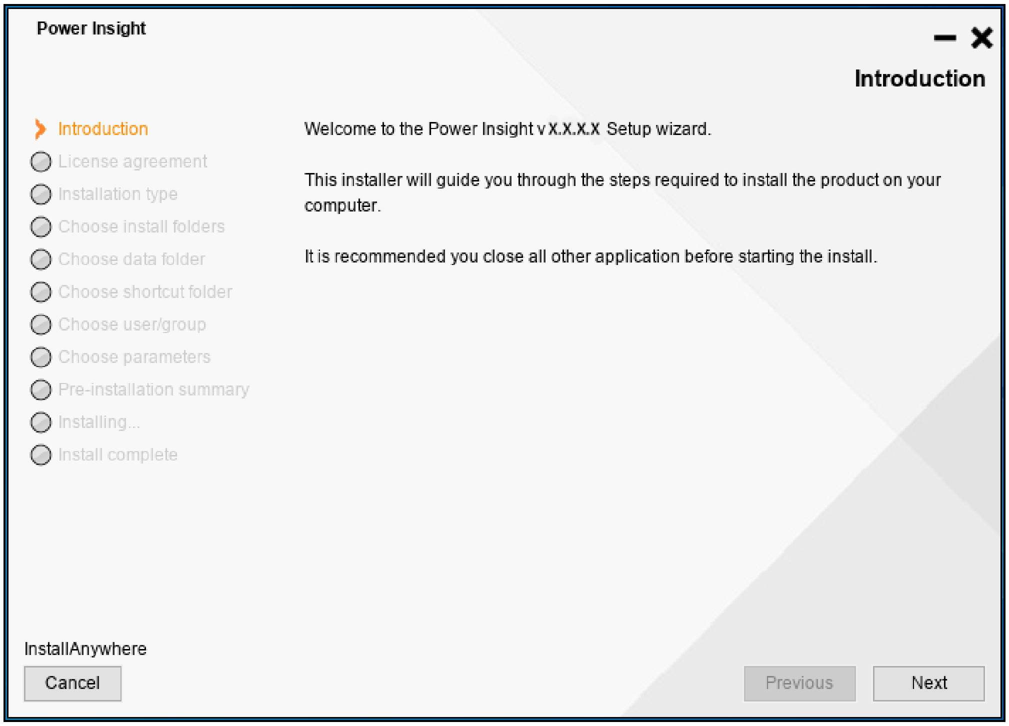


Figure 2.8

4. Click *Next on the introduction screen.*



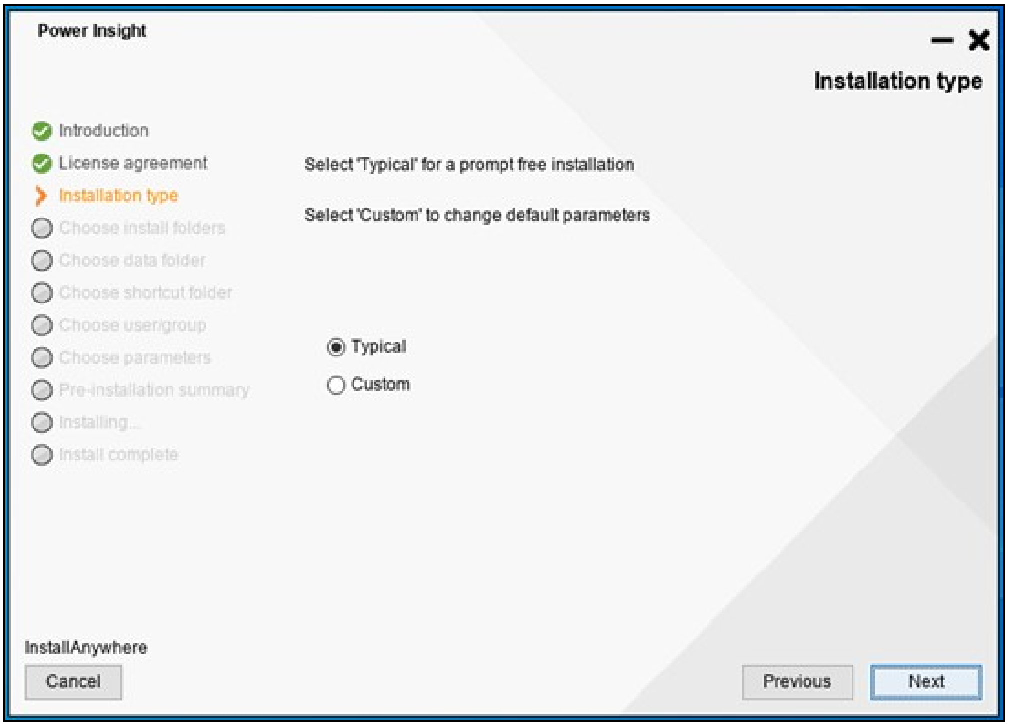
Welcome to the Power Insight v X.X.X.X Setup wizard.

This installer will guide you through the steps required to install the product on your computer.

It is recommended you close all other application before starting the install.

Figure 2.9

5. Click *the check box to accept the license agreement* and click *Next.*
6. Select *the radio button for a typical installation. If you select a typical installation, proceed to Step 9.*
   - Or-
   Select *the radio button for customize installation and click Next.*



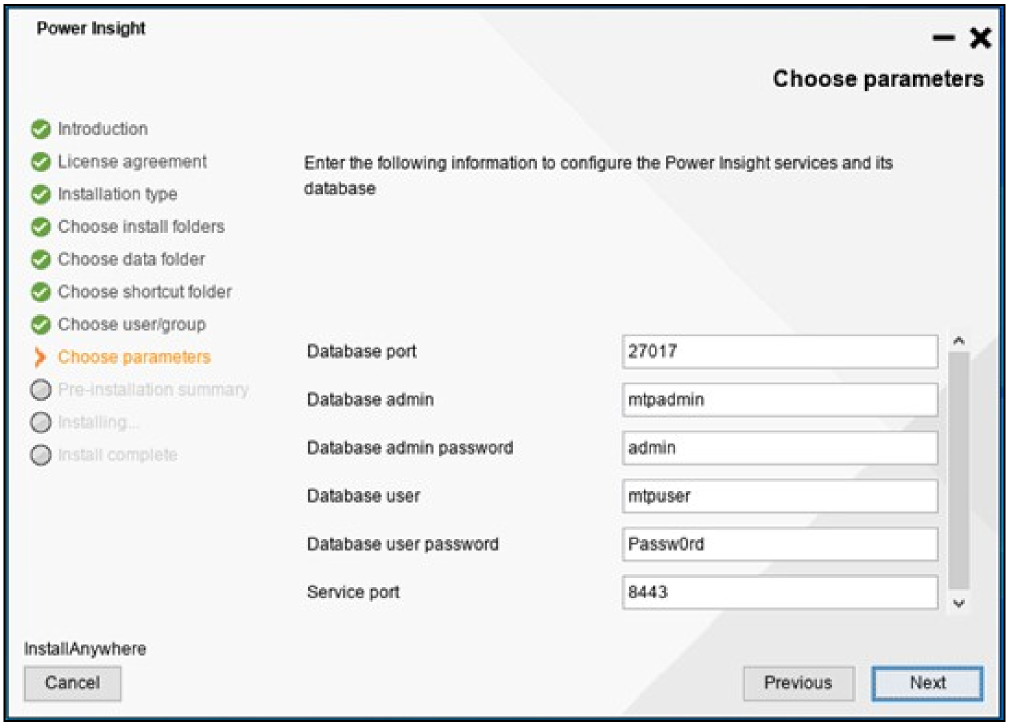
Select 'Typical' for a prompt free installation

Select 'Custom' to change default parameters

● Typical
○ Custom

Figure 2.10

7. Select *the installation location and click Next.*
8. Select *the location of the data catalog and click Next.*
9. Select *the shortcut folder and click Next.*
10. Select *the parameters and click Next.*



Enter the following information to configure the Power Insight services and its database

Database port: 27017
Database admin: mtpadmin
Database admin password: admin
Database user: mtpuser
Database user password: Passw0rd
Service port: 8443

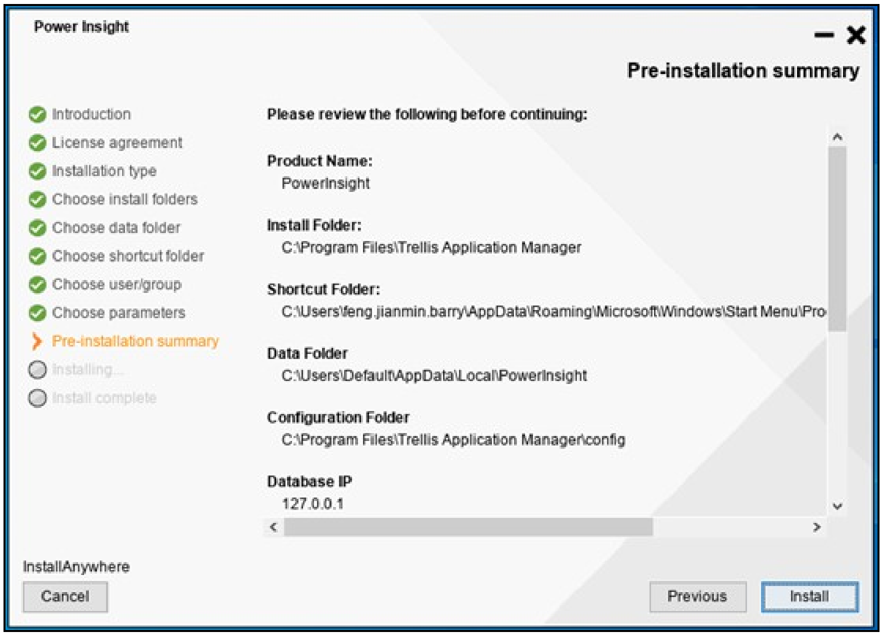
Figure 2.11

Table 2.1 Default parameter window values

PARAMETER	DESCRIPTION	DEFAULT VALUE
Database port	Default port the database uses. Be sure the port selected is not in use.	27017
Database admin	Administrator of the database	mtpadmin
Database admin password	The administrator's password. It is highly recommended to change this password.	admin
Database user	Owner of the database	mtpuser
Database user password	The password of the database owner. It is highly recommended to change this password.	Password
Application service port	Port the services run on. Be sure the port selected is not in use.	8443

NOTE: If there is a port error, you will be prompted to change the port.

11. Click *the install button in the pre-installation summary window.*



Pre-installation summary

Please review the following before continuing:

Product Name:
PowerInsight

Install Folder:
C:\Program Files\Trellis Application Manager

Shortcut Folder:
C:\Users\feng.jianmin.barry\AppData\Roaming\Microsoft\Windows\Start Menu\Pro

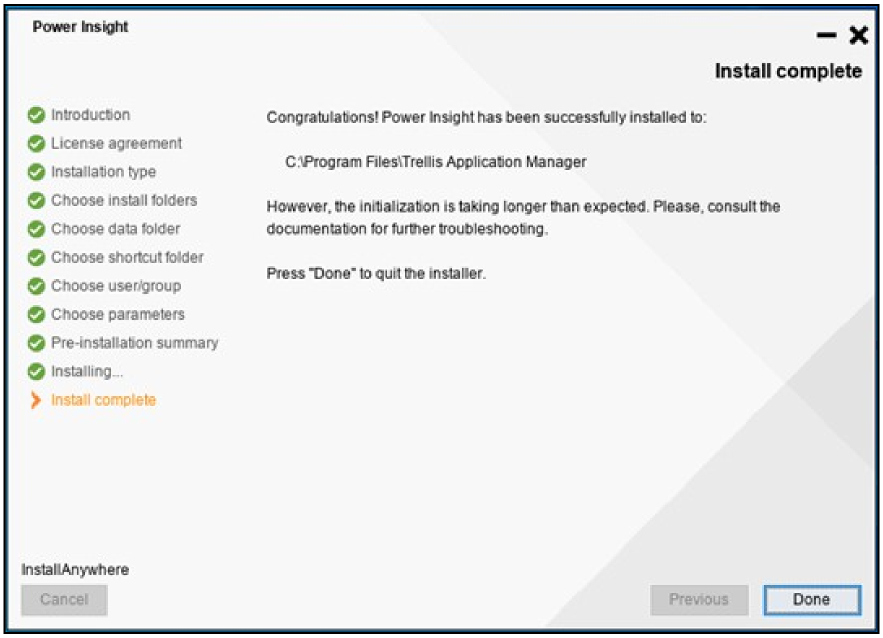
Data Folder
C:\Users\Default\AppData\Local\PowerInsight

Configuration Folder
C:\Program Files\Trellis Application Manager\config

Database IP
127.0.0.1

Figure 2.12

12. Once installed, click *Done*. Shortcuts are added to the location selected during the installation process.



Install complete

Congratulations! Power Insight has been successfully installed to:

C:\Program Files\Trellis Application Manager

However, the initialization is taking longer than expected. Please, consult the documentation for further troubleshooting.

Press "Done" to quit the installer.

Figure 2.13

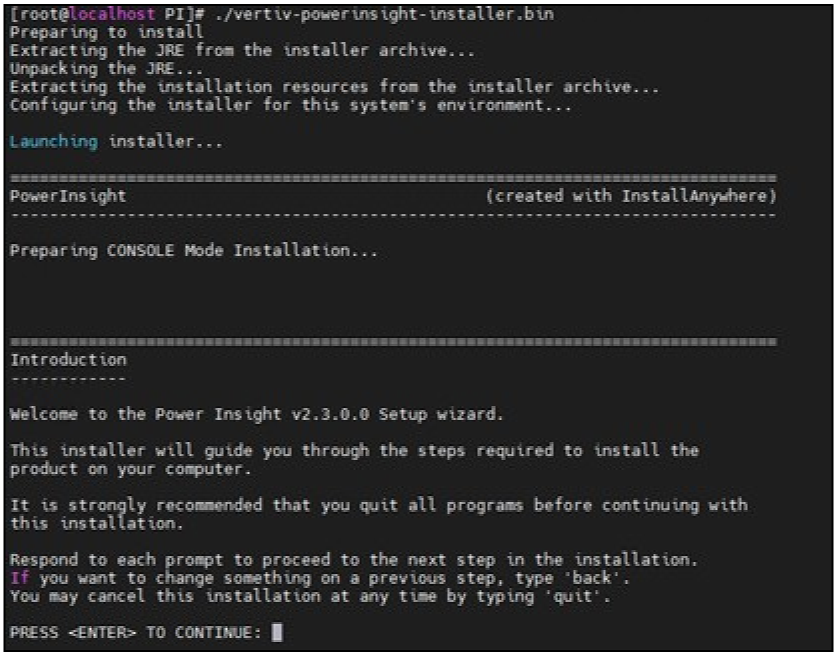
Steps to install the application on a Linux Operating System:

NOTE: You must have root privileges to install the application.

1. Go *to the folder where Power Insight 2.4.0 Windows.tar.gz file is located.*
2. Extract *the installer from the tar.gz file.*
3. Open *a terminal window.*
4. Navigate *to the directory where the file is copied.*
5. If you log in *to the console as a root user,* enter *./trellispowerinsightinstaller.bin.*
   - Or-
   If you have Superuser (SUDO) privileges, enter *sudo ./trellispowerinsightinstaller.bin*.
6. If you are logged in *to the Graphical User Interface (GUI) as a root user*, enter *./trellispowerinsightinstaller.bin-i GUI.*
   - Or-
   If you have SUDO privileges, enter *sudo ./trellispowerinsightinstaller.bin -i GUI to run the GUI installer.*

NOTE: For the installation steps of the graphical user interface, please refer to the "Installation Steps on Windows Operating System" section. The following installation steps are based on the terminal window installation.

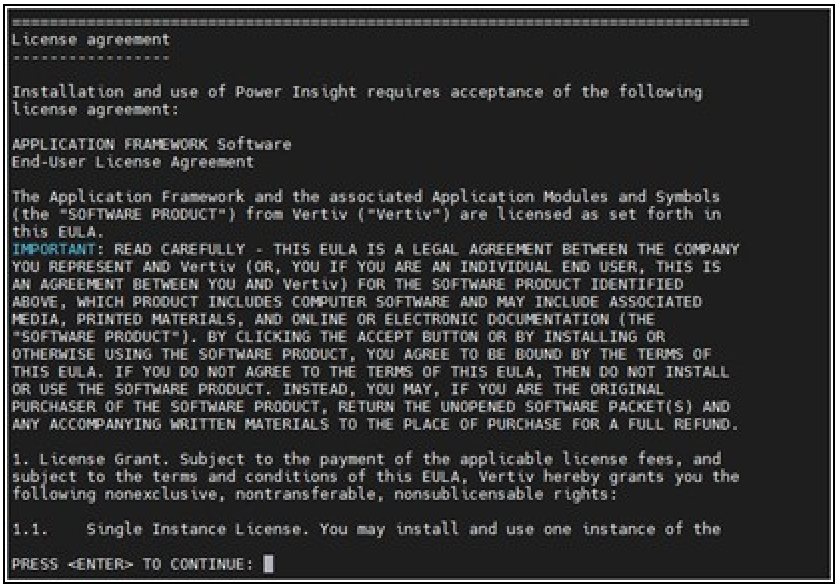
7. Install *the dependencies and press enter key.*



```
[root@localhost PI]# ./vertiv-powerinsight-installer.bin
Preparing to install
Extracting the JRE from the installer archive...
Unpacking the JRE...
Extracting the installation resources from the installer archive...
Configuring the installer for this system's environment...

Launching installer...

===============================================================================
PowerInsight                                     (created with InstallAnywhere)
-------------------------------------------------------------------------------

Preparing CONSOLE Mode Installation...




===============================================================================
Introduction
------------

Welcome to the Power Insight v2.3.0.0 Setup wizard.

This installer will guide you through the steps required to install the
product on your computer.

It is strongly recommended that you quit all programs before continuing with
this installation.

Respond to each prompt to proceed to the next step in the installation.
If you want to change something on a previous step, type 'back'.
You may cancel this installation at any time by typing 'quit'.

PRESS <ENTER> TO CONTINUE: █
```

Figure 2.14

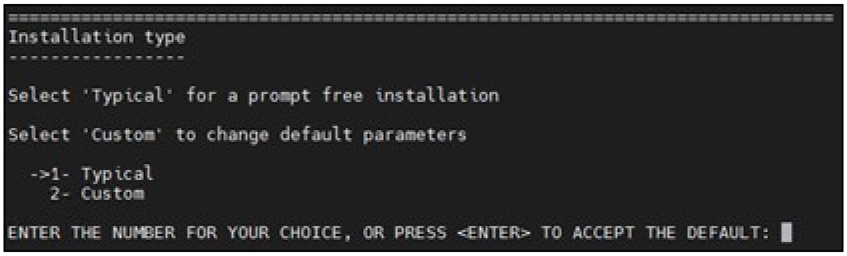
8. Read *the End User License Agreement (EULA) and eventually enter Y to accept the license terms.*



```
===============================================================================
License agreement
-----------------

Installation and use of Power Insight requires acceptance of the following
license agreement:

APPLICATION FRAMEWORK Software
End-User License Agreement

The Application Framework and the associated Application Modules and Symbols
(the "SOFTWARE PRODUCT") from Vertiv ("Vertiv") are licensed as set forth in
this EULA.
IMPORTANT: READ CAREFULLY - THIS EULA IS A LEGAL AGREEMENT BETWEEN THE COMPANY
YOU REPRESENT AND Vertiv (OR, YOU IF YOU ARE AN INDIVIDUAL END USER, THIS IS
AN AGREEMENT BETWEEN YOU AND Vertiv) FOR THE SOFTWARE PRODUCT IDENTIFIED
ABOVE, WHICH PRODUCT INCLUDES COMPUTER SOFTWARE AND MAY INCLUDE ASSOCIATED
MEDIA, PRINTED MATERIALS, AND ONLINE OR ELECTRONIC DOCUMENTATION (THE
"SOFTWARE PRODUCT"). BY CLICKING THE ACCEPT BUTTON OR BY INSTALLING OR
OTHERWISE USING THE SOFTWARE PRODUCT, YOU AGREE TO BE BOUND BY THE TERMS OF
THIS EULA. IF YOU DO NOT AGREE TO THE TERMS OF THIS EULA, THEN DO NOT INSTALL
OR USE THE SOFTWARE PRODUCT. INSTEAD, YOU MAY, IF YOU ARE THE ORIGINAL
PURCHASER OF THE SOFTWARE PRODUCT, RETURN THE UNOPENED SOFTWARE PACKET(S) AND
ANY ACCOMPANYING WRITTEN MATERIALS TO THE PLACE OF PURCHASE FOR A FULL REFUND.

1. License Grant. Subject to the payment of the applicable license fees, and
subject to the terms and conditions of this EULA, Vertiv hereby grants you the
following nonexclusive, nontransferable, nonsublicensable rights:

1.1.    Single Instance License. You may install and use one instance of the

PRESS <ENTER> TO CONTINUE:
```

Figure 2.15

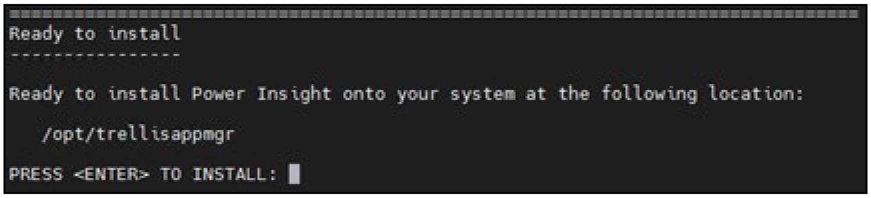
9. Select *the installation type*. If you select *a typical installation, enter "1"*, press *Enter key* and skip *to step 9*. - Or- If you choose *a custom installation*, enter *"2"* and press *enter key*.



```
==================================================================================
Installation type
-----------------

Select 'Typical' for a prompt free installation

Select 'Custom' to change default parameters

  ->1- Typical
    2- Custom

ENTER THE NUMBER FOR YOUR CHOICE, OR PRESS <ENTER> TO ACCEPT THE DEFAULT:
```

Figure 2.16

10. Enter *the location of the program installation directory and* press *ente key*.
11. Enter *the location of the data storage directory* and press *enter key*.
12. Select *the shortcut folder* and press *enter*.
13. Enter *the user/group*, enter *the username*, press *the enter key*, then *enter the group name*, press *the enter key*.
14. Select *the parameters*, enter *the relevant parameters*, the specific parameters meaning refer to the Table 2.1 on page 13 .
15. After confirming the installation path again, press *enter key to start installation*.



```
==================================================================================
Ready to install
----------------

Ready to install Power Insight onto your system at the following location:

   /opt/trellisappmgr

PRESS <ENTER> TO INSTALL:
```

Figure 2.17

NOTE: If there is a port error, you will be prompted to change the port.

16. After installation is complete, press *enter*.

NOTE: A "/var/opt/trellisappmgr" directory will be created during installation. The log files are stored in this directory.

2.3.2 Automation Agent Installation

Automation Agent is an application that accepts the Power Insight shutdown command. To enable Server Shutdown, Automation Agent must be installed on the server.

Steps to install Automation Agent on the Windows server side

1. Sign Login into *the server with administrative rights*.
2. Find *the downloaded installation package* and *unzip the file*. Double-click *trellis-automation-agent-install.exe*.

NOTE: If it is Microsoft Windows Server or Microsoft Hyper-V Server operating system, after logging in, *navigate to the installation file directory*, enter *trellis-automation-agent-install.exe*, and press *Enter*.

3. Under the new window that pops up, select *both English and Chinese*. For English, enter *1* and press "*Enter key*.
4. Read *the End User License Agreement (EULA)* and eventually *enter Y to accept the license terms*.
5. Select *the location of program installation directory* and press *Enter key*.
6. Create *an account name and password*.

NOTE: The password length must be between 8-32 characters.

NOTE: This password will be used when the server selects a new communication rule.

7. Enter *the port address* and press *Enter key*.
8. Press *Enter key to install Automation Agent*.

Steps to install Automation Agent on the Linux server side

1. Sign-in *to the server with administrative rights*.
2. Find *the downloaded installation package* and unzip *the file*. If you log in to the console as a root user, enter *./trellis-automation-agent-install.bin*.
   - Or-
   If you have SUDO privileges, enter *sudo ./trellis-automation-agent-install.bin*.
3. Under the new window that pops up, select *both English and Chinese*. Enter *1 for English and for Chinese, enter 2*.
4. Read *the End User License Agreement (EULA)* and eventually enter *Y to accept the license terms*.
5. Select the *location of program installation directory and press "Enter" key*.
6. Create *an account name and password*.

NOTE: The password length must be between 8-32 characters.

NOTE: This password will be used when the server selects a new communication rule.

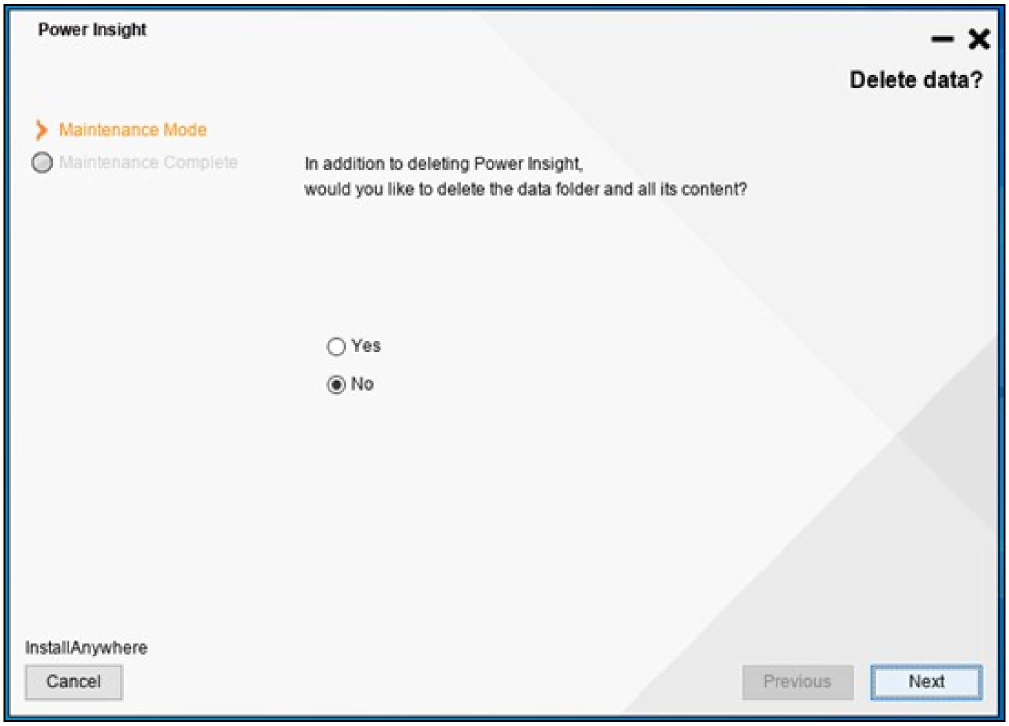
7. Enter *the port address* and press *Enter key*.
8. Press *Enter key to install Automation Agent*.

2.4 Software Uninstall

2.4.1 Power Insight uninstall

To uninstall from a Windows operating system:

1. Run *Control Panel - Programs and Features*.
2. Find *Trellis Power Insight in the list of programs*. Run *the uninstall*.
3. Click *Next*.
4. In the "Get User Input" window, if you keep *the original data*, click *"Next"*.
   - Or-
   If you don't need to keep the data, click "*Yes"* and click "*Next*".



In addition to deleting Power Insight,
would you like to delete the data folder and all its content?

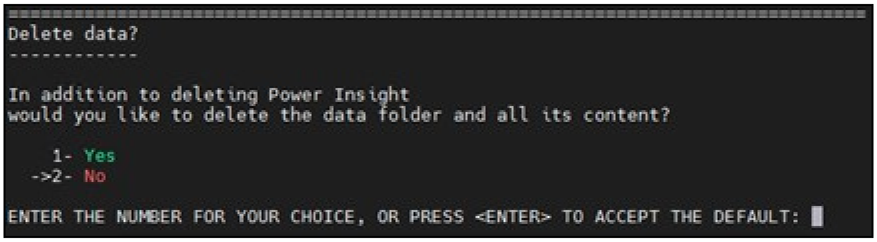
○ Yes
● No

Figure 2.18

5. Click *Done* when the process is completed.

To uninstall from a Linux operating system:

1. If you are logged in *to the console as a root user*, enter *"/<installdir>/_installation/trellisappmgruninstall"*.
2. On the Delete Data window, press *Enter to accept the default (No).*
   -or-
   Enter *"1" (Yes) to delete the data.*



```
===============================================================================
Delete data?
------------

In addition to deleting Power Insight
would you like to delete the data folder and all its content?

    1- Yes
  ->2- No

ENTER THE NUMBER FOR YOUR CHOICE, OR PRESS <ENTER> TO ACCEPT THE DEFAULT:
```

Figure 2.19

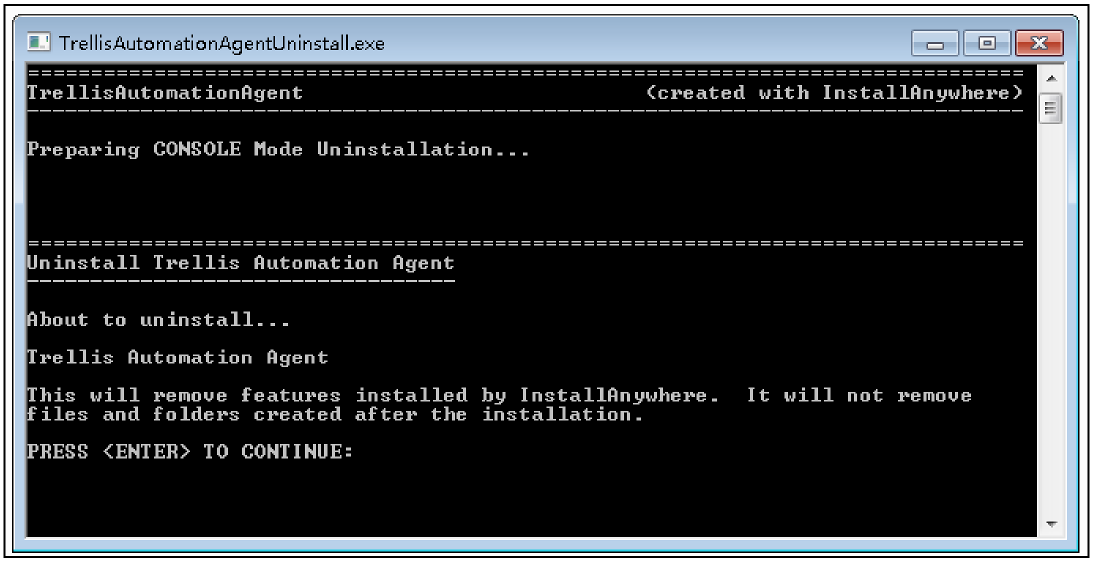
3. Press *"Enter" key to wait for the uninstall to complete.*

2.4.2 Automation Agent uninstall

Windows server side uninstall setup

1. Log in *to the remote server and run Control Panel- Programs and Features.*
2. Find "*Trellis AutomationAgent" in the list of programs*. Run *the uninstall.*

NOTE: If it is Microsoft® Windows Server® or Microsoft® Hyper-V Server® operating system, after logging in, navigate to the installation file directory, enter "TrellisAutomationAgentUninstall.exe", and press “Enter” key.



```
===============================================================================
TrellisAutomationAgent                                (created with InstallAnywhere)
-------------------------------------------------------------------------------

Preparing CONSOLE Mode Uninstallation...



===============================================================================
Uninstall Trellis Automation Agent
----------------------------------

About to uninstall...

Trellis Automation Agent

This will remove features installed by InstallAnywhere.  It will not remove
files and folders created after the installation.

PRESS <ENTER> TO CONTINUE:
```

Figure 2.20

3. Press *“Enter” key to continue* and wait *until uninstallation is complete.*

Server side uninstall setup

1. Log in *to the Linux server as a root user.*
2. Enter the *terminal*, enter *“/<install dir>/_installation/TrellisAutomationAgentUninstall”* and press the *“enter” key* to run the uninstallation program.
3. Wait *until uninstallation is completed.*

3 Software Login and Main Interface

3.1 Software login

3.1.1 User registration

If visiting Power Insight for the first time, you need to register an administrator user and password.

Sign up Steps:

1. Open *a web browser on your local computer* and enter "*https://localhost:SERVICE_PORT.*"where the service port is the service portnumber, such as 8443. In this example, the address is "https://localhost:8443".
   - Or-
   On the computer in which the application is installed, double-click *the Power Insight Console shortcut icon.*

Figure 3.1

2. To login on a remote computer, enter "*https:// <remote IP address>: <service port>; where the <remote IP address> is the IP address for the installation of Power Insight, and the <service port> is the service port number, for example, 8443.*
3. Enter the *email address which you want to receive the alert notification,* and then click *Continue.*

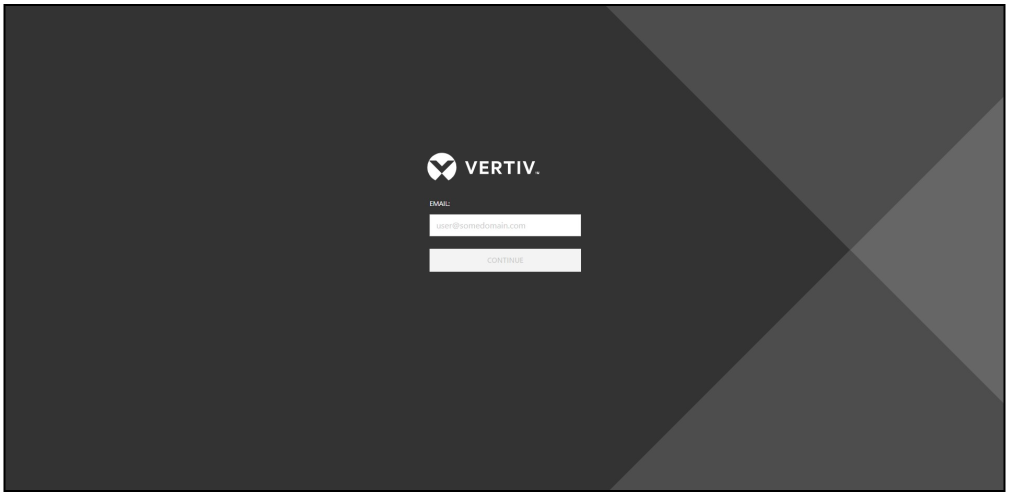


Figure 3.2

NOTE:

- **The email address entered only receives alert notifications and not your account name. The default account name for the application is "admin".**
- **In addition to the default email address, users can also add different e-mail addresses to the system to receive alert notifications, specifically referring to the "other address book settings" in Detailed Features on page 60 .**

4. Create a *new password*and enter the Password and Confirm Password fields, and then click *Continue.*

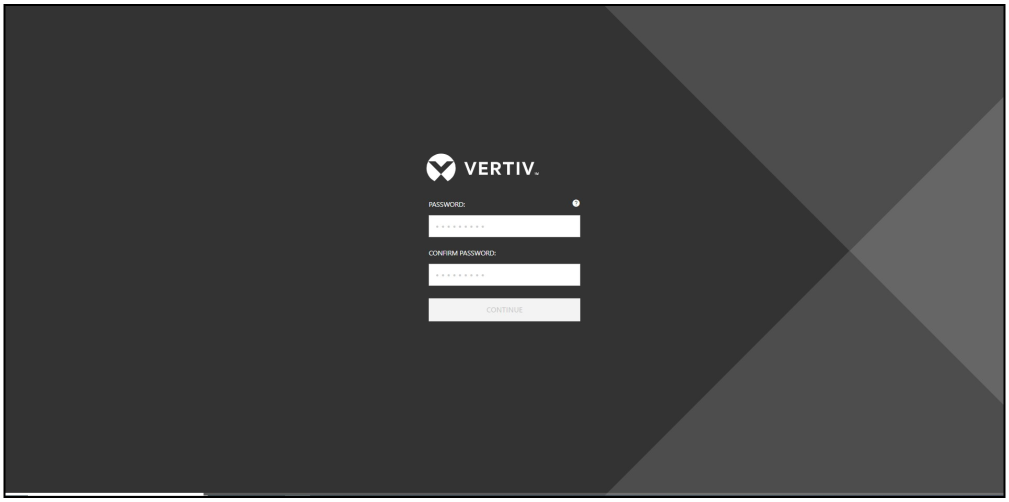


Figure 3.3

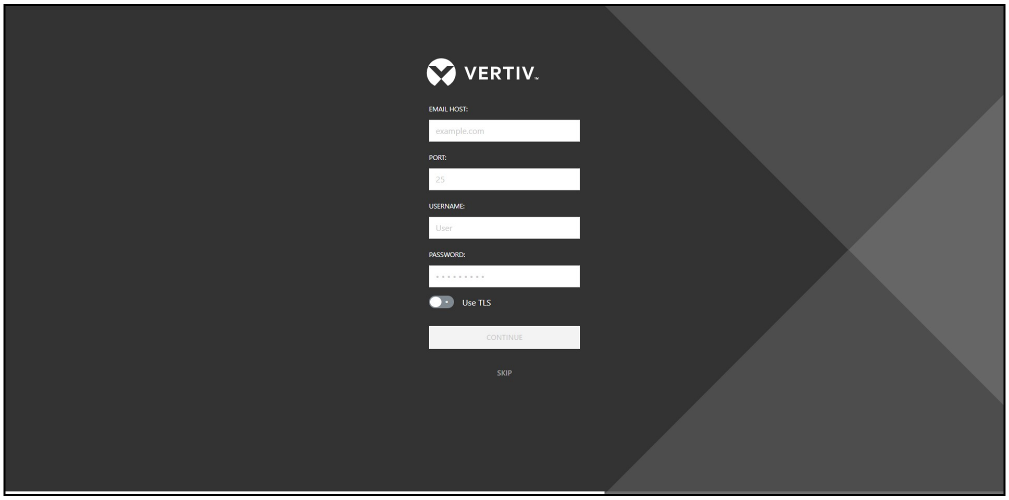
NOTE: Passwords must be between 10 and 128 characters long and contain at least one capital letter, one lowercase letter, and one number.

5. Select *the configuration*. If you need to configure your email server in advance, click *Configure the server.*
   - Or-
   Click *Skip* and go to step 7.

NOTE: If the e-mail server is not configured at this time, you can also complete the configuration by accessing to Email and SMS notification settings on page 62 to complete the configuration.

Enter the *IP address or host name of the e-mail server* in the E-Mail Host field. Enter the *email port number* (the default is 25), email server account name, and password in the appropriate field. Click the *Use TLS slider* to enable secure communication. When complete, click *Continue.*

NOTE: The Use TLS button is enabled by default. When enabled, an email server account name and password is required. When disabled, an email server account name and password is not required.



EMAIL HOST: example.com

PORT: 25

USERNAME: User

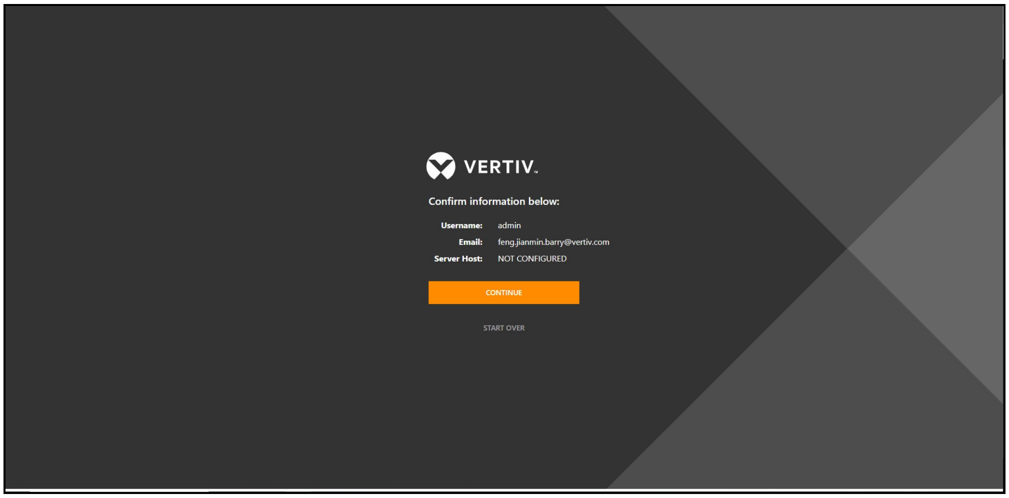
PASSWORD: •••••••••

Figure 3.4

Go to Installation of the software on page 3 to start the initial sign-in process from scratch, click *Start Over*.

