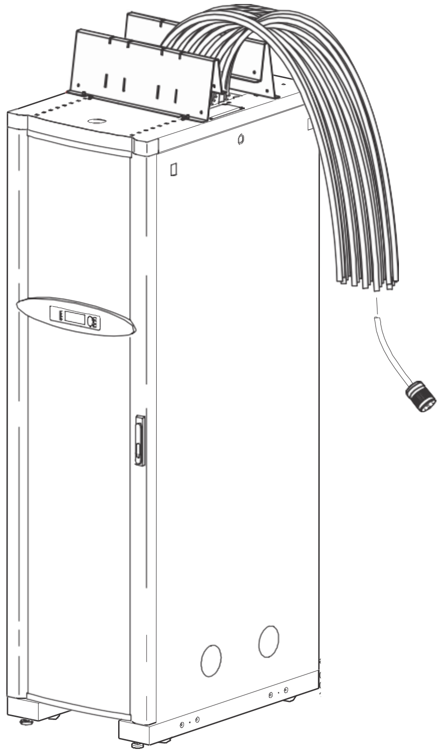
# User Manual

## 40 and 60 kW
## InfraStruxure™ Power Distribution Units

**PD40E5EK20-M, PD40H5EK20-M, PD40G6FK1-M, PD40F6FK1-M, PD40L6FK1-M, PDRPPNX10-M, PD60G6FK1, PD60F6FK1, PD60L6FK1, PDRPPNX10**

**990-5875B**

**Publication Date: 2/2024**



Schneider Electric

www.se.com

# Legal Information

The information provided in this document contains general descriptions, technical characteristics and/or recommendations related to products/solutions.

This document is not intended as a substitute for a detailed study or operational and site-specific development or schematic plan. It is not to be used for determining suitability or reliability of the products/solutions for specific user applications. It is the duty of any such user to perform or have any professional expert of its choice (integrator, specifier or the like) perform the appropriate and comprehensive risk analysis, evaluation and testing of the products/solutions with respect to the relevant specific application or use thereof.

The Schneider Electric brand and any trademarks of Schneider Electric SE and its subsidiaries referred to in this document are the property of Schneider Electric SE or its subsidiaries. All other brands may be trademarks of their respective owner.

Schneider Electric reserves the right to make changes or updates with respect to or in the content of this document or the format thereof, at any time without notice.

**To the extent permitted by applicable law, no responsibility or liability is assumed by Schneider Electric and its subsidiaries for any errors or omissions in the informational content of this document, as well as any non-intended use or misuse of the content thereof**

# Table of Contents

# Introduction

## Overview

### Features

Your Schneider Electric InfraStruxure™ PDU provides power distribution and management of electrical power to equipment racks. In each unit, the Network Management Card (NMC) provides full management capabilities over a network using the following standards:

- Telnet
- Secure SHell (SSH)
- HyperText Transfer Protocol (HTTP)
- HTTP over Secure Sockets Layer (HTTPS)
- File Transfer Protocol (FTP)
- Simple Network Management Protocol (SNMP) versions 1 and 3
- TCP/IP v4 and v6
- Secure Copy (SCP)
- SMTP-based e-mail
- RADIUS (Remote Access Dial In User Service)

The unit also provides the following features:

- There are four user types; multiple users can be logged in simultaneously.
- You can export a configuration (.ini) file from a configured unit to one or more unconfigured units.
- You can use a Dynamic Host Configuration Protocol (DHCP) server to provide the network (TCP/IP) values for the unit.
- Data and event logs are available.
- You can set up notification through the event logging, Syslog servers, e-mail, and SNMP traps and queries, and the Schneider Electric Remote Monitoring Service. You can configure notification for single events or groups of events, based on the severity level or category of events.
- A selection of security protocols for authentication and encryption is available.

## Getting Started

### Connect the unit

A Cat-5 cable is plugged into the Ethernet port on the unit. Connect the other end of the cable to the LAN.

A local computer can be connected to the Console port (on the PDU monitoring Unit) with a serial cable (part 940-0103). Connect the other end of the serial cable to the local computer.
**NOTE:** Consult the *Operation Manual on* **www.apc.com** for your equipment to locate the Ethernet port and Console port.

## Initial setup

To start using the unit:

- Install the unit using the *Installation Instructions* on **www.apc.com**.
- Apply power and connect to your network. Follow the directions in the *Installation Instructions*.
- Establish network settings. Three TCP/IP settings must be defined for the Network Management Card of the unit before it can operate on the network:
  - IP address of the unit’s Network Management Card
  - Subnet mask
  - IP address of the default gateway

| ***NOTICE*** |
|---|
| Do not use the loopback address as the default gateway. Doing so disables the unit. You must then log on using a serial connection and reset TCP/IP settings to their defaults. |

If a default gateway is unavailable, use the IP address of a computer (that is usually running) located on the same subnet as the unit. The unit uses the default gateway to test the network when traffic is light.

**NOTE:** See the *Operation Manual* on **www.apc.com** for detailed instructions.

## Accessible interfaces

Begin using the unit with one of the following interfaces:

1. “The Web Interface” on page 52
2. “Command Line Interface (CLI)” on page 6
3. The display interface on the front of the unit. See the *Operation Manual* **on www.apc.com** for instructions.

## Network management features

These applications and utilities work with a PDU that connects to the network through its Network Management Card:

- Schneider Electric StruxureWare® Data Center Expert—Provide enterprise-level power management and management of Schneider Electric agents, PDUs, information controllers, and environmental monitors
- APC by Schneider Electric PowerNet™ Management Information Base (MIB) with a standard MIB browser—Perform SNMP SETs and GETs and to use SNMP traps
- APC by Schneider Electric Device IP Configuration Wizard—Configure the basic settings of one or more units over the network
- APC by Schneider Electric Security Wizard—Create the components needed for high security for the unit when using Secure Sockets Layer (SSL)/Transport Layer Security (TLS) and related protocols and encryption routines

## User account overview

The InfraStruxure PDU arrives configured with three user types and associated user names:

- *Super User* (user name: apc)
- *Device* (user name: device)
- *Read-Only* (user name: readonly).

The initial default password for each of these is **apc**. All levels of access require user name and password permissions.

Both user names and passwords are case-sensitive, and have a 64 byte maximum, supporting up to 64 ASCII characters; less for multi-byte languages.

The Super User can define additional user accounts, as well as set other variables for the additional users. It is generally recommended that non-default user name and passwords be set.

**NOTE:** The Super User cannot be renamed or deleted, but it can be disabled. It is recommended that the Super User account is disabled once any additional Administrator accounts are created. Make sure that there is at least one Administrator account enabled before the Super User account is disabled.

To manage user settings from the web interface:

1. Enter the NMC IP address into the address bar.
2. Select **Configuration > Security > Local Users > Management**.
3. Click **Add User.**

You can add the following user types:

- **Administrator:** The Administrator has full access just as the Super User does, but this user type can be deleted.
  **NOTE:** A Super User account must be enabled before all administrator accounts are deleted or disabled.
- **Device:** The Device User has read-write access to the device-related menus only. The Administrator can enable or disable the Device User account.
- **Read-Only:** The Read-Only User account has read-only access, through the web interface, to view status but not to control a device or change any configured value. The Administrator can enable or disable the Read-Only User account.
- **Network-Only:** The Network-Only User has read-write access to the network-related menus only. The Administrator can enable or disable the Network-Only User account.

# Recover from a Lost Password

You can access the command line interface (CLI) via a local computer either via serial port (available on all PDU models) or USB console port (USB console port is not available on older PDU models).

1. At the local computer, do one of the following:
   – Select a serial port and disable any service that uses it. Connect the provided serial cable (part 940-0103) between the selected serial port on the local computer and the serial port on the PDU, OR

   – Connect the provided standard USB cable between the PDU USB console port and the computer USB port. A virtual serial port will be discovered on the computer.
2. Open a terminal program (such as HyperTerminal®) and configure the port for:
   – `9600 bps` (USB serial works with any other baud rate automatically)
   – `8 data bits`
   – `no parity`
   – `1 stop bit`
   – `no flow control`
3. Press ENTER, repeatedly if necessary, to display the **User Name** prompt. If you are unable to display the **User Name** prompt, verify the following:
   – The serial port is not in use by another application.
   – The correct cable is being used as specified in step 1.
   – The terminal settings are correct as specified in step 2.

4. Press the **Reset** button on the back of the unit. The Status LED will flash. Press the **Reset** button a second time while the LED is flashing to temporarily reset the user name and password to the default.
5. Press ENTER as many times as necessary to redisplay the **User Name** prompt, then use the default user name and password, **apc**. (If you take longer than 30 seconds to log on after the **User Name** prompt is redisplayed, you must repeat step 5 and log on again.)
6. In the CLI, use the following commands to change the password for the Super User account. (The user name is always **apc**, and the password is now temporarily **apc.):**

    ```
    user -n apc -pw yourNewSuperUserPassword
    ```

    Example: to change the Super User's password to p@ssword type:

    ```
    user -n apc -pw p@ssword
    ```

    **NOTE:** Because the Super User can also reset the password for any account, you can reset other user's passwords as well.