- Or-

Go to Software Login and Main Interface on page 21 click Continue in the next window. Complete the registration.



Confirm information below:

Username: admin

Email: feng.jianmin.barry@vertiv.com

Server Host: NOT CONFIGURED

Figure 3.5

3.1.2 User login

You can log in once you're registered.

Sign in Steps:

1. Open *a web browser on your local computer* and enter*"https://localhost:SERVICE_PORT*."where the <service port> is the service port number, such as 8443. In this example, the address is "https://localhost:8443".
   - Or-
   On the computer on which the application is installed, double-click *the Power Insight Console shortcut icon*.

Figure 3.6

2. To login on a remote computer, enter *"https:// <remote IP address>: <service port>*; where the <remote IP address> is the IP address for the installation of Power Insight, and the <service port> is the service port number, for example, 8443.
3. Enter *your username (admin by default) and password*, and then click *login*. Complete your *login*.Please refer Figure 3.7 below

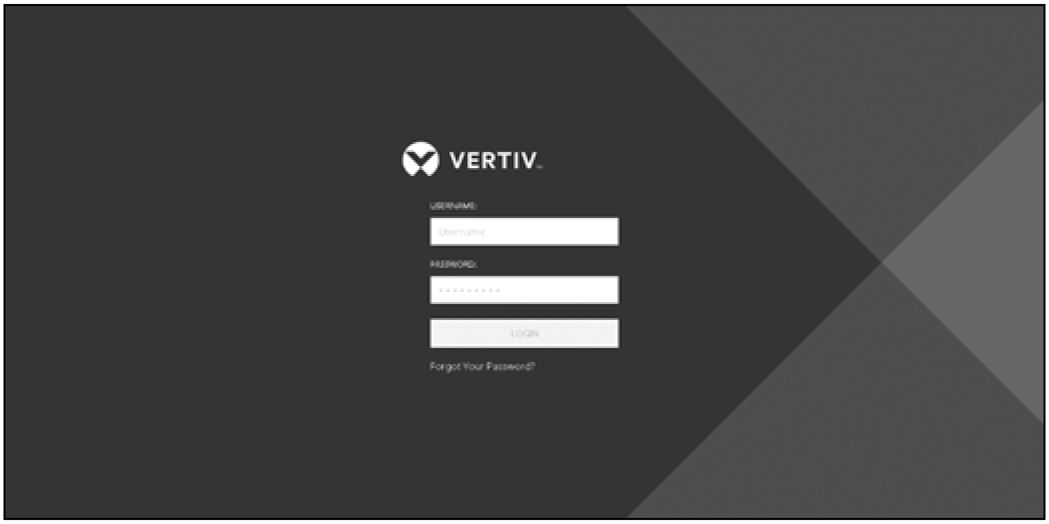


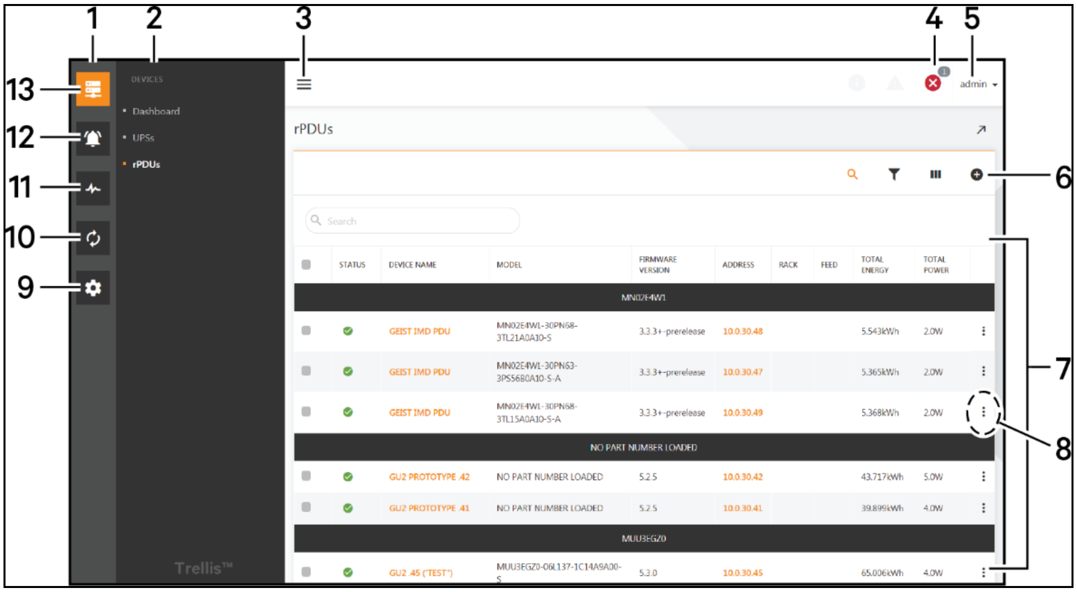
Figure 3.7

3.2 User Interface

The user interface contains several areas that help you manage the devices being monitored by the Power Insight application. The pivot bar and context menu on the left contain items that provide access to devices, alarm information, discovery configurations and administrative tools. The pivot bar and context menu can be expanded or collapsed using the menu icon at the top of the window.

Alarm notifications on the top right corner of the window are activated when SNMP traps are triggered from the device. The Profile icon, also on the top right corner of the window, is used to sign-out, set profile information and access help topics. Use the icons on the toolbar to customize each window or complete tasks.

Icons that allow you to customize the content information are static and appear on the toolbar when you access the window. Icons that allow you to complete tasks can be accessed in two ways. You can select a row in the table to view and use the available icons on the toolbar or select the vertical ellipsis icon in the row to access the same icons. In the following sections, you will be guided to select the vertical ellipsis icon to access these icons.



	STATUS	DEVICE NAME	MODEL	FIRMWARE VERSION	ADDRESS	RACK	FEED	TOTAL ENERGY	TOTAL POWER	
MN02E4W1										
□	✓	GEIST IMD PDU	MN02E4WL-30PN68-3TL21A0A10-S	3.3.3+-prerelease	10.0.30.48			5.543kWh	2.0W	⋮
□	✓	GEIST IMD PDU	MN02E4WL-30PN63-3PS56B0A10-S-A	3.3.3+-prerelease	10.0.30.47			5.365kWh	2.0W	⋮
□	✓	GEIST IMD PDU	MN02E4WL-30PN68-3TL15A0A10-S-A	3.3.3+-prerelease	10.0.30.49			5.368kWh	2.0W	⋮
NO PART NUMBER LOADED										
□	✓	GU2 PROTOTYPE .42	NO PART NUMBER LOADED	5.2.5	10.0.30.42			43.717kWh	5.0W	⋮
□	✓	GU2 PROTOTYPE .41	NO PART NUMBER LOADED	5.2.5	10.0.30.41			39.899kWh	4.0W	⋮
MUU3EGZ0										
□	✓	GU2 .45 ('TEST')	MUU3EGZ0-06L137-1C14A9A00-S	5.3.0	10.0.30.45			65.006kWh	4.0W	⋮

Figure 3.8

Number	Name	Description
1	Pivot bar	Provides access to the Devices (devices on a network icon), Alarms (bells icon), Monitoring (heart monitor icon), Automation (process arrows icon), Administration (gear icon) and App Manager (grid icon) context menus
2	Context menu	Provides the list of options for the selected icon from the pivot bar.
3	Expand menu icon	Expands or collapses the pivot bar and context menu.
4	Alarm notifications	Incremental alarm notifications for warning and critical alarms.
5	Profile menu	System and user tools such as help, password reset, application and email settings for the current user.
6	Toolbar	Contains icons that allow you to perform various functions for a selected row or an entire table.
7	Table	Details concerning the menu item selected. Each row contains a vertical ellipsis icon at the right end that expands to display functions that can be performed on the row.
8	Vertical ellipsis icon	Contains the function icons that allow you to edit, delete and run a configuration or view details.

Number	Name	Description
9	Administration	Contains context menu items: • Events • Notification Settings • System Settings • User Defined Properties • System Health • Address Book Contacts • Trust Store
10	Monitoring	Contains context menu items: • Discovery Configurations • Discovered Devices • Communication Profiles • Server Shutdown Profiles
11	Alarms	Contains context menu items: • Alarms • Active Alarms • Alarm History Automation • Actions • Action Sets • Automation Rules
12	Devices	Contains context menu items: • Dashboard • UPSs • rPDUs

4 Add UPS, rPDU

4.1 Overview

The first step in running Power Insight is to add the UPS or rPDU that needs to be monitored to the device list, and when you're done, real-time data and alert information for your device is available.

4.2 Get started quickly

4.2.1 Quick deployment steps

Adding a UPS or PDU can be done in two ways

1. Add manually
2. Search Add

4.2.2 Example

Add UPS manually

1. Select *Device List in the level 1 menu*, and to add *a device that is UPS*, click *"UPSs" in the secondary menu*. The page as shown below is displayed:

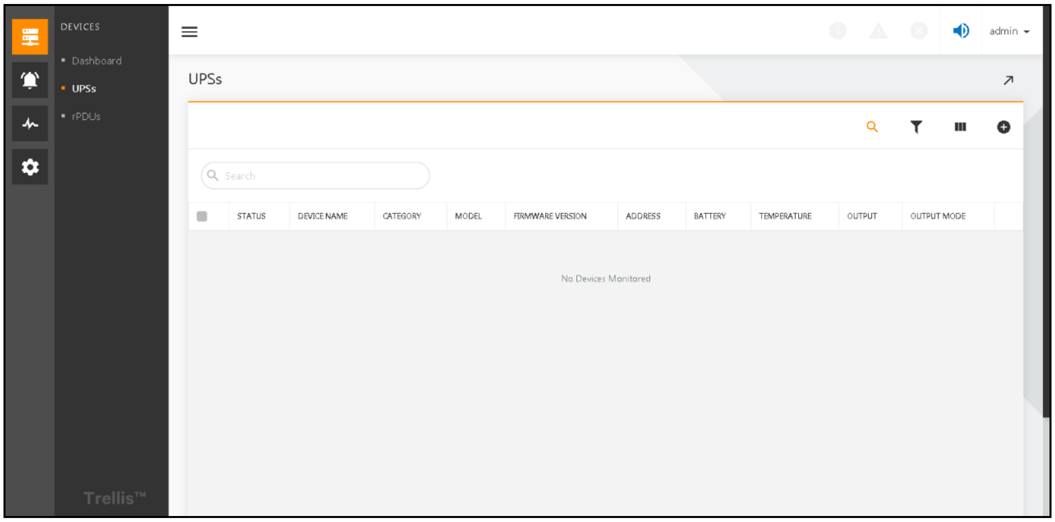
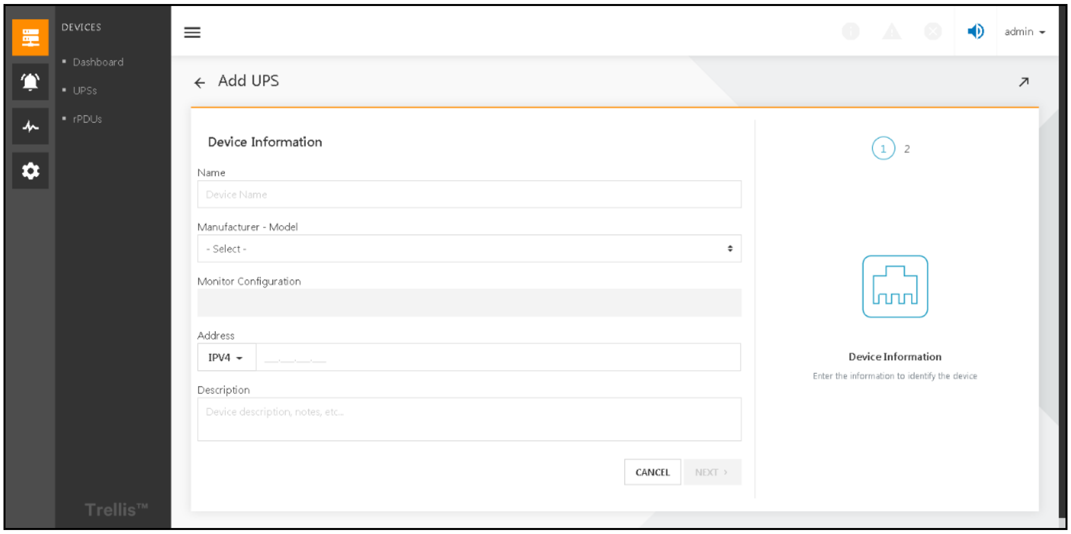


Figure 4.1

2. Click *on the* *sign in the upper right corner to go to the device configuration page.*



Device Information

Name: Device Name

Manufacturer - Model: - Select -

Monitor Configuration

Address: IPV4 ___.___.___.___

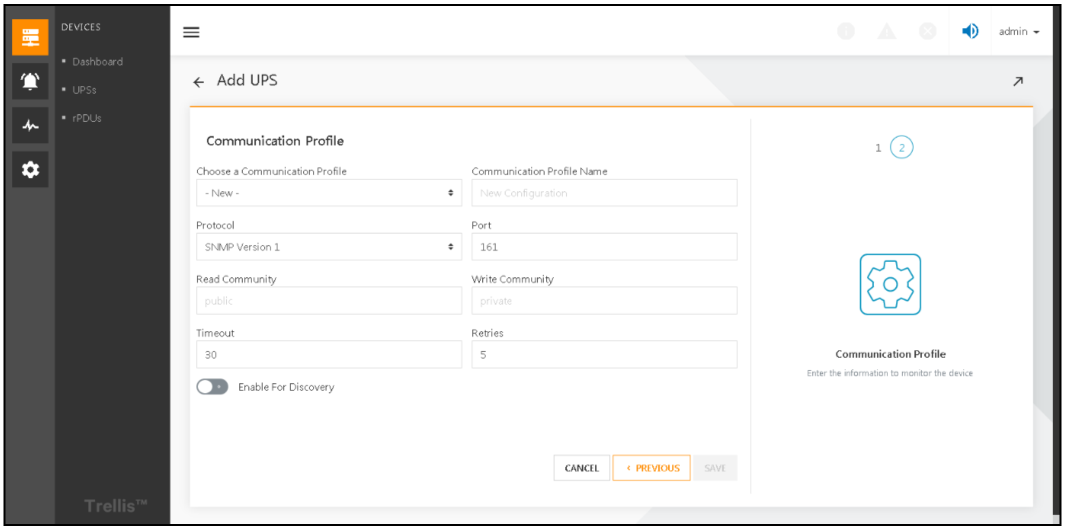
Description: Device description, notes, etc...

Device Information

Enter the information to identify the device

Figure 4.2

3. Fill in the *name of the device, manufacturer model (i.e. UPS model), monitor configuration (communication card model), IPV4 address (IP address of the communication card) and other relevant parameters*, click the *next step* into the communication profile page. (For specific parameters refer to Add a device UPS on page 33).



Communication Profile

Choose a Communication Profile: - New -

Communication Profile Name: New Configuration

Protocol: SNMP Version 1

Port: 161

Read Community: public

Write Community: private

Timeout: 30

Retries: 5

Enable For Discovery

Communication Profile

Enter the information to monitor the device

Figure 4.3

4. In the communication profile page, choose *communication profile from existing configuration*, generally select SNMPv2, other parameters will be filled in accordingly. Then click “*Save*” and the entire UPS manual addition process is complete. (For specific parameters refer to Add a device UPS on page 33).

NOTE: Additionally, to configure SNMP on the Power Insight, also configure SNMP on the communication card side and add the IP address of the server installed by Power Insight to the SNMP white list of the communication card. Similarly, pay attention to reading communication words and writing communication words to be consistent.

Add PDU manually

1. Select *Device List* in the level 1 menu , and to add a device that is PDU, click *"PDUs*" in the secondary menu. The page as shown below is displayed.

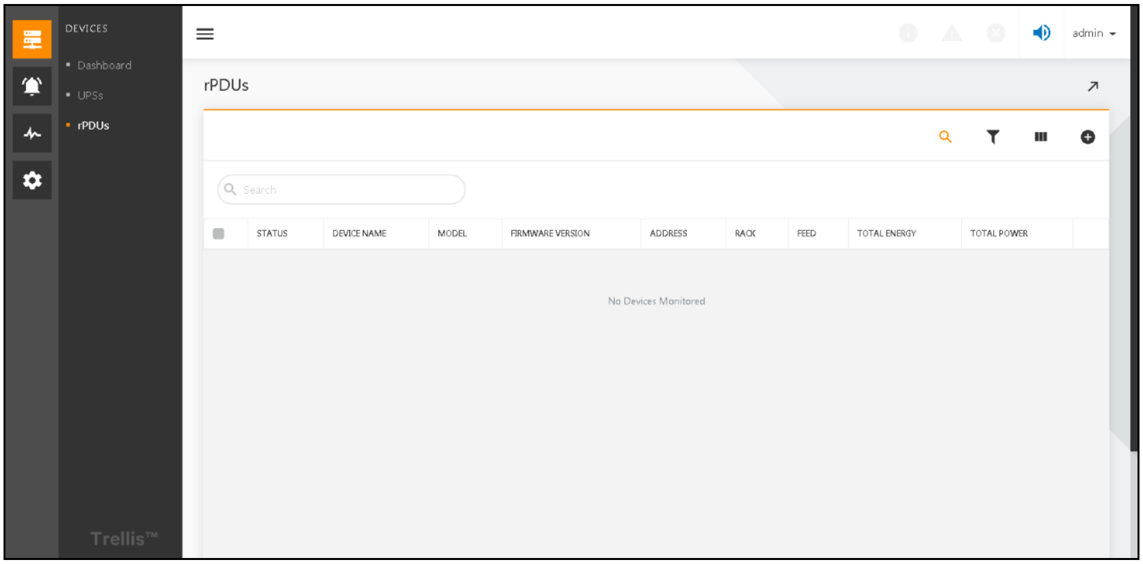


Figure 4.4

2. Click on the "⊕ " *sign* in the upper right corner to go to the device Information page.

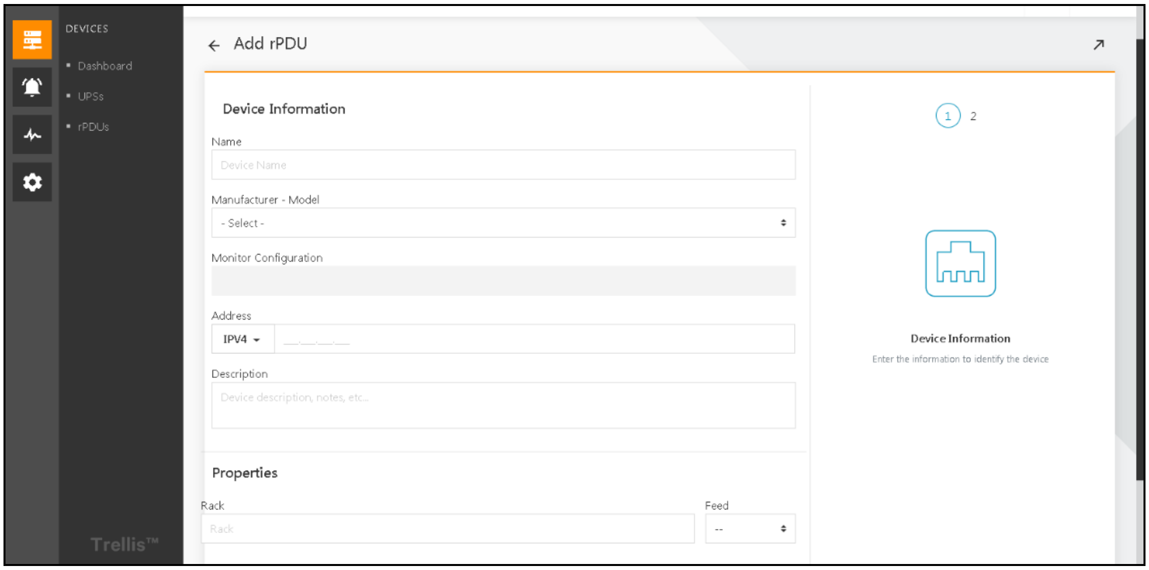
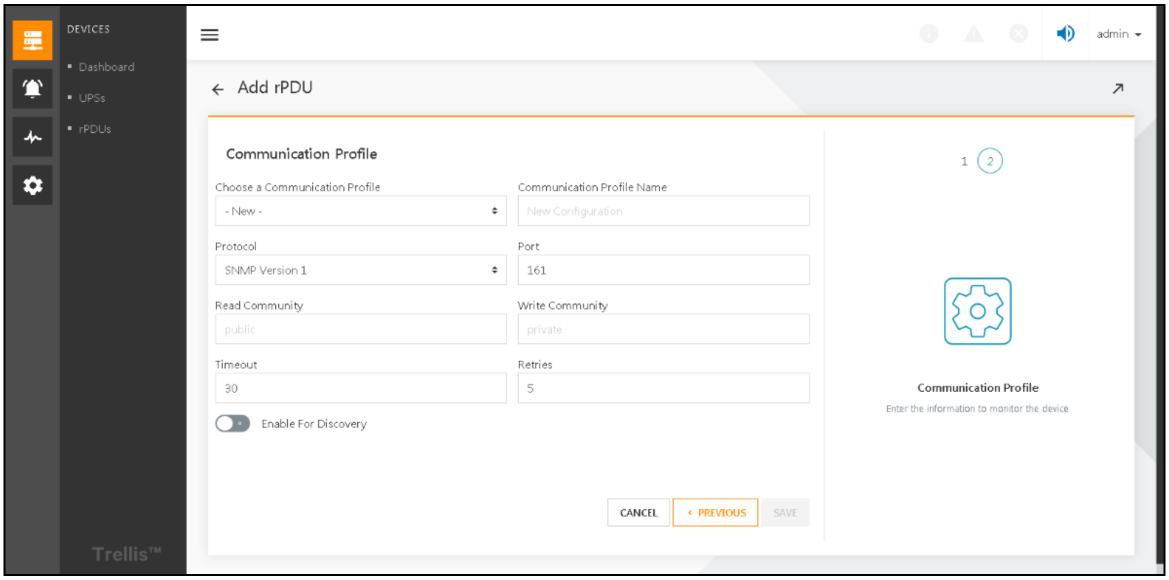


Figure 4.5

3. Fill in the *name of the device, manufacturer model (i.e. PDU model), monitoring configuration (communication card model), IPV4 address (IP address of the communication card) and other relevant parameters*, click *the next step* into the communication profile page. (For specific parameters refer to Add a device UPS on page 33).



Add rPDU

Communication Profile

Choose a Communication Profile: - New -

Communication Profile Name: New Configuration

Protocol: SNMP Version 1

Port: 161

Read Community: public

Write Community: private

Timeout: 30

Retries: 5

Enable For Discovery

CANCEL ‹ PREVIOUS SAVE

Communication Profile

Enter the information to monitor the device

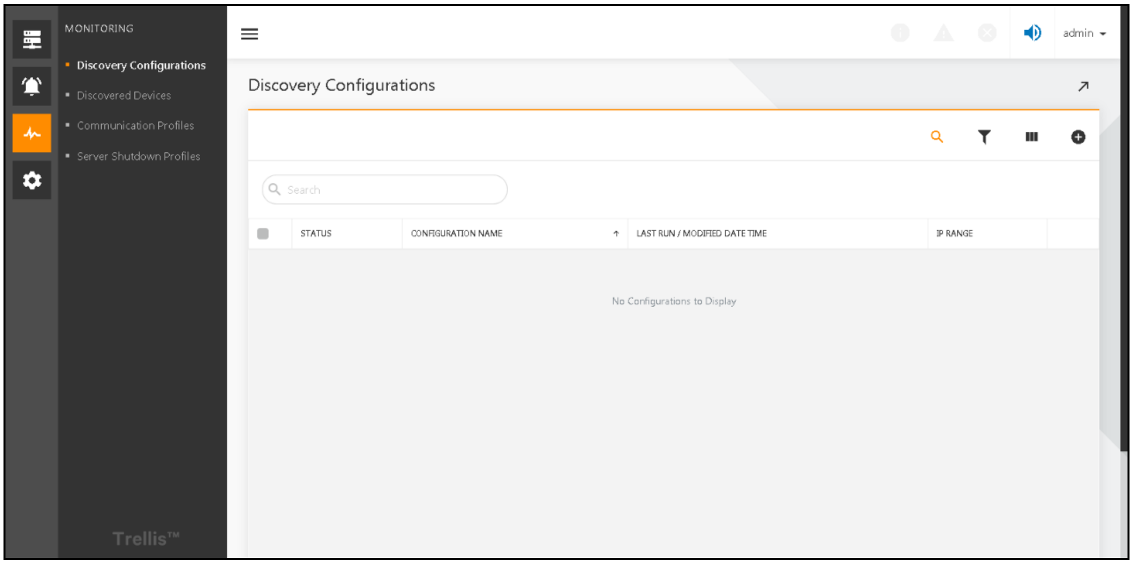
Figure 4.6

4. In the communication file page, choose communication profile from existing configuration, generally select *SNMPv2*, other parameters will be filled in accordingly. Then click *Save*, the entire PDU manual lying process is complete. (For specific parameters refer to Add a device UPS on page 33)

NOTE: Additionally, to configure SNMP on the Power Insight, also configure SNMP on the acquisition card side and add the IP address of the server installed by Power Insight to the SNMP white list of the acquisition card while taking care to keep the word read and write consistent.

Auto discovery configuration

1. Select Monitoring “ ”in the level 1 menu and click Discovery Configuration in the secondary menu. The page as shown is displayed.



Discovery Configurations

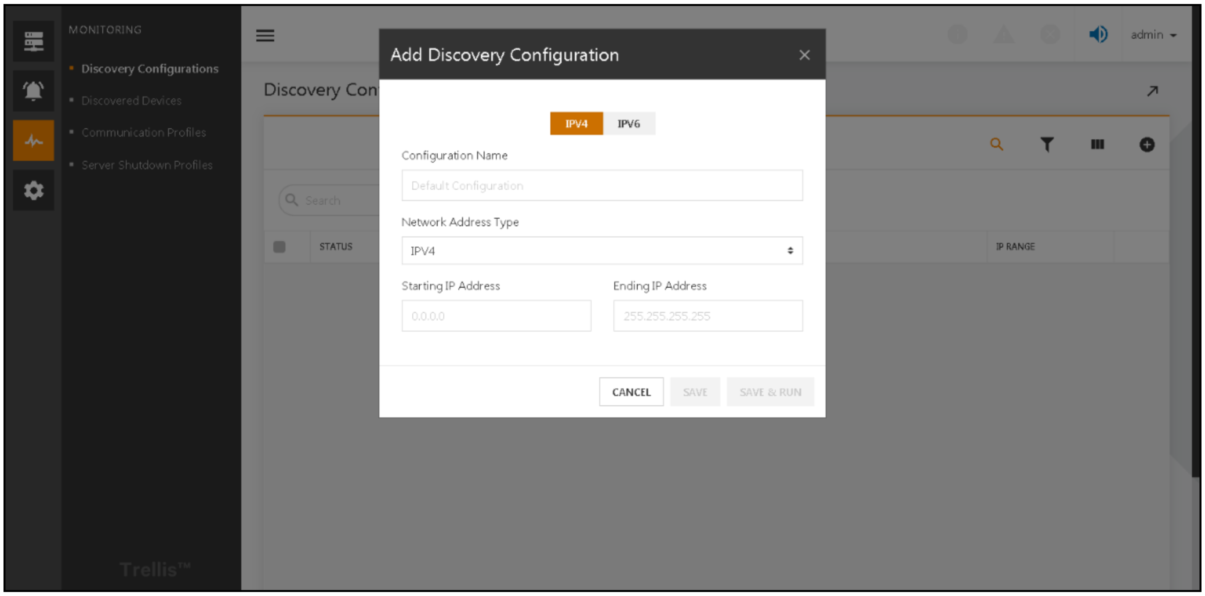
Search

	STATUS	CONFIGURATION NAME	LAST RUN / MODIFIED DATE TIME	IP RANGE

No Configurations to Display

Figure 4.7

2. Click on the ⊕ *sign* in the upper right corner. The "Add Discovery configuration" pop up window will display.



Add Discovery Configuration

Configuration Name: Default Configuration

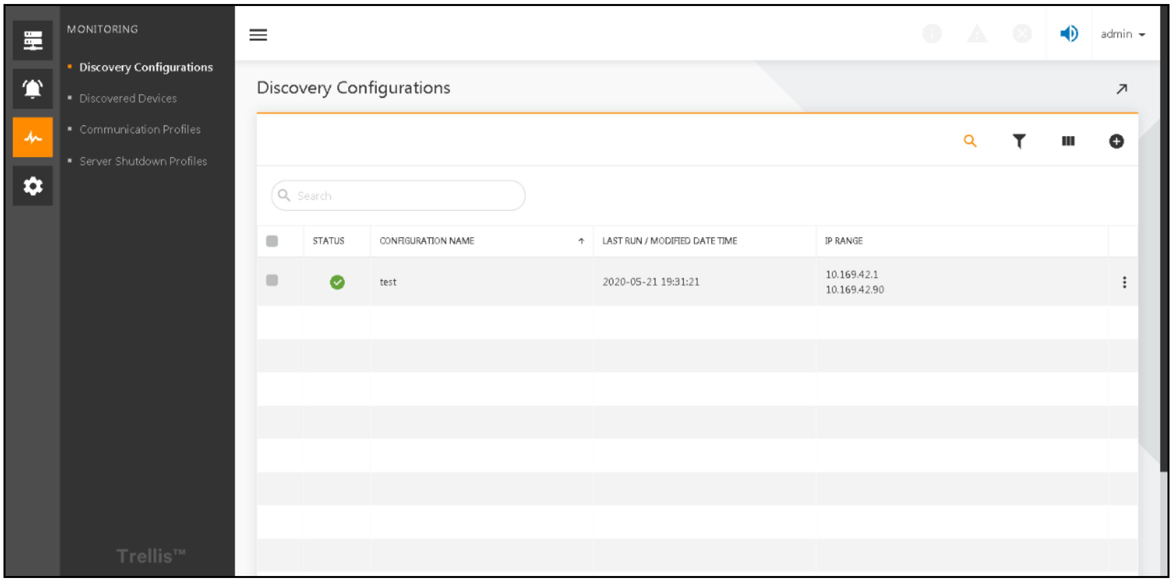
Network Address Type: IPV4

Starting IP Address: 0.0.0.0

Ending IP Address: 255.255.255.255

Figure 4.8

3. Fill in *the configuration name, network address type (IPV4 or IPV6), starting IP address, ending IP address 4 parameters*, click *Save and run.*
4. When the run is over, the status turns green. Refer **Figure 4.9** below .

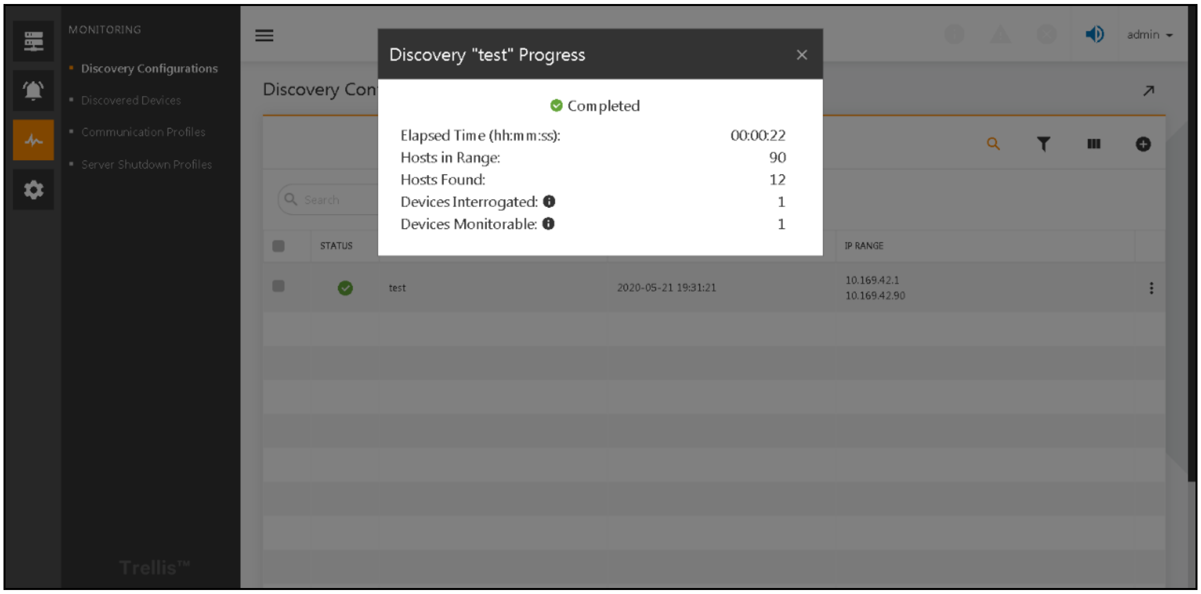


Discovery Configurations

STATUS	CONFIGURATION NAME	LAST RUN / MODIFIED DATE TIME	IP RANGE
✓	test	2020-05-21 19:31:21	10.169.42.1 10.169.42.90

Figure 4.9

5. Click *on the green icon and the pop-up window shows the number of devices searched for to communicate:*



Discovery "test" Progress

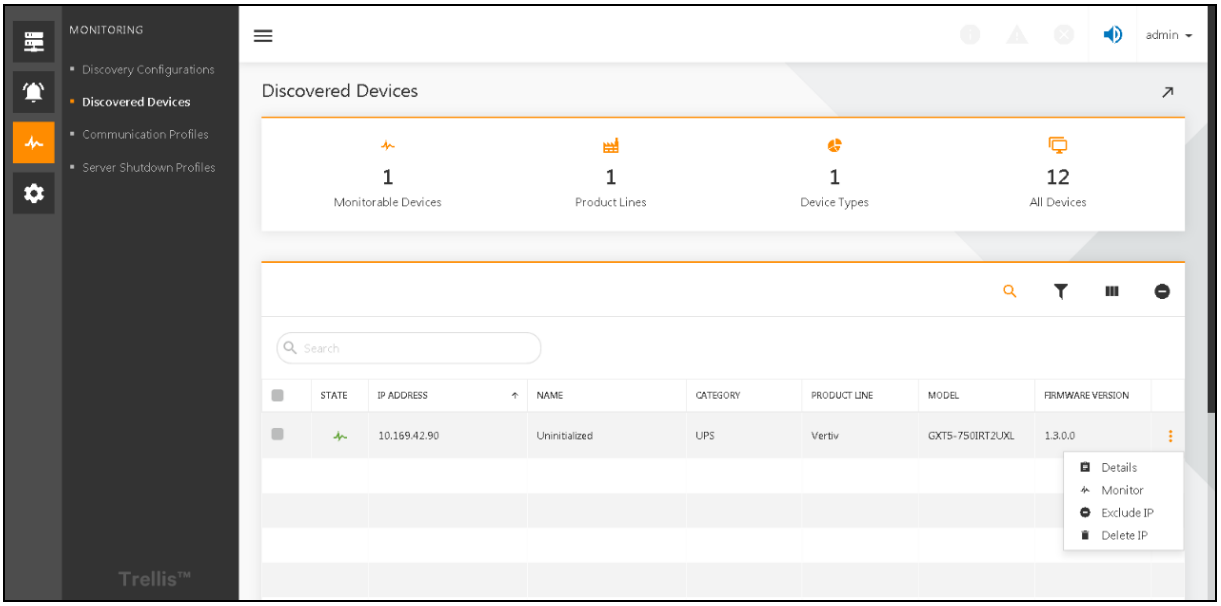
Completed

Elapsed Time (hh:mm:ss):	00:00:22
Hosts in Range:	90
Hosts Found:	12
Devices Interrogated:	1
Devices Monitorable:	1

STATUS			IP RANGE
✓	test	2020-05-21 19:31:21	10.169.42.1 10.169.42.90

Figure 4.10

6. If the number of monitorable devices is greater than one, click *"Discovered Devices" in the level 2 (secondary) menu which displays specific communicable devices. Click the ellipsis "⋮"on the right side of the "firmware version" and click on "Monitor".*



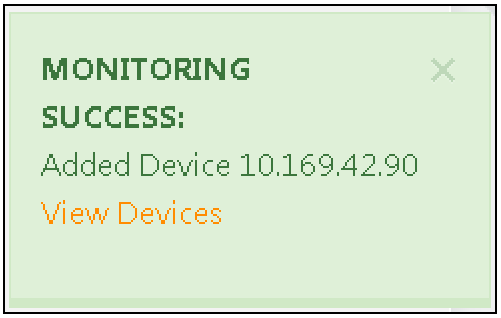
Discovered Devices

1	1	1	12
Monitorable Devices	Product Lines	Device Types	All Devices

STATE	IP ADDRESS	NAME	CATEGORY	PRODUCT LINE	MODEL	FIRMWARE VERSION
	10.169.42.90	Uninitialized	UPS	Vertiv	GXT5-750IRT2UXL	1.3.0.0

Figure 4.11

7. If there is no problem, a green window pops up in the lower right corner to indicate that the device was added successfully.



MONITORING SUCCESS:

Added Device 10.169.42.90

View Devices

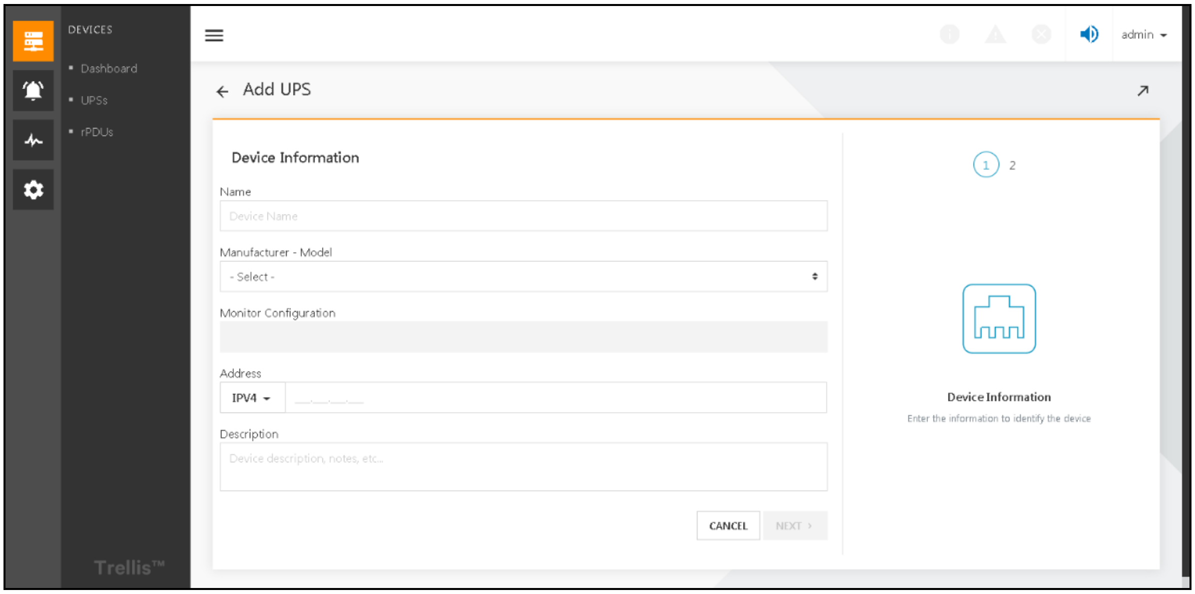
Figure 4.12

NOTE: Additionally, to configure SNMP on the Power Insight, also configure SNMP on the acquisition card side and add the IP address of the server installed by Power Insight to the SNMP white list of the acquisition card while taking care to keep the word read and write consistent.

4.3 Detailed Features

4.3.1 Add a device UPS

Click on *the first-level menu to select "Monitor", click on "Discovery Configuration" in the secondary menu*, then click *on the "+" sign in the upper right corner*, enter *the add device UPS page*, enter *the following information*: *name (UPS name, user-customizable), manufacturer-model (actual UPS model), monitoring configuration (UPS communication card model), address (UPS IP address), description (device description, information, cannot be filled in)*. When you're done, click "*Next*".



Add UPS

Device Information

Name

Device Name

Manufacturer - Model

- Select -

Monitor Configuration

Address

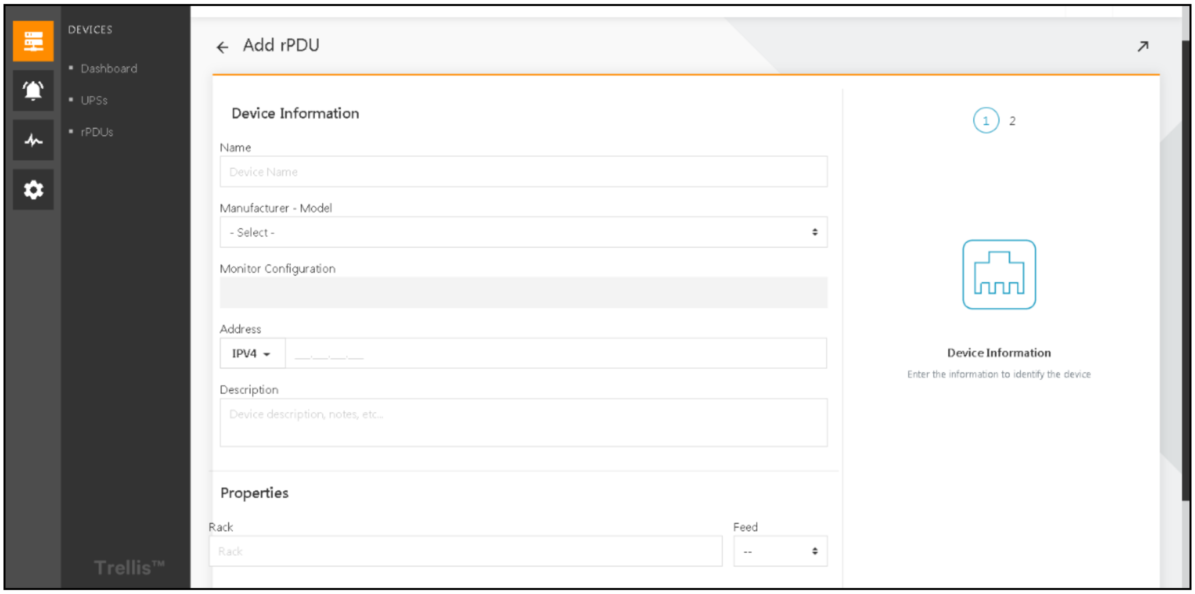
IPV4 ▾ ___.___.___.___

Description

Device description, notes, etc...

Figure 4.13

For rPDUs, in addition to the above parameters, Properties section is added. Users can enter: rack (rack name, not filled), feed (feed phase A or B, cannot be filled).



Device Information

Name: Device Name

Manufacturer - Model: - Select -

Monitor Configuration

Address: IPV4 ___.___.___.___

Description: Device description, notes, etc...

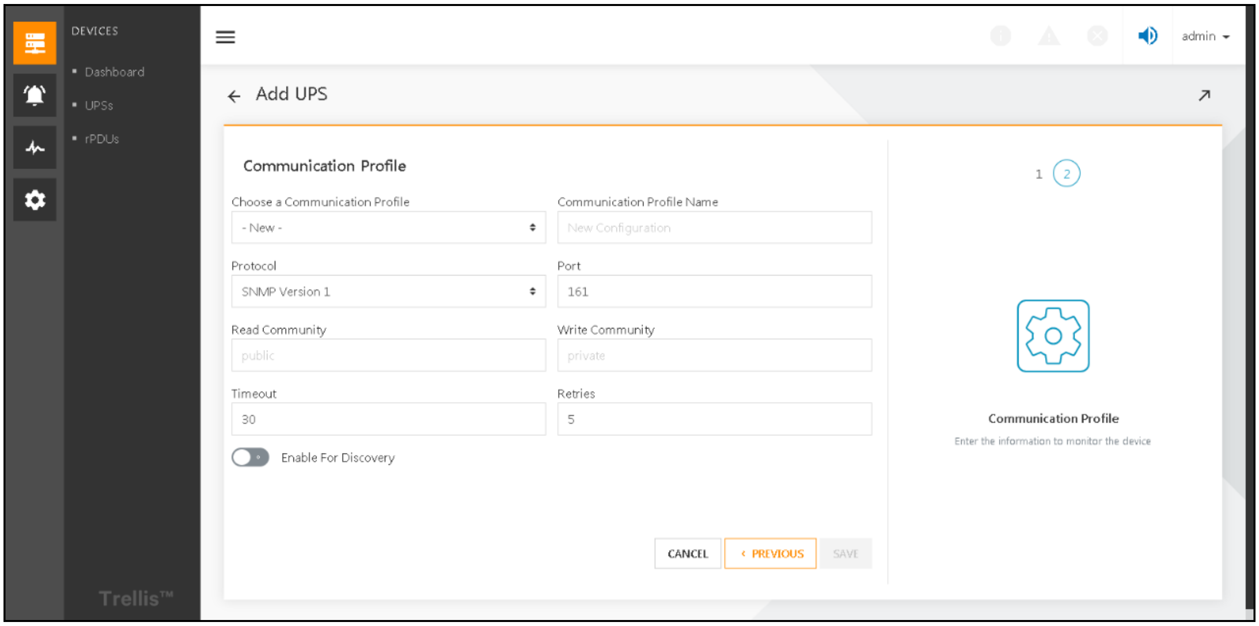
Properties

Rack: Rack

Feed: --

Figure 4.14

Go to *the second page of Add UPS and enter the following information*: Select *the device communication profile (which contains all the default communication profile options), the communication profile name (the name of the communication profile, which the user can customize), the protocol (SNMP protocol type, V1, V2, V3), the port (communication port, default is 161), read community (SNMP's read operation password), write community (SNMP's write operation password), time out (no response time for the operation, if the time is exceeded, the same operation will be re-performed), retries (time-out retry), enable for discovery (used for device search).* When you're done, click *"Save"*.



Communication Profile

Choose a Communication Profile: - New -

Communication Profile Name: New Configuration

Protocol: SNMP Version 1

Port: 161

Read Community: public

Write Community: private

Timeout: 30

Retries: 5

○ Enable For Discovery

Figure 4.15

5 Device Monitoring

5.1 Overview

After adding UPSs or PDUs they can be monitored. The Power Insight interface helps to monitor device's power parameter information (input, output, load, etc.) and environmental parameter information (temperature). If a device is not added, refer to Add UPS, rPDU on page 27 .

5.1.1 Function Module

- Status panel
- List on devices
- Device real-time signal
- Device details
- Alert Notice

5.2 Get started quickly

5.2.1 Quick Deployment Steps

1. Refer Quick deployment steps on page 27 .
2. Quickly monitor entrances:
    - Click on the 🖥 , then click on the Status panel to browse the global device status statistics.
    - Click on the 🖥 , then click on the UPS list and browse the asset information and real-time status for all UPS devices.
    - Click on 🖥 , and then click on the PDU, enter the PDU list and browse through the asset information and real-time status for all PDU devices.
    - In the list of UPS or PDU, click the button on the right side of the list and select the device details in the list, click on the ⋮ pop-up box to view the device's detailed assets.
    - In the list of UPS or PDU, click the button on the right side of the list and select the device's live signal in the pop-up box to monitor the device's detailed real-time status.

5.2.2 Example

Refer Example on page 27 .

5.3 Detailed Features

5.3.1 Dashboard

Each time you log in, you have an at-a-glance overview of all the devices monitored by the application via the Dashboard.

Click on *the list of devices* 🖥 in the level one directory will enter the dashboard interface by default.

Dashboard (shown in **Figure 5.1** on the next page)

It displays status of all UPS devices on the left half portion and status of all rPDU devices on the right half portion. Above the UPS or PDU icon indicates the total number of devices that are currently monitored by the application, and below the icon indicates the number of devices in various states. The UPS device status are further divided by its mode of operation and number of alarms its generating such as “In alarm”(UPS devices with one or more active alarms), “In bypass” (number of devices that are receiving power directly from an electric utility, bypassing the UPS), “Offline” (UPS devices that are not sending data to the application), and “Battery mode” (Number of devices that are receiving power from a UPS not receiving power from an electric utility). The PDU device status are further divided by important alarms such as “In Warning” (number of rPDU devices with one or more active warnings), In Critical (number of rPDU devices with one or more critical warnings), and Offload (rPDU devices that are not sending data to the application). The pie chart on the left is a summary of the state of the device: it shows green when all devices are online and in a normal state, it shows red-green pie chart in proportion when there is an abnormal state of the devices.

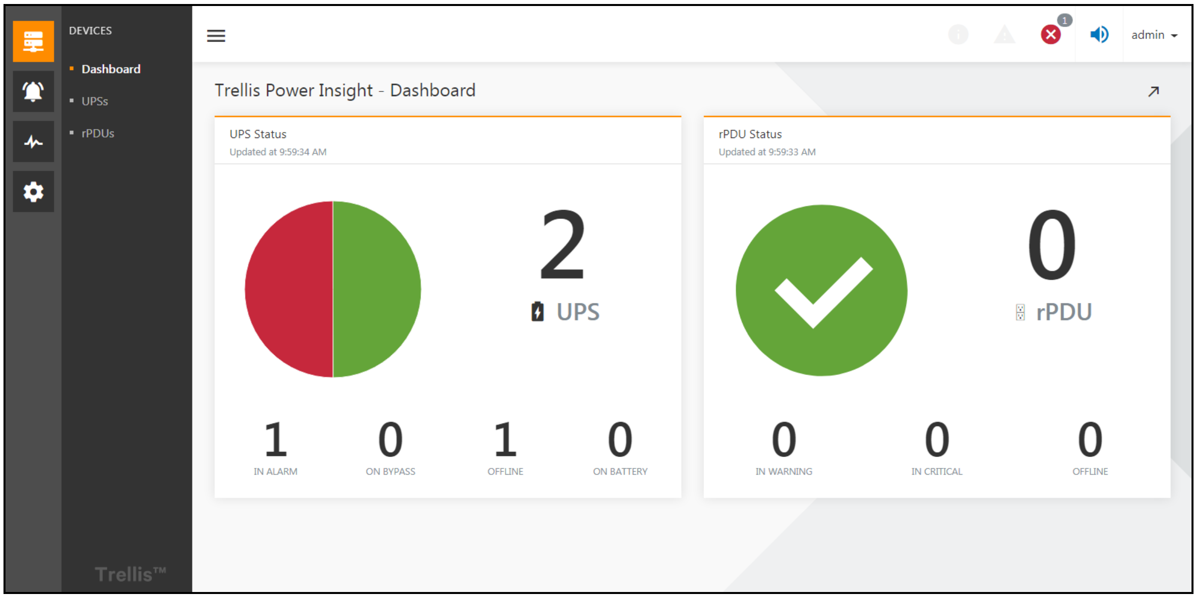


Figure 5.1

Each category shown on the System Status panel is a link that directs you to a Device List window that only displays the devices in that category.

5.3.2 Device List

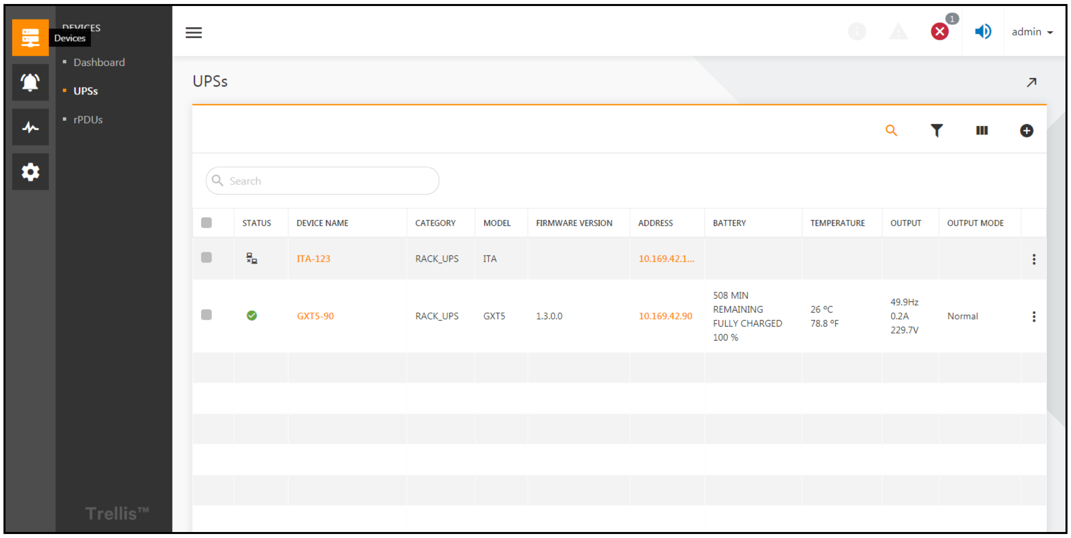
Select the *Devices icon* to access the Device List window. This window allows you to add or access devices monitored by the application. The Device List window contains the following information for each monitored power supply:

NOTE: Some categories are hidden by default. To view all categories, click the *Columns Icon*.

The UPS list has the following twelve columns as shown in Figure 5.2 on the facing page .

1. Check the *box*: You can use this to select the device when you perform batch operations on the device.
2. Status: The real-time status of the device is displayed by icon, there are three kinds of status: normal, alarm, and offline.
3. Device name
4. Category: Product category
5. Model: Product-specific model
6. Firmware version: Firmware version of the UPS
7. Address: IP address of UPS communication card

8. Battery: UPS battery state, with three lines of information: battery remaining available time, battery drain status, percentage of remaining charge
9. Temperature: divided into degrees Celsius and Fahrenheit
10. Output: divided into three lines: output frequency, output current, output voltage
11. Output mode: Characterizes the state in which the output of UPS is in, there are four types: Normal, Off, Bypass Mode, and Battery Mode. Bypass mode indicates direct use of power supply, and battery mode indicates that UPS is powered by battery.
12. Drop-down selection box: After clicking, three selection items will pop up, device detailed information, device real-time signal, and delete. You can jump to device detailed information, device real-time signal, and delete device, respectively.



□	STATUS	DEVICE NAME	CATEGORY	MODEL	FIRMWARE VERSION	ADDRESS	BATTERY	TEMPERATURE	OUTPUT	OUTPUT MODE	
□		ITA-123	RACK_UPS	ITA		10.169.42.1...					⋮
□	✓	GXT5-90	RACK_UPS	GXT5	1.3.0.0	10.169.42.90	508 MIN REMAINING FULLY CHARGED 100 %	26 °C 78.8 °F	49.9Hz 0.2A 229.7V	Normal	⋮

Figure 5.2

The rPDU list has the following twelve columns:

1. Check the *box*: You can use this to select the device when you perform batch operations on the device.
2. Status: The real-time status of the device is displayed by icon, there are three kinds of status: normal, alarm, and offline.
3. Device name
4. Category: Product category
5. Model: Product-specific model
6. Firmware version: Firmware version of the rPDU
7. Address: IP address of rPDU communication card
8. Rack
9. Feed
10. Total energy
11. Total power
12. Drop-down selection box: After clicking, three selection items will pop up, device detailed information, device real-time signal, and delete. You can jump to device detailed information, device real-time signal, and delete device, respectively.

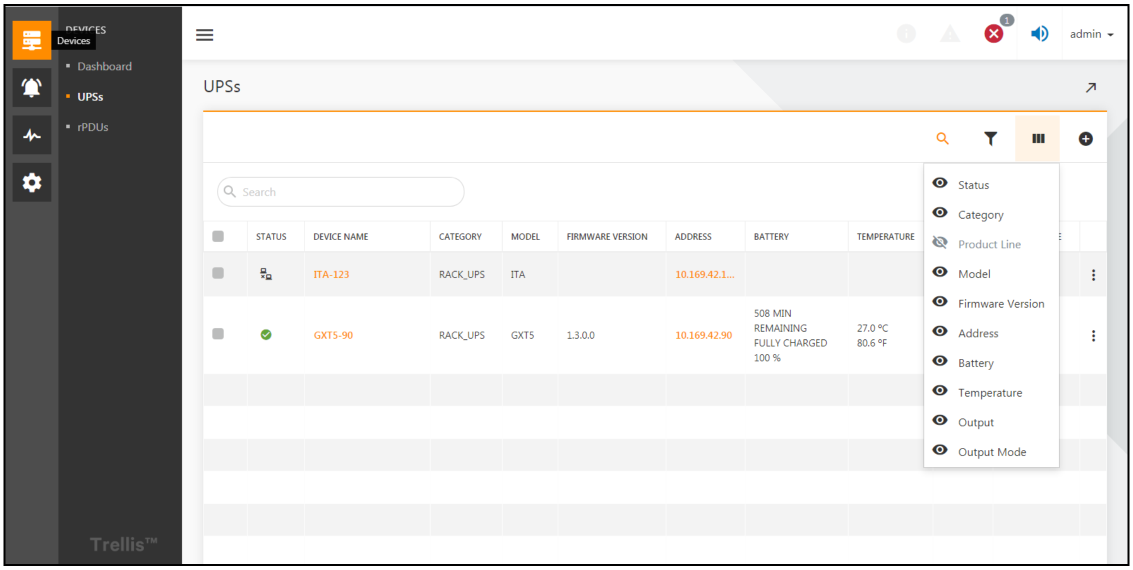
Common list of operations:

Search for a device:

As shown in **Figure 5.2** on the previous page , there is a search 🔍 button in the upper right corner of the list. Click the button to display or hide the search bar. By entering information in the search bar, such as GXT5, you can filter the items in the list against the keyword GXT5 and filter out the item that contains GXT5 information. Search information supported by different lists is inconsistent. For example, the UPS list only supports searching the device names, categories, models, firmware versions, and addresses.

Column Hide:

As shown in **Figure 5.3** below , clicking on the ▥ button in the upper right corner of the list will bring up a drop-down box which lists columns that can be hidden. Click the *drop-down box option* to show or hide the column. 👁 Indicates that the column is being displayed, 👁 indicates that the column is hidden.

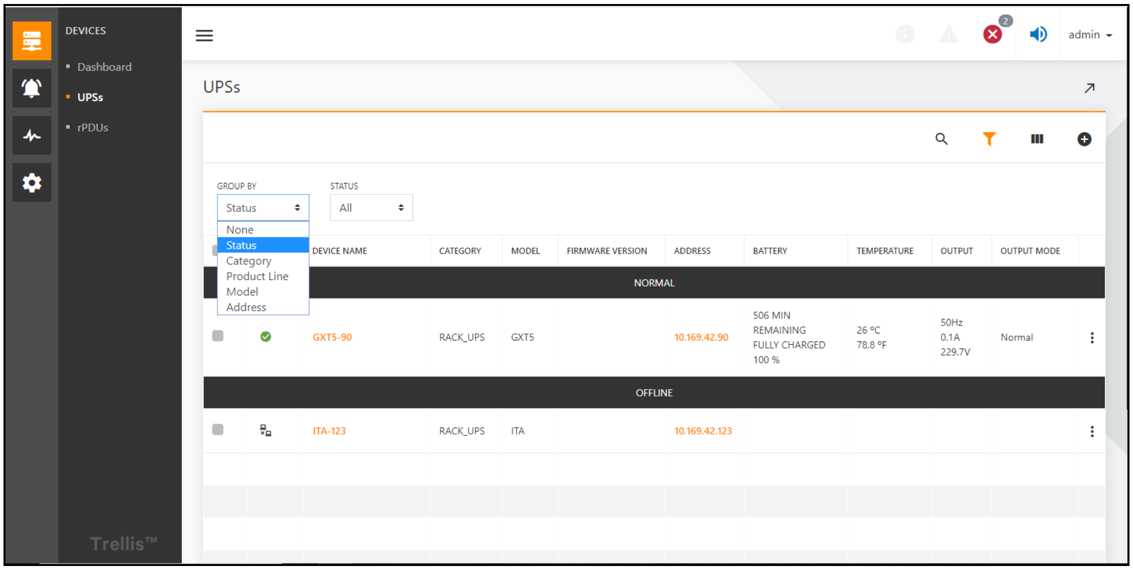


	STATUS	DEVICE NAME	CATEGORY	MODEL	FIRMWARE VERSION	ADDRESS	BATTERY	TEMPERATURE
□		ITA-123	RACK_UPS	ITA		10.169.42.1...		
□	✓	GXT5-90	RACK_UPS	GXT5	1.3.0.0	10.169.42.90	508 MIN REMAINING FULLY CHARGED 100 %	27.0 °C 80.6 °F

Figure 5.3

Item filtering:

As shown in **Figure 5.4** on the facing page , there is a filter button “▼” in the upper right corner of the list and click to display or hide the filter options bar (shown in the top left of **Figure 5.4** on the facing page). There are two single selection drop-down boxes in the filter options bar for grouping and status. Selecting grouping can help you group and display list items, as shown in **Figure 5.4** on the facing page . In addition to selecting grouping, the other drop-down boxes are used to filter the status of the listed devices. As shown in **Figure 5.5** on the facing page , the device is filtered for status properties, and only devices whose status is offline are displayed.



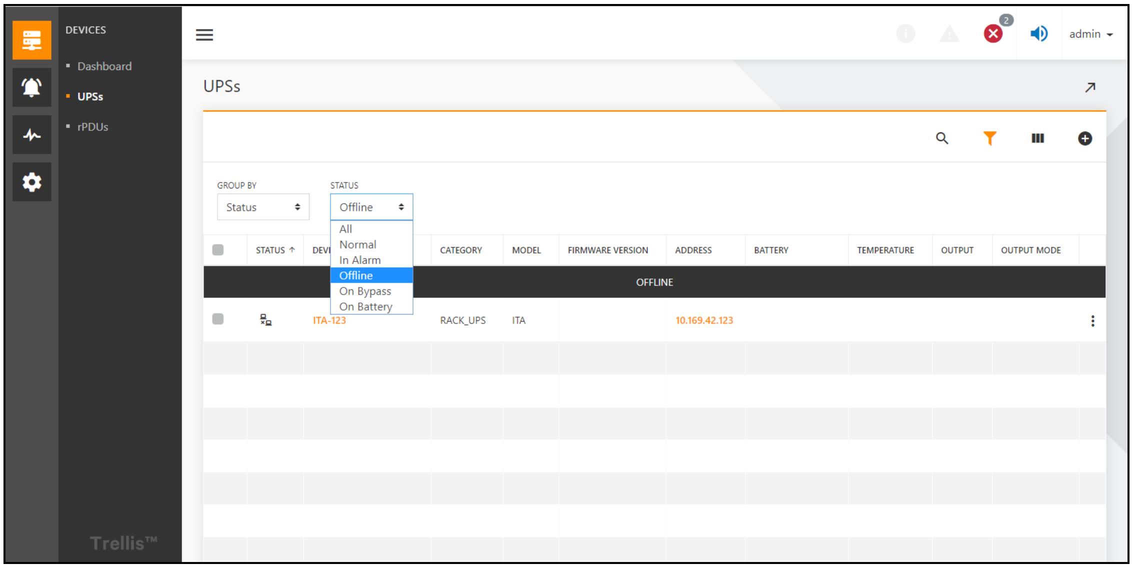
UPSs

GROUP BY: Status

STATUS: All

	DEVICE NAME	CATEGORY	MODEL	FIRMWARE VERSION	ADDRESS	BATTERY	TEMPERATURE	OUTPUT	OUTPUT MODE
NORMAL									
✓	GXT5-90	RACK_UPS	GXT5		10.169.42.90	506 MIN REMAINING FULLY CHARGED 100 %	26 °C 78.8 °F	50Hz 0.1A 229.7V	Normal
OFFLINE									
	ITA-123	RACK_UPS	ITA		10.169.42.123				

Figure 5.4



UPSs

GROUP BY: Status

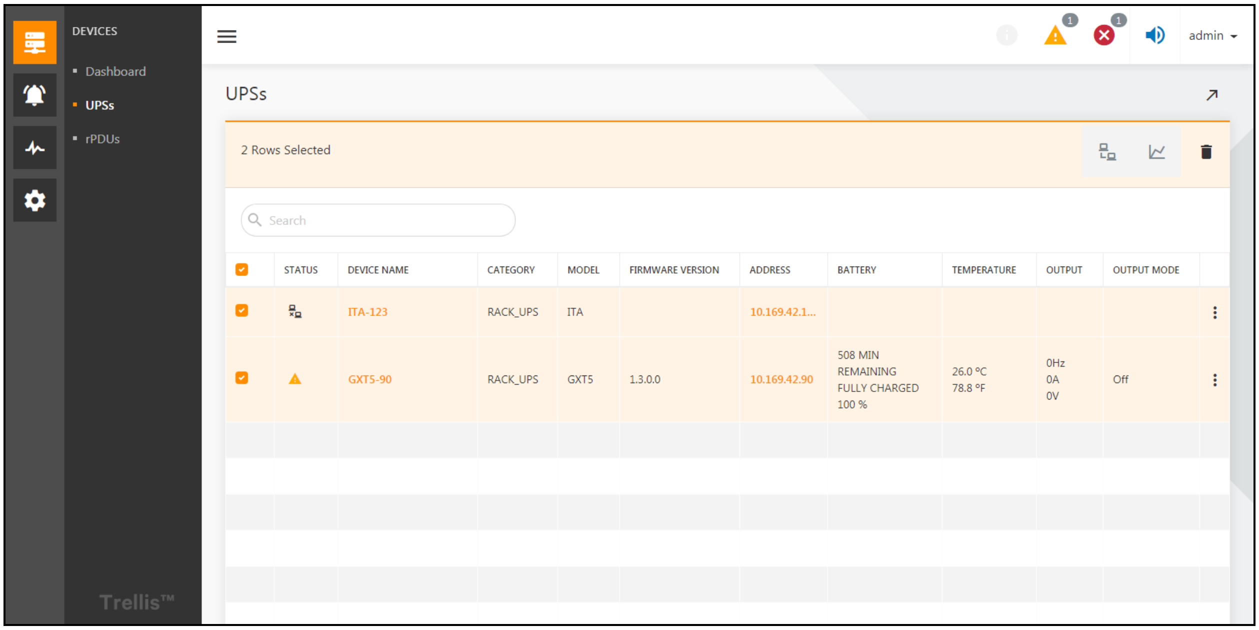
STATUS: Offline

STATUS ↑	DEVI	CATEGORY	MODEL	FIRMWARE VERSION	ADDRESS	BATTERY	TEMPERATURE	OUTPUT	OUTPUT MODE
OFFLINE									
	ITA-123	RACK_UPS	ITA		10.169.42.123				

Figure 5.5

Batch operation:

Click on the *check box* on the left side of the list, by selecting multiple items, the action button will appear on top of the list where the gray icons can only operate for a single item in the list and the ungrayed icon can perform the batch operation of the corresponding selected device, For example, click “🗑 ” can delete the devices in bulk.



2 Rows Selected

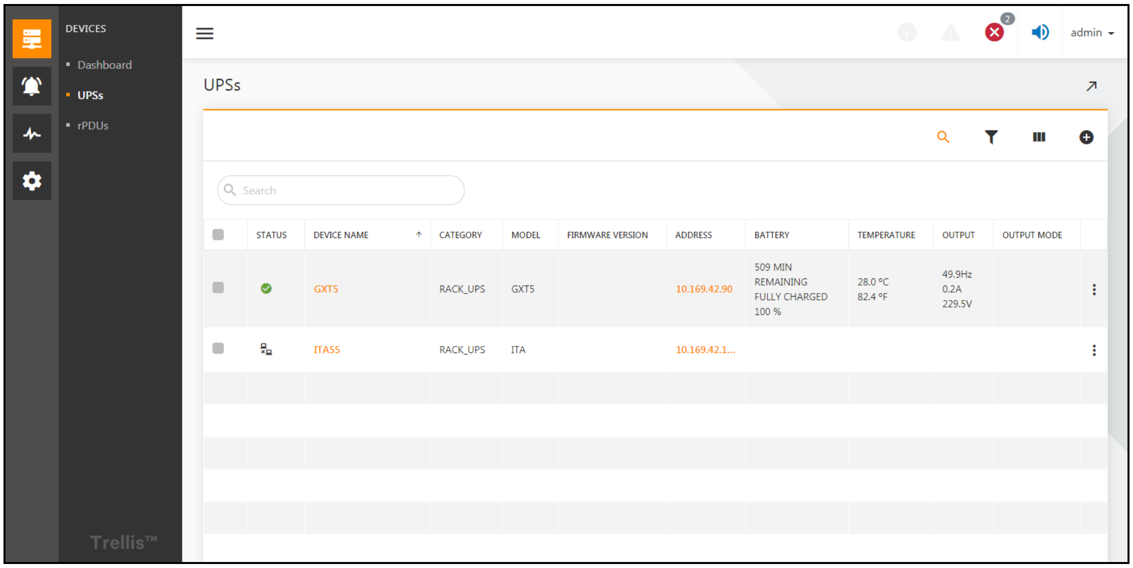
Search

☑	STATUS	DEVICE NAME	CATEGORY	MODEL	FIRMWARE VERSION	ADDRESS	BATTERY	TEMPERATURE	OUTPUT	OUTPUT MODE
☑		ITA-123	RACK_UPS	ITA		10.169.42.1...				
☑	⚠	GXT5-90	RACK_UPS	GXT5	1.3.0.0	10.169.42.90	508 MIN REMAINING FULLY CHARGED 100 %	26.0 °C 78.8 °F	0Hz 0A 0V	Off

Figure 5.6

Sorting the list:

Hovering an item in the list header, if there is no 🚫 icon prohibiting operation, you can sort the list by clicking the table header. The ascending arrow represents the positive sequence, and the descending arrow represents the reverse sequence, as shown in Figure 5.7 below , which is to sort in the forward direction based on the device name. The sorting algorithm varies depending on the data format of the column in which the header is clicked, in general, the string uses a dictionary order, the numbers are sorted from small to large, and the normal status on the top.



Search

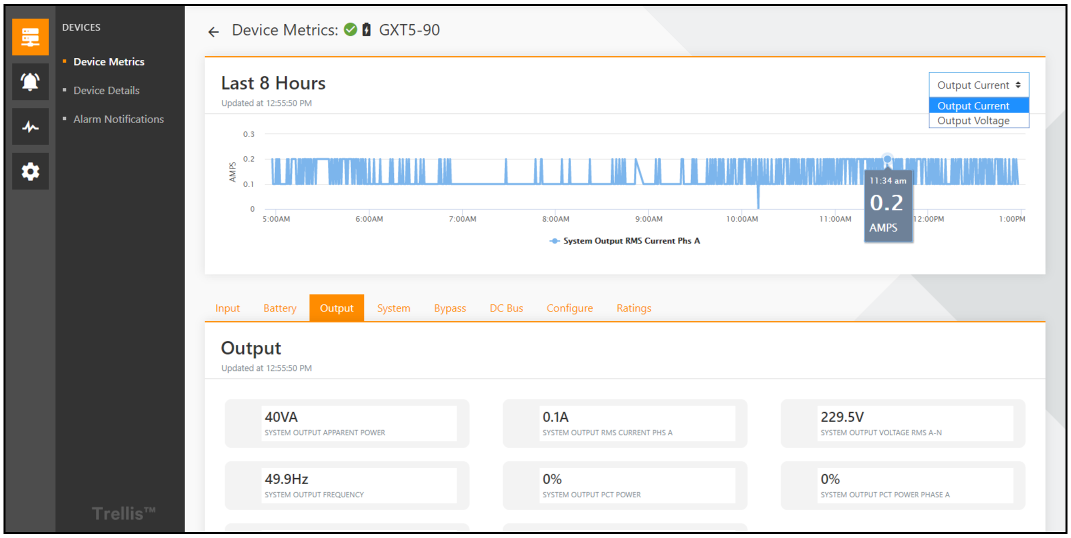
□	STATUS	DEVICE NAME ↑	CATEGORY	MODEL	FIRMWARE VERSION	ADDRESS	BATTERY	TEMPERATURE	OUTPUT	OUTPUT MODE
□	✓	GXT5	RACK_UPS	GXT5		10.169.42.90	509 MIN REMAINING FULLY CHARGED 100 %	28.0 °C 82.4 °F	49.9Hz 0.2A 229.5V	
□		ITAS5	RACK_UPS	ITA		10.169.42.1...				

Figure 5.7

5.3.3 Device Metrics

In the list of UPS or PDU, click the ⋮ button on the right side of the list and select the device metrics in the pop-up box to enter the device metrics page. The Device Metrics window contains the metrics information of the selected device from the last eight hours.

Figure 5.6 on the previous page shows device metrics window page of the UPS GXT5-90 UPS. The device metrics interface consists of two blocks. The top block shows the output current and the output voltage line chart for the last 8 hours. Hover the mouse on to the line chart there pops up the dialogue box to see the output current or output voltage at a specific moment. Below the chart, you can view detailed information of the device, and mouse movement on the grouping allows you to switch groups. The upper left corner of the window page shows the time stamp for the data acquisition. The number of groups and the number of data metrics within each group will vary depending on the type of device and the model of the device.



Output
Updated at 12:55:50 PM

40VA
SYSTEM OUTPUT APPARENT POWER

0.1A
SYSTEM OUTPUT RMS CURRENT PHS A

229.5V
SYSTEM OUTPUT VOLTAGE RMS A-N

49.9Hz
SYSTEM OUTPUT FREQUENCY

0%
SYSTEM OUTPUT PCT POWER

0%
SYSTEM OUTPUT PCT POWER PHASE A

Figure 5.8

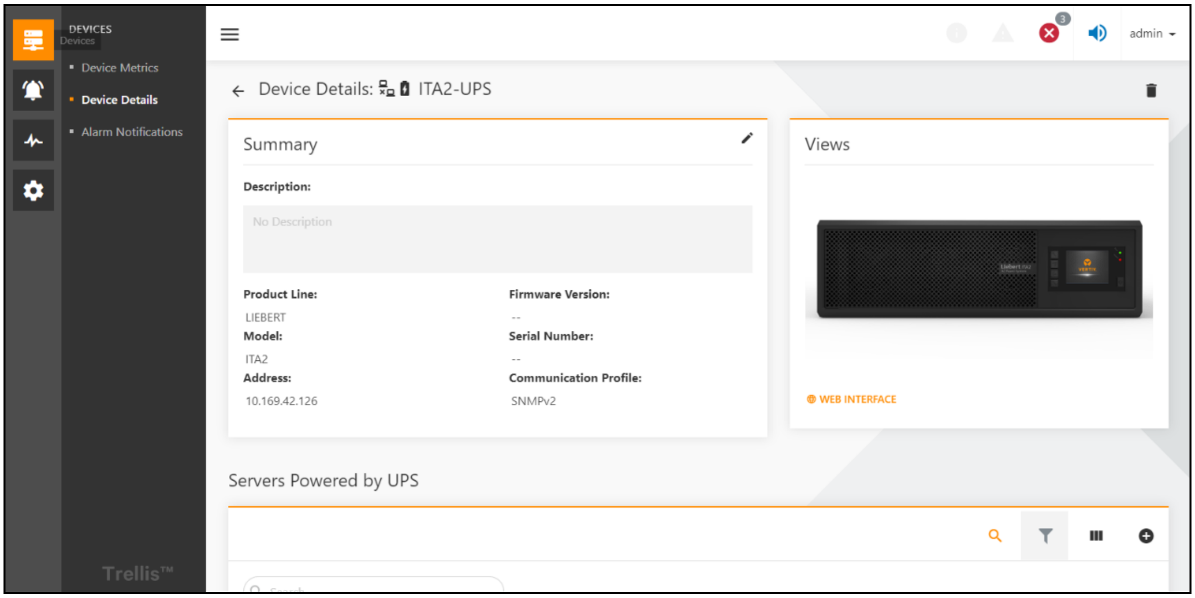
5.3.4 Device details

In the list of UPS or PDU, click the ⋮ button on the right side of the list and select the device details in the pop-up box to enter the device details page. This window

displays detailed information about the device and allows you to access the device's web interface and the Summary tab. It

also displays the servers powered by the UPS. The title shows the device name and device status, and the icon ✓ represents the device status is healthy.

The configuration and function of the servers powered by UPS will be described in detail in Server List on page 80 . The summary tab displays the device description, product line, firmware version, model name, serial number, address, and communication profile information.



Description: No Description

Product Line: LIEBERT

Model: ITA2

Address: 10.169.42.126

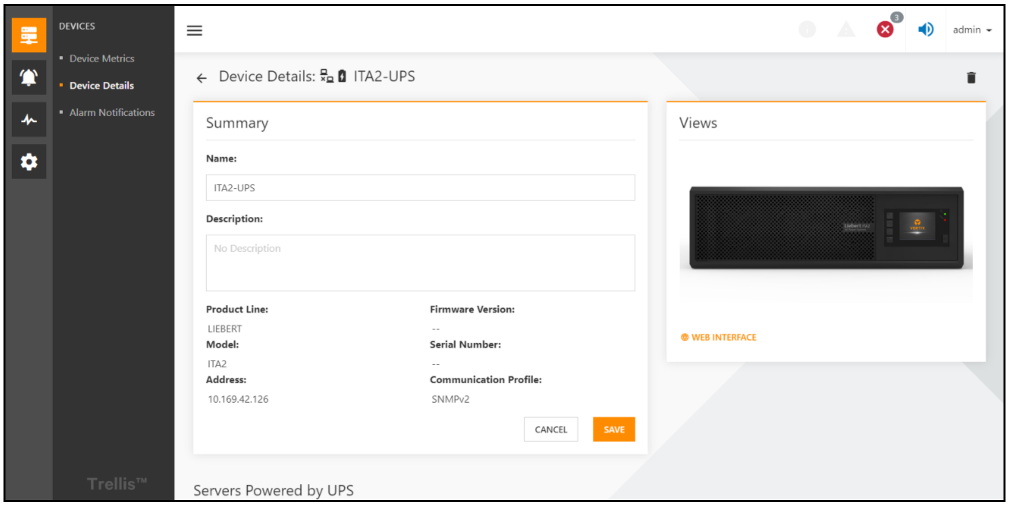
Firmware Version: --

Serial Number: --

Communication Profile: SNMPv2

Figure 5.9

Click the *edit button* under summary tab to edit the name and description of the device, as shown in **Figure 5.10** below .