    Example: to change the password for user bmadmin to p@ssword type:

    ```
    user -n bmadmin -pw p@ssword
    ```

    **NOTE:** Changing user name information is no longer supported via the command line interface. If a user name needs to be changed, it must be deleted and re-created. The Super User will also have access now to log in and adjust any other user's password.
7. To log off, type `quit`, `exit`, or `bye`, and then press ENTER. Reconnect any serial cable you may have disconnected, and restart any service you may have disabled.

# Watchdog Features

## Overview

To detect internal problems and recover from unanticipated inputs, the unit uses internal, system-wide watchdog mechanisms. When it restarts to recover from an internal problem, a **Network Interface Restarted** event is recorded in the event log.

## Network interface watchdog mechanism

Watchdog mechanisms protect the NMC from becoming inaccessible over the network. If it does not receive any network traffic for 9.5 minutes, it assumes there is a problem with its interface and restarts. The watchdog mechanism is only enabled on a unit that discovers an active network interface connection at start-up.

## Reset the network timer

To ensure that the unit does not restart if the network is quiet for 9.5 minutes, the unit attempts to contact the default gateway every 4.5 minutes. If the gateway is present, it responds to the unit, and the response restarts the 9.5-minute timer. If your application does not require or have a gateway, specify the IP address of a computer that is running on the network and is on the same subnet. The network traffic of that computer will restart the 9.5-minute time frequently enough to prevent the unit from restarting.

## Automatic logout

By default, users will be automatically logged out of the unit's web and command line interfaces after 3 minutes of inactivity. The default logout time can be adjusted through the web interface **Configuration > Security > Local Users > Management**.

1. Select the user name for the account you want to change.
2. Under **Session Timeout**, modify the number of minutes.

| Automatic Logout | Duration (min) |
|---:|:---:|
| Minimum | 1 |
| Maximum | 60 (1 Hr) |

# Command Line Interface (CLI)

You can use the CLI to view, configure, and manage the unit settings and status. The CLI also enables you to create scripts for automated operation. You can configure all parameters of a unit (including those for which there are not specific CLI commands) by using the CLI to transfer an .ini file to the unit. The CLI uses XMODEM to perform the transfer. However, you cannot read the current .ini file through XMODEM.

# Log on to the CLI

To access the CLI, you can use either a local (serial) connection or a remote (Telnet or SSH) connection with a computer on the same network as your PDU. Once you configure the network settings, you can access the CLI through Telnet. You can also configure the network settings to enable CLI access through SSH or disable CLI access through Telnet and SSH.

## Local access to the CLI via serial port

Use a computer that connects to the PDU through the serial port to access the CLI:

1. Select a serial port at the computer and disable any service that uses the port.
2. Connect the provided serial cable (part 940-0103) from the selected port on the computer to the configuration port at the PDU.
3. Run a terminal program such as HyperTerminal, and configure the selected port for 9600 bps, 8 data bits, no parity, 1 stop bit, and no flow control.

Press ENTER, and at the prompts, enter your user name and password.

## Local access to the CLI via USB port

Use a computer that connects to the PDU through the USB console port to access the CLI. Note that USB console port is not available on older PDU models.

1. Connect the provided standard USB cable between the PDU USB console port and the computer USB port.
2. A virtual serial port will be discovered on the computer.
3. Open a terminal program/emulator (such as HyperTerminal®) and configure the virtual serial port for:
   a. `Default baud rate`: 9600 bps (USB serial works with any other baud rate automatically)
   b. Data bits: 8
   c. Parity: None
   d. Stop Bits: 1
   e. Flow Control: None

Press ENTER, and at the prompts, enter your username and password.

## Remote access to the CLI

The super user or Administrator can enable remote access to the CLI through Telnet and/or SSH.

**Telnet for basic access:** Telnet provides the basic security of authentication by user name and password, but not the high-security benefits of encryption.

To access the CLI through Telnet:

1. From a computer on the same network as the unit, at a command prompt, type telnet and the System IP address for the unit (for example, `telnet 139.225.6.133`, when the unit uses the default Telnet port of 23), and press ENTER.

If the unit uses a non-default port number (5000 to 32768), you must include a colon or a space, depending on your Telnet client, between the IP address (or DNS name) and the port number.

2. Enter the user name and password.

**SSH for high-security access:** If you use the high security of SSL/TLS for the web interface, use Secure SHell (SSH) for access to the CLI. SSH encrypts user names, passwords and transmitted data. The interface, user accounts, and user access rights are the same whether you access the CLI through SSH or Telnet, but to use SSH, you must first configure SSH and have an SSH client program installed on your computer.

# CLI Home Screen

## Sample home screen

The following is an example of the screen that displays when you log on to the CLI.

```
User Name  : apc
Password   : ***

Schneider Electric                      Network Management Card AOS    v6.4.6
(c) Copyright 2016 All Rights Reserved  XPDU                           v6.4.0

----------------------------------------------------------------------------------
Name       : apcF3821D                                   Date  : 03/01/2016
Contact    : Raghav                                      Time  : 13:57:38
Location   : LAB1                                        User  : Super User
Up Time    : 0 Days 1 Hour 45 Minutes                    Stat  : P+ N4+ N6+ A+

Type ? for command listing
Use tcpip command for IP address<-i>, subnet<-s), and gateway<-g>

apc>
```

## Information and status fields

Two fields identify the APC operating system (AOS) and application (XPDU) firmware versions:

```
Network Management Card AOS v6.4.6
XPDU v6.4.0
```

Three fields identify the system name, contact person, and location values:

```
Name: apcF3821D
Contact: Raghav
Location: LAB1
```

The **Up Time** field reports how long the unit has been running:

```
Up Time: 0 Days 1 Hour 45 Minutes
```

Two fields identify the current system **Date** and **Time**:

```
Date : 3/1/2016
Time : 13:57:38
```

- The **User** field identifies the type of logged user; whether **Super User**, **Administrator** or **Device User** account.

```
User : Super User
```

### System and network status fields

- The **Stat** field reports the unit status: `Stat: P+ N+ A+`

| | |
|---|---|
| P+ | The APC operating system (AOS) is functioning properly. |

| IPv4 only | IPv6 only | IPv4 and IPv6* | Description |
|---|---|---|---|
| N+ | N+ | N4+ N6+ | The network is functioning properly. |
| N? | N6? | N4? N6? | A BOOTP request cycle is in progress. |
| N- | N6- | N4- N6- | The InfraStruxure PDU failed to connect to the network. |
| N! | N6! | N4! N6! | Another device is using the InfraStruxure PDU IP address. |
| * The N4 and N6 values can be different from one another: you could, for example, have N4- N6+. | | | |

| | |
|---|---|
| A+ | The application is functioning properly. |
| A- | The application has a bad checksum. |
| A? | The application is initializing. |
| A! | The application is not compatible with the AOS. |

**NOTE:** If P+ is not displayed, contact the Schneider Electric support staff at **www.apc.com/support** even if you can still access the unit.

# Using the CLI

At the CLI, you can use commands to configure the InfraStruxure PDU. To use a command, type the command and press ENTER. Commands and arguments are valid in lowercase, uppercase, or mixed case. Options are case-sensitive.

While using the CLI, you can also do the following:

- Type `?` and press ENTER to view a list of available commands. Available commands will vary based on your account type.
- To obtain information about the purpose and syntax of a specified command, type the command, a space, and `?` or the word `help`. For example, to view RADIUS configuration options, type:

  ```
  radius ?
  ```

  or

  ```
  radius help
  ```

- Press the UP arrow key to view the command that was entered most recently in the session. Use the UP and DOWN arrow keys to scroll through a list of up to ten previous commands.
- Type at least one letter of a command and press the TAB key to scroll through a list of valid commands that match the text you typed in the command line.
- Type `exit`, `quit`, or `bye` to close the connection to the command line interface.

# Command Syntax

<table>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>-</td><td>Options are preceded by a hyphen.</td></tr>
<tr><td>< ></td><td>Definitions of options are enclosed in angle brackets. For example:<br>-dp <device password></td></tr>
<tr><td>[ ]</td><td>If a command accepts multiple options or an option accepts mutually exclusive arguments, the values may be enclosed in brackets.</td></tr>
<tr><td>|</td><td>A vertical line between items enclosed in brackets or angle brackets indicates that the items are mutually exclusive. You must use one of the items.</td></tr>
</table>

### Example of a command that supports multiple options:

```
ftp [-p <port number>] [-S <enable | disable>]
```

In this example, the `ftp` command accepts the option `-p`, which defines the port number, and the option `-S`, which enables or disables the FTP feature.

To change the FTP port number to 5010 and enable FTP:

1. Type the ftp command, the port option, and the argument `5010`:
   `ftp -p 5010`
2. After the first command succeeds, type the ftp command, the enable/disable option, and the `enable` selection:
   `ftp -S enable`

### Example of a command that accepts mutually exclusive arguments for an option:

```
alarmcount {-p <all | warning | critical>]
```

In this example, the option -p accepts only three arguments: all, warning, or critical. For example, to view the number of active critical alarms, type:

```
alarmcount [-p <critical>]
```

The command will fail if you type an argument that is not specified.