Name: ITA2-UPS

Description: No Description

Product Line: LIEBERT

Model: ITA2

Address: 10.169.42.126

Firmware Version: --

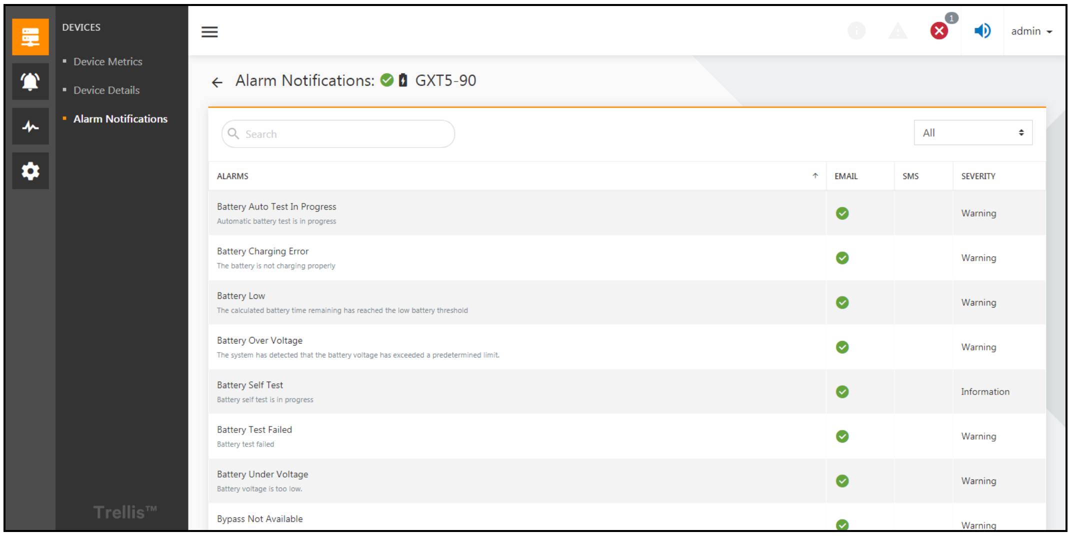
Serial Number: --

Communication Profile: SNMPv2

Figure 5.10

5.3.5 Alarm Notifications

On the device details or device metrics page, click on the “Alarm Notifications” in the secondary directory to enter the alarm notifications interface, as shown in **Figure 5.11** on the facing page . Alarm Notifications is a read-only window that displays which of the device alarms will trigger an email or SMS text. The e-mail and SMS columns in the list indicate whether the alert is currently allowed to send an email or text message as per rules defined in the Actions and Automated rules, the symbol ✓ which represents that it has been allowed. Using the search feature, you can also filter alarms based on their severity and locate a specific alarm in the list.



Alarm Notifications: ✓ GXT5-90

Search

All

ALARMS	EMAIL	SMS	SEVERITY
Battery Auto Test In Progress Automatic battery test is in progress	✓		Warning
Battery Charging Error The battery is not charging properly	✓		Warning
Battery Low The calculated battery time remaining has reached the low battery threshold	✓		Warning
Battery Over Voltage The system has detected that the battery voltage has exceeded a predetermined limit.	✓		Warning
Battery Self Test Battery self test is in progress	✓		Information
Battery Test Failed Battery test failed	✓		Warning
Battery Under Voltage Battery voltage is too low.	✓		Warning
Bypass Not Available	✓		Warning

Figure 5.11

This page intentionally left blank

6 Alarm Management

6.1 Overview

Alarms are the main functional modules for monitoring alarms throughout the Power Insight platform and obtaining alarm information, and users can obtain the active alarms and alarm history in the alarm module and can export the alarm list so that the user can grasp the alarm status of the equipment under the site.

6.1.1 Function Module

The Alarm includes the following function modules, each of which is detailed in this manual under Detailed Features on page 48 :

- Active alarm
- Alarm history

6.2 Get Started Quickly

6.2.1 Quick deployment steps

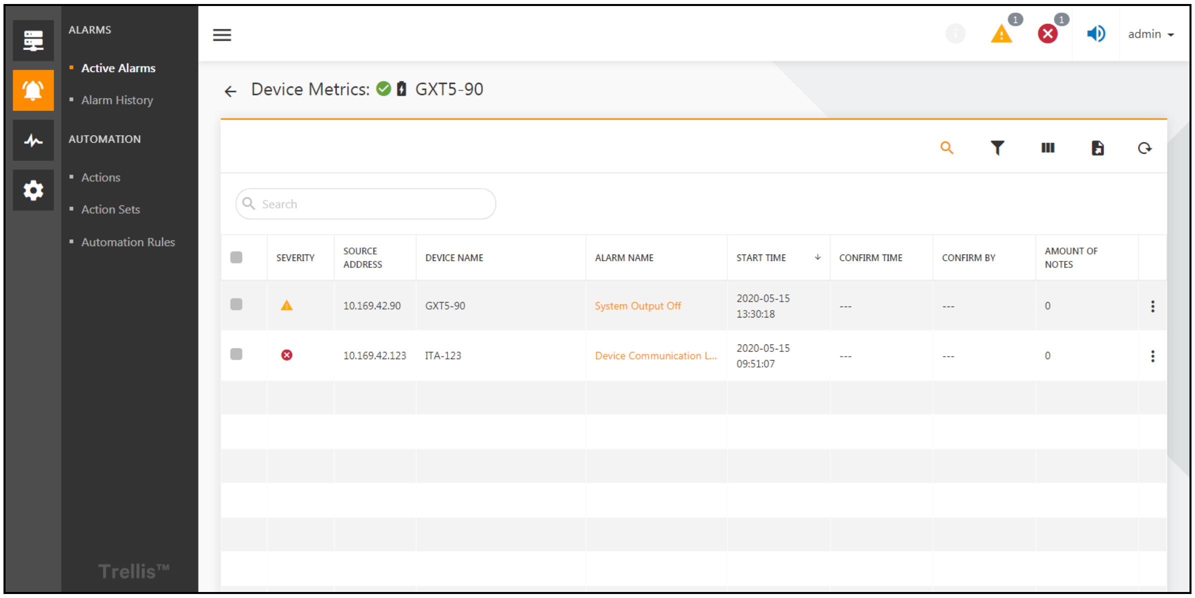
To ensure that you can view the alarm information, you need to:

- View the Alarm list
- View the Alarm history

6.2.2 Examples

Active Alarms

As shown in Figure 6.1 on the next page Selecting the Alarms icon provides access to the Active Alarms by default, and the severity, source address, device name, alarm name, start time, confirm time, confirm by and amount of notes appear in the active alarm list. Alarm list according to the support list of searches, filtering, column hiding functions, can refer to Device List on page 36 . The Active Alarms window (as shown in Figure 6.1 on the next page) displays alarms that have not been cleared. Each alarm has a severity of either warning or critical, represented by an exclamation point in a yellow triangle or an x in a red circle, respectively. There's also an Information severity, represented by an "i" inside of a circle. The toolbar allows you to filter the alarm list. You can choose to display alarms from a specific time period and group them based on certain criteria. You can also retrieve the most current alarm notification using the Reload icon located on the toolbar and store notes on any alarm on the Alarm Details window.



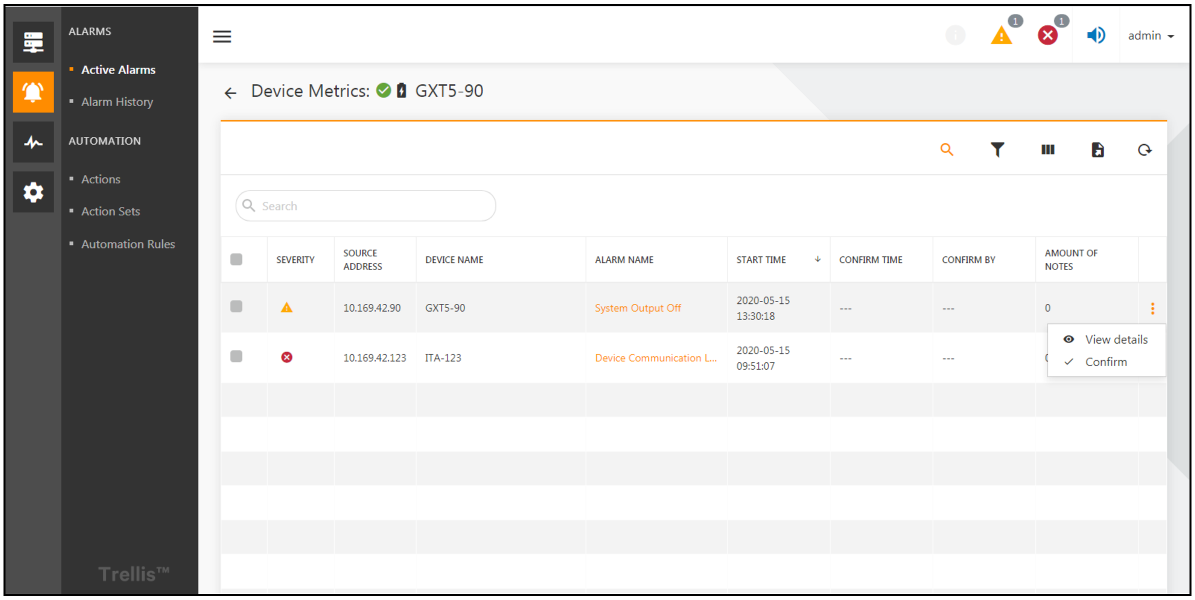
Device Metrics: GXT5-90

	SEVERITY	SOURCE ADDRESS	DEVICE NAME	ALARM NAME	START TIME	CONFIRM TIME	CONFIRM BY	AMOUNT OF NOTES
□	⚠	10.169.42.90	GXT5-90	System Output Off	2020-05-15 13:30:18	---	---	0
□	⊗	10.169.42.123	ITA-123	Device Communication L...	2020-05-15 09:51:07	---	---	0

Figure 6.1

View Alarm Details

As shown in **Figure 6.2** below , on the active alarm or alarm history page, click the “⋮”button on the right side of a warning line and click to see the details.



Device Metrics: GXT5-90

	SEVERITY	SOURCE ADDRESS	DEVICE NAME	ALARM NAME	START TIME	CONFIRM TIME	CONFIRM BY	AMOUNT OF NOTES
□	⚠	10.169.42.90	GXT5-90	System Output Off	2020-05-15 13:30:18	---	---	0
□	⊗	10.169.42.123	ITA-123	Device Communication L...	2020-05-15 09:51:07	---	---	0

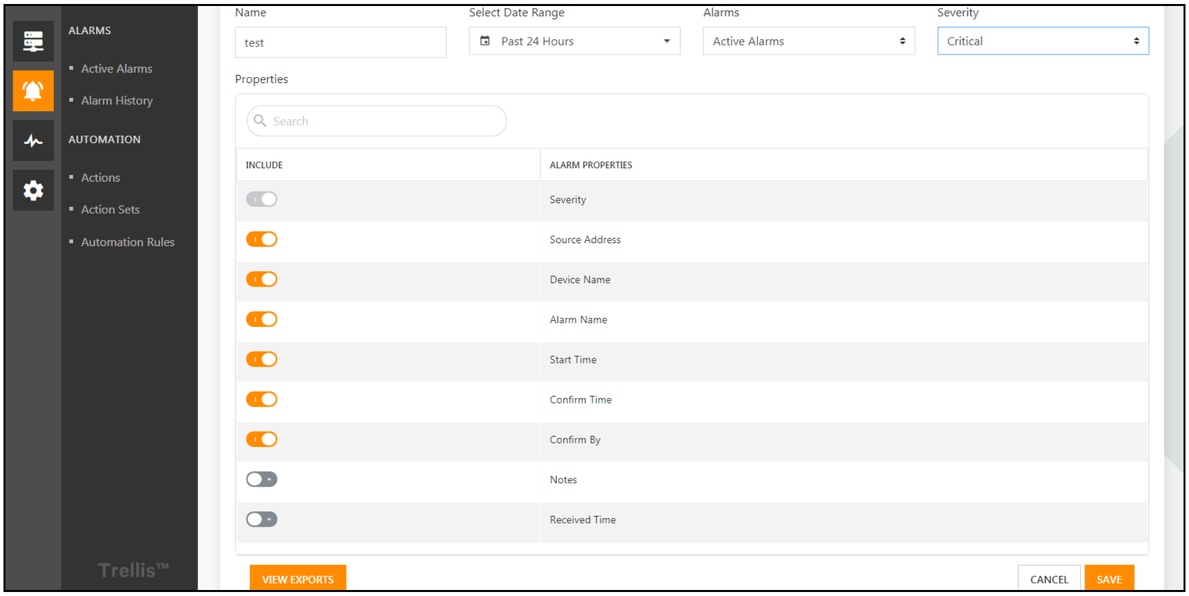
Figure 6.2

NOTE:

- **When alarm data is not available, "No data" appears on the alarm list.**
- **The purpose of the alarm confirmation button is not to end the alarm, but to stop the alarm notification. It is not allowed to end the alarm manually, only by the alarm device itself, to determine that the trigger condition for alarm is no longer present and thus automatically end an alarm.**

Export Alarms

As shown in Figure 6.3 below , on the alarm list page, click the button in the upper right corner, enter the file name to export, select the type of an alarm, the date range, alarm severity, and the properties to export. Click *Save*.



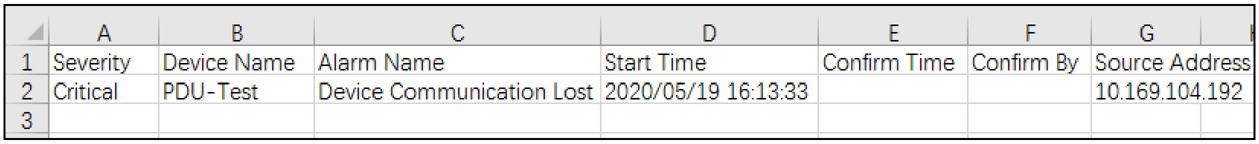
Name: test
Select Date Range: Past 24 Hours
Alarms: Active Alarms
Severity: Critical

Properties

INCLUDE	ALARM PROPERTIES
●	Severity
●	Source Address
●	Device Name
●	Alarm Name
●	Start Time
●	Confirm Time
●	Confirm By
○	Notes
○	Received Time

Figure 6.3

After the export is successful, you can prompt for the export success in the lower right corner. Click to view the exports and enter the list of export records, and then click on the download button of the file you want to export, you can successfully download the exported record. The contents of the file after download are shown in Figure 6.4 below . The header field contained in the file is consistent with the selection in Figure 6.3 above .



	A	B	C	D	E	F	G
1	Severity	Device Name	Alarm Name	Start Time	Confirm Time	Confirm By	Source Address
2	Critical	PDU-Test	Device Communication Lost	2020/05/19 16:13:33			10.169.104.192
3							

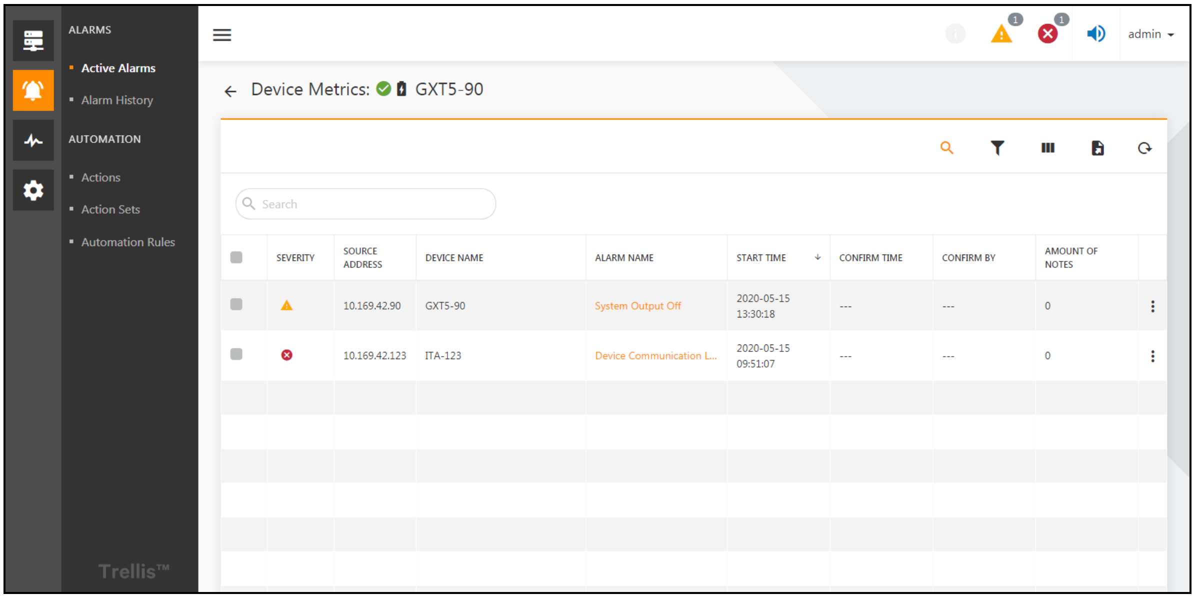
Figure 6.4

6.3 Detailed Features

6.3.1 Active Alarms

Select the level one menu the “🔔”alarm icon to open the active alarm window page.

The Active Alarms window (as shown in Figure 6.4 on the previous page) displays alarms that have not been cleared. Each alarm has a severity of either warning or critical, represented by an exclamation point in a yellow triangle or an x in a red circle, respectively. There's also an Information severity, represented by an "i" inside of a circle. The toolbar allows you to filter the alarm list. You can choose to display alarms from a specific time period and group them based on certain criteria. You can also retrieve the most current alarm notification using the Reload icon located on the toolbar and store notes on any alarm on the Alarm Details window.



Device Metrics: ✓ GXT5-90

□	SEVERITY	SOURCE ADDRESS	DEVICE NAME	ALARM NAME	START TIME ↓	CONFIRM TIME	CONFIRM BY	AMOUNT OF NOTES
□	⚠	10.169.42.90	GXT5-90	System Output Off	2020-05-15 13:30:18	---	---	0
□	⊗	10.169.42.123	ITA-123	Device Communication L...	2020-05-15 09:51:07	---	---	0

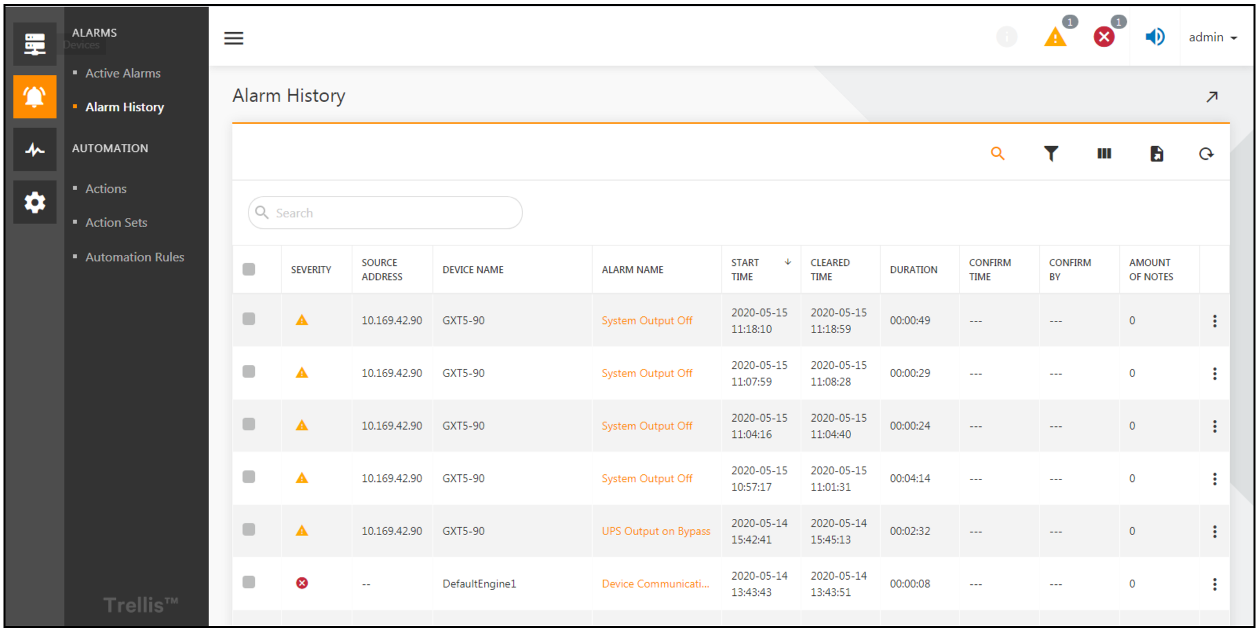
Figure 6.5

NOTE:

- **When an alarm is not available, "No alarm" appears on the list.**
- **The search button 🔍 in the table is orange by default, the search box is displayed by default, when you click the Search 🔍 Button, the button turns black and the search box is hidden.**

6.3.2 Alarm History

Click 🔔 icon in the level one directory and select alarm history. The Alarm History window contains a list of cleared and historical alarms. The window displays details about each alarm, including the time cleared, the duration of the alarm and its severity. Additional alarm details are stored on the Alarm Details window, which is accessed by clicking View details. The alarm Details window allows you to add notes to the alarm and view the action history.



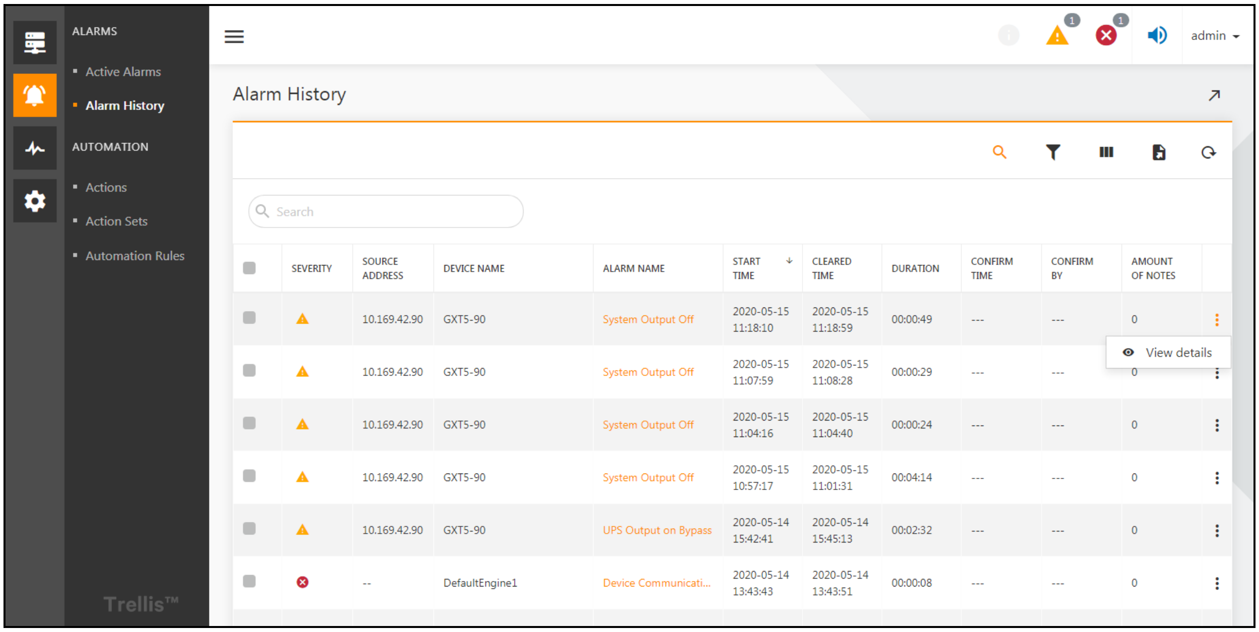
□	SEVERITY	SOURCE ADDRESS	DEVICE NAME	ALARM NAME	START TIME ↓	CLEARED TIME	DURATION	CONFIRM TIME	CONFIRM BY	AMOUNT OF NOTES	
□	⚠	10.169.42.90	GXT5-90	System Output Off	2020-05-15 11:18:10	2020-05-15 11:18:59	00:00:49	---	---	0	⋮
□	⚠	10.169.42.90	GXT5-90	System Output Off	2020-05-15 11:07:59	2020-05-15 11:08:28	00:00:29	---	---	0	⋮
□	⚠	10.169.42.90	GXT5-90	System Output Off	2020-05-15 11:04:16	2020-05-15 11:04:40	00:00:24	---	---	0	⋮
□	⚠	10.169.42.90	GXT5-90	System Output Off	2020-05-15 10:57:17	2020-05-15 11:01:31	00:04:14	---	---	0	⋮
□	⚠	10.169.42.90	GXT5-90	UPS Output on Bypass	2020-05-14 15:42:41	2020-05-14 15:45:13	00:02:32	---	---	0	⋮
□	⊗	--	DefaultEngine1	Device Communicati...	2020-05-14 13:43:43	2020-05-14 13:43:51	00:00:08	---	---	0	⋮

Figure 6.6

6.3.3 View Alarm Details

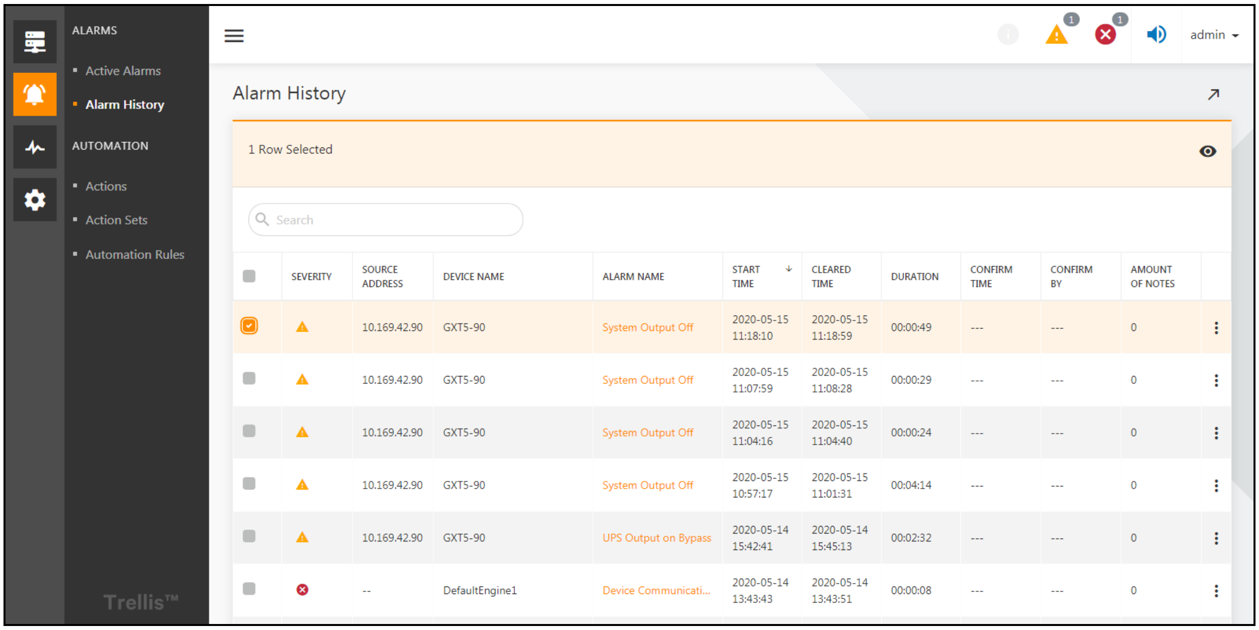
There are two ways to view alarm details:

1. As shown in **Figure 6.7** on the next page , on the active alarms or alarm history page, click the "⋮" button on the right side of a warning line and click to view the details.
2. As shown in **Figure 6.8** on the next page , click a warning in the left multi-select box, and on the top of search box will show a row selected, click the 👁 button on the right to see the view details.



	SEVERITY	SOURCE ADDRESS	DEVICE NAME	ALARM NAME	START TIME	CLEARED TIME	DURATION	CONFIRM TIME	CONFIRM BY	AMOUNT OF NOTES
□	⚠	10.169.42.90	GXT5-90	System Output Off	2020-05-15 11:18:10	2020-05-15 11:18:59	00:00:49	---	---	0
□	⚠	10.169.42.90	GXT5-90	System Output Off	2020-05-15 11:07:59	2020-05-15 11:08:28	00:00:29	---	---	0
□	⚠	10.169.42.90	GXT5-90	System Output Off	2020-05-15 11:04:16	2020-05-15 11:04:40	00:00:24	---	---	0
□	⚠	10.169.42.90	GXT5-90	System Output Off	2020-05-15 10:57:17	2020-05-15 11:01:31	00:04:14	---	---	0
□	⚠	10.169.42.90	GXT5-90	UPS Output on Bypass	2020-05-14 15:42:41	2020-05-14 15:45:13	00:02:32	---	---	0
□	⊗	--	DefaultEngine1	Device Communicati...	2020-05-14 13:43:43	2020-05-14 13:43:51	00:00:08	---	---	0

Figure 6.7



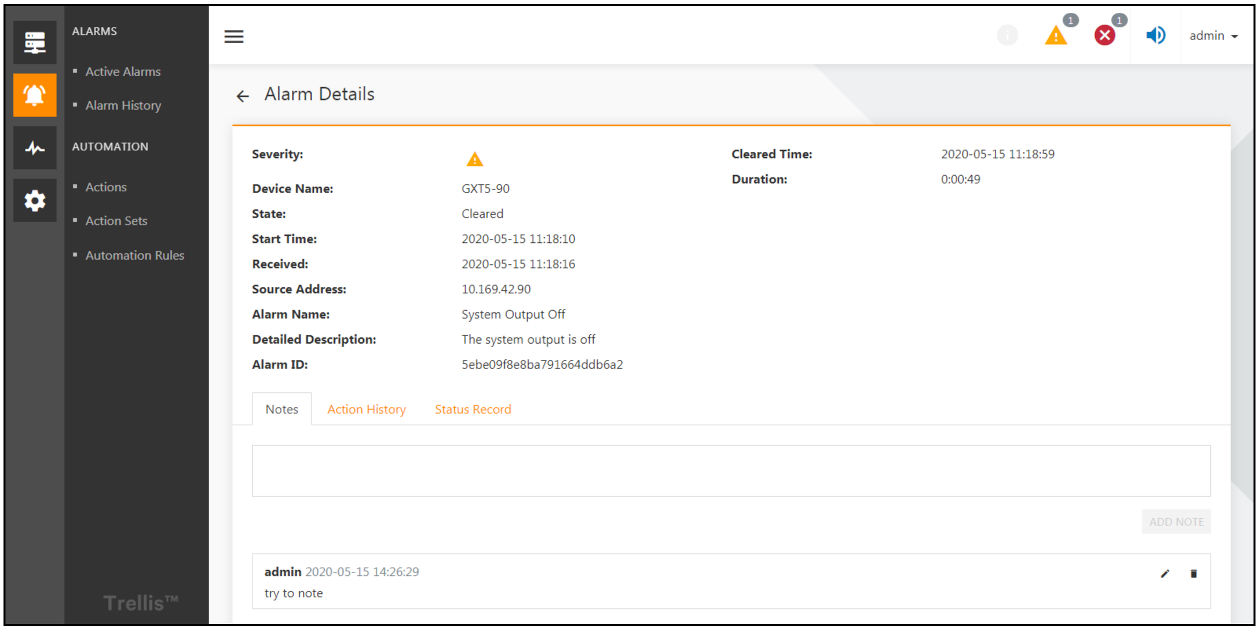
	SEVERITY	SOURCE ADDRESS	DEVICE NAME	ALARM NAME	START TIME	CLEARED TIME	DURATION	CONFIRM TIME	CONFIRM BY	AMOUNT OF NOTES
☑	⚠	10.169.42.90	GXT5-90	System Output Off	2020-05-15 11:18:10	2020-05-15 11:18:59	00:00:49	---	---	0
□	⚠	10.169.42.90	GXT5-90	System Output Off	2020-05-15 11:07:59	2020-05-15 11:08:28	00:00:29	---	---	0
□	⚠	10.169.42.90	GXT5-90	System Output Off	2020-05-15 11:04:16	2020-05-15 11:04:40	00:00:24	---	---	0
□	⚠	10.169.42.90	GXT5-90	System Output Off	2020-05-15 10:57:17	2020-05-15 11:01:31	00:04:14	---	---	0
□	⚠	10.169.42.90	GXT5-90	UPS Output on Bypass	2020-05-14 15:42:41	2020-05-14 15:45:13	00:02:32	---	---	0
□	⊗	--	DefaultEngine1	Device Communicati...	2020-05-14 13:43:43	2020-05-14 13:43:51	00:00:08	---	---	0

Figure 6.8

The alert details page, in addition to the properties displayed in the alarm list, also includes the add alarm notes, action history, and status records.

6.3.4 Alarm Notes

On the alarm details page, click on the notes tab page below, enter the relevant notes in the input box, and then click the *"Add Note" button*. Adding a successful note appears in the list of notes below, and you can click ✎ to *Edit Notes* and Click 🗑 to *delete Notes*.



Alarm Details

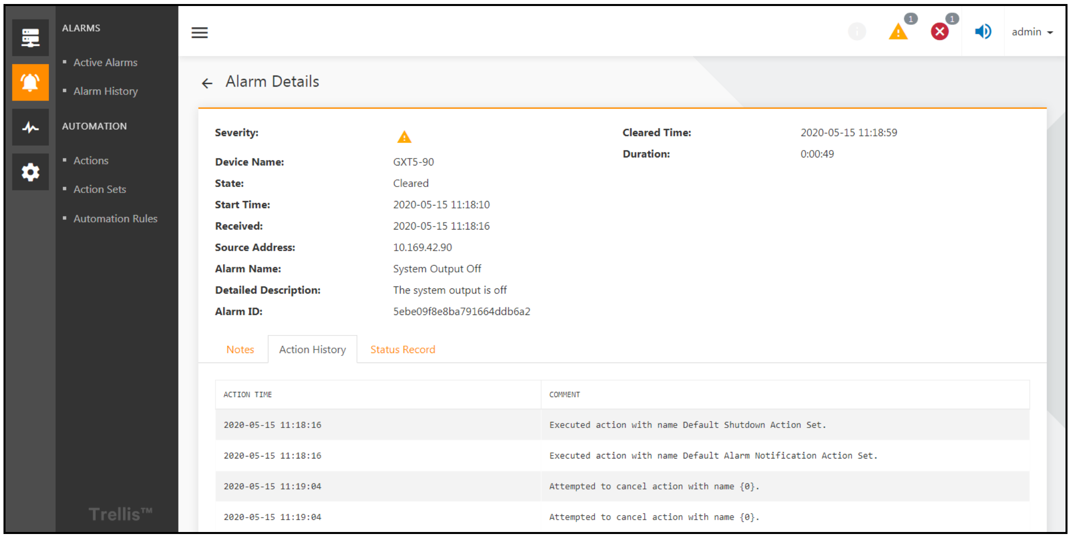
Severity:	⚠	**Cleared Time:**	2020-05-15 11:18:59
Device Name:	GXT5-90	**Duration:**	0:00:49
State:	Cleared		
Start Time:	2020-05-15 11:18:10		
Received:	2020-05-15 11:18:16		
Source Address:	10.169.42.90		
Alarm Name:	System Output Off		
Detailed Description:	The system output is off		
Alarm ID:	5ebe09f8e8ba791664ddb6a2		

admin 2020-05-15 14:26:29
try to note

Figure 6.9

6.3.5 Action History

On the alert details page, click on the Action history Tab page below to show a history of the action. Refer to Alarm Notification on page 55 for the configuration of actions and automation rules.



Alarm Details

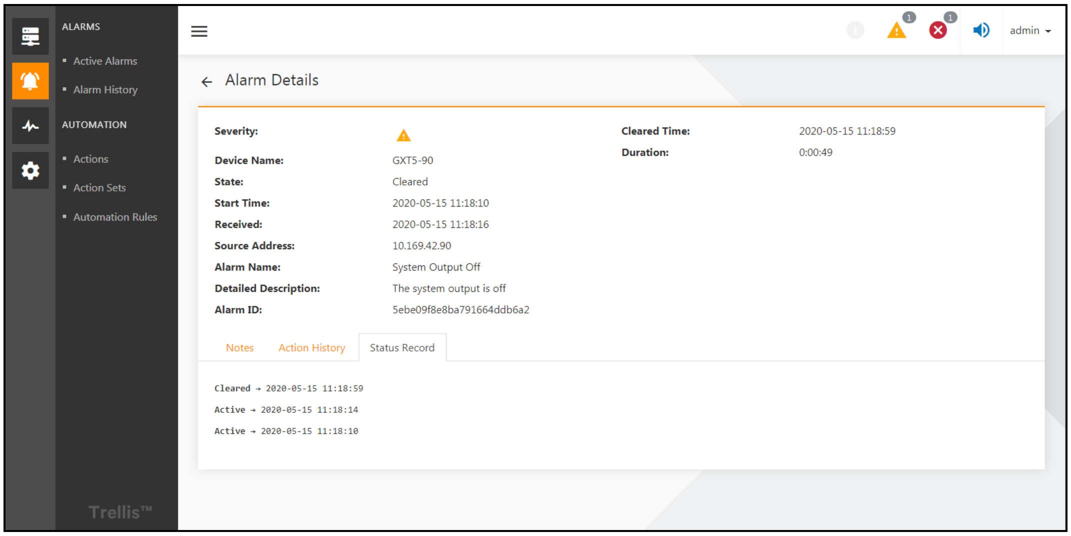
Severity:	⚠	**Cleared Time:**	2020-05-15 11:18:59
Device Name:	GXT5-90	**Duration:**	0:00:49
State:	Cleared		
Start Time:	2020-05-15 11:18:10		
Received:	2020-05-15 11:18:16		
Source Address:	10.169.42.90		
Alarm Name:	System Output Off		
Detailed Description:	The system output is off		
Alarm ID:	5ebe09f8e8ba791664ddb6a2		

ACTION TIME	COMMENT
2020-05-15 11:18:16	Executed action with name Default Shutdown Action Set.
2020-05-15 11:18:16	Executed action with name Default Alarm Notification Action Set.
2020-05-15 11:19:04	Attempted to cancel action with name {0}.
2020-05-15 11:19:04	Attempted to cancel action with name {0}.

Figure 6.10

6.3.6 Alert Status Record

On the alert details page, click on the status record Tab below to display the status record of the alarm (information such as when the alarm was generated, and the alarm ended).



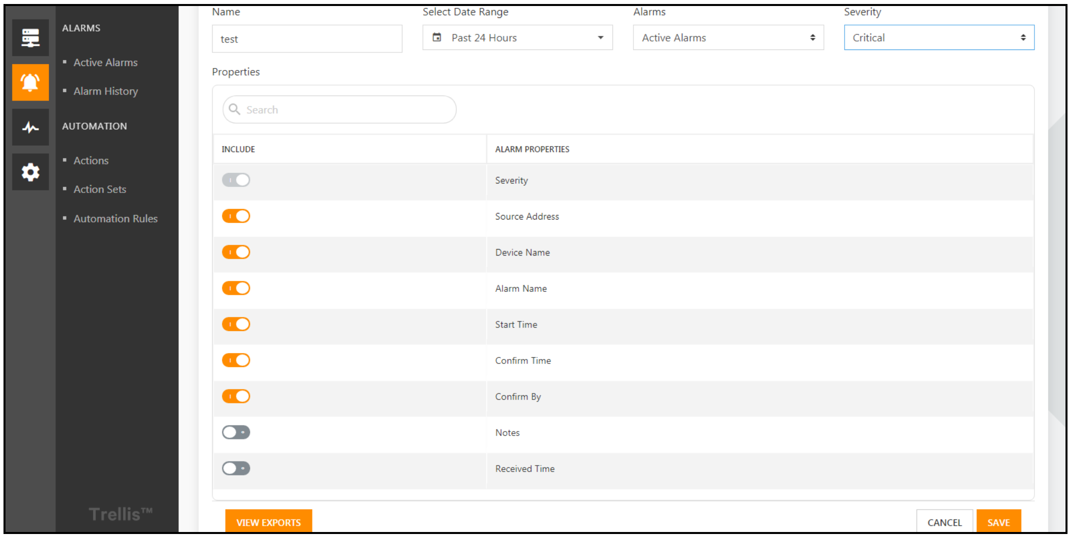
Severity:	⚠
Device Name:	GXT5-90
State:	Cleared
Start Time:	2020-05-15 11:18:10
Received:	2020-05-15 11:18:16
Source Address:	10.169.42.90
Alarm Name:	System Output Off
Detailed Description:	The system output is off
Alarm ID:	5ebe09f8e8ba791664ddb6a2
Cleared Time:	2020-05-15 11:18:59
Duration:	0:00:49

```
Cleared → 2020-05-15 11:18:59
Active → 2020-05-15 11:18:14
Active → 2020-05-15 11:18:10
```

Figure 6.11

6.3.7 Export Alerts

On the alarms list page, click the *button in the upper right corner*, enter the *export file name*, select the type of alarm to export, the date range, the severity of an alarm, and the properties to export. Click on *"Save"*.



Name: test

Select Date Range: Past 24 Hours

Alarms: Active Alarms

Severity: Critical

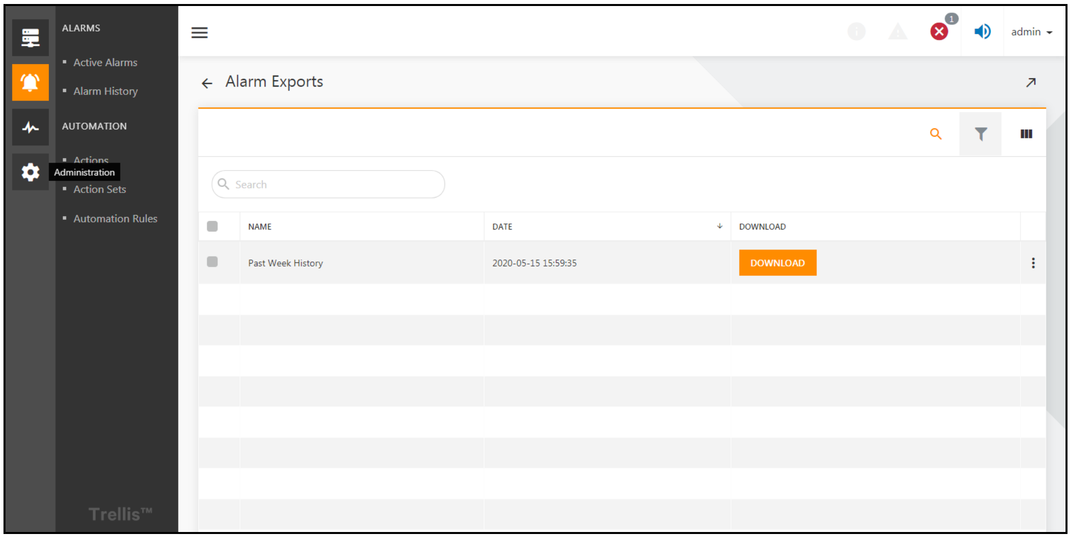
Properties

INCLUDE	ALARM PROPERTIES
●	Severity
●	Source Address
●	Device Name
●	Alarm Name
●	Start Time
●	Confirm Time
●	Confirm By
○	Notes
○	Received Time

Figure 6.12

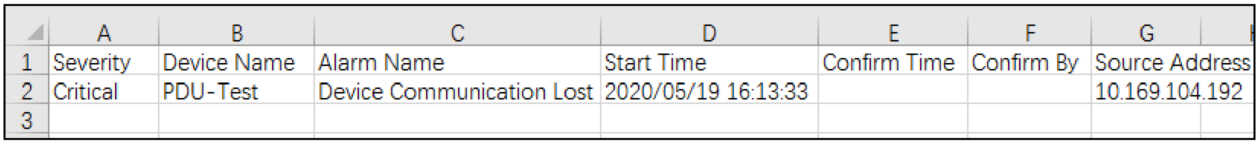
After the export is successful, you can prompt for the export success in the bottom right corner. Click to *view the Alarm exports* (Figure 6.13 on the facing page) and enter the *list of export records*, and then click on the *download button* of the file you want to export, you can successfully download the exported record.

The contents of the file after download are shown in Figure 6.14 on the facing page . The header field contained in the file is consistent with the selection in Figure Figure 6.7 on page 50 .



NAME	DATE	DOWNLOAD
Past Week History	2020-05-15 15:59:35	DOWNLOAD

Figure 6.13



	A	B	C	D	E	F	G
1	Severity	Device Name	Alarm Name	Start Time	Confirm Time	Confirm By	Source Address
2	Critical	PDU-Test	Device Communication Lost	2020/05/19 16:13:33			10.169.104.192
3							

Figure 6.14

This page intentionally left blank

7 Alarm Notification

7.1 Overview

Alarms generated by the monitoring system needs to be notified to the user by mail and text message. This chapter describes how to set up these two notification methods.

7.1.1 Functional Module

The following functional modules are set for the alarm notification. For detailed introduction of each function module, please refer to Detailed Features on page 60 Detailed Functions in this manual:

1. Email and SMS notification settings
2. Action settings
3. Action sets settings
4. Automation rules settings

7.2 Get Started Quickly

7.2.1 Quick Deployment Steps

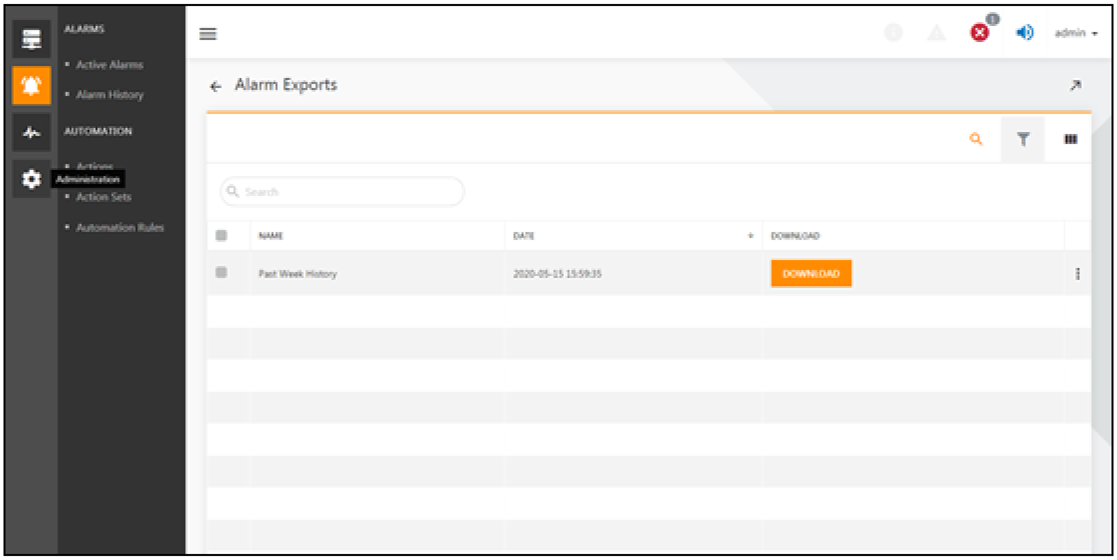
Follow the below steps to setup the alarm notification:

1. Set up contacts
2. Configure the email server connection and SMS modem connection respectively
3. Set the action
4. Configure the action sets
5. Set automation rules

7.2.2 Example

Set up Contact Information

Click on the **"admin"** drop-down box in the upper right corner, and then click on the **"User Profile"** option. Click the edit option to enter the email address and phone number of your admin account. Refer to section Detailed Features on page 60 for detailed functions that can be configured with contacts.


ALARMS
- Active Alarms
- Alarm History

AUTOMATION
- Actions
- Action Sets
- Automation Rules

Administration

admin

Alarm Exports

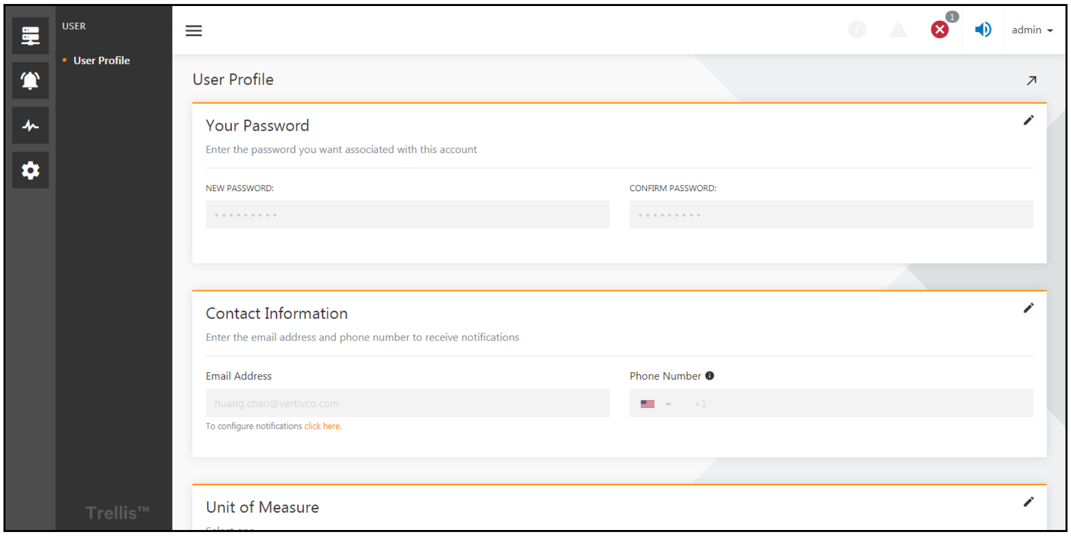
Search

NAME	DATE	DOWNLOAD
Past Week History	2020-05-15 15:59:35	DOWNLOAD

Figure 7.1

Mail and SMS Server Configuration

Click on "⚙" icon, then click on the **"Notification Settings"** menu to enter the notification settings page, click on edit icon "✎" in the email server connection configuration to fill the required fields, as shown in **Figure 7.3** on the facing page . click on edit icon "✎" in the SMS modem configuration to fill the required fields, as shown in **Figure 7.4** on the facing page .


USER
- User Profile

Trellis™

admin

User Profile

Your Password

Enter the password you want associated with this account

NEW PASSWORD: ·········

CONFIRM PASSWORD: ·········

Contact Information

Enter the email address and phone number to receive notifications

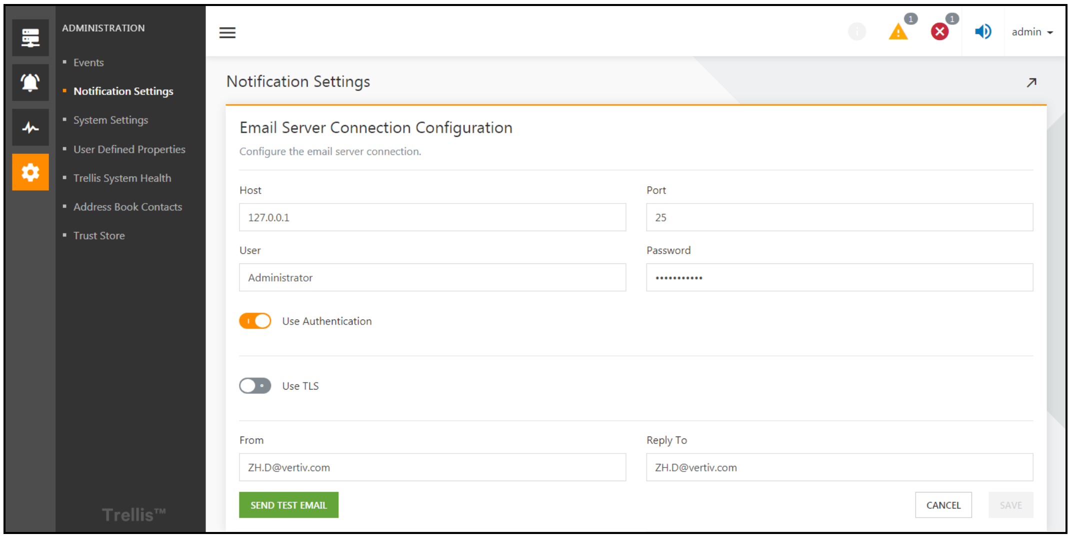
Email Address: huang.chao@vertivco.com

Phone Number: +1

To configure notifications click here.

Unit of Measure

Figure 7.2



Notification Settings

Email Server Connection Configuration

Configure the email server connection.

Host
127.0.0.1

Port
25

User
Administrator

Password
•••••••••••

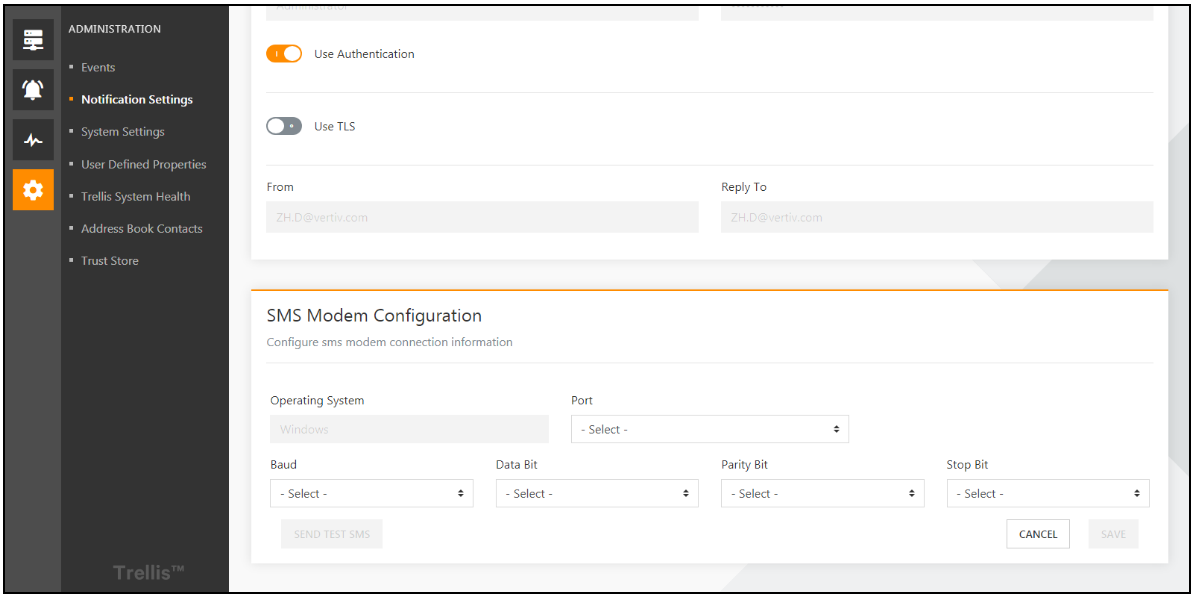
● Use Authentication

○ Use TLS

From
ZH.D@vertiv.com

Reply To
ZH.D@vertiv.com

Figure 7.3



● Use Authentication

○ Use TLS

From
ZH.D@vertiv.com

Reply To
ZH.D@vertiv.com

SMS Modem Configuration

Configure sms modem connection information

Operating System
Windows

Port
- Select -

Baud
- Select -

Data Bit
- Select -

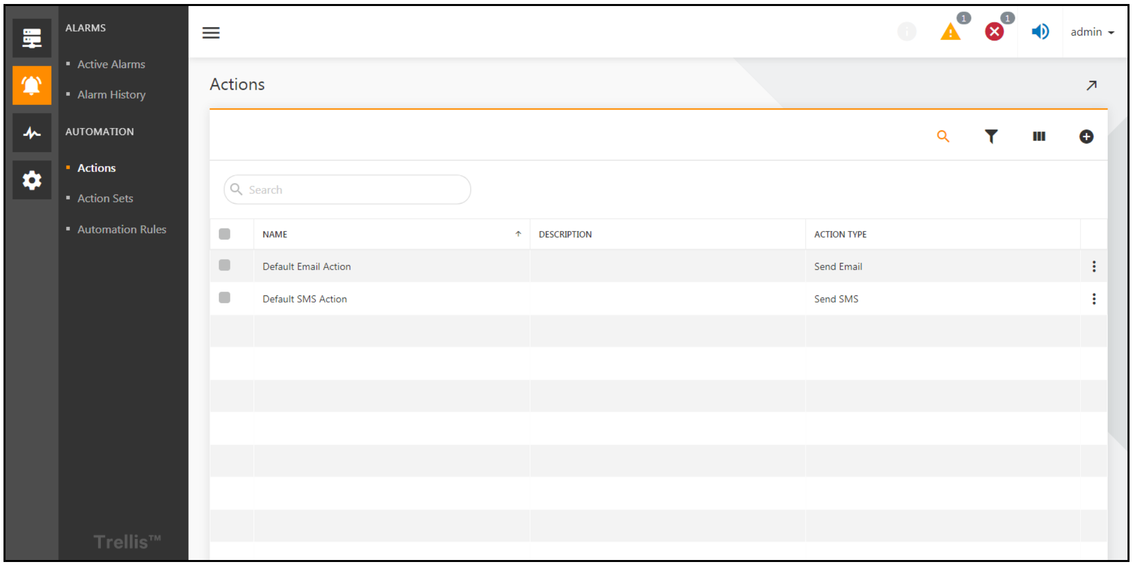
Parity Bit
- Select -

Stop Bit
- Select -

Figure 7.4

Set the Action

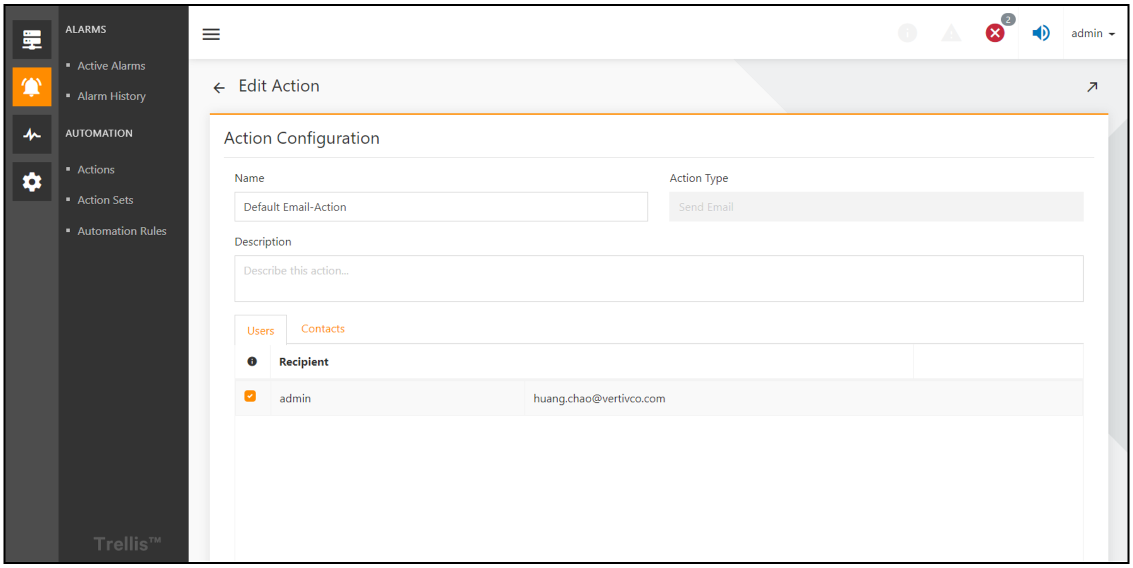
1. Click on "🔔" icon, then click on the "Actions" to enter the Actions settings page, as shown in **Figure 7.5** on the next page . Click the button on the right to edit the default email notification action or the default SMS notification action.



NAME	DESCRIPTION	ACTION TYPE
Default Email Action		Send Email
Default SMS Action		Send SMS

Figure 7.5

2. Go to the action configuration interface, as shown in **Figure 7.6** below . Check the user admin to accept the email notification after click Save. The same way into the default SMS notification action editing interface, check the user admin to accept the SMS notification after click Save.



Name: Default Email-Action

Action Type: Send Email

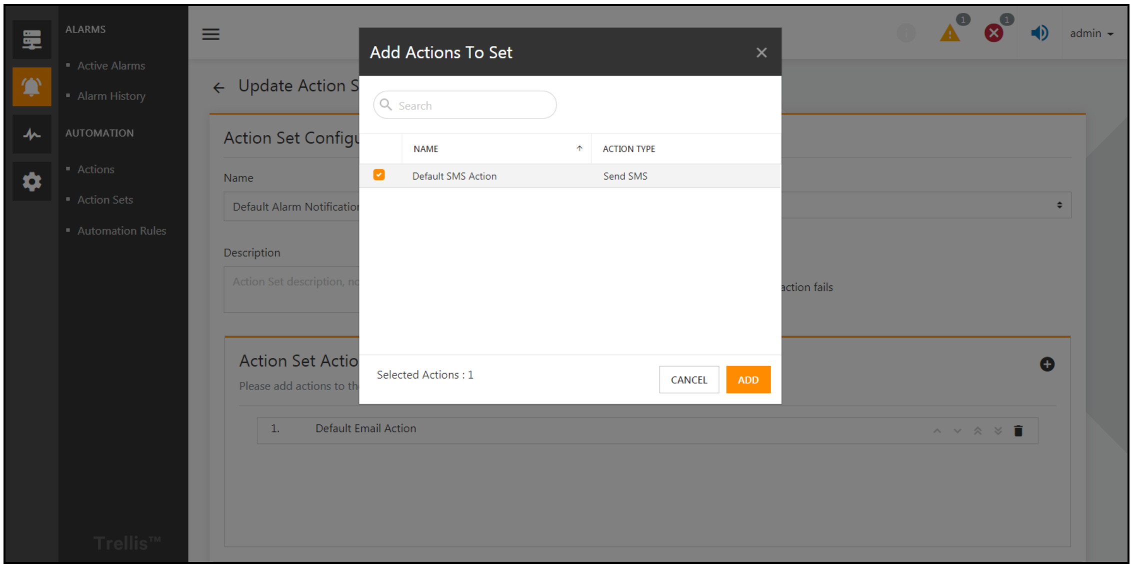
Description: Describe this action...

	Recipient	
☑	admin	huang.chao@vertivco.com

Figure 7.6

Configure Action Sets

Click on “🔔” icon, and then click on the **“Action sets”** to go to the Action sets page. Click the “⊕” button on the right to enter the Default action set editing interface, and then click on “⊕” button brings up Add actions to set interface, as shown in **Figure 7.7** below . Add the default SMS notification action to the default action type.



Add Actions To Set

Search

NAME	ACTION TYPE
☑ Default SMS Action	Send SMS

Selected Actions : 1

Name: Default Alarm Notificatio

Description: Action Set description, n

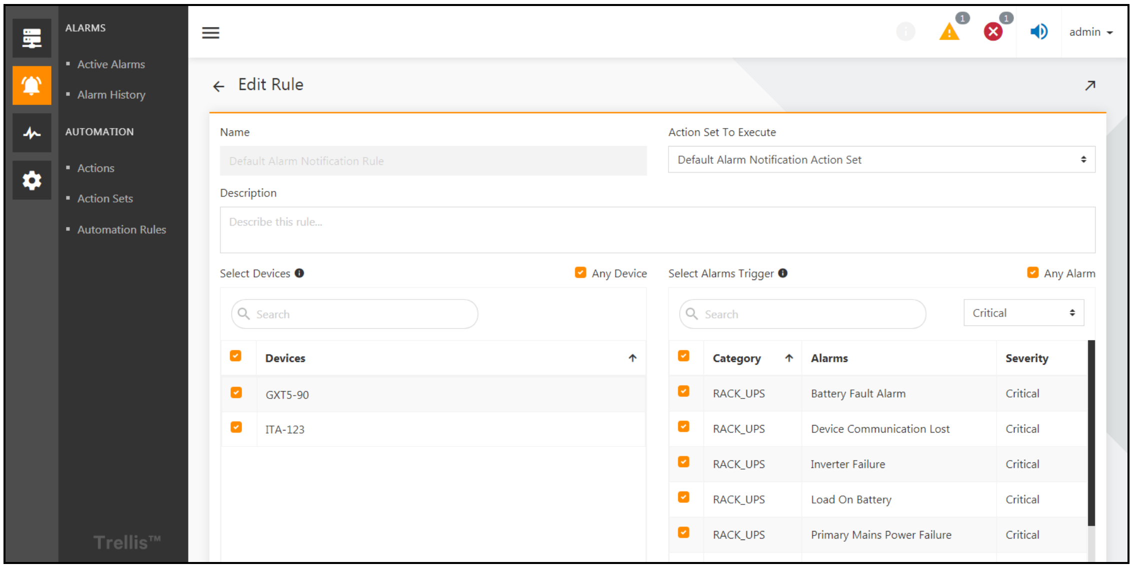
action fails

1. Default Email Action

Figure 7.7

Set Automation Rules

Click on 🔔 icon, then click on the **“Automation rules”** to enter the Automation rules interface. Click the ⋮ button on the right to enter the edit rules interface, and then select any device check box of the device and select any alarm check box of the alarm and click **Save.**



Edit Rule

Name: Default Alarm Notification Rule

Action Set To Execute: Default Alarm Notification Action Set

Description: Describe this rule...

Select Devices ☑ Any Device

Search

☑	Devices
☑	GXT5-90
☑	ITA-123

Select Alarms Trigger ☑ Any Alarm

Search Critical

☑	Category	Alarms	Severity
☑	RACK_UPS	Battery Fault Alarm	Critical
☑	RACK_UPS	Device Communication Lost	Critical
☑	RACK_UPS	Inverter Failure	Critical
☑	RACK_UPS	Load On Battery	Critical
☑	RACK_UPS	Primary Mains Power Failure	Critical

Figure 7.8

The quick deployment of the alarm notification is completed, and if power insight finds a new alert, it sends a text message to the admin configured phone number, as well as to the admin configured mailbox.

7.3 Detailed Features

7.3.1 Contacts Settings

Contacts settings for admin account

Click on the **“admin”** drop-down box in the upper right corner, and then click on the **“User Profile”** option as shown in **Figure 7.9** below .

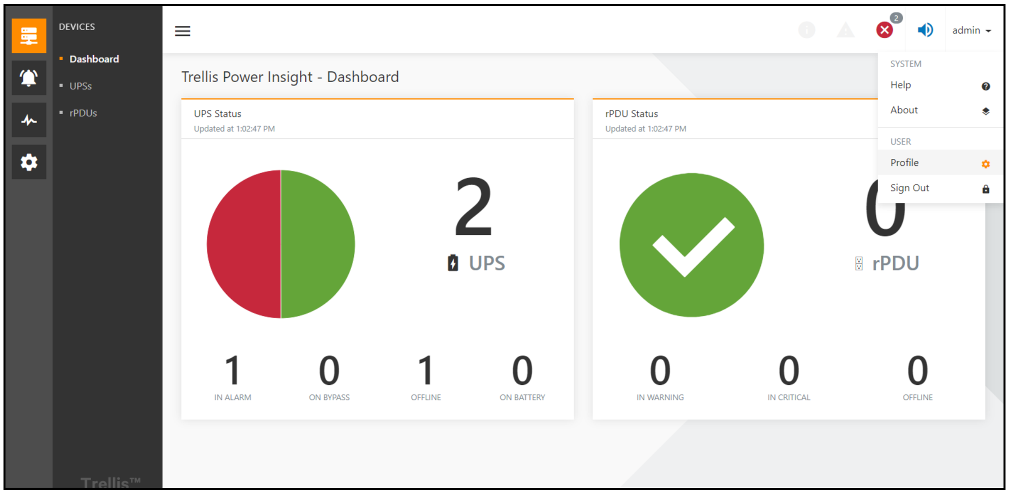
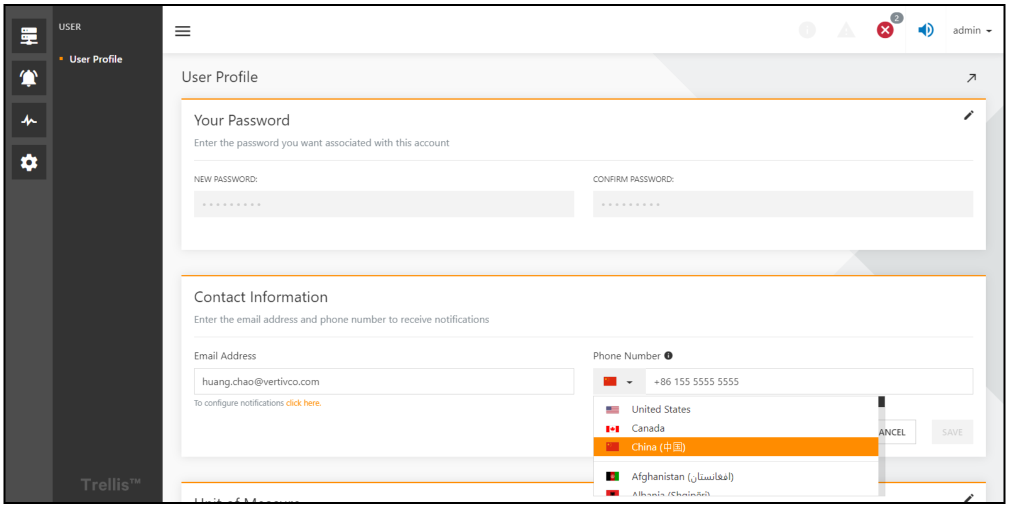


Figure 7.9

Enter the user profile editing interface, click the button in the contact information, you can edit the **email address**, of admin, and save the **phone number**, click “🇨🇳 ▾ ” the drop-down button to select different countries.



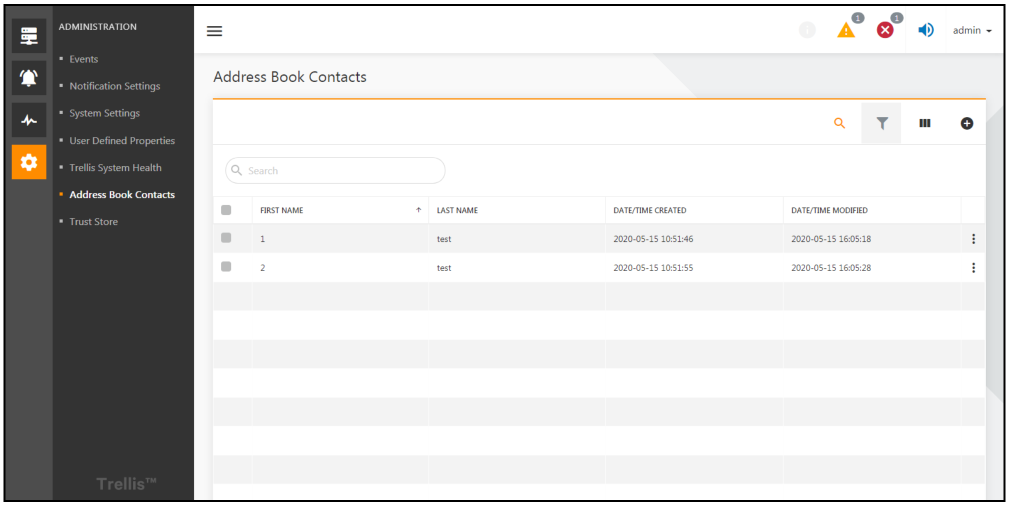
Email Address: huang.chao@vertivco.com

Phone Number: +86 155 5555 5555

Figure 7.10

Other Contacts Settings

Click on "⚙", then click on the "Address book contacts "to enter the address book contacts page, click "⋮" button to select edit or delete the contacts that you have added. For the general operation of the address book contacts list, please refer to Device List on page 36 common List of Operations. All the lists in this chapter can be used for general list operation, which will not be repeated later.

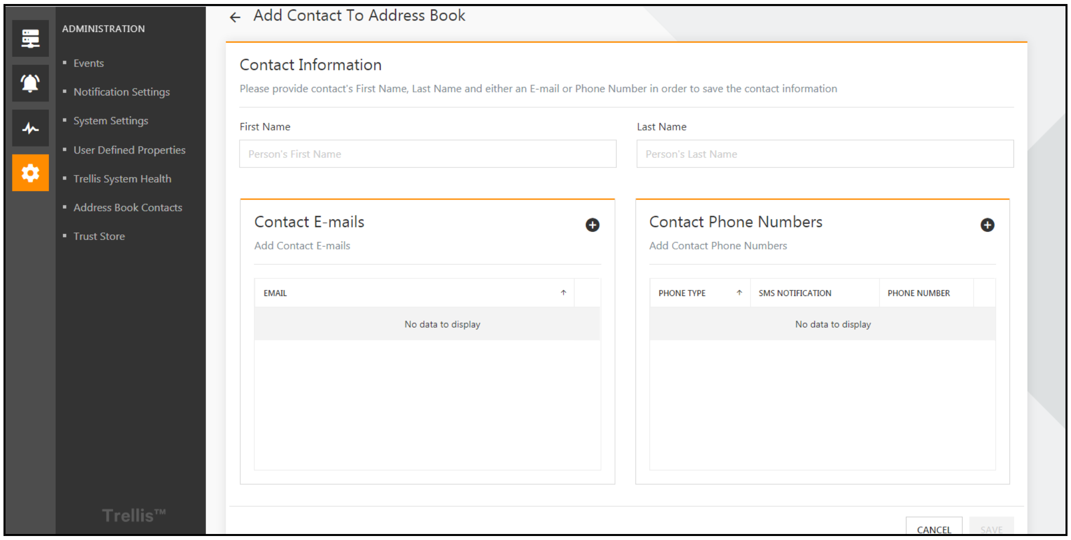


Address Book Contacts

FIRST NAME	LAST NAME	DATE/TIME CREATED	DATE/TIME MODIFIED
1	test	2020-05-15 10:51:46	2020-05-15 16:05:18
2	test	2020-05-15 10:51:55	2020-05-15 16:05:28

Figure 7.11

In the **Figure 7.11** above , Click on "⊕" plus symbol to enter the new contacts interface, as shown in **Figure 7.12** below . New contacts require first name, last name, contact email, and contact phone (optional). Click on *plus symbol* "⊕" on the contact E-mails section will pop-up Add contact E-mail window. After entering the email address click *Add* to add the contact email.



Add Contact To Address Book

Contact Information

Please provide contact's First Name, Last Name and either an E-mail or Phone Number in order to save the contact information

First Name: Person's First Name

Last Name: Person's Last Name

Contact E-mails

Add Contact E-mails

EMAIL
No data to display

Contact Phone Numbers

Add Contact Phone Numbers

PHONE TYPE	SMS NOTIFICATION	PHONE NUMBER
No data to display		

Figure 7.12

When you click on plus button "⊕" on the contact phone numbers section as shown in **Figure 7.12** above , the Add contact phone number box pops up as shown in **Figure 7.13** on the next page where you enter your phone type, phone number, and move slide button to activate/deactivate SMS notification, then click ADD button. After adding a phone number and email ID, click on **Save**.

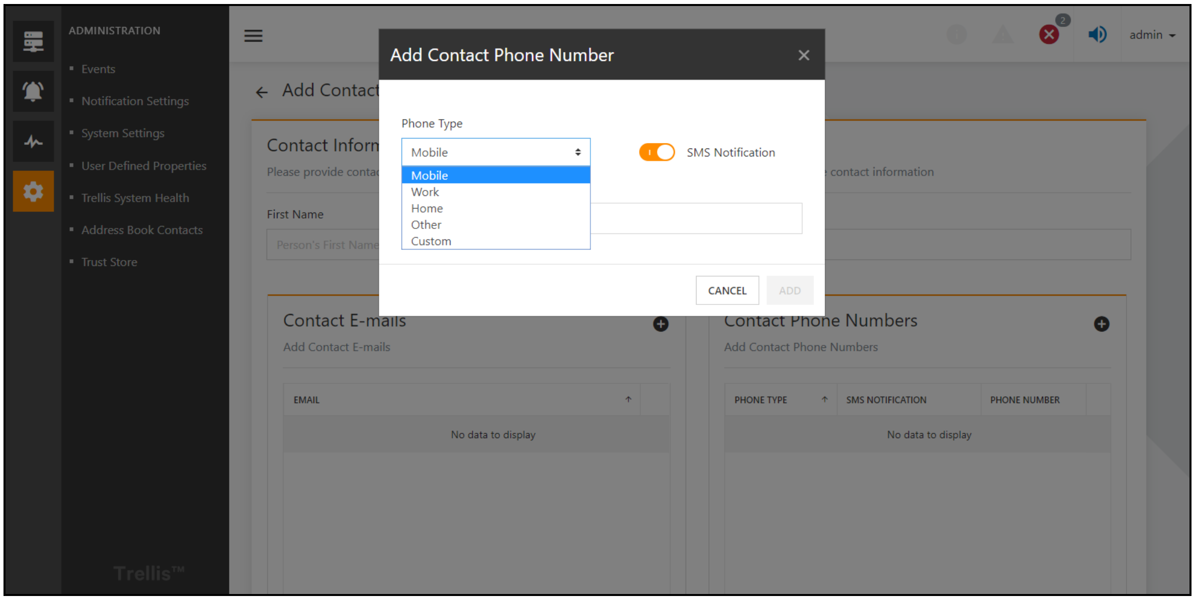


Figure 7.13

NOTE: A single contact can add multiple email slots and phone numbers.

NOTE: After you've added your contact email and phone number, remember to click the Save button in the contact information add interface.

NOTE: When you add a contact to an action's address book, all the contact's email addresses are notified if the action is to send a message. If the action is to send a text message, the contact's mobile phone number will only accept the text message if the number that initiates the SMS notification.

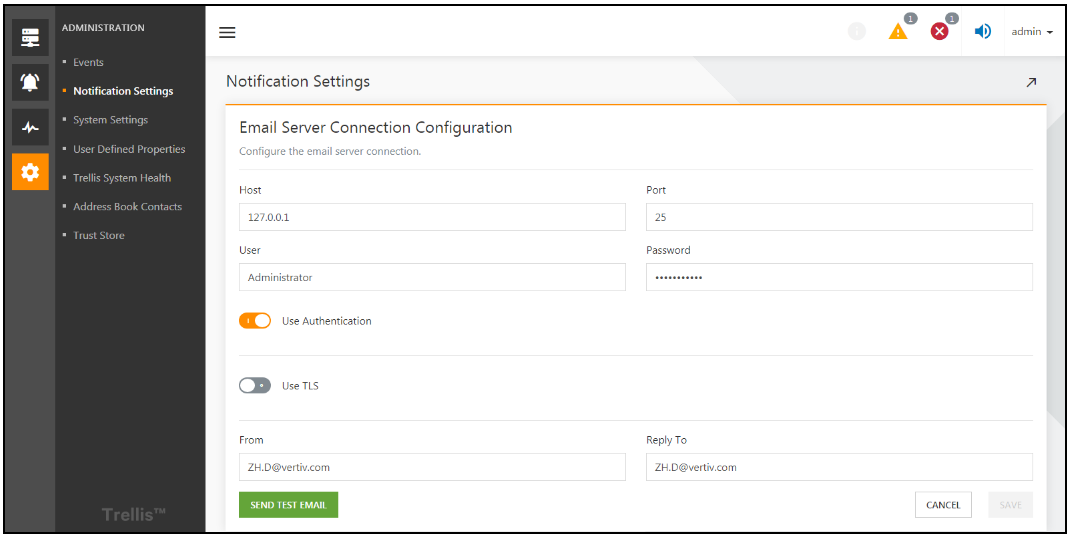
7.3.2 Email and SMS notification settings

Click on “⚙ ” icon, then click **Notification Settings** menu to enter the notification settings page, click edit icon “✎” to configure the email server connection, as shown in **Figure 7.14** on the facing page . Enter following information to configure the e-mail server: the host (the host IP address where the mail server is located), the port (mail server process port number),the user (the user set by the mail server), the password (password set by the mail server), use authentication, use TLS protocol, sender's mailbox (the sender address needed when the mail server sends the mail), and reply mailbox (the email address used by the mail server to accept the external mail). After the mail server configuration is configured, it is recommended to send a test email first, and then click **“Save”** configuration after test s successful.

NOTE: The user and password are not the username and password used by the host to log on, but the username and password configured by the mail server process on the host.