# Command Response Codes

The command response codes enable scripted operations to detect error conditions reliably without having to match error message text:

The CLI reports all command operations with the following format:

```
E [0-9] [0-9] [0-9]: Error message
```

| Code | Message |
|---|---|
| E000 | Success |
| E001 | Successfully Issued |
| E002 | Reboot required for change to take effect |
| E100 | Command failed |
| E101 | Command not found |
| E102 | Parameter Error |
| E103 | Command Line Error |
| E104 | User Level Denial |
| E105 | Command Prefill |
| E106 | Data Not Available |
| E107 | Serial communication with the unit has been lost |

# Command Editing

The BACKSPACE key will delete the last character of the command string the user is currently entering and is the only editing function available to the user during command entry.

## Auto-completion

The CLI supports command auto-completion. If a partial command is entered, the TAB key can be used to complete the command to the first available matched command. If such a match exists, the command line shall be completed by the CLI.

Additional presses of the TAB key will select the next available command match. Once all available commands have been scrolled through, the original partially entered command is displayed.

## Command history

Pressing the UP ARROW key presents the previously entered command onto the command line. The UP ARROW and DOWN ARROW keys permit the user to navigate the command history. In addition, pressing the BACKSPACE key deletes the last character of the command string the user is currently entering.
The command history buffer supports up to 10 previous commands.

## Delimiter

The CLI will use `<space>` (ASCII 0x20) as the delimiter between commands and arguments. Extra white space between commands and arguments will be ignored. Command responses will have all fields delimited with commas for efficient parsing.

## Security lockout

If a valid user name is used with an invalid password consecutively for the number of times specified in the web interface (see “Password Requirements” on page 67) or CLI (see “userdflt” on page 40), the account will be locked until a Super User re-enables it. A Super User cannot be locked out.

# Network Management Card Command Descriptions

## ? or help

**Access:** Super User, Administrator, Device User, Network User, Read Only

**Description:** View a list of all the CLI commands available to your account type. To view help text for a specific command, type the command followed by a question mark.

**Parameters:** `[<command>]`

**Example 1:**

```
apc> ?

System Commands:
---------------------------------------------------------------------
For command help: command ?

?          about       alarmcount  boot       bye         cd

clrrst     console     date        delete     dir         dns

email      eventlog    exit        firewall   format      ftp

help       lang        lastrst     ledblink   logzip      netstat

ntp        ping        portspeed   prompt     pwd         quit

radius     reboot      resetToDef  session    smtp        snmp

snmptrap   snmpv3      system      tcpip      tcpip6      user

userdflt   web         whoami      xferINI    xferStatus


Device Commands:
---------------------------------------------------------------------

pdSts      pdOutThr    pdInThr     pdBrkrSts  pdBrkrCfg   pdBrkEdit

envIc      envOr       envMap      pduInfo
```

**Example 2:**

```
apc> help boot

Usage: boot -- Configuration Options

   boot  [-b <dhcp | bootp | manual>] (IPv4 Boot Mode)

[-c <enable | disable>]    (Require DHCP Cookie)

         [-v <vendor class>]

         [-i <client id>]

         [-u <user class>]
```

**Error Message:** `E000, E102`

## about

**Access:** Super User, Administrator, Device User, Network User, Read Only

**Description:** Displays system information (Model Number, Serial Number, Manufacture Dates, etc.)

**Parameters:** None

**Example:** `apc> about`

```
E000: Success

Hardware Factory

---------------------

Model Number:XXXXXXXX

Serial Number:XXXXXXXXXXXX

Hardware Revision:05

Manufacture Date:3/4/2016

MAC Address:00 00 A0 10 00 00

Management Uptime:0 Days 1 Hour 42 Minutes

Application Module
---------------------
Name:xpdu
Version:v6.4.7
Date:Mar 3 2017
Time:16:39:08

APC OS(AOS)
---------------------
Name:aos
Version:v6.4.6
Date:Oct 6 2016
Time:17:46:25

APC Boot Monitor
---------------------
Name:bootmon
Version:v1.0.8
Date:Apr 8 2014
Time:10:59:40
```

**Error Message:** `E000`

## alarmcount

**Access:** Super User, Administrator, Device User, Network User, Read Only

**Description: Displays alarms present in the system.**

**Parameters:**

| Option | Argument | Description |
|---|---|---|
| `-p` | `all` | View the number of active alarms reported by the PDU. Information about the alarms is provided in the event log. |
| | `warning` | View the number of active warning alarms. |
| | `critical` | View the number of active critical alarms. |
| | `informational` | View the number of active informational alarms. |

**Example:** To view all active warning alarms, type:

```
apc> alarmcount -p all
E000: Success
AlarmCount: 0
```

**Error Message:** `E000, E102`

## boot

**Access:** Super User, Administrator

**Description:** Allows the user to get/set the network startup configuration of the device, such as setting boot mode (DHCP vs BOOTP vs MANUAL).

**Parameters:**

| Option | Argument | Description |
|---|---|---|
| `-b` | `<dhcp\|bootp\|manual>` | Define how the IPv4 settings will be configured when the unit turns on, resets, or restarts. See “Configure network settings” on page 71 for information about each boot mode setting. |
| `-c` | `<enable\|disable>` | `dhcp` and `dhcpBootp` boot modes only. Enable or disable the requirement that the DHCPv4 server provide the APC cookie. |
| `-v` | `<vendor class>` | Set the vendor class (APC by default). |
| `-i` | `<client id>` | The MAC address of the unit, which uniquely identifies it on the network. |
| `-u` | `<user class>` | The name of the application firmware module. |

**Example:** Use a DHCP server to obtain network settings:

```
apc> boot

E000: Success


Boot Mode: manual

DHCP Cookie: enabled
Vendor Class: APC

Client id: XX XX XX XX XX XX

User class: XPDU
```

**Error Message:** `E000, E102`

## bye, exit, or quit

**Access:** Super User, Administrator, Device User, Network User, Read Only

**Description:** Exit from the CLI session.

**Parameters:**

| Argument | Description |
|---|---|
| `<exit|quit|bye>` | Exit the CLI. |

**Example:**

```
apc> exit

Bye
```

**Error Message:** None

## cd

**Access:** Super User, Administrator, Device User, Network User, Read Only

**Description:** Allows the user to set the working directory of the file system. The working directory is set back to the root directory '/' when the user logs out of the CLI.

**Parameters:**

| Argument | Description |
|---|---|
| `<directory name>` | Type the name of the directory. |

**Example:**

```
apc> cd logs
E000: Success

apc> cd /
E000: Success
```

**Error Message:** `E000, E102`

## clrrst

**Access:** Super User, Administrator, Device User, Network User

**Description:** Clear the last reset reason.

**Parameters:** None

**Error Message:** None

## console

**Access:** Super User, Administrator

**Description:** Define whether users can access the command line interface using Telnet or Secure SHell (SSH), which provides protection by transmitting user names, passwords, and data in encrypted form. You can change the Telnet or SSH port setting for additional security. Alternately, disable network access to the command line interface.

**Parameters:**

| Option | Argument | Description |
|---|---|---|
| `-t` | `<enable\|disable>` | Enable or disable Telnet. |
| `-s` | `<enable\|disable>` | Enable or disable SSH. Enabling SSH enables SCP and disables Telnet. |
| `-pt` | `<telnet port n>` | Define the Telnet port used to communicate with the NMC of the PDU (23 by default, 5000–32768 possible). |
| `-ps` | `<SSH port n>` | Define the SSH port used to communicate with the NMC of the PDU (22 by default, 5000–32768 possible). |
| `-b` | `<2400\|9600\|19200\|38400>` | Configure the speed of the serial port connection (9600 bps by default). |

**Example 1:** To enable SSH access to the command line interface, type:

```
console -s ssh
```

**Example 2:** To change the Telnet port to 5000, type:

```
apc> console -pt <5000>
E002: Success
Reboot required for change to take effect.
```

**Error Message:**`E000, E102`

## date

**Access:** Super User, Administrator

**Description:** Get and set the date and time of the system. To configure an NTP server to define the date and time for the InfraStruxure PDU, see “> Date/Time > Mode” on page 86.