NOTE: The mail server configuration in Power Insight needs to be consistent with the parameters configured by the mail server process on the remote host.

NOTE: The use of authentication and the TLS protocol can enhance the security of the mail server, but the configuration of Power Insight is not effective until configuration modifications are made synchronously by the mail server process on the remote host.



Notification Settings

Email Server Connection Configuration

Configure the email server connection.

Host: 127.0.0.1

Port: 25

User: Administrator

Password: •••••••••••

Use Authentication: on

Use TLS: off

From: ZH.D@vertiv.com

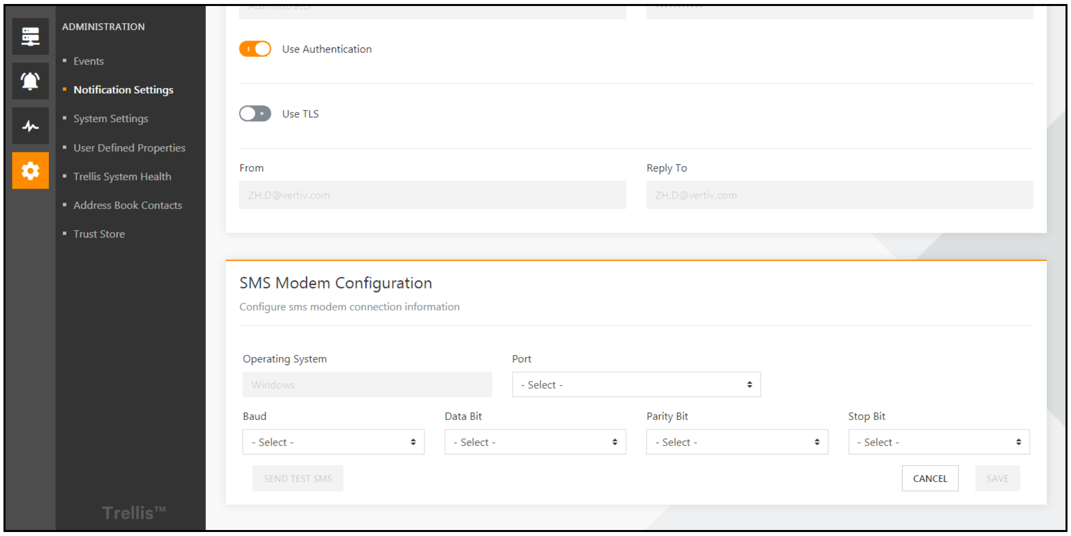
Reply To: ZH.D@vertiv.com

Figure 7.14

In the **Notification Settings** interface, click the edit icon “✎” to configure SMS modem connection information as shown in Fig **Figure 7.15** below . Users need to select the following information: port (try to select the recommended port), port rate, data bit, parity code, stop bit. Before saving the configuration, it is recommended that the user to send a text message to ensure that the configuration is correct.

NOTE: The operating system is automatically read by PI, the operating system of the host installed by the Power Insight.

NOTE: Before you configure a SMS modem, you need to connect the SMS modem to the host installed by Power Insight, and then install the drive and initialization configuration for the SMS modem. Power Insight's SMS modem configuration should be as consistent as possible with the SMS modem initial configuration.



Use Authentication: on

Use TLS: off

From: ZH.D@vertiv.com

Reply To: ZH.D@vertiv.com

SMS Modem Configuration

Configure sms modem connection information

Operating System: Windows

Port: - Select -

Baud: - Select -

Data Bit: - Select -

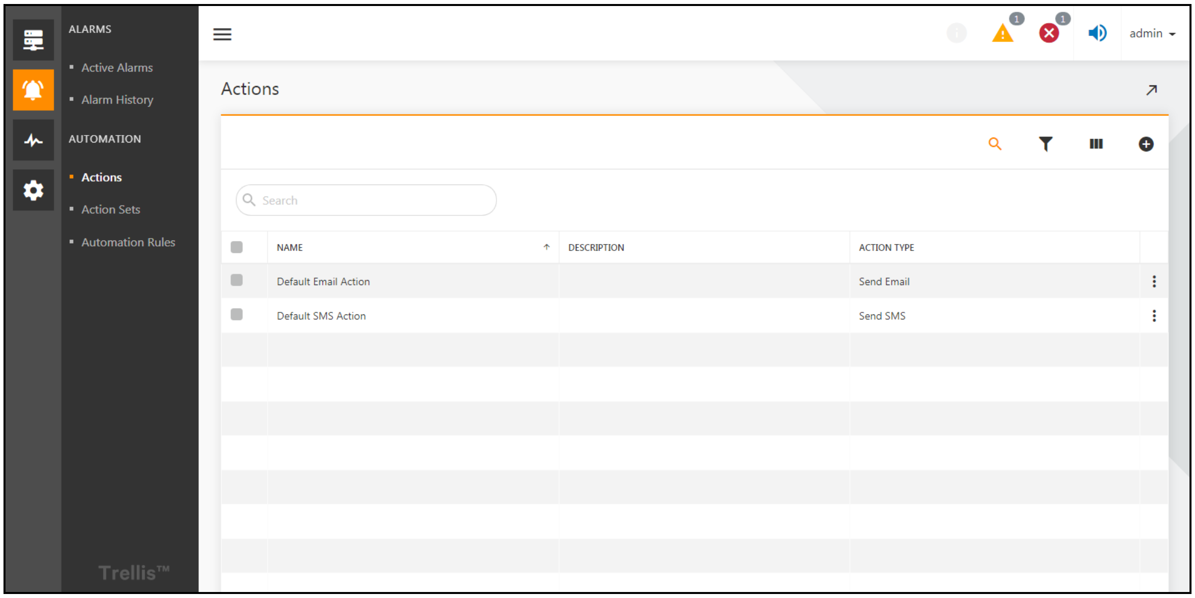
Parity Bit: - Select -

Stop Bit: - Select -

Figure 7.15

7.3.3 Actions Settings

1. Click on bell icon"🔔", then click on the Actions menu to enter the actions page, as shown in **Figure 7.16** below . The system creates the default email notification action and the default SMS notification action by default. Click the button "⋮" on the right to select edit, delete, and copy existing actions. Action role: The action that the system needs to perform when an alarm is triggered.

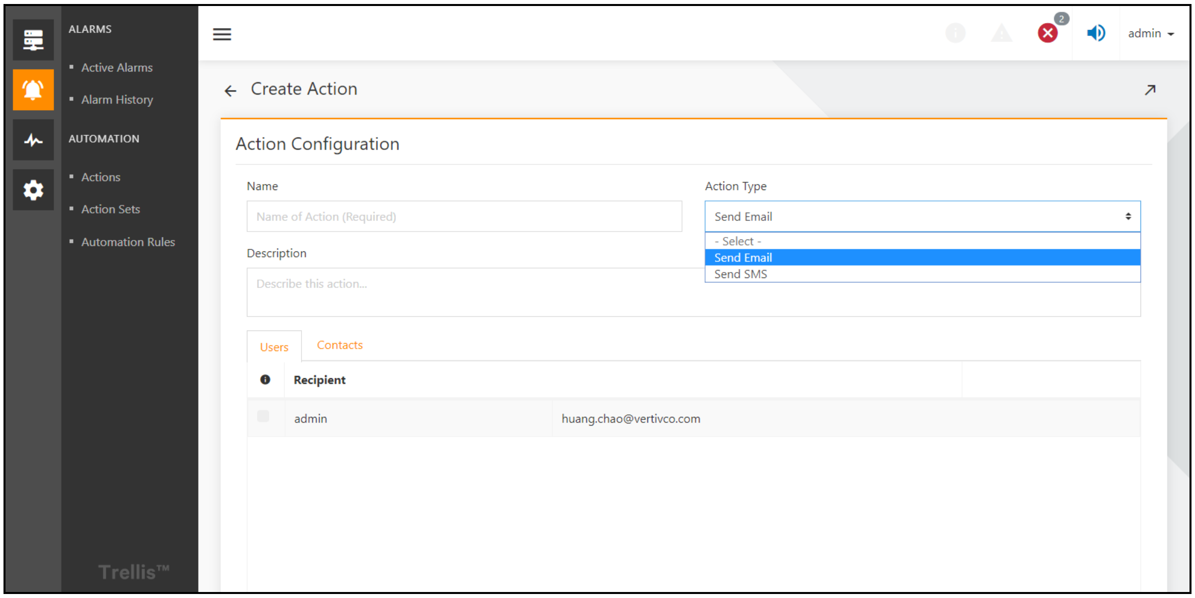


NAME	DESCRIPTION	ACTION TYPE
Default Email Action		Send Email
Default SMS Action		Send SMS

Figure 7.16

2. Click on add icon "⊕" to enter the create Action interface, as shown in **Figure 7.17** on the facing page . Enter the following information: name, action type (send a text message or email), description (optional), and recipient. The recipient can select an admin user, or the contact that the user adds to the contacts. Users can select multiple recipients.

NOTE: Recipient information varies with the choice of action type, and when you select the type to send a message, only the users and contacts who have configured the email address are displayed in the recipient list. The same is true of the type of text message that is sent.



Create Action

Action Configuration

Name: Name of Action (Required)

Action Type: Send Email

- Select -
Send Email
Send SMS

Description: Describe this action...

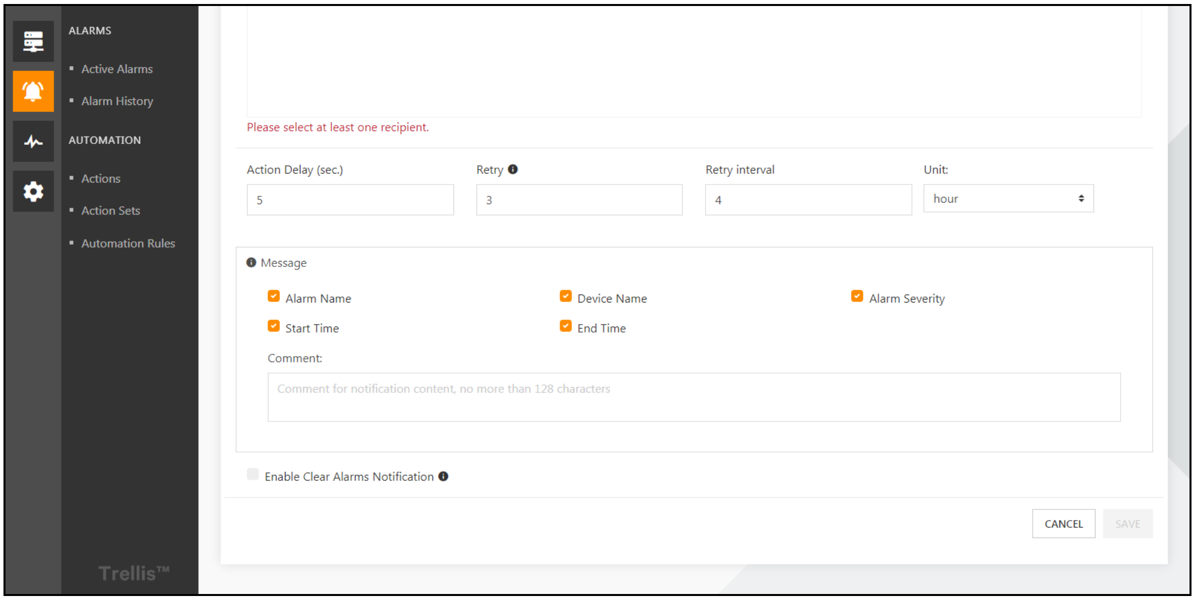
Users | Contacts

	Recipient	
□	admin	huang.chao@vertivco.com

Figure 7.17

As shown in **Figure 7.18** below , Scroll down to configure the "Action Delay" (default 5 seconds, representing the delay time of action start), Retry (the number of repeated notifications when the alarm is not acknowledged), the retry interval. You can view the content of preset notifications for alarm notification input including: alarm name, device name, alarm severity, start time, end time. Scroll down to configure whether to enable end of alarm notification, and then click Save.

NOTE: After an alarm triggers an action, if the alarm is completed by the system within the time of the operation delay, the action will be cancelled.



Please select at least one recipient.

Action Delay (sec.): 5

Retry: 3

Retry interval: 4

Unit: hour

Message

☑ Alarm Name ☑ Device Name ☑ Alarm Severity

☑ Start Time ☑ End Time

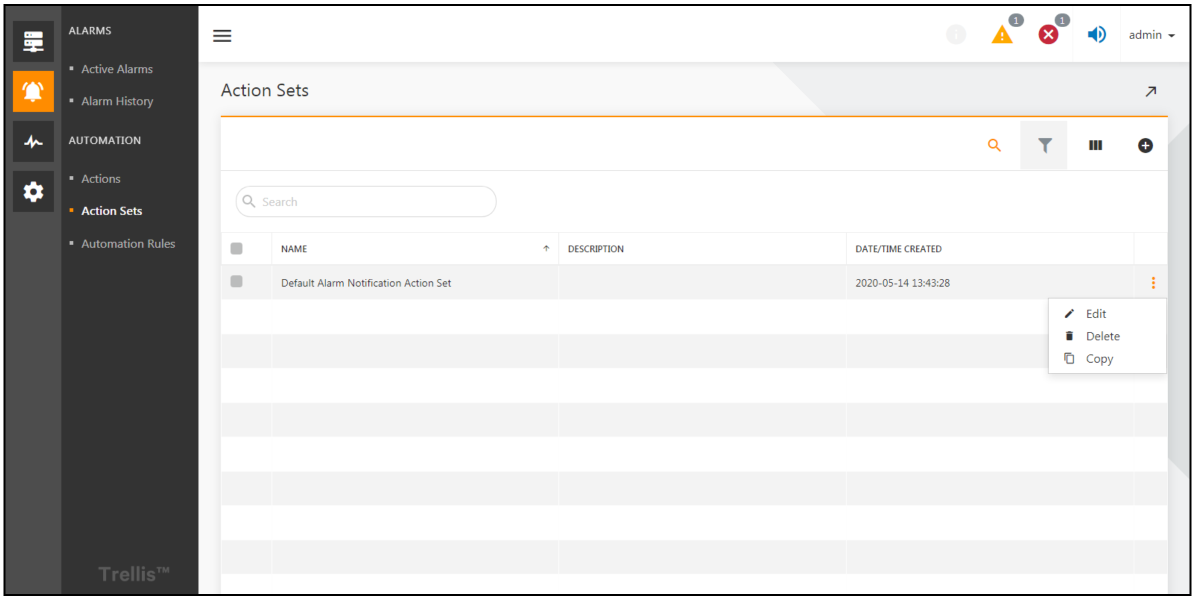
Comment: Comment for notification content, no more than 128 characters

□ Enable Clear Alarms Notification

Figure 7.18

7.3.4 Action Sets Settings

1. Click on the “ ” icon, then click **“Action sets”** to enter the Action sets page. The Action Sets context menu item allows you to group actions and configure their execution when an alarm condition is met. For example, you can group an email and SMS text notification to be sent at the same time or one after the other when an alarm is triggered. The system creates a default action sets by default, and the default action combination contains only the default message notification action. Click the ”⋮” button on the right to edit, delete, and copy the action sets.



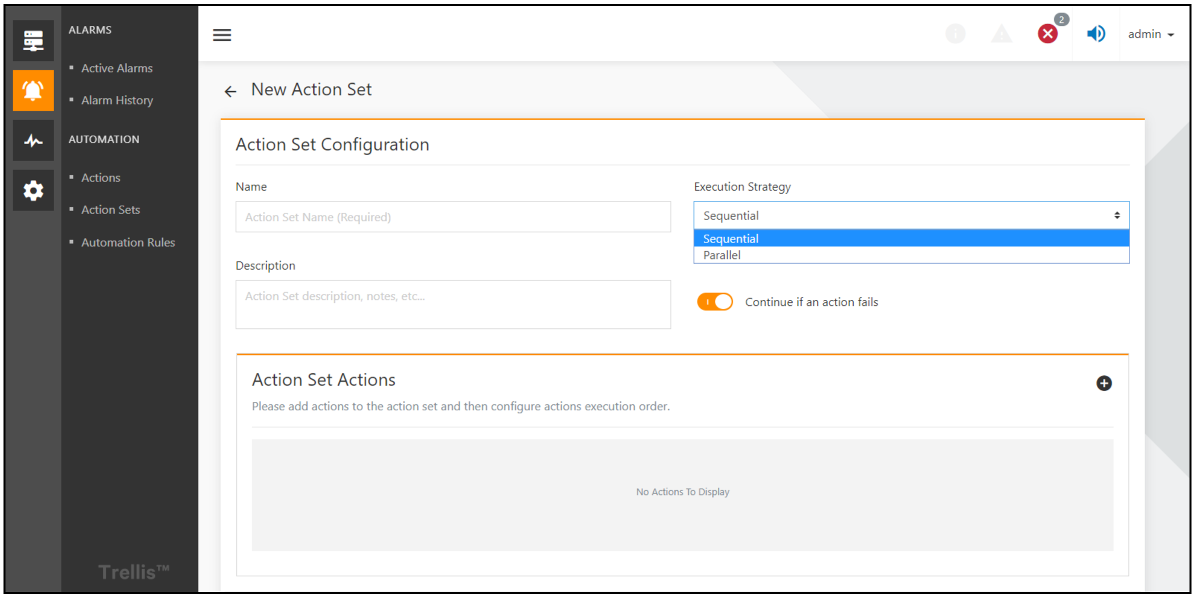
NAME	DESCRIPTION	DATE/TIME CREATED
Default Alarm Notification Action Set		2020-05-14 13:43:28

Figure 7.19

Click “⊕“ to enter the New Action set interface, where the action set configuration requires the name, description, execution strategy (serial or parallel), and action list. If the selected execution strategy is serial, you also need to choose whether to continue to execute the next action when an action fails to execute.

NOTE: Serial execution strategy: The actions in the group are arranged in a queue order, and the actions in the queue are executed in sequence. Next action can be continued only when the execution of the previous action ends.

NOTE: Parallel execution strategy: All actions are started simultaneously, in no particular order



← New Action Set

Action Set Configuration

Name: Action Set Name (Required)

Execution Strategy: Sequential
- Sequential
- Parallel

Description: Action Set description, notes, etc...

Continue if an action fails

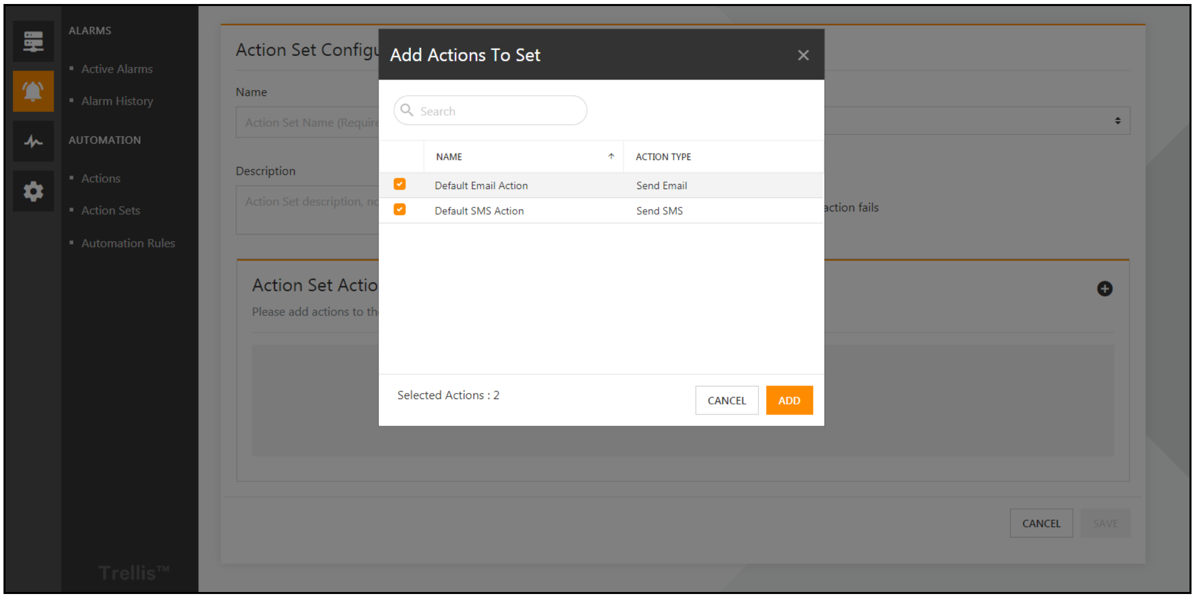
Action Set Actions

Please add actions to the action set and then configure actions execution order.

No Actions To Display

Figure 7.20

Click the add “⊕ ” icon on Action set Actions panel popup the add actions to set window, as shown in **Figure 7.21** below . Select the actions to add to the action set and click ADD.



Add Actions To Set ✕

Search

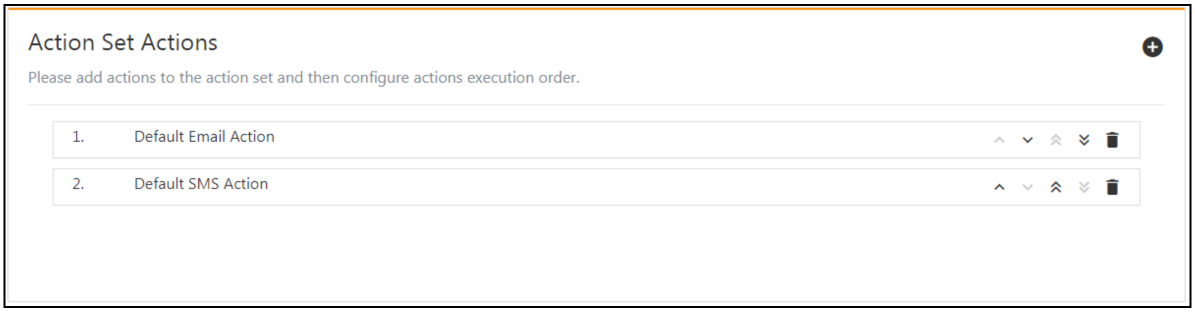
	NAME ↑	ACTION TYPE
☑	Default Email Action	Send Email
☑	Default SMS Action	Send SMS

Selected Actions : 2

CANCEL ADD

Figure 7.21

After you add an action to the action set actions list, you can adjust the order of the actions in the action list, as shown in **Figure 7.22** on the next page ⌃ ⌄ ⇑ ⇓ The four buttons represent move up, down, move to the top, and move to the bottom. Finally, remember to click **Save.**



Action Set Actions

Please add actions to the action set and then configure actions execution order.

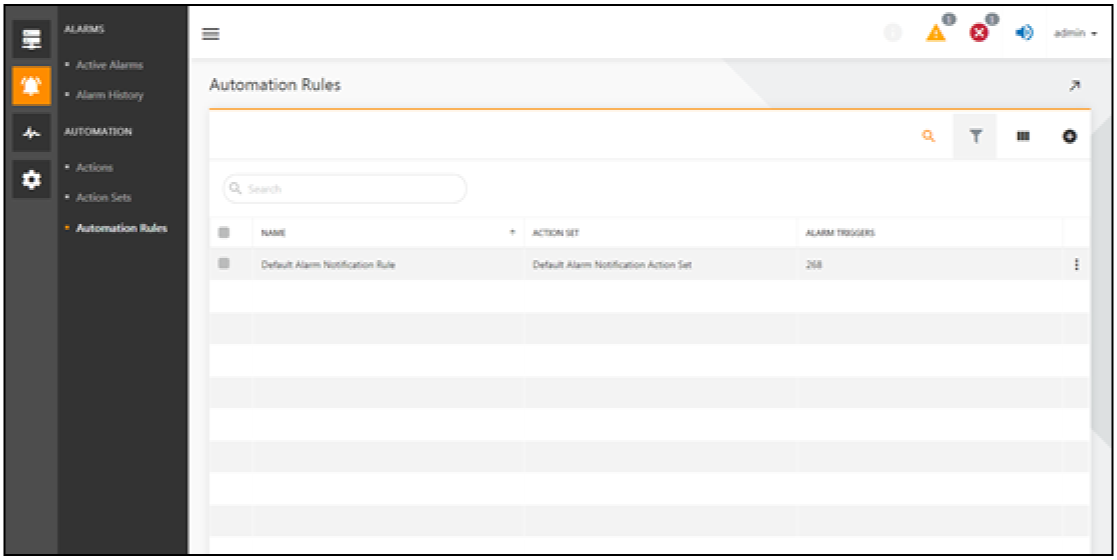
1.	Default Email Action
2.	Default SMS Action

Figure 7.22

7.3.5 Automation Rules Settings

Click on " " icon, then click on the Automation rules menu to enter the Automation rules page, as shown inFigure 7.23 below . The Power Insight application allows you to create automation rules to map action sets to an alarm. Automation rules tell the system what actions to execute when alarms are triggered. In the default Alarm

Notification automation rule, any alarm on any device will trigger the Default Alarm Notification Action Set. Configure which devices which alarms can trigger which action combinations. Click the "⋮" button on the right to select edit, delete, and copy existing automation rules.



Automation Rules

Search

NAME	ACTION SET	ALARM TRIGGERS
Default Alarm Notification Rule	Default Alarm Notification Action Set	268

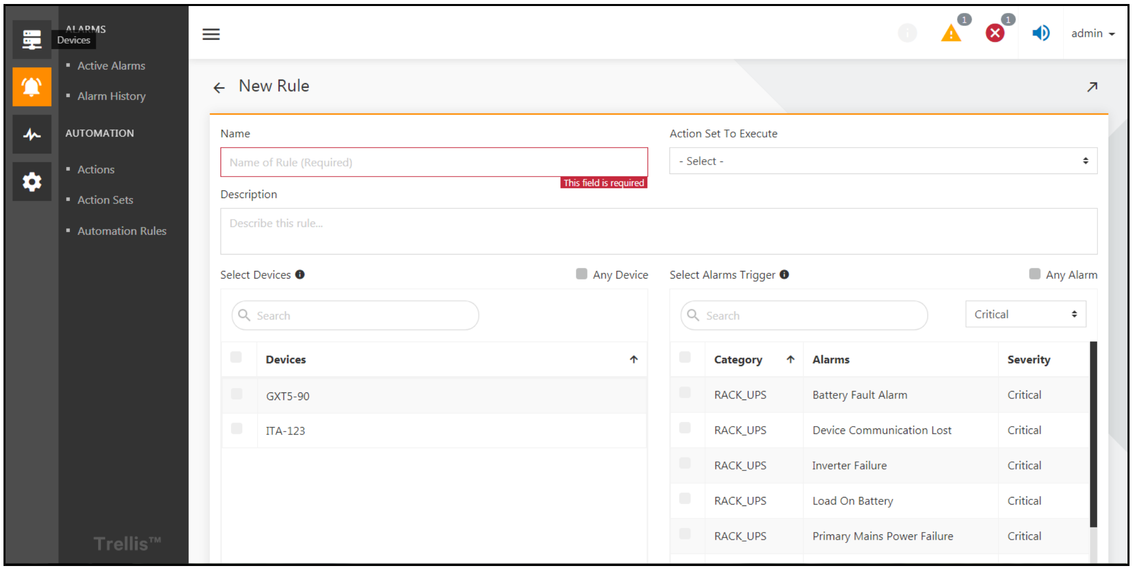
Figure 7.23

Click the "⊕" icon in Figure 7.23 above to enter the new rule interface, as shown in Figure 7.24 on the facing page . Then enter the automation rules name, description, and Select the action set from the Action Set To Execute drop-down list. Finally, Select the devices to which the automated rule will be applied and Select the alarms to activate the automated rule and click SAVE.

NOTE: Select the device can select any device, select the alarm can also select any alarm, so that all current devices and alarms will be selected, and the new equipment will be automatically selected in the future. In this configuration, then, all alarms for all devices trigger the configuration-bound action combination.

NOTE: The alarm list will only show the alarm supported by the added device.

NOTE: Both the device list and the alarm list can be searched for list, and the alarm list can also be filtered according to the alarm severity.



New Rule

Name: Name of Rule (Required) — This field is required

Action Set To Execute: - Select -

Description: Describe this rule...

Select Devices — □ Any Device

Search

□	Devices ↑
□	GXT5-90
□	ITA-123

Select Alarms Trigger — □ Any Alarm

Search — Critical

□	Category ↑	Alarms	Severity
□	RACK_UPS	Battery Fault Alarm	Critical
□	RACK_UPS	Device Communication Lost	Critical
□	RACK_UPS	Inverter Failure	Critical
□	RACK_UPS	Load On Battery	Critical
□	RACK_UPS	Primary Mains Power Failure	Critical

Figure 7.24

7.3.6 Alarm Notification Trigger Logic

When you complete the configuration from Detailed Features on page 60 to Automation Rules Settings on the previous page , software can trigger an alarm notification. If the output of UPS123 has an off alarm, the trigger process is as follows:

1. First check whether the existing automation rules has UPS123 selected in the device list, and at the same time check the alarm list that contain the output off alarm, if so, then execute automation rules.
2. The action set is executed, and all actions in the action sets are executed according to the execution strategy of the action set.
3. When performing an action, if the type of action is to send a text message, the text message is sent to the configured contact person in the action according to the text message content configuration in the action configuration.

This page intentionally left blank

8 Communication Profile Configuration

8.1 Overview

Communication profiles define how and through what methods the application communicates with devices. The Power Insight application allows you to search for saved profiles and view devices that are associated with the profile you created.

8.1.1 Function Module

Communication profile configuration contains the following function modules, refer toDetailed Features on the next page detailed functions for detailed information of each function module.

Communication profile configuration list

1. New communication profile
2. List of devices

8.2 Get Started Quickly

8.2.1 Quick Deployment Steps

The quick deployment steps for communication profile configuration are as follows:

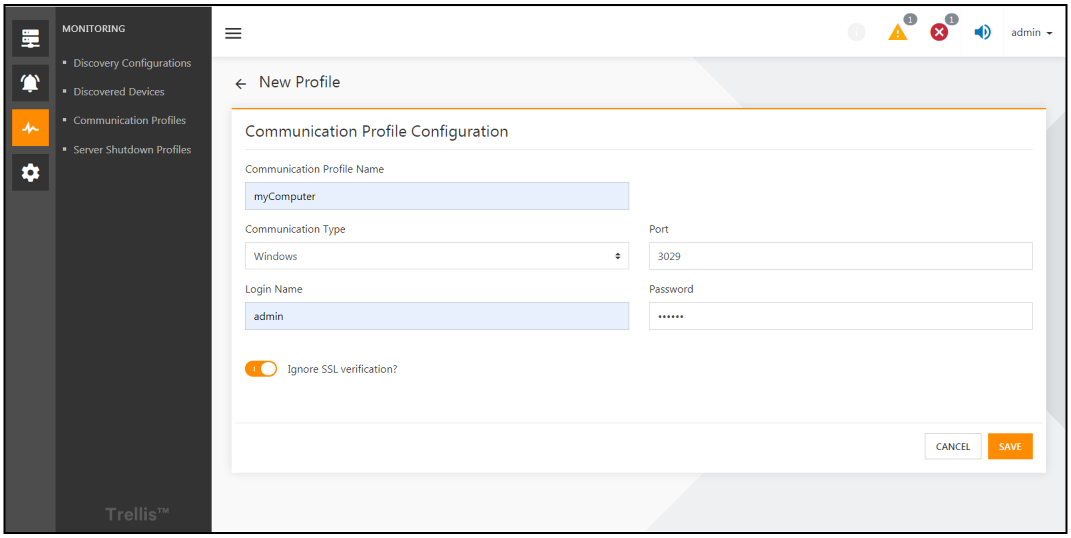
1. New server communication configuration.

8.2.2 Example

Because the communication protocols used by the existing UPS and PDU are both SNMP V1 or SNMP V2, and the communication configurations of SNMP V1 and SNMP V2, the system has been created by default. Therefore, the communication profile of the UPS and PDU need not be considered in a rapid deployment, only the communication parameter configuration that is created for the server.

Before you can create a server communication configuration, you need to install the server shutdown agent on the server refer to Installation of the software on page 3 .

Click on the monitoring icon "∿", then click **Communication Profiles** to enter the communication profile configuration. Click add icon "⊕" on the communication profile configuration page to enter the new profile window, select the communication type such as windows/ VMWareESXi / Linux / Hyperos based on the server operating system, as shown in **Figure 8.2** on the next page . After entering the communication profile name, port (the port number used by the shutdown agent installed on the server, the default is 3029, no change is required), the login name (the remote login name set by the server shutdown agent), the password (the remote login password set by the server shutdown agent), ignore the SSL authentication (because communication with the server shutdown agent temporarily does not support SSL authentication, so the user will be checked this option). After entering the above information and click Save, the deployment of the communication profile configuration is complete.



New Profile

Communication Profile Configuration

Communication Profile Name: myComputer

Communication Type: Windows

Port: 3029

Login Name: admin

Password: ••••••

Ignore SSL verification?

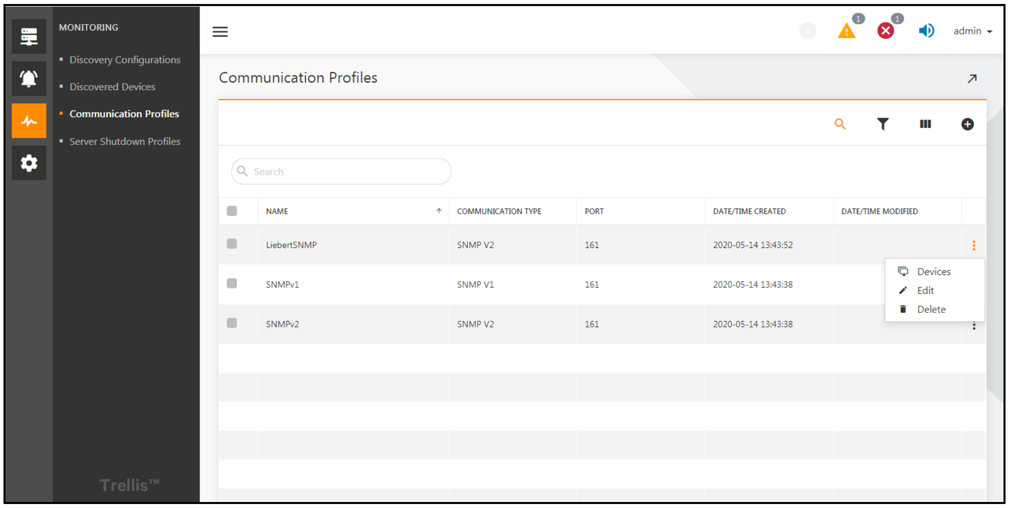
Figure 8.1

8.3 Detailed Features

8.3.1 List of Communication Profile Configurations

Click on the monitoring icon “”, then click Communication profile Configuration to enter the communication profile configuration page, as shown in Figure 8.2 below . Click “⋮” the button on the right to select to edit, delete, or browse the list of devices configured with that communication profile. The system has three communication profile configurations by default: SNMPv1, SNMPv2, Liebert SNMP. The list also supports common list of operations refer to section 5.3.2 on page 36 for more details, which are not repeated later in this chapter.

NOTE: Communication configuration SNMPv1 is a communication configuration that uses the protocol SNMPv1 and the default read and write communication word (public, private). Communication configuration SNMPv2 and Liebert SNMP are both SNMPv2 protocols, but communication configuration SNMPv2 reads and writes the communication words are private, respectively, and Liebert SNMP's read and write communication words are Liebert EM.



Communication Profiles

NAME	COMMUNICATION TYPE	PORT	DATE/TIME CREATED	DATE/TIME MODIFIED
LiebertSNMP	SNMP V2	161	2020-05-14 13:43:52	
SNMPv1	SNMP V1	161	2020-05-14 13:43:38	
SNMPv2	SNMP V2	161	2020-05-14 13:43:38	

Figure 8.2

8.3.2 New Communication Profile Configuration

In **Figure 8.2** on the previous page , click the add icon “⊕” to enter the new profile configuration interface.

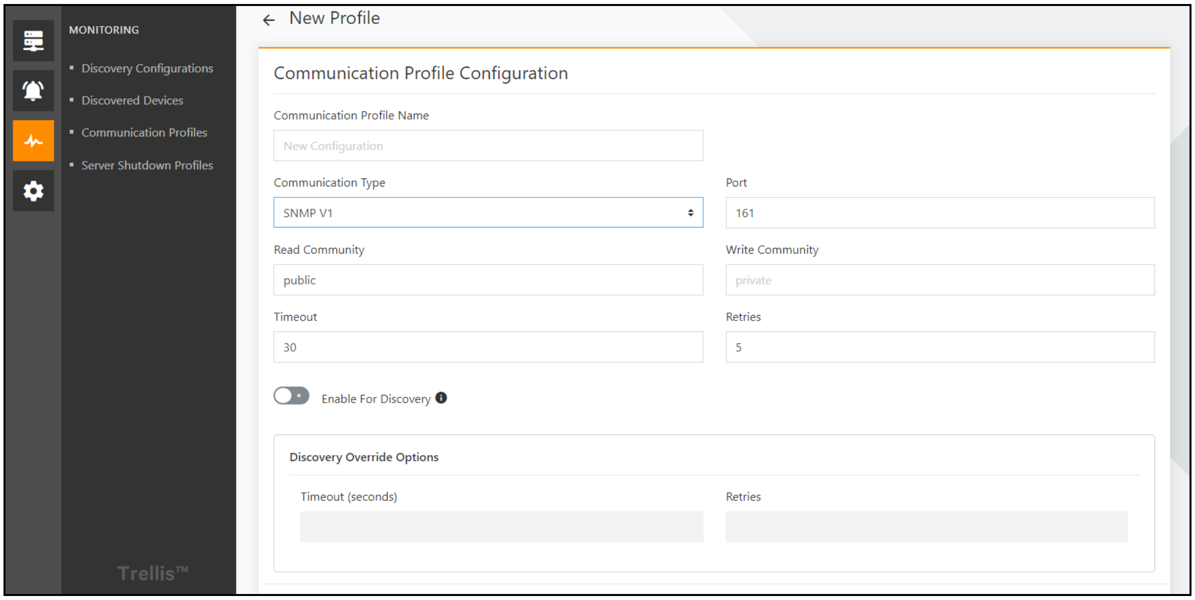
1. New communication profile configuration for SNMP protocol supported devices.

SNMPv1 or SNMPv2

Click on the *monitoring icon* “ “, then click *Communication Profile Configuration* to enter the communication profile configuration page. Click on the *add icon* “⊕” to enter the new profile configuration interface, select the communication type SNMPv1 or SNMPv2, then the interface in **Figure 8.3** below appears.