**Parameters:**

| Option | Argument | Description |
|---|---|---|
| `-d` | `<“datestring”>` | Set the current date. The format must match the current `-f` setting. |
| `-t` | `<“timestring”>` | Configure the current time, in hours, minutes, and seconds. Use the 24-hour clock format (00:00:00). |
| `-f` | `<mm/dd/yy\|`<br>`dd.mm.yyyy\|`<br>`mmm-dd-yy\|`<br>`dd-mmm-yy\|`<br>`yyyy-mm-dd>` | Select the numerical format in which to display all dates in this user interface. Each letter m (for month), d (for day), and y (for year) represents one digit. Single-digit days and months are displayed with a leading zero. |
| `-z` | `<time zone offset>` | Set the difference with GMT in order to specify your time zone. This enables you to synchronize with other people in different time zones. |

**Example 1:** To display the date using the format yyyy-mm-dd, type:

```
date -f yyyy-mm-dd
```

**Example 2:** To define the date as March 30, 2016, using the format configured in the preceding example, type:

```
date -d “2016-03-30”
```

**Example 3:** To define the time as 5:21:03 p.m., type:

```
date -t 17:21:03
```

**Error Message:** `E000, E100, E102`

## delete

**Access:** Super User, Administrator

**Description:** Delete a file in the file system.

**Parameters:**

| Argument | Description |
|---|---|
| `<file name>` | Type the name of the file to delete. |

**Example:**

```
apc> delete /db/prefs.dat

E000: Success
```

**Error Messages:** `E000, E102`

## dir

**Access:** Super User, Administrator, Device User, Network User, Read Only

**Description:** Display the content of the working directory.

**Parameters:** None

**Example:**

```
apc> dir

E000: Success

3145728 Mar 3  2015 aos.bin

3145728 Mar 4  2015 app.bin
45000 Mar 6  2015 config.ini
0 Mar 3  2015 db/
0 Mar 3  2015 ssl/
0 Mar 3  2015 ssh/
0 Mar 3  2015 logs/
0 Mar 3  2015 sec/
0 Mar 3  2015 dbg/
0 Mar 3  2015 pdu/
```

**Error Messages:** `E000`

## dns

**Access:** Super User, Administrator

**Description:** Configure the manual Domain Name System (DNS) settings.

**Parameters:**

| Option | Argument | Description |
|---|---|---|
| `-OM` | `<enable\|disable>` | Override the manual DNS settings. |
| `-p` | `<primary DNS server>` | Set the primary DNS server. |
| `-s` | `<secondary DNS server>` | Set the secondary DNS server. |
| `-d` | `<domain name>` | Set the domain name. |
| `-n` | `<domain name IPv6>` | Set the IPv6 domain name. |
| `-h` | `<host name>` | Set the host name. |
| `-y` | `<enable\|disable>` | Enable or disable system-hostname sync. |

**Example:**

```
apc> dns
E00 Success

Active primary DNS Server:XX.XXX.XX.XXX
Active secondary DNS Server:XX.XXX.XX.XXX

Override Manual DNS Settings:enabled
Primary DNS Server:XX.XXX.XX.XXX
Secondary DNS Server: XX.XXX.XX.XXX
Domain Name: example.com
Domain Name IPv6: example.com
System Name Sync: Disabled
Host Name:apcF3821D
```

**Error Message:** `E000`

## email

**Access:** Super User, Administrator, Device User

**Description:** View and configure e-mail settings.

**Parameters:**

| Parameters | Argument | Description |
|---|---|---|
| `-g[n]` | `<enable|disable>` | Enable or disable e-mail generation. |
| `-t[n]` | `<To Address>` | Set the To address. |
| `-o[n]` | `<long|short>` | Set the format. |
| `-l[n]` | `<Language Code>` | Set a language code supported by the current language pack. |
| `-r[n]` | `<Local|recipient|custom>` | Set the e-mail route. |
| `Custom Route Option` | | |
| `-f[n]` | `<From Address>` | Set the From address. |
| `-s[n]` | `<SMTP Server>` | Set the SMTP server address. |
| `-p[n]` | `<Port>` | Set the port. |
| `-a[n]` | `<enable|disable>` | Enable or disable authentication. |
| `-u[n]` | `<User Name>` | Set the user name for authentication. |
| `-w[n]` | `<Password>` | Set the password for authentication. |
| `-e[n]` | `<none|ifsupported|always|implicit>` | Define when to use encryption. |
| `-c[n]` | `<enable|disable>` | Enable or disable certificate requirement. |
| `-i[n]` | `<Certificate File Name>` | Set the certificate file name. |
| `[n]` = e-mail Recipient Number (1,2,3 or 4) | | |

**Example:**

```
apc> email
E000 Success

Recipient: 1
Generation: enabled
Address: example@example.com
Format: long
Language: enUs - English
Route: local

Recipient: 2
Generation:enabled
Address: example@example.com
Format: short
Language: enUs - English
Route: local
```

**Error Message:** `E000, E102`

## eventlog

**Access:** Super User, Administrator, Device User, Network User, Read Only

**Description:** View the date and time you retrieve the event log, the status of the InfraStruxure PDU, and the status of sensors connected to the InfraStruxure PDU. View the most recent device events and the date and time they occurred. Use the following keys to navigate the event log:

| Key | Description |
|---|---|
| ESC | Close the event log and return to the command line interface. |
| ENTER | Update the log display. Use this command to view events that were recorded after you last retrieved and displayed the log. |
| SPACEBAR | View the next page of the event log. |
| B | View the preceding page of the event log. This command is not available at the main page of the event log. |
| D | Delete the event log. Follow the prompts to confirm or deny the deletion. Deleted events cannot be retrieved. |

**Example:**

```
apc> eventlog
E000: Success

------ Event Log -----------------------------------------------------------------------------

     Date: 03/06/2015 Time: 13:22:26

     ------------------------------------------------------

PDU Status: No Alarms Present

Date Time User Event

     -----------------------------------------------------------------------------------------------

     03/06/2015 13:17:22System Set Time.

     03/06/2015 13:16:57 System Configuration change. Date format
preference.

     03/06/2015 13:16:49 System Set Date.

     03/06/2015 13:16:35 System Configuration change. Date format
preference.

     03/06/2015 13:16:08 System Set Date.

     03/05/2015 13:15:30 System Set Time.

     03/05/2015 13:15:00 System Set Time.

     03/05/2015 13:13:58 System Set Date.

     03/05/2015 13:12:22 System Set Date.

     03/05/2015 13:12:08 System Set Date.

     03/05/2015 13:11:41 System Set Date.

<ESC>- Exit, <ENTER>- Refresh, <SPACE>- Next, <D>- Delete
```

**Error Message:** `E000, E100`

## exit

See “bye, exit, or quit” on page 16.

## firewall

**Access:** Super User, Administrator

**Description:** Establish a barrier between a trusted, secure internal network and another network.

**Parameters:**

| Options | Argument | Description |
|---|---|---|
| `-S` | `<enable|disable>` | Enable or disable the firewall. |
| `-f` | `<file name to activate>` | Name of the firewall to activate. |
| `-t` | `<file name to test>`<br>`<duration time in minutes>` | Set the firewall to test and duration of the test in minutes. |
| `-fe` | `No argument. List only` | Shows active file errors. |
| `-te` | `No argument. List only` | Shows test file errors. |
| `-c` | `No argument. List only` | Cancel a firewall test. |
| `-r` | `No argument. List only` | Shows active firewall rules. |
| `-l` | `No argument. List only` | Shows firewall activity log. |

**Example:**

```
apc> firewall
E000: Success
Firewall: disabled
File Name: example.fwl
```

**Error Message:** `E000, E102`

## format

**Access:** Super User, Administrator

**Description:** Format the FLASH file system. This will delete all configuration data, event and data logs, certificates, and keys.

**Parameters:** None

**Example:**

```
apc> format


Format FLASH file system


Warning: This will delete all configuration data,

event and data logs, certs and keys.


Enter 'YES' to continue or <ENTER> to cancel:

apc> YES
```

**Error Message:** None

## ftp

**Access:** Super User, Administrator

**Description:** Get/set the ftp configuration data.
**NOTE:** The system will reboot if any configuration is changed.

**Parameters:**

| Option | Argument | Definition |
|---|---|---|
| `-p` | `<port number>` | Define the TCP/IP port that the FTP server uses to communicate with the NMC of the PDU (21 by default, 5000-32768 possible). The FTP server uses both the specified port and the port one number lower than the specified port. |
| `-S` | `<enable\|disable>` | Configure access to the FTP server. |

**Example:**To change the TCP/IP port to 5001, type:

```
apc> ftp -p 5001
E000: Success


apc> ftp
E000: Success
Service:        Enabled
Ftp Port:       5001


apc> ftp -p 21
E000: Success
```

**Error Message:** `E000, E102`

## help

See “? or help” on page 12.

## lang

**Access:** Super User, Administrator, Device User, Network User, Read Only

**Description:** Show language configuration options.

**Parameters:** None

**Example:**

```
apc> lang
E000: Success

Languages
enUs - English
```

**Error Message:** None

## lastrst

**Access:** Super User, Administrator, Network User, Device User

**Description:** Last reset reason.

**Parameters:** None

**Example:**

```
apc> lastrst
09 Coldstart Reset

E000: Success
```

**Error Message:** None

## ledblink

**Access:** Super User, Administrator, Network User, Device User

**Description:** Sets the LED on the unit to blink for a specified number of minutes.

**Parameters:**

| Argument | Description |
|---|---|
| `<duration time in minutes>` | Set the number of minutes the LED will blink. |

**Example:** To set the LED to blink for 10 minutes, type:

```
apc> ledblink 10
```

**Error Message:** None

## logzip

**Access:** Super User, Administrator, Network User, Device User

**Description:** Place large logs into a zip file before sending.

**Parameters:**

| Option | Argument | Description |
|---|---|---|
| `-m` | `<email recipient#>` | Set e-mail recipients by number(1-4). |

**Example:**

```
logzip -m 1
Generating files

Compressing files into /dbg/debug_ZA1023006009.tar

E000: Success
```

**Error Message:**`E000`

## netstat

**Access:** Super User, Administrator, Device User, Network User, Read Only

**Description:** Display incoming and outgoing network connections.

**Parameters:** None

**Example:**

```
apc> netstat

Current IP Information:


Family mHome Type   IPAddress Status

IPv6   4     auto   FE80::2C0:B7FF:FE51:F304/64 configured

IPv6   0     manual ::1/128 configured

IPv4   0     manual 127.0.0.1/32 configured
```

**Error Message:** None

## ntp

**Access:**Super User, Administrator

**Description:**Synchronize the time to a computer client or server.

**Parameters:**

| Option | Argument | Definition |
|---|---|---|
| -OM | <enable\|disable> | Override the manual settings. |
| -p | <primary NTP server> | Specify the primary server. |
| -s | <secondary NTP server> | Specify the secondary server. |
| -e | <enable\|disable> | Enable or disable NTP. |
| -u | <update now> | Update the time on your device. |

**Example 1:** To enable the override of manual setting, type:

```
ntp -OM enable
```

**Example 2:** To specify the primary NTP server, type:

```
ntp -p 150.250.6.10
```

**Error Message:** E000, E102

## ping

**Access:** Super User, Administrator, Device User

**Description:** Perform a network 'ping' to any external network device.

**Parameters:**

| Argument | Description |
|---|---|
| `<IP address or DNS name>` | Type an IP address with the format *xxx.xxx.xxx.xxx*, or the DNS name configured by the DNS server. |

**Example:**

```
apc> ping 192.168.1.50

E000: Success

Reply from 192.168.1.50: time(ms)= <10

Reply from 192.168.1.50: time(ms)= <10

Reply from 192.168.1.50: time(ms)= <10

Reply from 192.168.1.50: time(ms)= <10
```

**Error Message:** `E000, E100, E102`

## portspeed

**Access:** Super User, Administrator

**Description:** Get/set the network port speed.

**NOTE:** The system will reboot if any configuration is changed.

**Parameters:**

| Option | Arguments | Description |
|---|---|---|
| -s | <auto\|10H\|10F\|100 H\|100 F> | Define the communication speed of the Ethernet port. The auto command enables the Ethernet devices to negotiate to transmit at the highest possible speed. See "> Port Speed:" on page 73 for more information about port speed settings. |
| H = Half Duplex | | 10 = 10 Megabits per second (Mbps) |
| F = Full Duplex | | 100 = 100 Mbps |

**Example:**

```
apc> portspeed
E000: Success
Port Speed: Auto_negotiation
Current Port Speed: 100 Full_Duplex


apc> portspeed -s 10h

E000: Success


apc> portspeed

E000: Success

Port Speed: 10 Half_Duplex


apc> portspeed -s auto

E000: Success
```

**Error Message:** E000, E102

## prompt

**Access:**Super User, Administrator, Device User

**Description:**Change the format of the prompt to short or long.

**Parameters:**

| Option | Argument | Description |
|---|---|---|
| `-s` | `long` | The prompt includes the account type of the currently logged-in user. |
| | `short` | The default setting. The prompt is four characters long: `apc>` |

**Example:**

```
apc> prompt -s long

E000: Success


Administrator@apc>prompt -s short

E000: Success
```

**Error Message:**`E000, E102`

## pwd

**Access:** Super User, Administrator, Device User, Read Only

**Description:** Output the path of the current working directory.

**Parameters:** None

**Example:**

```
apc> pwd
/
```

**Error Message:**None

## Quit

See “bye, exit, or quit” on page 16.

## radius

**Access:** Super User, Administrator

**Description:** View the existing RADIUS settings, enable or disable RADIUS authentication, and configure basic authentication parameters for up to two RADIUS servers.

For a summary of RADIUS server configuration and a list of supported RADIUS servers, see “Summary of the Configuration Procedure:” on page 69. For detailed information about configuring your RADIUS server, see the *Security Handbook*, available at **www.apc.com**.

Additional authentication parameters for RADIUS servers are available at the web interface of the InfraStruxure PDU. See “> RADIUS:” on page 68 for more information.

**Parameters:**

| Option | Argument | Description |
|---|---|---|
| `-a` | `<local\|`<br>`radiusLocal\|`<br>`radius>` | Configure RADIUS authentication:<br><br>`local`: RADIUS is disabled. Local authentication is enabled.<br><br>`radiusLocal`: RADIUS, then Local Authentication. RADIUS and local authentication are enabled. Authentication is requested from the RADIUS server first. If the RADIUS server fails to respond, local authentication is used.<br><br>`radius`: RADIUS is enabled. Local authentication is disabled. |
| `-p1`<br>`-p2` | `<server IP>` | The IP address of the primary or secondary RADIUS server. |
| `-o1`<br>`-o2` | `<server port>` | The server port of the primary or secondary RADIUS server.<br><br>**NOTE:** RADIUS servers use port 1812 by default to authenticate users. To use a different port, add a colon followed by the new port number to the end of the RADIUS server name or IP address. The unit supports ports 1812, 5000 to 32768. |
| `-s1`<br>`-s2` | `<server secret>` | The shared secret between the primary or secondary RADIUS server and the unit. |
| `-t1`<br>`-t2` | `<server timeout>` | The time in seconds that the unit waits for a response from the primary or secondary RADIUS server. |

**Example 1:**To view the existing RADIUS settings for the InfraStruxure PDU, type `radius` and press ENTER.

```
apc>radius
E000: Success
Access: Local Only
Primary Server: 0.0.0.0
Primary Server Port: 1812
Primary Server Secret: <Password Hidden>
Primary Server Timeout: 5
Secondary Server: 0.0.0.0
Secondary Server Port: 1812
Secondary Server Secret: <Password Hidden>
Secondary Server Timeout: 5
```

**Example 2:** To enable RADIUS and local authentication, type:

```
radius -a radiusLocal
```

**Example 3:** To configure a 10-second timeout for a secondary RADIUS server, type:

```
radius -t2 10
```

**Error Message:** `E000, E102`

## reboot

**Access:** Super User, Administrator

**Description:** Restart the NMC interface of the unit only; this forces the network device to reboot. You must confirm this operation by entering a “YES” after the command has been entered.

**Parameters:** None

**Example:**

```
apc> reboot

E000: Success

Reboot Management Interface

Enter 'YES' to continue or <ENTER> to cancel : <user enters ‘YES’>

Rebooting...
```

**Error Message:** `E000, E100`

## resetToDef

**Access:** Super User, Administrator

**Description:** Reset all parameters to their default.

**Parameters:**

| Option | Arguments | Description |
|---|---|---|
| `-p` | `<all\|keepip>` | `all`: all configuration data, including the IP address.<br>`keepip`: all configuration data, except the IP address.<br>Reset all configuration changes, including event actions, device settings, and, optionally, TCP/IP configuration settings. |

**Example:** To reset all of the configuration changes *except* the TCP/IP settings for the InfraStruxure PDU, type:

```
resetToDef -p keepip

Enter 'YES' to continue or <ENTER> to cancel : : <user enters ‘YES’>

all User Names, Passwords.

Please wait...


Please reboot system for changes to take effect!
```

**Error Message:** `E000, E100`

## session

**Access:** Super User, Administrator, Device User

**Description:** Record which user is logged in, the interface, address, logged in time, and ID.

**Parameters:**

| Option | Arguments | |
|---|---|---|
| `-d` | `<session ID>` | Delete session ID. |
| `-m` | `<Enable \| disable>` | Enable or disable multi-user mode. |
| `-a` | `<enable \| disable` | Enable or disable remote authentication override. |

**Example:**

```
apc> session

User InterfaceAddressLogged In TimeID
---------------------------------------------------------------------------------------------------------------------------
apc Serial xx.xxx.xxx.xxx00:00:05 1
```

**Error Message:** `E000, E102`

## smtp

**Access:** Super User, Administrator, Device User

**Description:** Internet standard for electronic mail.

| Option | Argument | Description |
|---|---|---|
| `-f` | `<From Address>` | Set smtp server. |
| `-s` | `<SMTP Server>` | Set e-mail from address. |
| `-p` | `<Port>` | Set e-mail recipient port number. Port options are 25, 465, 587, 2525, and 5000 to 32768. |
| `-a` | `<enable\|disable>` | Enable or disable authentication. |
| `-u` | `<User Name>` | Set user name (authentication). |
| `-w` | `<Password>` | Set e-mail password (authentication). |
| -e | <none\|ifavail\|always\|implicit> | Define when encryption is used. |
| `-c` | `<enable\|disable>` | Enable or disable certificate requirement. |
| `-i` | `<Certificate File Name>` | Set the certificate file name. |

**Example:**

```
apc> smtp
E000: Success

From:          address@example.com
Server:        mail.example.com
Port:          25
Auth:          disabled
User:          User
Password:      <not set>
Encryption:    none
Req. Cert:     disabled
Cert File:     <n/a>
```

**Error Message:** `E000, E102`

## snmp

**Access:** Super User, Administrator

**Description:** Enable or disable SNMP version 1.

| Option | Arguments | Description |
|---|---|---|
| `-S` | `<enable\|disable>` | Enable or disable SNMPv1. |
| `-c[n]` | `<Community>` | Set community name for access control. |
| `-a[n]` | `<read\|write\|writeplus\|disable>` | Set the access level. |
| `-n[n]` | `<IP or Domain Name>` | Set NMS IP address for access control. |
| `[n]` = Access Control # (1,2,3, or 4) | | |