After entering the communication profile name, port, read community, write community, time out (trying to establish an SNMP connection, in seconds), retries (the number of retries after the connection failed), click *Save.*

You can also choose to set timeouts and retries specifically for device searches. Because device search requires efficiency and performance, specific default timeouts and retries are typically used. Here you can override the default device search configuration by clicking on enable discovery and then entering a customized timeout (seconds) and retries, click *Save.*



Communication Profile Configuration

Communication Profile Name: New Configuration

Communication Type: SNMP V1

Port: 161

Read Community: public

Write Community: private

Timeout: 30

Retries: 5

Enable For Discovery

Discovery Override Options

Timeout (seconds)

Retries

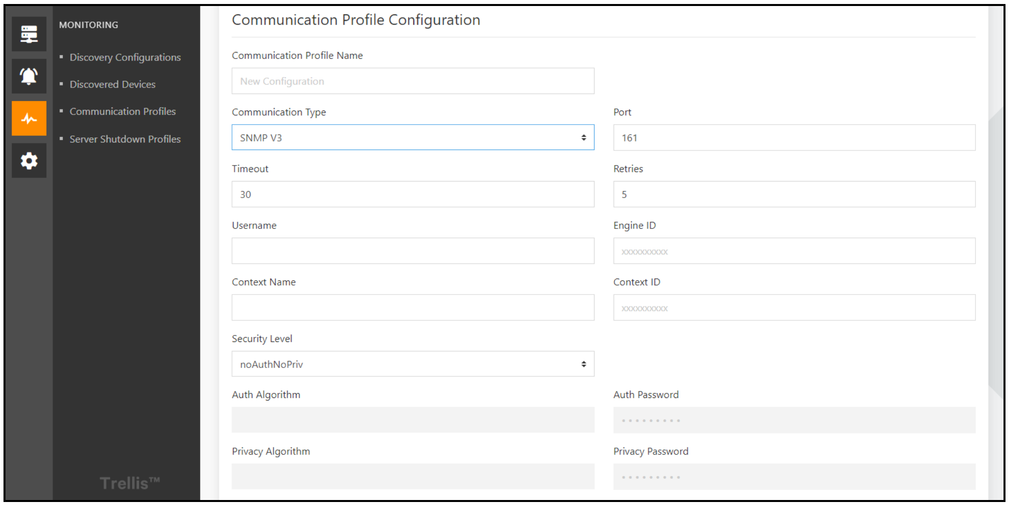
Figure 8.3

SNMPv3

Click on the *monitoring icon* “ “, then click Communication Profile Configuration to enter the communication profile configuration page. Click on the *add icon* “⊕” to enter the new profile configuration interface, select the communication type Is SNMPv3, then the interface appears as shown in **Figure 8.4** on the next page .

The input configuration of SNMPv3 in Power Insight needs to be the same as the configuration of SNMPv3 of the connected device. At the same time, there are three levels of security: no authentication and no encryption, authorization and no encryption, and authorization & encryption. selecting a different level of security requires different security information to enter.

Currently, few devices connected to Power Insight use SNMPv3, so it is generally not necessary to create an SNMPv3 communication configuration.



Communication Profile Configuration

Communication Profile Name: New Configuration

Communication Type: SNMP V3

Port: 161

Timeout: 30

Retries: 5

Username:

Engine ID: xxxxxxxxxx

Context Name:

Context ID: xxxxxxxxxx

Security Level: noAuthNoPriv

Auth Algorithm:

Auth Password: ••••••••••

Privacy Algorithm:

Privacy Password: ••••••••••

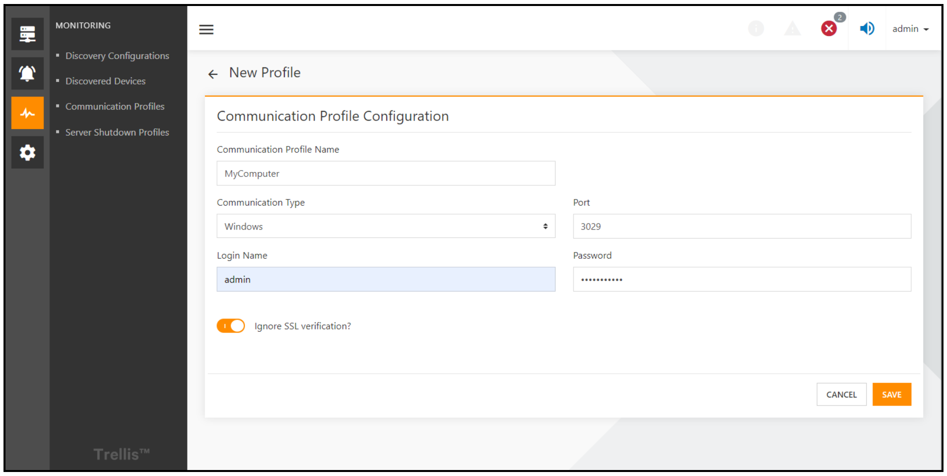
Figure 8.4

2. New Server Communication Profile Configuration

Before you can add a server communication profile configuration, you need to install the server shutdown agent on the server refer to Installation of the software on page 3 .

Click on the monitoring icon “ ” , then click Communication Profile Configuration to enter the communication profile configuration page. Click on add icon “⊕” to enter the new profile configuration interface, select the communication type such as windows/ VMWareESXi / Linux / Hyperos based on the server operating system, as shown in Figure 8.5 below . After entering the communication profile name, port (the port number used by the shutdown agent installed on the server, the default is 3029, no change is required),the login name (the remote login name set by the server shutdown agent), the password (the remote login password set by the server shutdown agent), ignore the SSL authentication (because communication with the server shutdown agent temporarily does not support SSL authentication, so the user will be checked this option). After entering the above information and click *Save*, the deployment of the communication profile configuration is complete.

NOTE: The information in the server communication profile configuration needs to be consistent with the parameter configuration of the server shutdown agent installed by the server, otherwise the configuration doesn't not work.



New Profile

Communication Profile Configuration

Communication Profile Name: MyComputer

Communication Type: Windows

Port: 3029

Login Name: admin

Password: •••••••••••

Ignore SSL verification? (on)

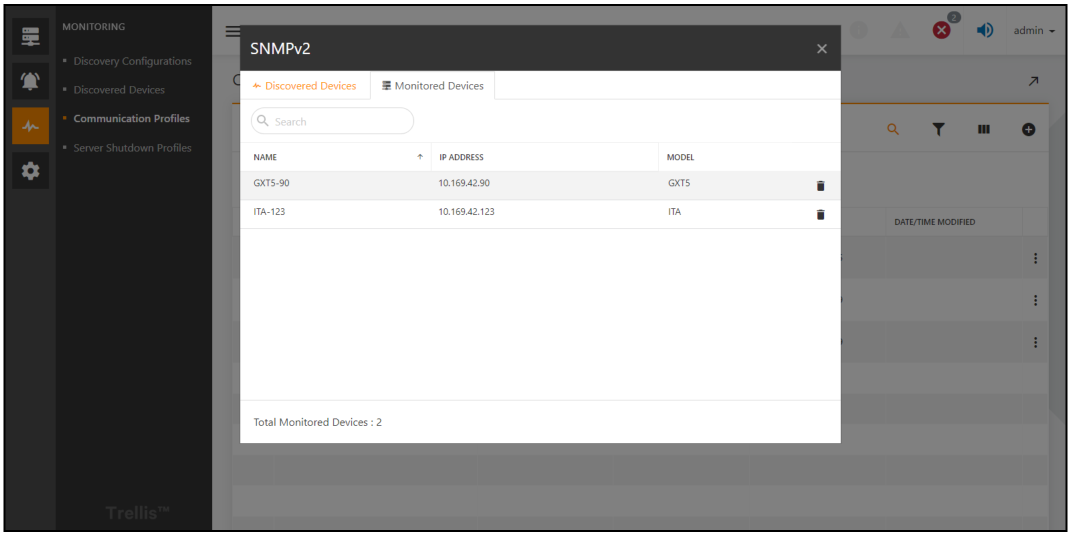
Figure 8.5

8.3.3 Device List

Click monitoring icon “∿ ”, then click the communication profile configuration to enter the communication profile configuration page, and finally click “⋮” icon located on the right side of the device list pops up the window and click the *Devices*.

If the communication profile configuration to which the device list belongs is the configuration of the SNMP protocol, the interface shown in Figure 8.6 below pops up. The list of devices for the SNMP protocol is divided into two-tab pages: all discovered devices, monitored devices, and showing all IP devices that use this communication configuration. Usually we only need to care about the monitored device. For the source of the device information here, please see the automatic device discovery and manual device addition in Add UPS, rPDU on page 27 . If you remove a device from the list of devices, Power Insight will completely delete all information about the device.

If the communication configuration to which the device list belongs is the server communication configuration, the interface shown in Figure 8.7 below pops up. The interface shows which communication configurations are used on servers added to Power Insight. For the server information source, please refer to Server Shutdown Profile on page 77 to add a server.



SNMPv2

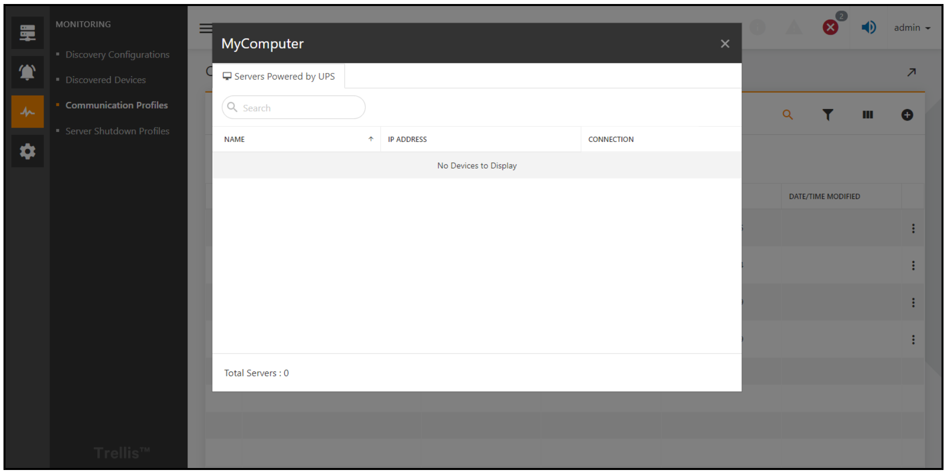
Discovered Devices | Monitored Devices

Search

NAME	IP ADDRESS	MODEL
GXT5-90	10.169.42.90	GXT5
ITA-123	10.169.42.123	ITA

Total Monitored Devices : 2

Figure 8.6



MyComputer

Servers Powered by UPS

Search

NAME	IP ADDRESS	CONNECTION
No Devices to Display		

Total Servers : 0

Figure 8.7

This page intentionally left blank

9 Server Shutdown Profile

9.1 Overview

When an alarm is received and an automated rule is applied, the application begins the designated action you set up. When the designated action is a server shutdown, the application looks for the servers powered by the UPS or rPDU and begins the server shutdown process. Server Shutdown profiles indicate for the servers which alarms and delay timers will be used to trigger a shutdown. For example, you can arrange for the servers powered by a UPS with a Load on Battery alarm to shut down later than those powered by a UPS that have a Low Battery alarm. You can also create profiles that shut down critical servers sooner than non-critical servers. The Power Insight application contains a default shutdown profile with three alarms to trigger a server shutdown. You can set the timer for the shutdown process to complete for each triggered alarm via the Server Shutdown Profile context menu item.

Each server can have only one Server Shutdown Profile and the profile should include all alarms that cause a shutdown from all UPSs and rPDUs that power the server.

9.1.1 Function Module

Server shutdown profile management include the following functional modules, each of which is detailed in this manual in List of Server Shutdown Profiles on page 83

1. List of servers
2. New servers
3. List of server shutdown profiles
4. New server shutdown profiles

9.2 Get Started Quickly

9.2.1 Quick Deployment Steps

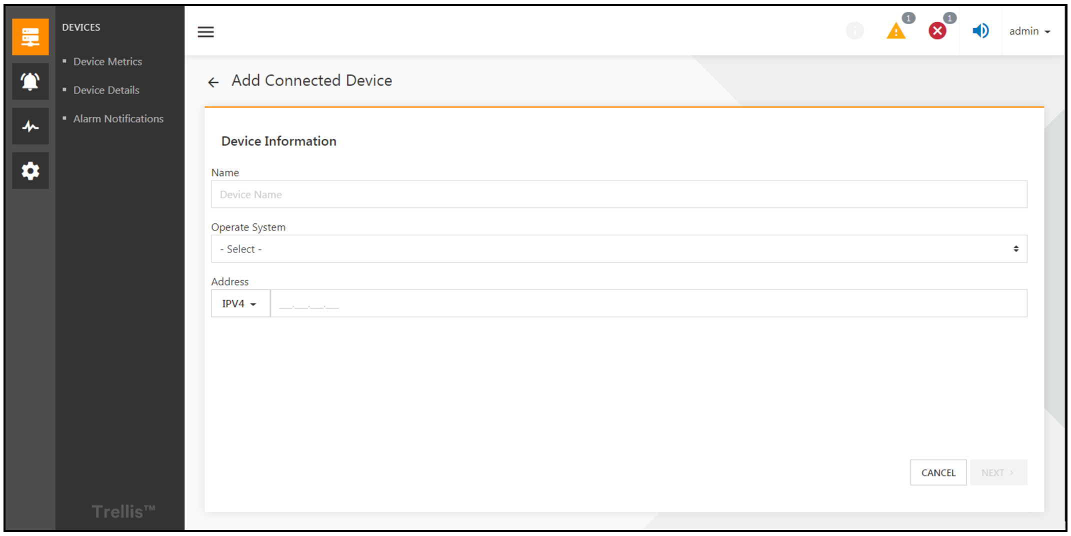
The quick deployment steps for server shutdown profile management are as follows:

1. Add a new server and bind the shutdown configuration.

9.2.2 Example

If you want to add a server powered by ITA2-UPS now.

Click on device icon “🖥”, then click on the UPSs list. By clicking “⋮” button on the far right of the ITA2-UPS list item, a small window pops up and click on the device details to enter device information where you can see the list of servers powered by UPS, click the add icon “⊕” button in the list to open the new server page, as shown in **Figure 9.1** on the next page , enter the server name, select the operating system type (windows / VMWare ESXi / Linux / Hyperos), enter the IP address and click next.



Add Connected Device

Device Information

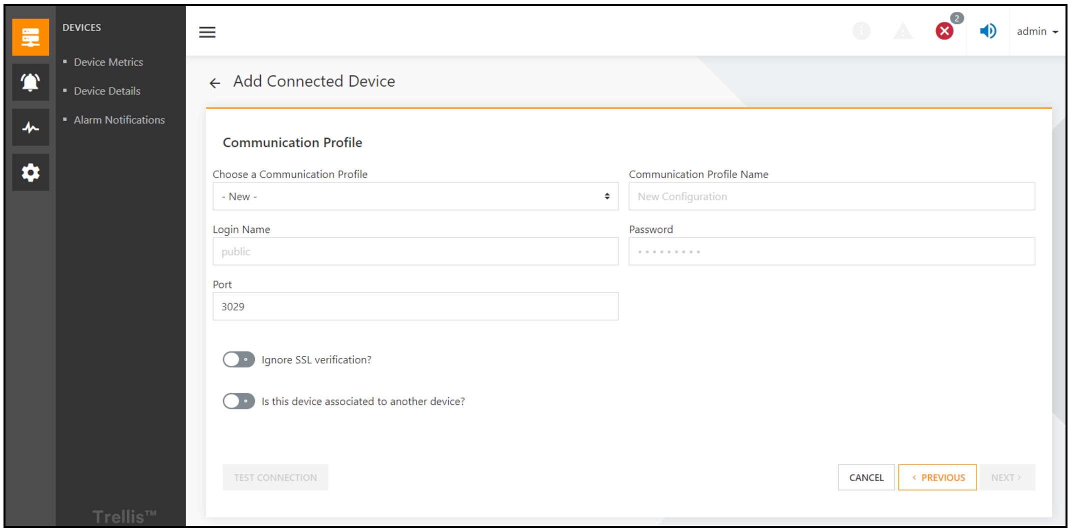
Name: Device Name

Operate System: - Select -

Address: IPV4 __.__.__.__

Figure 9.1

Then go to the second page, as shown in **Figure 9.2** below , to configure the server communication profile. Here you can choose an existing communication profile, or you can create a new communication profile on this interface. Refer to New Communication Profile Configuration on page 73 explains detailed steps to configure communication profile. After the configuration of the communication, it is recommended to test the connection first, and then click Next after success. If you select whether this device is associated with another device, go to the interface shown in **Figure 9.3** on the facing page , select a different UPS or PDU device, and click *Next*. This allows you to connect the new server to other devices at the same time.



Add Connected Device

Communication Profile

Choose a Communication Profile: - New -

Communication Profile Name: New Configuration

Login Name: public

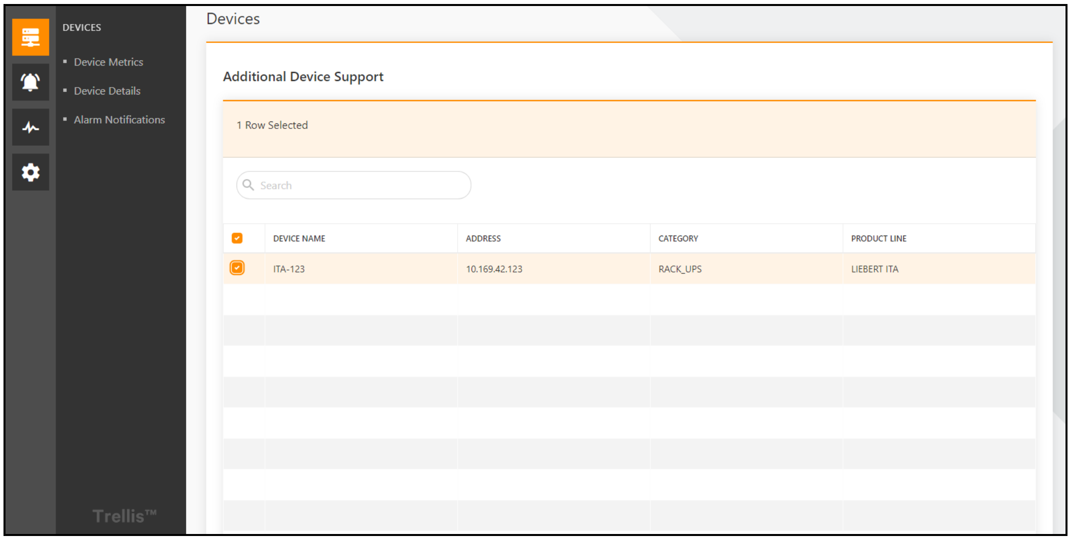
Password: •••••••••

Port: 3029

Ignore SSL verification?

Is this device associated to another device?

Figure 9.2



Devices

Additional Device Support

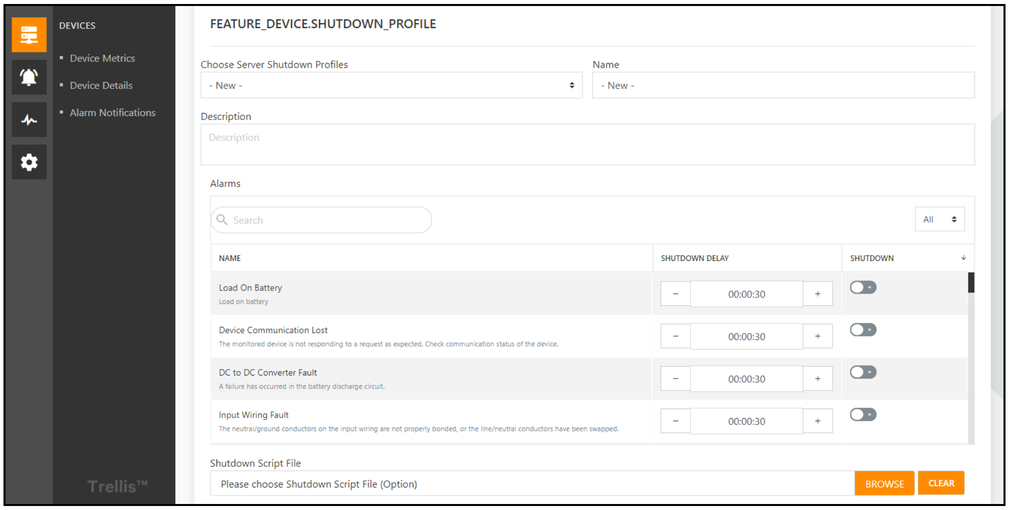
1 Row Selected

Search

☑	DEVICE NAME	ADDRESS	CATEGORY	PRODUCT LINE
☑	ITA-123	10.169.42.123	RACK_UPS	LIEBERT ITA

Figure 9.3

Go to the *next step*, binding the server shutdown configuration, as shown in **Figure 9.4** below . The system will help you select the default shutdown configuration by default. The default shutdown configuration contains three alarms that trigger a server to shut down: the load is battery-powered, the battery power is low, and the battery is discharged. If you need to execute a shutdown script when the server shuts down, you can browse and import shut down script from the local computer, and then click *Save*. After saving successfully, return to the list of servers powered by UPS. At the same time, the load of ITA2-UPS uses battery power supply, low battery power, battery discharge alarm can also trigger the server to shut down.



FEATURE_DEVICE.SHUTDOWN_PROFILE

Choose Server Shutdown Profiles: - New -

Name: - New -

Description: Description

Alarms

Search　All

NAME	SHUTDOWN DELAY	SHUTDOWN
Load On Battery Load on battery	− 00:00:30 +	○
Device Communication Lost The monitored device is not responding to a request as expected. Check communication status of the device.	− 00:00:30 +	○
DC to DC Converter Fault A failure has occurred in the battery discharge circuit.	− 00:00:30 +	○
Input Wiring Fault The neutral/ground conductors on the input wiring are not properly bonded, or the line/neutral conductors have been swapped.	− 00:00:30 +	○

Shutdown Script File: Please choose Shutdown Script File (Option)

Figure 9.4

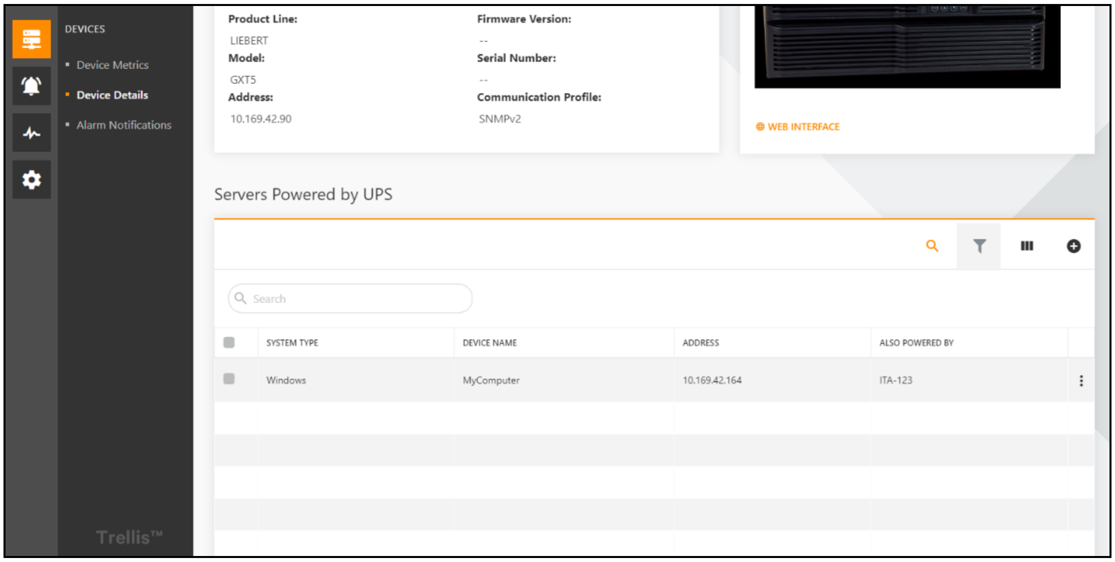
9.3 Detailed Features

9.3.1 Server List

Currently, Power Insight does not specifically manage servers, and all server lists are based on a list of servers powered by a device. There are currently two lists: a list of servers powered by UPS and a list of servers powered by the rPDU. The structure of the two is the same. Next, take the list of servers powered by UPS as an example.

Click on *device icon* "🖥", then click on the *UPSs list*. By clicking "⋮" button on the far right of the UPS list item, a small window pops up and click on the device details to enter device information where you can see the list of servers powered by UPS, as shown in Figure 9.5 below . You can see that the server My Computer has been added. And the list contains system type, device name, address, and powered by (there may be multiple devices connected to the same server). Click on "⋮" button right side of the list to edit and delete *the server*.

The server lists can also be used for common list of operations, for more details, refer to Device List on page 36 , common list of operations. The common list of operations in this chapter are no longer repeated.



Product Line: LIEBERT
Model: GXT5
Address: 10.169.42.90
Firmware Version: --
Serial Number: --
Communication Profile: SNMPv2

Servers Powered by UPS

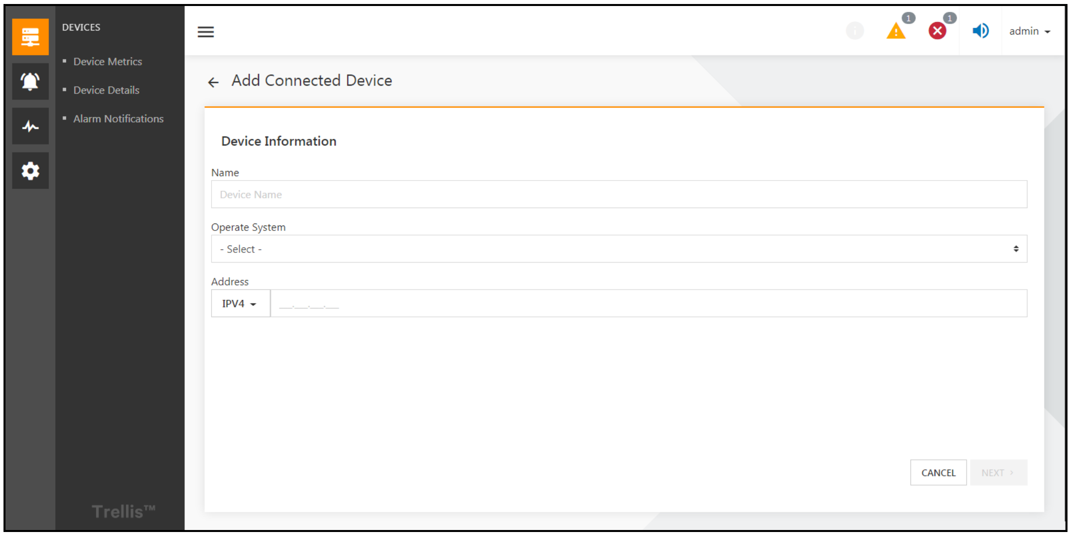
	SYSTEM TYPE	DEVICE NAME	ADDRESS	ALSO POWERED BY	
□	Windows	MyComputer	10.169.42.164	ITA-123	⋮

Figure 9.5

9.3.2 New Servers

Click the *add icon* "⊕" button in Figure 9.5 above to enter the *new server page*, as shown in Figure 9.6 on the facing page . Enter the *server name*, select the *operating system type (windows/VMWare ESXi/Linux/Hyperv(via OS)*, enter the *IP address* and click *next*.

NOTE: If you select an operating system type that is VMWare, the server cannot and a shutdown script configuration for subsequent use because VMWare does not currently support shutdown scripts.



Add Connected Device

Device Information

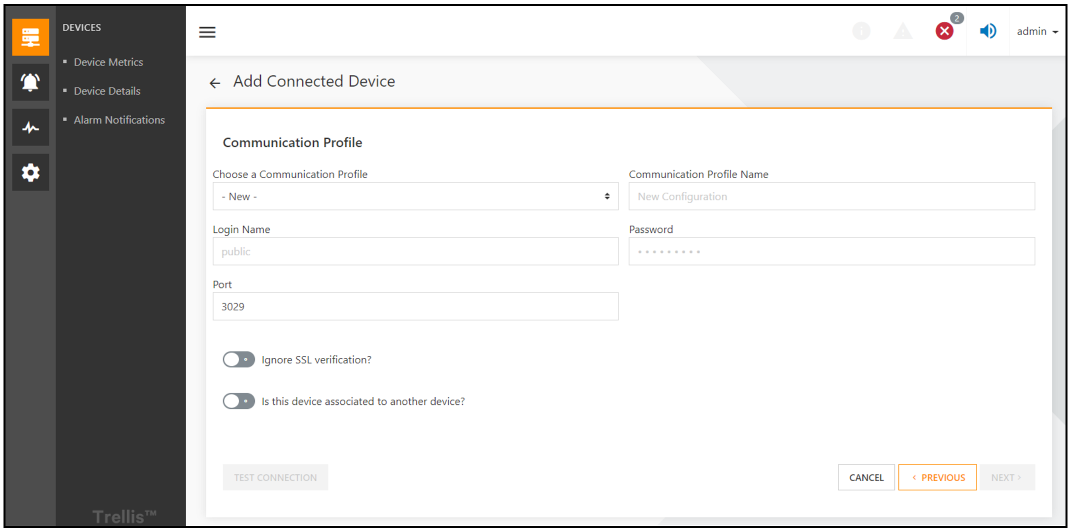
Name: Device Name

Operate System: - Select -

Address: IPV4

Figure 9.6

Then go to the second page, as shown in **Figure 9.2** on page 78 , to configure the server communication profile. Here you can choose an existing communication profile, or you can create a new communication profile on this interface. Refer to New Communication Profile Configuration on page 73 section explains detailed steps to configure communication profile. After the configuration of the communication, it is recommended to test the connection first, and then click Next after success. If you select whether this device is associated with another device, go to the interface shown in **9.2** on page 77 , select a different UPS or PDU device, and click Next. This allows you to connect the new server to other devices at the same time.



Add Connected Device

Communication Profile

Choose a Communication Profile: - New -

Communication Profile Name: New Configuration

Login Name: public

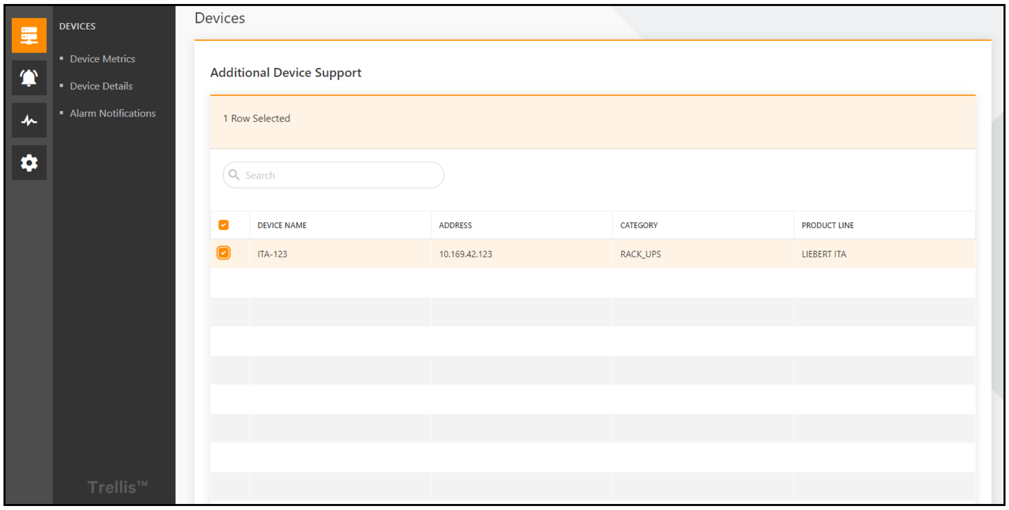
Password: •••••••••

Port: 3029

○ Ignore SSL verification?

○ Is this device associated to another device?

Figure 9.7



Additional Device Support

1 Row Selected

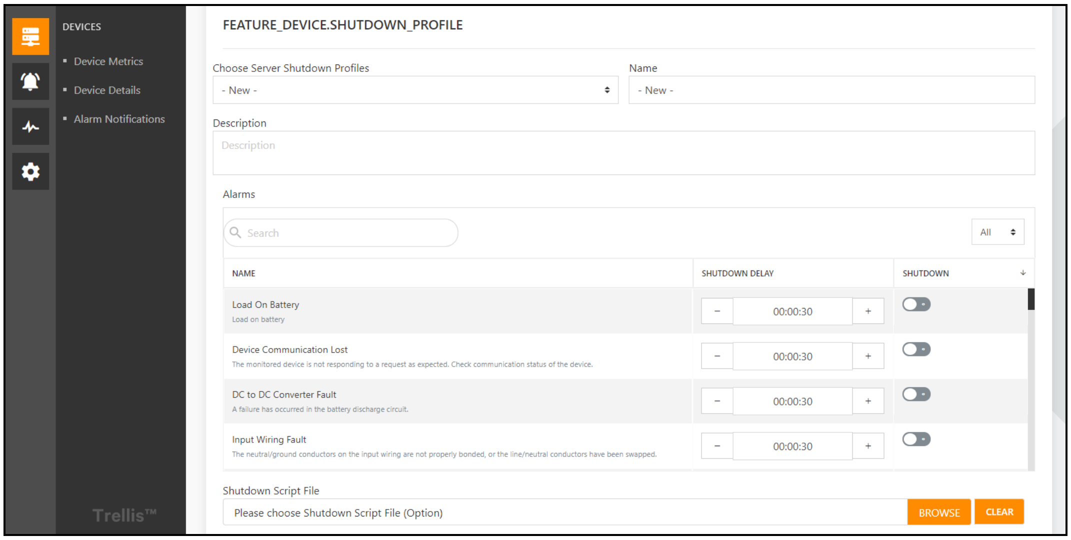
Search

☑	DEVICE NAME	ADDRESS	CATEGORY	PRODUCT LINE
☑	ITA-123	10.169.42.123	RACK_UPS	LIEBERT ITA

Figure 9.8

Go to the next step, binding the server shutdown configuration, as shown in **Figure 9.9** below . The system will help you select the default shutdown configuration by default. The default shutdown configuration contains three alarms that trigger a server to shut down: the load is battery-powered, the battery power is low, and the battery is discharged. You can also select New in the Select Server Shutdown configuration. This allows the new server shutdown configuration in this interface and binds to the current server by default. For details of the new server shutdown configuration, please refer to Alarm Trigger Server Shutdown Process on page 85 .

If you need to execute a shutdown script when the server shuts down, you can browse the shutdown script from local computer and import it, and then click Save. After saving successfully, return to the list of servers powered by UPS. At the same time, some alerts for UPS can also trigger the server to shut down and execute the script that you specified before shutting down.



FEATURE_DEVICE.SHUTDOWN_PROFILE

Choose Server Shutdown Profiles: - New -

Name: - New -

Description: Description

Alarms

Search | All

NAME	SHUTDOWN DELAY	SHUTDOWN
Load On Battery Load on battery	− 00:00:30 +	○
Device Communication Lost The monitored device is not responding to a request as expected. Check communication status of the device.	− 00:00:30 +	○
DC to DC Converter Fault A failure has occurred in the battery discharge circuit.	− 00:00:30 +	○
Input Wiring Fault The neutral/ground conductors on the input wiring are not properly bonded, or the line/neutral conductors have been swapped.	− 00:00:30 +	○

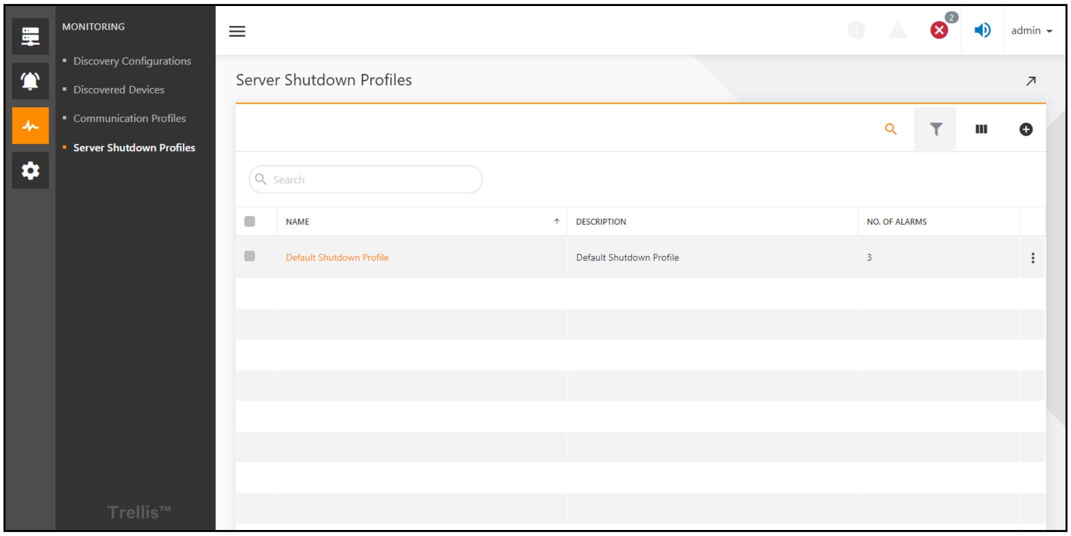
Shutdown Script File

Please choose Shutdown Script File (Option)

Figure 9.9

9.3.3 List of Server Shutdown Profiles

Click on *monitoring icon* “∿”, then click on the *Server Shutdown Profiles* to enter Server shutdown profiles page, as shown in Figure 9.10 below . The system creates a default shutdown configuration by default. This configuration only binds three alarms: the load uses battery power, the battery is low, and the battery is discharged. And the default delay for the alarm is 30 seconds. Click on *icon* “⋮” button right side of the list to edit and delete the server shutdown configuration.



NAME	DESCRIPTION	NO. OF ALARMS
Default Shutdown Profile	Default Shutdown Profile	3

Figure 9.10

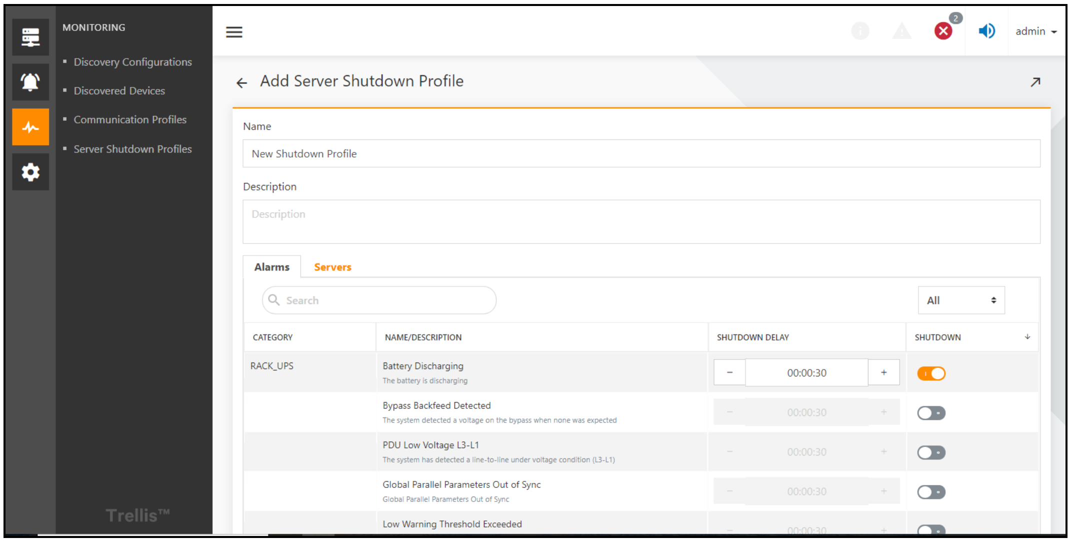
9.3.4 New Server Shutdown Configuration

Click the *add* “⊕” button in Figure 9.10 above to enter the new interface of the server shutdown configuration, as shown in Figure 9.11 on the next page . Enter the name and description of the server shutdown configuration, and then the newly added server shutdown configuration is divided into the alarm configuration and the associated server.

Alarm Configuration

As shown on the alarm tab page in Figure 9.11 on the next page , the alarm configuration shows all the alarms supported in Power Insight in the form of a list. Users can enable or disable the alarm by clicking "○" . When some alarm is enabled, if the server is bound to the server shutdown configuration, and the connected power supply device triggers an alarm, and the server will be shut down. After enabling certain alarms, shutdown delay can be edited. The battery discharge alarm in Figure 9.11 on the next page is enabled, and the default shutdown delay is 30 seconds, after which the shutdown delay can be modified. The maximum shutdown delay is 8 hours. The effect of shutdown delay: When an alarm is triggered, the server shutdown is delayed for a period of time.

NOTE: After the alarm is triggered, during the shutdown countdown, if the alarm is ended by the system, the shutdown countdown is canceled, and the server will not be shut down.