**Example:** To enable SNMP version 1, type:

```
apc> snmp -S enable
```

**Error Message:** `E000, E102`

## snmpv3

**Access:** Super User, Administrator

**Description:** Enable or disable SNMP version 3.

**Parameters:**

| Option | Arguments | Description |
|---|---|---|
| `-S` | `<enable\|disable>` | Enable or disable SNMPv3. |
| `-u[n]` | `<User Name>` | Set user name for access control. |
| `-a[n]` | `<Auth Phrase>` | Set authentication pass phrase for access control. |
| `-c[n]` | `<Crypt Phrase>` | Set encryption phrase for access control. |
| `-ap[n]` | `<sha\|md5\|none>` | Set authentication protocol for access control. |
| `-pp[n]` | `<aes\|des\|none>` | Set encryption protocol for access control. |
| `-ac[n]` | `<enable\|disable>` | Enable or disable access control. |
| `-au[n]` | `<User Profile name>]` | Set User Profile name for access control. |
| `-n[n]` | `<Nms Ip>` | Set NMS IP address for access control. |
| `[n]` = Access Control # (1,2,3, or 4) | | |

**Example:** To enable SNMP version 3, type:

```
apc> snmpv3 -S enable
```

**Error Message:** `E000, E102`

## snmptrap

**Access:** Super User, Administrator

**Description:** Configure, enable, or disable SNMP trap generation.

**Parameters:**

| Option | Argument | Description |
|---|---|---|
| `-c[n]` | `<Community>` | Define the community name for trap receiver. |
| `-r[n]` | `<Receiver NMS IP>` | Enter the NMS IP address for trap receiver. |
| `-l[n]` | `<Language>` | Enter the Language code for trap receiver. |
| `-t[n]` | `<snmpV1\|snmpV3>` | Enter the trap type for trap receiver. |
| `-g[n]` | `<enable\|disable>` | Enable or disable trap generation for trap receiver. |
| `-a[n]` | `<enable\|disable>` | Enable or disable trap authentication for trap receiver. |
| `-u[n]` | `<profile1\|profile2\|profile3 \|profile4>` | Define user names for trap receiver. |
| `n` = Trap receiver #(1,2,3,4,5 or 6) | | |

**Example:**

```
apc> snmptrap
E000: Success

SNMP Trap Configuration

Index: 1
Receiver IP: xx.xxx.xxx.xx
Community: public
Trap Type: SNMPV1
Generation: enabled
Auth Traps: enabled
User Name: apc snmp profile 1
Language: enUs - English

Index: 2
Receiver IP: xx.xxx.xxx.xx
Community: public
Trap Type: SNMPV1
Generation: enabled
Auth Traps: disabled
User Name: apc snmp profile 1
Language: enUs - English
```

**Error Message:** `E000, E102`

## system

**Access:** Super User, Administrator

**Description:** View and set the system name, contact, and location. View up time; date and time; your user name; high-level system status P, N, A (see “CLI Home Screen” on page 7 for more information about system status); and current versions of Bootmon, AOS, and application modules.

**Parameters:**

| Option | Argument | Description |
|---|---|---|
| `-n` | `<system-name>` | Define the device name, the name of the person responsible for the device, and the physical location of the device.<br>**NOTE:** If you define a value with more than one word, you must enclose the value in quotation marks.<br>These values are also used by StruxureWare and the NMC’s SNMP agent. |
| `-c` | `<system-contact>` | |
| `-l` | `<system-location>` | |
| `-m` | `<system-message>` | When defined, a custom message will appear on the logon screen for all users. |
| `-s` | `<enable\|disable>]` | Allow the host name to be synchronized with the system name so both fields automatically contain the same value.<br>**NOTE:** When enabling this feature, the system name identifier can no longer contain a space character (since it will be synchronized to the host name field). |

**Example 1:** To set the device location as `Test Lab`, type:

```
system -l “Test Lab”
```

**Example 2:** To set the system name as `Rack 5`, type:

```
system -n “Rack 5”
```

**Error messages:** `E000, E102`

## tcpip

**Access:** Super User, Administrator

**Description:** View and manually configure IPv4 settings for the InfraStruxure PDU:

**Parameters:**

| Option | Argument | Description |
|---|---|---|
| `-S` | `<enable|disable>` | Enable or disable IPv4. |
| `-i` | `<IP address>` | Type the IP address of the unit, using the format *xxx.xxx.xxx.xxx* |
| `-s` | `<subnet mask>` | Type the subnet mask for the unit. |
| `-g` | `<gateway>` | Type the IP address of the default gateway. **Do not** use the loopback address (127.0.0.1) as the default gateway. |
| `-d` | `<domain name>` | Type the DNS name configured by the DNS server. |
| `-h` | `<host name>` | Type the host name that the unit will use. |

**Example 1:** To view the network settings of the unit, type `tcpip` and press ENTER.

```
apc> tcpip
E000: Success

Active IPv4 Settings
---------------------
Active IPv4 Address: 192.168.1.49
Active IPv4 Subnet Mask: 255.255.255.0
Active IPv4 Gateway: 192.168.1.1

Manually configured IPv4 Settings
---------------------------------
IPv4: enabled
Manual Settings: enabled
IPv4 Address: 192.168.1.49
Subnet Mask: 255.255.255.0
MAC Address: XX XX XX XX XX XX
Gateway: 192.168.1.1
Domain Name: example.com
Host Name: HostName
```

**Example 2:** To manually configure an IP address of `150.250.6.10` for the unit, type:

```
tcpip -i 10.179.229.50 -s 255.255.252.0 -g 10.179.228.1
```

**Error messages:** `E000, E102`

## tcpip6

**Access:** Super User, Administrator

**Description:** Enable IPv6. View and configure IPv6 network settings for the InfraStruxure PDU.

**Parameters:**

| Option | Argument | Description |
|---|---|---|
| `-S` | `<enable\|disable>` | Enable or disable IPv6. |
| `-i` | `<IPv6 address>` | Set the manual IPv6 address of the unit. |
| `-g` | `<IPv6 gateway>` | Set the IPv6 address of the default gateway. |
| `-man` | `<enable\|disable>` | Enable manual addressing for the IPv6 address of the unit. |
| `-auto` | `<enable\|disable>` | Enable the unit to automatically configure the IPv6 address. |
| `-d6` | `<router\|stateful`<br>`\|stateless\|never>` | Set the DHCPv6 mode, with parameters of router controlled, stateful (for address and other information, they maintain their status), stateless (for information other than address, the status is not maintained), never. |

**Example 1:** To view the network settings of the unit, enter

```
tcpip6
```

**Example 2:** To configure an IPv6 address of `2001:0:0:0:0:FFD3:0:57ab for the` unit, enter:

```
tcpip6 -i 2001:0:0:0:0:FFD3:0:57ab  -g <Valid IPv6 gateway>
```

**Error messages:** `E000, E102`

## user

**Access:** Super User, Administrator

**Description:** Configure the user name, password, and inactivity timeout for each account type. You can't edit a user name; you must delete it and then create a new user. For information on the permissions granted to each account type, see "User account overview" on page 2.

| Option | Argument | Description |
|---|---|---|
| `-cp` | `<current password>` | Required for Super User Account |
| `-pw` | `<user password>` | Specify the user password. |
| `-pe` | `<Admninstrator\|Device\|Read-Only\|Network Only>` | Set user permission. |
| `-d` | `<user description>` | Specify the user description. |
| `-e` | `<enable\|disable>` | Enable or disable access for specified user. |
| `-st` | `<session timeout>` | Specify how many minutes a session lasts before logging off a user when the keyboard is idle. |
| `-sr` | `<enable\|disable>` | Bypass RADIUS by using the serial console (CLI) connection, also known as Serial Remote Authentication Override |
| `-el` | `<enable\|disable>` | Enable or disable Event Log color coding. |
| `-lf` | `<tab\|csv>` | Set the format for exporting a log file. |
| `-ts` | `<us\|metric>` | Set the temperature scale, Fahrenheit or Celsius. |
| `-df` | `<mm/dd/yyyy\|dd.mm.yyyy\|mmm-dd-yy\|dd-mmm-yy\|yyyy-mm-dd>` | Set the date format. |
| `-lg` | `<language code>` | Set the user language `(e.g. enUs).` |
| `-del` | `<user name>` | Delete the specified user. |
| `-l` | `n/a` | Display the current user list. |

**Example 1:** To change the Administrator user name to XYZ, type:

```
user -n XYZ
```

**Example 2:** To change the log off time to 10 minutes, type:

```
user -st 10
```

## userdflt

**Access:** Super User, Administrator

**Description:** This command is a complimentary function to “user” establishing default user preferences. There are two main features for the default user settings:

Determine the default values to populate in each of the fields when the Super User or Administrator-level account creates a new user. These values can be changed before the settings are applied to the system.

For remote users (user accounts not stored in the system that are remotely authenticated such as RADIUS) these are the values used for those that are not provided by the authenticating server. For example, if a RADIUS server does not provide the user with a temperature preference, the value defined in this section will be used.

**Parameters:**

| Options | Argument | Description |
|---|---|---|
| `-e` | `<enable\|disable>` | By default, users will be enabled or disabled upon creation. |
| `-pe` | `<Administrator\|Device\|Read-Only\|Network-Only>` | Set the default permission level and account type. |
| `-d` | `<user description>` | Provide a user description. |
| `-st` | `<session timeout>` | Provide a default session timeout (minutes). |
| `-bl` | `<bad login attempts>` | Number of incorrect login attempts a user has before the system disables their account. Upon reaching this limit, a message is displayed informing the user the account has been locked. The Super User or an Administrator-level account is needed to re-enable the account to allow the user to log back in.<br>**NOTE:** A Super User account cannot be locked out, but can be manually disabled if necessary. |
| `-el` | `<enable\|disable>` | Enable or disable event log color coding. |
| `-lf` | `<tab\|csv>` | Specify the log export format: tab or CSV. |
| `-ts` | `<us\|metrics>` | Specify the user's temperature scale. This setting is also used by the system when a user preference is not available (for example, e-mail notifications). |
| `-df` | `<mm/dd/yyyy\|dd.mm.yyyy\|mmm-dd-yy\|dd-mmm-yy\|yyyy-mm-dd>` | Specify the user's preferred date format. |
| `-lg` | `<language code>` | Set the user language `(enUs, etc).` |
| `-sp` | `<enable\|disable>` | Enable or disable strong password requirements. |
| `-pp` | `<interval in days>` | Set the number of days between required password changes. |

**Example:**

```
apc> userdflt
E000: Success
Access: Disabled
User Permission: Administrator
User description: User Description
Session Timeout: 3 minutes
Bad Login Attempts: 0
Event Log color Coding: Enabled
Export Log Format: Tab
Temperature Scale: Metric
Date Format: mm/dd/yyyy
Language: English (enUs)
Strong Passwords: Disabled
Require Password Change: 0 day(s) (Disabled)
```

**Error Message:** `E100, E102`

## web

**Access:** Super User, Administrator

**Description:** Enable access to the web interface using HTTP or HTTPS.

For additional security, you can change the port setting for HTTP and HTTPS to any unused port from 5000 to 32768. Users must then use a colon (:) in the address field of the browser to specify the port number. For example, for a port number of 5000 and an IP address of 152.214.12.114, type:

```
http://152.214.12.114:5000
```

**Parameters:**

| Option | Argument | Definition |
|---|---|---|
| -h | <enable\|disable> | Enable or disable access to the user interface for HTTP. |
| -s | <enable\|disable> | Enable or disable access to the user interface for HTTPS.<br>When HTTPS is enabled, data is encrypted during transmission and authenticated by digital certificate. |
| -ph | <http port #> | Specify the TCP/IP port used by HTTP to communicate with the unit (80 by default). The other available range is 5000–32768. |
| -ps | <https port #> | Specify the TCP/IP port used by HTTPS to communicate with the unit (443 by default). The other available range is 5000–32768. |
| -mp | <SSL3.0\|TLS1.0\|TLS1.1\|<br>TLS1.2>‘ | Specify the minimum HTTPS protocol to use. |

**Example 1:** To prevent all access to the web interface, type:

```
web -s disable
```

**Example:** To define the TCP/IP port used by HTTP, type:

```
apc> web

E000: Success

Http:        enabled
Https: disabled

Http Port:      5000

Https Port:     443
Minimum Protocaol: TLS1.1


apc> web -ph 80

E000: Success
```

**Error Message:** `E000, E102`

## whoami

**Access:** Super User, Administrator, Device Only, Read Only

**Description:** Show the user name of the current user.

**Parameters:** None

**Example:**

```
apc> whoami

E000: Success

admin
```

**Error Message:** `E000`

## xferINI

**Access:** Super User, Administrator

**Description:** Use XMODEM to upload an .ini file while you are accessing the CLI through a serial connection. After the upload completes:

- If there are any system or network changes, the CLI restarts and you must log on again.
- If you selected a baud rate for the file transfer that is not the same as the default baud rate for the InfraStruxure PDU, you must reset the baud rate to the default to reestablish communication with the InfraStruxure PDU.

**Parameters:** None

**Example:**

```
apc> xferINI

Enter 'YES' to continue or <ENTER> to cancel : <user enters ‘YES’>

------- File Transfer Baud Rate------------------------------

       1- 2400

       2- 9600

       3- 19200

       4- 38400

> <user enters baudrate selection>

Transferring at current baud rate (9600), press <ENTER>...

<user presses <ENTER>>

Start XMODEM-CRC Transfer Now!

CC

<user starts sending INI>

150 bytes have successfully been transmitted.

apc>
```

**Error Message:** None

### xferStatus

**Access:** Super User, Administrator

**Description:** View the result of the last file transfer. See “Verify Upgrades and Updates” on page 104 for descriptions of the transfer result codes.

**Parameters:** None

**Example:**

```
apc> xferStatus

E000: Success

Result of last file transfer: Failure unknown
```

**Error Message:** `E000`

# Device Command Descriptions

### pdSts

**Access:** Super User, Administrator, Device User

**Description:** View detailed power distribution status.

**Parameters:**

| Option | Description |
|---|---|
| `-o` | System output status |
| `-i` | System input status |
| `-al` | System alarm status |
| `-br` | System breakers status |

**Example:** View the system output status.

```
apc> pdSts -o
E000: Success

L1–2 L2–3 L31 Units
--------------------------------
Voltage 209 208 209 V

L1 L2 L3Neutral Units
--------------------------------
Voltage 122 122 123 V
Curent 000 000 001 002 A

L1 L2 L3 Total Units
---------------------------------
Power 00.0 00.0 00.0 00.0 kW
Apparent Power 00.0 00.0 00.0 00.0 kVA
Power Factor 1.00 1.00 1.00 1.00

Frequency 60.0 Hz
```

**Error Message:** `E102`

## pdOutThr

**Access:** Super User, Administrator, Device User

**Description:** Configure output thresholds. Outputs above or below the configured thresholds will generate alarms.

**Parameters:**

| Option | Argument | Description |
|---|---|---|
| -f | <0.0\|0.2\|0.5\|1.0\|1.5\|2.0\|3.0\|4.0\|5.0\|9.0> | Set frequency deviation. |
| -uv | <Thresh> | Set under voltage threshold (-30 to -1%) |
| -ov | <Thresh> | Set over voltage threshold (1 to 30%) |
| -uil | <Thresh> | Set under current L threshold (1 to 100%) |
| -oil | <Thresh> | Set over current L threshold (1 to 110%) |
| -oin | <Thresh> | Set over current N threshold (1 to 110%) |
| **NOTE:** Input <Thresh> value as 0 to disable the alarm.<br>**NOTE:** Negative values are implied by option -uv; do not use a negative sign in the argument for options -uv. | | |

**Example 1:**

```
apc> pdOutThr
E000: Success

Frequency Thresh         : Disabled
Under Voltage Thresh     : -20
Over Voltage Thresh      : 12%
Under Current L Thresh   : Disabled
Over Current L Thresh    :  80%
Over Current N Thresh    : 80%
```

**Error Message:** E102

## pdInThr

**Access:** Super User, Administrator, Device User

**Description:** Configure input thresholds. Inputs above or below the configured thresholds will generate alarms.

**Parameters:**

| Option | Argument | Description |
|---|---|---|
| -uv | <Thresh> | Under voltage threshold (-30 to -1%) |
| -ov | <Thresh> | Over voltage threshold (1 to 30%) |
| -ub | <Thresh> | Under bypass threshold (-30 to -1% ) |
| -ob | <Thresh> | Over bypass threshold (1 to 30%) |
| **NOTE:** Input <Thresh> value as 0 to disable the alarm.<br>**NOTE:** Negative values are implied by options -uv and -ub; do not use a negative sign in the arguments for these options. | | |

**Example:**

```
apc> pdInThr
E000: Success

Under Voltage Thresh: -10%
Over Voltage Thresh : 30%
Under Bypass Thresh : Not Installed
Over Bypass Thresh : Not Installed
```

**Error Message:** E102

## pdBrkrSts

**Access:** Super User, Administrator, Device User

**Description:** View branch circuit breaker status.

**Parameters:**

| Option | Argument | Description |
|---|---|---|
| -st | <pos#\|p1\|p2\|p3\|p4> | Display breaker status.<br>pos# indicates breaker position number<br>p# indicates panel number and shows status for entire panel:<br>• p1 for 1–41 (odd)<br>• p2 for 2–42 (even)<br>• p3 for 43–83 (odd)<br>• p4 for 44–84 (even) |