Add Server Shutdown Profile

Name: New Shutdown Profile

Description: Description

CATEGORY	NAME/DESCRIPTION	SHUTDOWN DELAY	SHUTDOWN
RACK_UPS	Battery Discharging The battery is discharging	00:00:30	●
	Bypass Backfeed Detected The system detected a voltage on the bypass when none was expected	00:00:30	○
	PDU Low Voltage L3-L1 The system has detected a line-to-line under voltage condition (L3-L1)	00:00:30	○
	Global Parallel Parameters Out of Sync Global Parallel Parameters Out of Sync	00:00:30	○
	Low Warning Threshold Exceeded	00:00:30	○

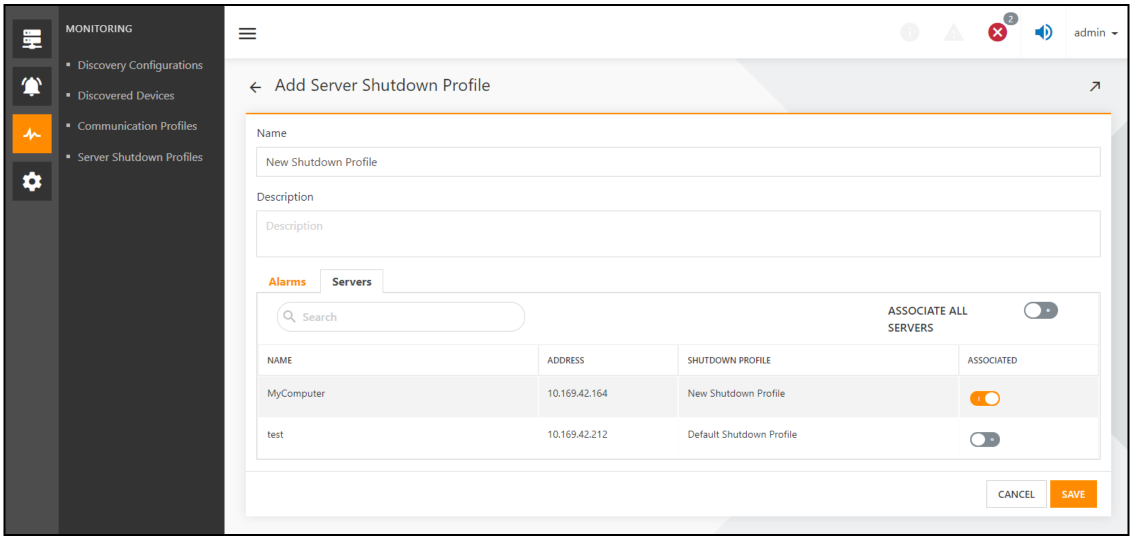
Figure 9.11

Associated Server

As shown in **Figure 9.12** below , the server lists all the servers in the current system, showing the name, address, shutdown profile (the shutdown configuration file currently bound to the server). Click the association button "○" in the last column of the list to associate or untie the server for the list item with the current server shutdown configuration. Click "○" Associate all servers or untie all servers with the current shutdown configuration.

NOTE: After you configure an alarm and associated server, remember to click the save button for the changes to take effect.

NOTE: When you click the association button to untie it, the shutdown file bound to the server will be restored to its previous state. (empty before unbound)



Add Server Shutdown Profile

Name: New Shutdown Profile

Description: Description

ASSOCIATE ALL SERVERS ○

NAME	ADDRESS	SHUTDOWN PROFILE	ASSOCIATED
MyComputer	10.169.42.164	New Shutdown Profile	●
test	10.169.42.212	Default Shutdown Profile	○

Figure 9.12

9.3.5 Alarm Trigger Server Shutdown Process

If the battery discharge alarm for UPS123 is triggered, the server shutdown process is as follows：

1. Find *all the servers that UPS123 is connected to and the shutdown configurations together they bind.*
2. Check that *battery discharge alarms are enabled* in the server's shutdown configuration.
3. If step 2 is established, the countdown is made to the shutdown delay of the battery discharge warning in the server shutdown configuration. The server shuts down after the countdown. If the battery discharge alarm for UPS123 is ended by the system during the countdown, the shutdown process is ended, and no shutdown is carried out.

NOTE: The server shutdown process includes: shutdown delay countdown, execution of shutdown script, execution of server shutdown.

NOTE: If more than one UPS is connected to the same server, the server will trigger the shutdown process only if all UPS is in an alert state and the active alert is enabled in the server's shutdown configuration.

NOTE: In the above case, the server will shut down only if the server shutdown process triggered by at least one alert in all UPS has completed the countdown.

This page intentionally left blank

10 System Settings

10.1 Overview

System settings are where Power Insight to view all event records, configure notification messages, text messages, security settings, user-defined properties, system diagnostics, contacts, and trust certificates.

10.1.1 Function Module

The system settings include the following functional modules:

- Event
- Notification Settings
- Security Settings
- User-defined Properties
- System health
- Contacts
- Trust store
- Integrated Management

10.2 Get Started Quickly

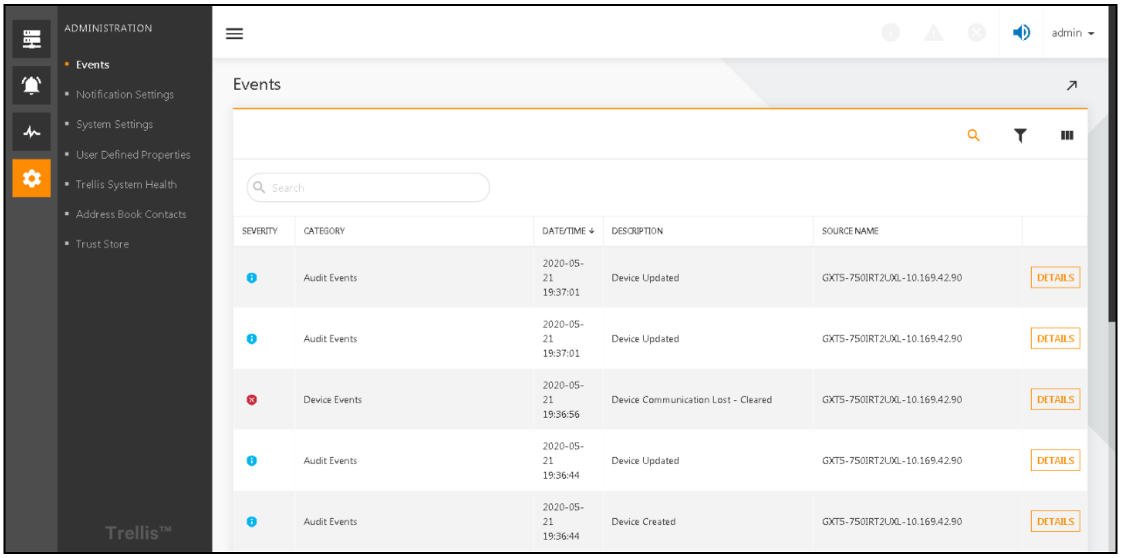
10.2.1 Rapid Deployment Steps

1. List of events
2. Security settings
3. System health
4. Trust store

10.2.2 Example

1. **List of events**

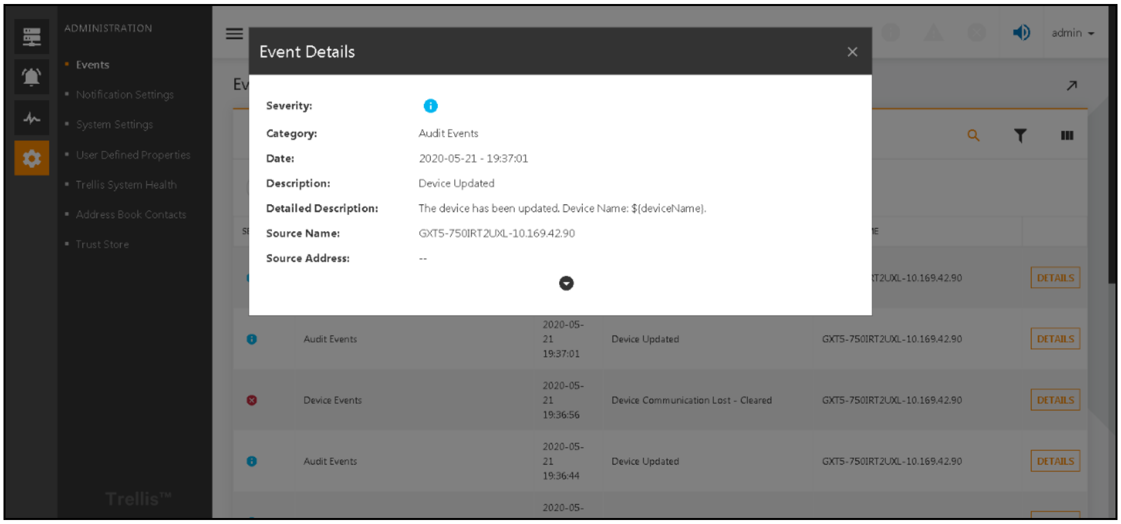
   Click on *Administration icon* "⚙" , then click "*Events*" in the secondary menu. A list of all user actions and device actions is displayed on the following page: (specific parameters reference Events on page 90)



SEVERITY	CATEGORY	DATE/TIME ↓	DESCRIPTION	SOURCE NAME	
●	Audit Events	2020-05-21 19:37:01	Device Updated	GXT5-750IRT2UXL-10.169.42.90	DETAILS
●	Audit Events	2020-05-21 19:37:01	Device Updated	GXT5-750IRT2UXL-10.169.42.90	DETAILS
☒	Device Events	2020-05-21 19:36:56	Device Communication Lost - Cleared	GXT5-750IRT2UXL-10.169.42.90	DETAILS
●	Audit Events	2020-05-21 19:36:44	Device Updated	GXT5-750IRT2UXL-10.169.42.90	DETAILS
●	Audit Events	2020-05-21 19:36:44	Device Created	GXT5-750IRT2UXL-10.169.42.90	DETAILS

Figure 10.1

Click on "Details" on the right of "Source Name" to see the specific information of the operation.



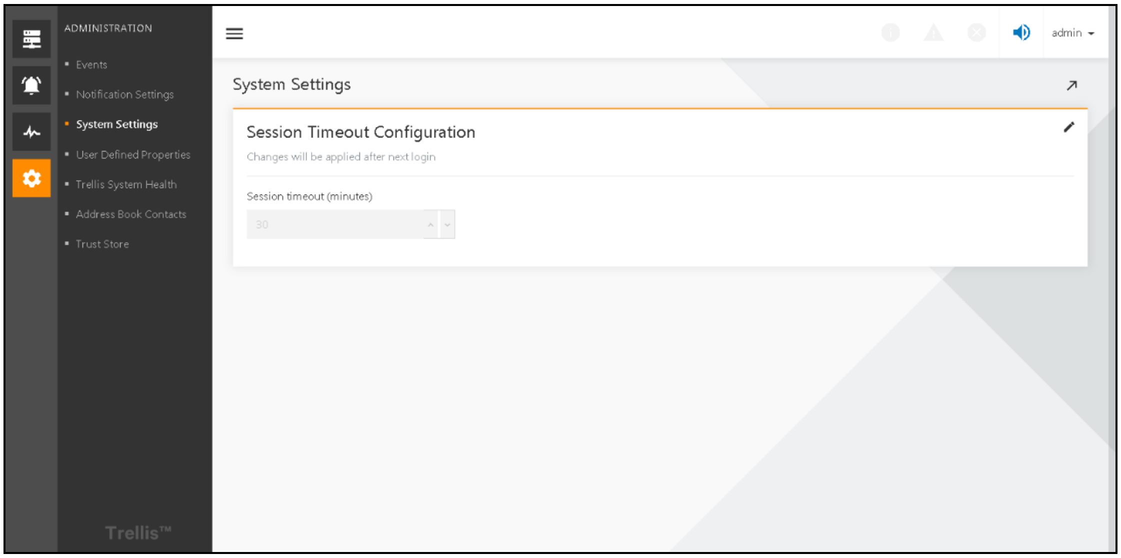
Event Details

Severity:	●
Category:	Audit Events
Date:	2020-05-21 - 19:37:01
Description:	Device Updated
Detailed Description:	The device has been updated. Device Name: ${deviceName}.
Source Name:	GXT5-750IRT2UXL-10.169.42.90
Source Address:	--

Figure 10.2

2. System settings

Click on *Administration icon* “⚙”, then click *System Settings* in the secondary menu displays session timeout configuration as shown in **Figure 10.3** on the facing page（Specific parameter stake Security Settings on page 91 ）



System Settings

Session Timeout Configuration

Changes will be applied after next login

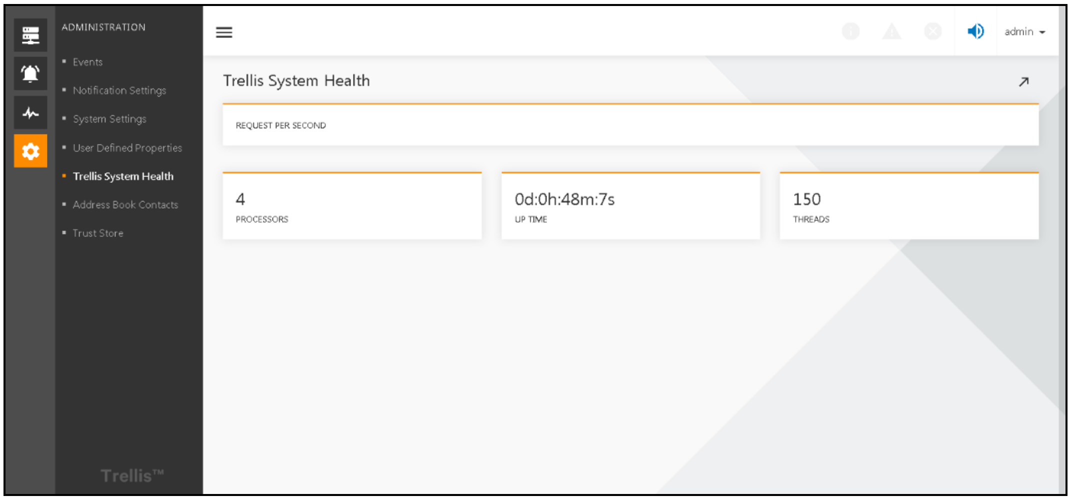
Session timeout (minutes): 30

Figure 10.3

Click on the "✎" symbol in the upper right corner to edit the time. Save *after editing to take effect.*

3. System Health

Click **on Administration icon** "⚙", then click Trellis system Health in the secondary menu. Some of the statuses of the server situated by Power Insight are displayed on the following page: (specific parameters reference System Health on page 91)



Trellis System Health

REQUEST PER SECOND

4 PROCESSORS

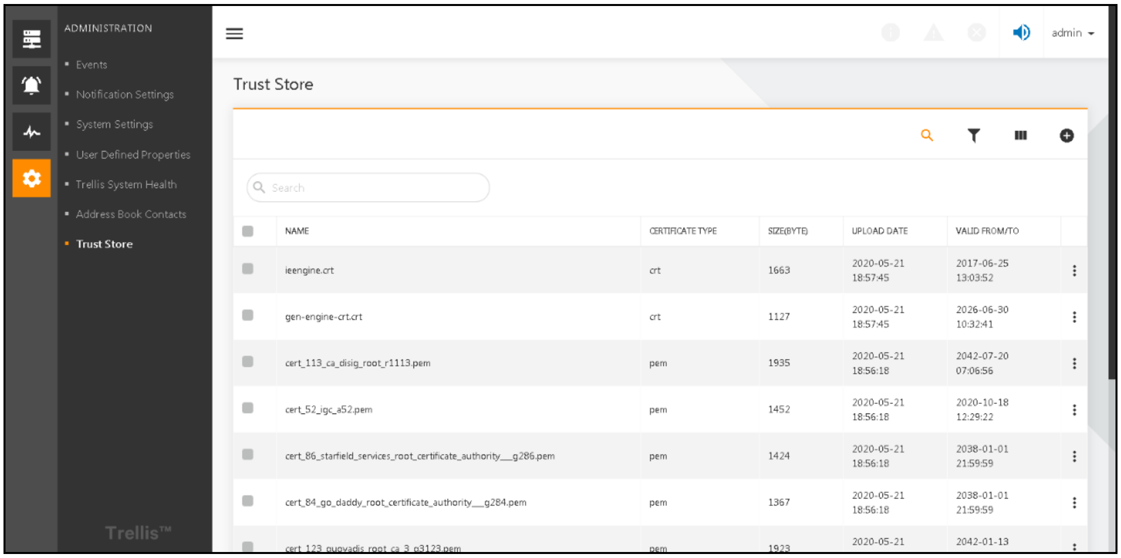
0d:0h:48m:7s UP TIME

150 THREADS

Figure 10.4

4. Trust Store

Click on Administration icon "⚙", then click Trust store in the secondary menu.
The certificates included in Power Insight are displayed on the following page: (specific parameters reference System Health on page 91)



Trust Store

	NAME	CERTIFICATE TYPE	SIZE(BYTE)	UPLOAD DATE	VALID FROM/TO	
□	ieengine.crt	crt	1663	2020-05-21 18:57:45	2017-06-25 13:03:52	⋮
□	gen-engine-crt.crt	crt	1127	2020-05-21 18:57:45	2026-06-30 10:32:41	⋮
□	cert_113_ca_disig_root_r1113.pem	pem	1935	2020-05-21 18:56:18	2042-07-20 07:06:56	⋮
□	cert_52_igc_a52.pem	pem	1452	2020-05-21 18:56:18	2020-10-18 12:29:22	⋮
□	cert_86_starfield_services_root_certificate_authority__g286.pem	pem	1424	2020-05-21 18:56:18	2038-01-01 21:59:59	⋮
□	cert_84_go_daddy_root_certificate_authority__g284.pem	pem	1367	2020-05-21 18:56:18	2038-01-01 21:59:59	⋮
□	cert_123_quovadis_root_ca_3_g3123.pem	pem	1923	2020-05-21	2042-01-13	⋮

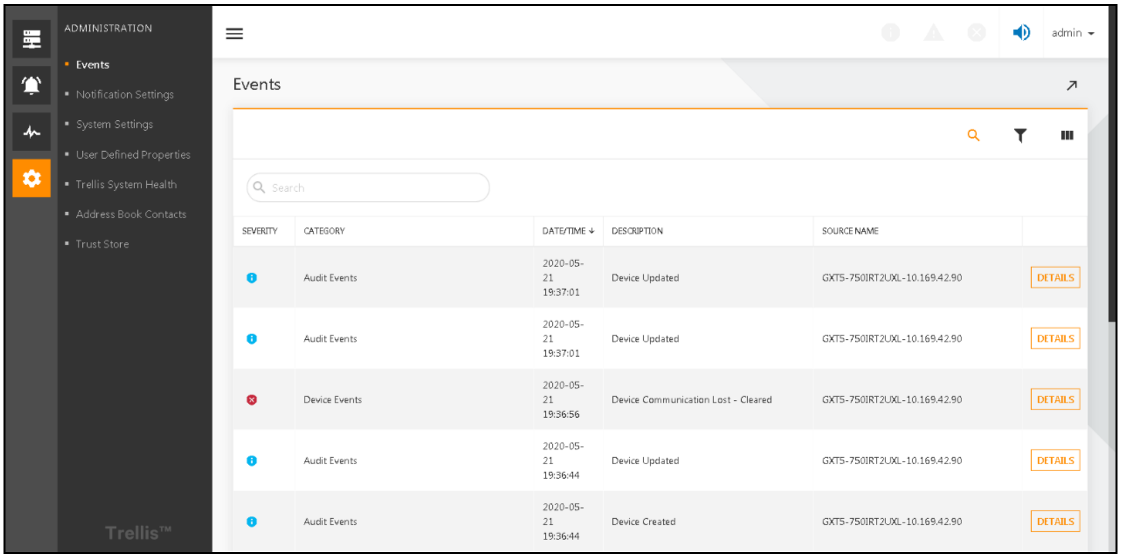
Figure 10.5

10.3 Detailed Features

10.3.1 Events

Click on *Administration icon* "⚙", then click *"Events*" in the secondary menu to see the list of events.

The Power Insight application records each action or event that occurs in the application. Events are grouped in categories that identify each event with a time/date stamp. They are categorized as Audit Events, Device Events, System Events, System Events-Administration, Authentication and User Profile Events and Application Level Events. Each event has a severity level of informational, warning or critical. You can also add or remove columns, filter to show only the events that are important to you and retrieve detailed information about each event listed under the link in the Details column.



Events

SEVERITY	CATEGORY	DATE/TIME ↓	DESCRIPTION	SOURCE NAME	
●	Audit Events	2020-05-21 19:37:01	Device Updated	GXT5-750IRT2UXL-10.169.42.90	DETAILS
●	Audit Events	2020-05-21 19:37:01	Device Updated	GXT5-750IRT2UXL-10.169.42.90	DETAILS
⊗	Device Events	2020-05-21 19:36:56	Device Communication Lost - Cleared	GXT5-750IRT2UXL-10.169.42.90	DETAILS
●	Audit Events	2020-05-21 19:36:44	Device Updated	GXT5-750IRT2UXL-10.169.42.90	DETAILS
●	Audit Events	2020-05-21 19:36:44	Device Created	GXT5-750IRT2UXL-10.169.42.90	DETAILS

Figure 10.6

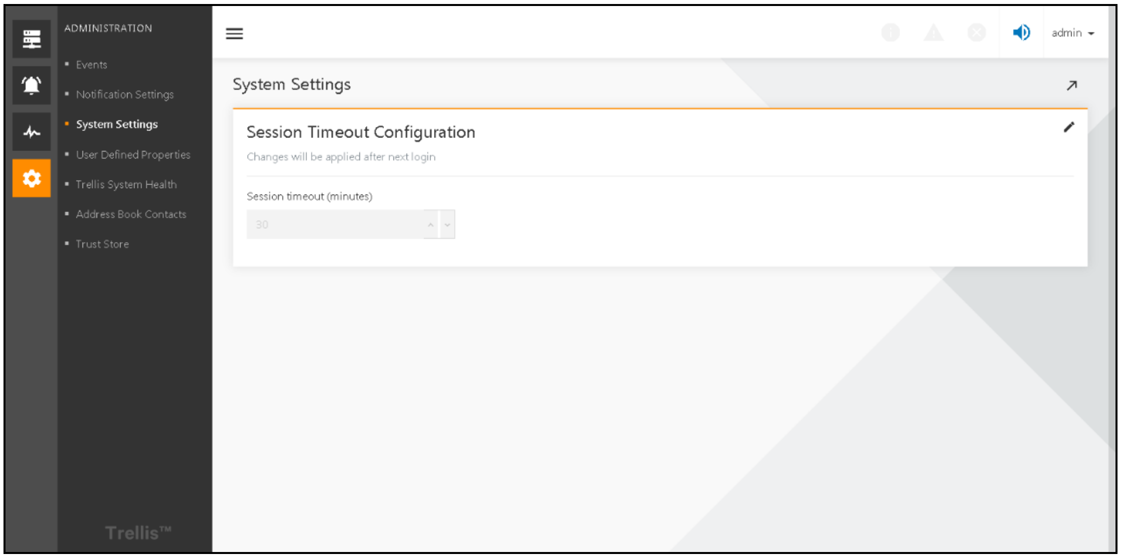
10.3.2 Security Settings

The application's system settings are used to configure the login session timeout in minutes for the application. Changes to reduce or extend the amount of time a user can remain logged in to the system are applied after the next log in.

To set a session timeout:

1. Click the *Administration icon* and click *System Settings*.
2. Click the *Edit icon* on the upper right corner of the window.
3. Enter *the number of minutes* in the Session Timeout field and click *SAVE*.

NOTE: Session timeouts range from 1 to 1440 minutes.



System Settings

Session Timeout Configuration

Changes will be applied after next login

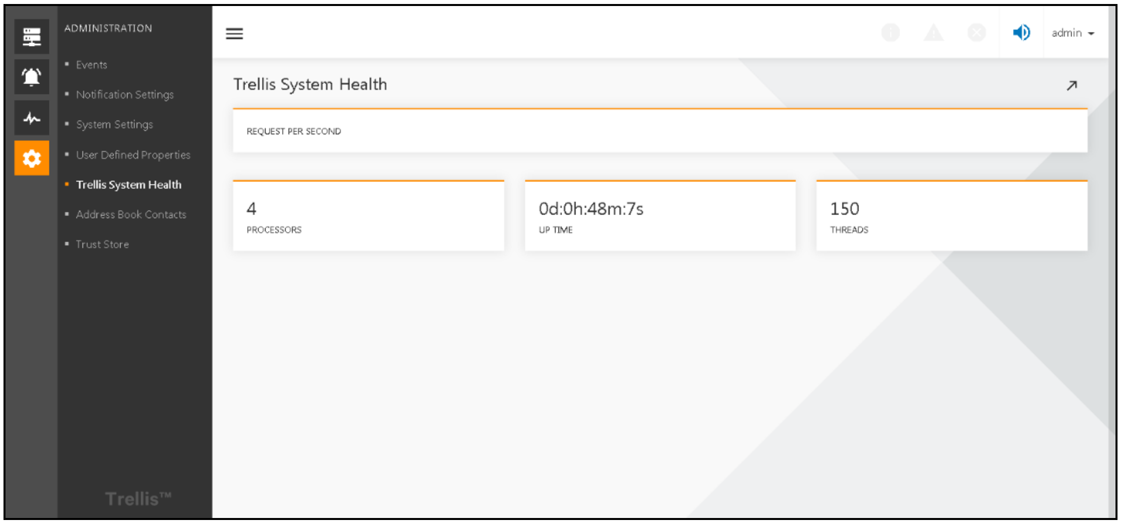
Session timeout (minutes)

30

Figure 10.7

10.3.3 System Health

The System Health window displays a visual dashboard illustrating how the host system running the Power Insight application is functioning. This window provides information on how many requests per second are being filtered through the computer. It also displays the number of processors in the computer and the total accumulated time the computer has run without interruption.



Trellis System Health

REQUEST PER SECOND

4
PROCESSORS

0d:0h:48m:7s
UP TIME

150
THREADS

Figure 10.8

10.3.4 Trust Store

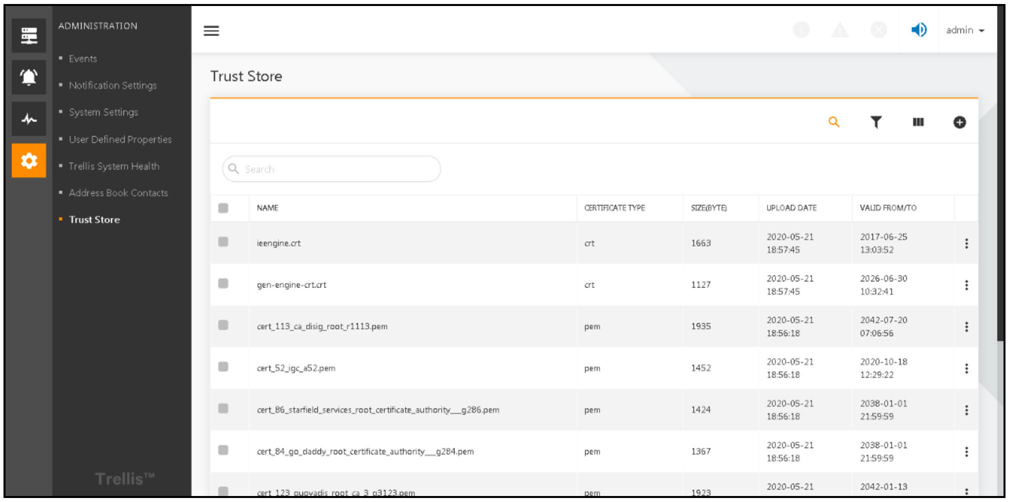
The Trust Store allows you to add, delete or review security certificates. The content includes a list of the current certificates and provides each certificates' type, size, date of validation and date it is added to the application.

To add a security certificate:

1. Click the *Administration icon* and click *Trust Store.*
2. Click the *Add ico*n and enter *the name of the certificate in the Name field.*
3. Click *Browse*, select a *certificate file* and click *Add Certificate.*

To delete a security certificate:

1. Click the *Administration icon* and click *Trust Store.*
2. Locate the *contact information*, click the **vertical ellipsis icon** in the same row and click Delete.
3. In the Confirmation window, click DELETE.



Trust Store

NAME	CERTIFICATE TYPE	SIZE(BYTE)	UPLOAD DATE	VALID FROM/TO
ieengine.crt	crt	1663	2020-05-21 18:57:45	2017-06-25 13:03:52
gen-engine-crt.crt	crt	1127	2020-05-21 18:57:45	2026-06-30 10:32:41
cert_113_ca_disig_root_r1113.pem	pem	1935	2020-05-21 18:56:18	2042-07-20 07:06:56
cert_52_igc_a52.pem	pem	1452	2020-05-21 18:56:18	2020-10-18 12:29:22
cert_86_starfield_services_root_certificate_authority___g286.pem	pem	1424	2020-05-21 18:56:18	2038-01-01 21:59:59
cert_84_go_daddy_root_certificate_authority___g284.pem	pem	1367	2020-05-21 18:56:18	2038-01-01 21:59:59
cert_123_quovadis_root_ca_3_g3123.pem	pem	1923	2020-05-21	2042-01-13

Figure 10.9

10.3.5 Integrated Management

Integrated management menu provides the generation of API key and API Secret for authentication between Power Insight and various plug-ins. Plug-in users can only obtain the monitoring information of Power Insight if they hold the API key and API Secret.

To generate an API key and API secrete to access the Plug-in:

1. Click the *Administrator icon.*
2. Click "*Integrated management*" menu option.
3. Click the *"+" icon* in the upper right corner of the Integrated management registration. A new plug-in registration box will pop up. Enter the following details:
   - In the Category field, drop down to select the company to which the plugin belongs.
   - In the Required Source Address field , enter the FQDN or IP address.
   - In the Description field, enter the *plug-in description.*
4. Click *Sure*. The API key and API Secret is generated. This is the authentication information that needs to be entered when the plug-in is registered.

To modify API key and API Secret:

1. Click the *More icon* against the API Key and API Secret that needs to be modified.

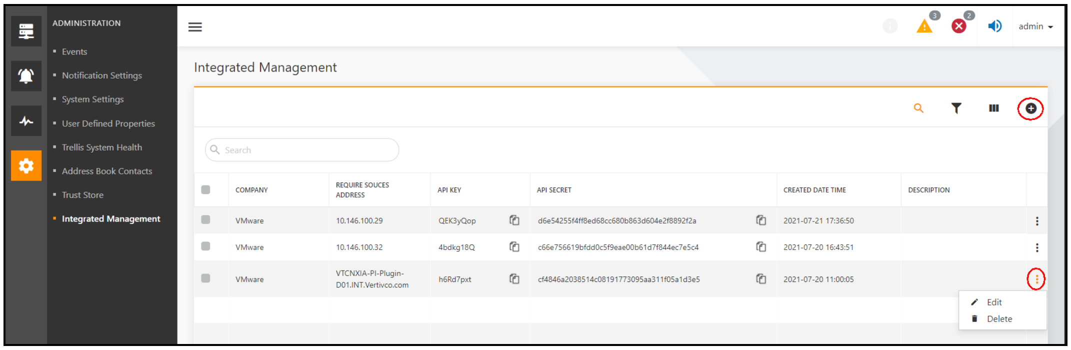
1. Click *Edit*. The Edit Registered Address pop-up box appears.
2. Modify the *FQDN or IP address of the plug-in* as needed.
3. Click *Sure.*

To Delete API key and API Secret:

1. Click the *More icon* against the API Key and API Secret that needs to be deleted.

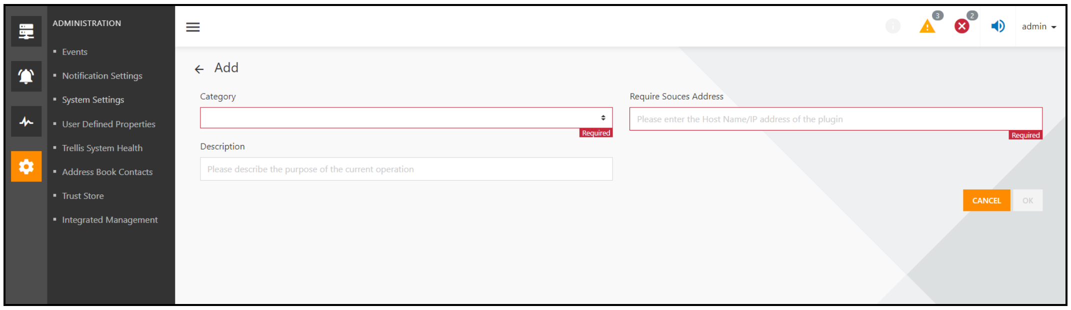
2. Click *Delete.* The Delete Registered Address pop-up box appears.

3. Click *Delete* in the pop-up box to delete the API Key and API Secret. Clicking Cancel will not Delete API Key and API Secret.



COMPANY	REQUIRE SOUCES ADDRESS	API KEY	API SECRET	CREATED DATE TIME	DESCRIPTION
VMware	10.146.100.29	QEK3yQop	d6e54255f4ff8ed68cc680b863d604e2f8892f2a	2021-07-21 17:36:50	
VMware	10.146.100.32	4bdkg18Q	c66e756619bfdd0c5f9eae00b61d7f844ec7e5c4	2021-07-20 16:43:51	
VMware	VTCNXIA-PI-Plugin-D01.INT.Vertivco.com	h6Rd7pxt	cf4846a2038514c08191773095aa311f05a1d3e5	2021-07-20 11:00:05	

Figure 10.10



← Add

Category

Required

Require Souces Address

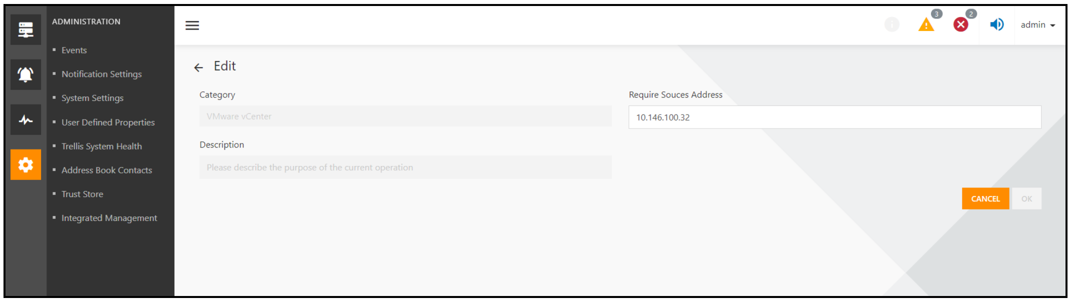
Please enter the Host Name/IP address of the plugin

Required

Description

Please describe the purpose of the current operation

Figure 10.11



← Edit

Category

VMware vCenter

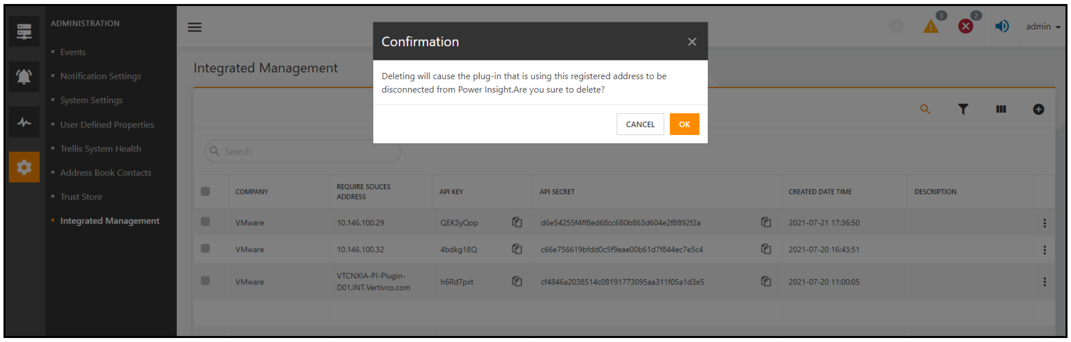
Require Souces Address

10.146.100.32

Description

Please describe the purpose of the current operation

Figure 10.12



Integrated Management

Confirmation

Deleting will cause the plug-in that is using this registered address to be disconnected from Power Insight.Are you sure to delete?

	COMPANY	REQUIRE SOUCES ADDRESS	API KEY	API SECRET	CREATED DATE TIME	DESCRIPTION
	VMware	10.146.100.29	QEK3yQop	d6e54255f4ff8ed68cc680b863d604e2f8892f2a	2021-07-21 17:36:50	
	VMware	10.146.100.32	4bdkg18Q	c66e756619bfdd0c5f9eae00b61d7f844ec7e5c4	2021-07-20 16:43:51	
	VMware	VTCNXIA-PI-Plugin-D01.INT.Vertivco.com	h6Rd7pxt	cf4846a2038514c08191773095aa311f05a1d3e5	2021-07-20 11:00:05	

Figure 10.13

11 Troubleshooting

11.1 Uninstalling the software

If the removal of the Power Insight application fails, use the following steps to clean up the system.

To uninstall the application:

1. Make sure *the user can view hidden files and folders.*
2. Click the *Windows logo* on the taskbar.
    a. Enter *hidden* in the search text box and click *Show Hidden Files and Folders.*
    b. Make sure *the Show hidden file, folder and drives option is enabled*.
    c. Remove the *install folder* created by the Power Insight application, C:\Program Files\TrellisPowerInsight.
3. Remove the *data folder* that was created by the application, C:\Users\Default\AppData\Local\TrellisPowerInsight.
4. Remove the *registry folder* that was created, C:\Program Files\Zero G Registry.

11.2 Upgrade Windows 10

During an automatic update of Windows 10 while the Power Insight application is running, the default data folder C:\Users\Default used by the PostgreSQL service is overwritten by C:\Users\Default.migrated.

Use the following steps to resolve this issue:

To correct PostgreSQL service overwrite:

1. Log in *as a Windows user with administrative privileges.*
2. Click *Start* and *type Regedit* to access the Windows Registry.
3. Navigate to*\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\postgresql-x64- 9.5 registry entry*.
4. Double-click on the *Image Path key and make sure the default data folder used by the PostgreSQL service points to C:\Users\Default as shown in the example below*:
   "C:\Program Files\Trellis Application Manager\postgreSQL\bin\pg_ctl.exe" runservice -N "postgresql-x64-9.5" -D "C:\Users\Default\AppData\Local\Trellis Application Manager\postgresdata" -w
5. You can restart *the machine*, which will restart the PostgreSQL and services, and skip the steps below.
6. Open *Windows Explorer*, type *Control Panel\All Control Panel Items\Administrative Tools* and press *Enter*.
7. Open the *Services application* and sort the *list of services by Name*.
8. Restart the *following:*

   48 TROUBLESHOOTING

    - Postgresql-x64-9.5 - PostgreSQL Server 9.5 service
    - Intelligence Engine MSS Engine service
    - Application Framework Database service.

11.3 Linux Dependent Package Installation

When installing the Linux version, connect to the external network and download the following installation packages that Linux depends on.

1. Red Hat (7.5, 7.6 or 7.7 repository)
    - net-tools
    - psmisc
    - log4cpp
    - jsoncpp
    - net-snmp
    - openssl
    - postgresql
    - postgresql-contrib
    - postgresql-server
    - libpqxx
    - glibmm24

11.4 Turn Off the Firewall Before Installation

Before installing Power Insight or Remote Agent under Windows or Linux, need to turn off the operating system firewall.

11.5 When the Power Supply Devices are Removed, the Servers to which they are Connected are Processed

If the server is connected to more than one power supply device, the server is not deleted, and if the device is connected only to the device that is currently deleted, the server is deleted.

Connect with Vertiv on Social Media

https://www.facebook.com/vertiv/

https://www.instagram.com/vertiv/

https://www.linkedin.com/company/vertiv/

https://www.twitter.com/Vertiv/

Vertiv.com | Vertiv Headquarters, 1050 Dearborn Drive, Columbus, OH, 43085, USA