**Example:**

```
apc> pdBrkrSts -st 1
E000: Success

Breaker Not Installed
```

**Error Message:** E102

## pdBrkrCfg

**Access:**Super User, Administrator, Device User

**Description:** Add or delete circuit breakers.

**Parameters:**

<table>
<tr><th>Option 1</th><th>Argument</th><th>Option 2</th><th>Argument</th><th>Description</th></tr>
<tr><td><code>-add</code></td><td><code>&lt; pos#|p1|p2|p3|p4&gt; &lt;pole#&gt; &lt; Breaker rating &gt;</code></td><td><code>n/a</code></td><td><code>n/a</code></td><td>Add a breaker</td></tr>
<tr><td><code>-del</code></td><td><code>&lt;pos#|p1|p2|p3|p4&gt;</code></td><td><code>n/a</code></td><td><code>n/a</code></td><td>Delete a breaker</td></tr>
<tr><td colspan="5">• <b>pos#:</b> Breaker position number. To add a subfeed, append <code>sub</code> to <code>pos#</code>. If you install a subfeed in position (31,33,35) or (37,39,41) or (32,34,36) or (38,40,42), enter <code>SUB</code> after the position number.<br>• <b>p#:</b> Panel number. Used to add/delete an entire panel: <code>p1</code> for [1 to 41](Odd), <code>p2</code> for [2 to 42](Even), <code>p3</code> for [43 to 83](Odd), <code>p4</code> for [44 to 84](Even).<br>• <b>pole#:</b> Number of poles.<br>• <b>Breaker rating:</b> Enter a rating between 1A and 350A. For special panel connections, the following may be entered:<br><code>ELCB</code> (Earth Leakage Circuit Breaker)<br><code>NEUT</code> (Neutral Connection)</td></tr>
</table>

**Example:**

```
apc> pdBrkrCfg -del 1
E000 Success
Breaker group deleted (3 positions).

apc> pdBrkrCfg -add 1 3 150
E000: Success

***Breakers added with default configuration, use command pdBrkEdit
to modify the breaker information
```

**Error Message:** `E102`

## pdBrkEdit

**Access:** Super User, Administrator, Device User

**Description:** Modify branch circuit breaker configuration.
**Parameters:**

| Option | Argument | Description |
|---|---|---|
| `-nm` | `<pos#> <Name string>` | Configure breaker name |
| `-loc` | `<pos#> <location string>` | Configure breaker location |
| `-rt` | `<pos#> <Breaker rating>` | Configure breaker rating |
| `-ith` | `<pos#> <max\|high\|low\|min> <Threshold>` | Configure breaker threshold (1-100%). Set threshold value to 0 to disable the threshold alarm. |
| **NOTE:** Breaker rating between 1A and 350A. For special panel connections, enter the following:<br>`ELCB` = Earth Leakage Circuit Breaker<br>`NEUT` = Neutral Connection | | |

**Example:**

```
apc> pdBrkEdit -nm 1 Brkr1
E000: Success
```

**Error Message:** `E102`

## envIc

**Access:** Super User, Administrator, Device User

**Description:** Configure Input contacts.

**Parameters:**

| Option | Argument | Description |
|---|---|---|
| `-st` | `<ic#>` | Input contact information |
| `-nm` | `<ic#> <name string>` | Configure input contact name |
| `-nor` | `<ic#> <open\|closed>` | Configure input contact normal state |
| **NOTE:** `ic#` = input contact of interest | | |

**Example:** View Input contact status for Input Contact 1:

```
apc> envIc -st 1

Input Contact 1
----------------------
Name : Input Contact1
State : Open
Normal State : Open
```

**Error Message:** `E102`

## envOr

**Access:** Super User, Administrator, Device User

**Description:** Configure output relays.

**Parameters:**

| Option | Argument | Description |
|---|---|---|
| `-st` | `<or#>` | Output relay status |
| `-nm` | `<or#> <name string>` | Configure Output relay name |
| `-nor` | `<or#> <open\|closed>` | Configure Output relay normal state |
| `or#` = Output relay of interest | | |

**Example:** View status for output relay 4:

```
apc> envOr -st 4
E000: Success
Output Relay 4
---------------------
Name : Output Relay 4
Normal state : Closed
State : Open
```

**Error Message:** `E102`

## envMap

**Access:** Super User, Administrator, Device User

**Description:** Enable or disable alarm mapping with output relays.

**Parameters:**

| Option | Argument | Description |
|---|---|---|
| `-l` | `<or#> <enable|disable>` | Any load alarm |
| `-ol` | `<or#> <enable|disable>` | Overload alarm |
| `-iv` | `<or#> <enable|disable>` | Input voltage alarm |
| `-ov` | `<or#> <enable|disable>` | Output voltage alarm |
| `-byp` | `<or#> <enable|disable>` | PDU in bypass |
| `-brk` | `<or#> <enable|disable>` | Any breaker alarm |
| `-ic1` | `<or#> <enable|disable>` | Contact 1 alarm |
| `-ic2` | `<or#> <enable|disable>` | Contact 2 alarm |
| `-ic3` | `<or#> <enable|disable>` | Contact 3 alarm |
| `-ic4` | `<or#> <enable|disable>` | Contact 4 alarm |
| `or#` = Output relay of interest | | |

**Example:**

```
apc> envMap
E000: Success

Alarm Status Relay1 Relay2 Relay3 Relay4
-----------------------------------------------------------------------------------------
Any Load Alarm Normal Disable Disable Disable
Overload Alarm Normal Enable Disable Disable
Input Voltage Alarm Normal Disable Disable Disable
Output Voltage Alarm Normal Disable Disable Disable
PDU in Bypass Normal Disable Disable Disable
Any Breaker Alarm Normal Disable Disable Disable
Contact 1 Normal Disable Disable Disable
Contact 2 Normal Disable Disable Disable
Contact 3 Normal Disable Disable Disable
Contact 4 Normal Disable Disable Disable
```

**Error Message:** `E102`

## pduInfo

**Access:** Super User, Administrator, Device User

**Description:** Show PDU Information.

**Parameters:**

| Option | Description |
|---|---|
| `-dd` | Display device details. |
| `-abt` | Display ISX-PDU information. |

**Example 1:** View ISX-PDU information:

```
apc> pduInfo -abt
E000: Success

Serial Number : xxxxxxxxxxx
Manufacturer Date : 09/03/2015
Model Number : APxxx
Product Name : apcF3821D
Hardware Revision : 02
Firmware Revision : 01.02
```

**Error Message:** `E102`

# The Web Interface

## Supported Web browsers

To access the web interface on Windows® operating systems, use Microsoft® Internet Explorer® (IE) 8.x or higher (with compatibility view turned on), or the latest release of Microsoft Edge®. To access the web interface on any operating system, use the latest releases of Mozilla®, Firefox®, or Google Chrome®. Other commonly available browsers also may work but have not been fully tested by Schneider Electric. The InfraStruxure PDU cannot work with a proxy server. Before accessing the Web interface of the PDU, do one of the following:

- Configure the browser to disable the use of a proxy server for your PDU.
- Configure the proxy server so that it does not proxy the specific IP address of your PDU.

## Log on

Use the DNS name or System IP address of the unit for the URL address of the web interface. Use your case-sensitive user name and password to log on.

The default user name differs by account type:

- **apc** for the Super User
- **device** for a Device User
- **readonly** for a Read-Only User

The Super User or an Administrator created by the Super User should define the user names, passwords, and other account characteristics for the lower tier users.

If you are using HTTPS (SSL/TLS) as your access protocol, your logon credentials are compared with information in a server certificate. If the certificate was created with the APC Security Wizard, and an IP address was specified as the common name in the certificate, you must use an IP address to log on to the unit. If a DNS name was specified as the common name on the certificate, you must use a DNS name to log on.

**URL address formats:** Type the unit DNS name or IP address in the web browser and press ENTER. When you specify a non-default web server port in Internet Explorer, you must include http:// or https:// in the URL.

### Common browser error messages at log-on

| Error Message | Browser | Cause of the Error |
|---|---|---|
| “This page cannot be displayed.” | Internet Explorer | Web access is disabled, or the URL was incorrect |
| “Unable to connect.” | Firefox | |

### URL format examples

- For a DNS name of Web1:
  - – `http://Web1` if HTTP is your access mode
  - – `https://Web1` if HTTPS (HTTP with SSL/TLS) is your access mode
- For a System IP address of 139.225.6.133 and the default web server port (80):
  - – `http://139.225.6.133` if HTTP is your access mode
  - – `https://139.225.6.133` if HTTPS (HTTP with SSL/TLS) is your access mode
- For a System IP address of 139.225.6.133 and a non-default web server port (5000):
  - – `http://139.225.6.133:5000` if HTTP is your access mode
  - – `https://139.225.6.133:5000` if HTTPS (HTTP with SSL/TLS) is your access mode

- For a System IPv6 address of 2001:db8:1::2c0:b7ff:fe00:1100 and a non-default web server port (5000):
  `http://[2001:db8:1::2c0:b7ff:fe00:1100]:5000` if HTTP is your access mode

## Web interface features

Read the following to familiarize yourself with basic web interface features for your unit.

**General information:** The following information is located in the upper right corner of each page:

- User name (select to change user preferences)
- Language (if available, select to change language preference)
- Log Off (select to log off of the web interface)
- Help (select to view help contents)
- 📌 (click to set the current web page as the home page)
  **NOTE:** Click ⊙ to revert to displaying the Home screen when you log on.

**Device status icons:** One or more icons and accompanying text indicate the current operating status of the unit. These are displayed on the Home page and in the upper-right corner of every page to indicate the status of the PDU. Critical and Warning icons are followed by the number of active alarms of each severity.

✖ **Critical:** A critical alarm exists, which requires immediate action.

⚠ **Warning:** An alarm condition requires attention and could jeopardize data or equipment if its cause is not addressed.

✓ **No Alarms Present:** The unit is operating normally.

**Quick links:** At the lower left on each page, there are three configurable links. You can also navigate to the Quick Links page: **Configuration > General > Quick Links**.

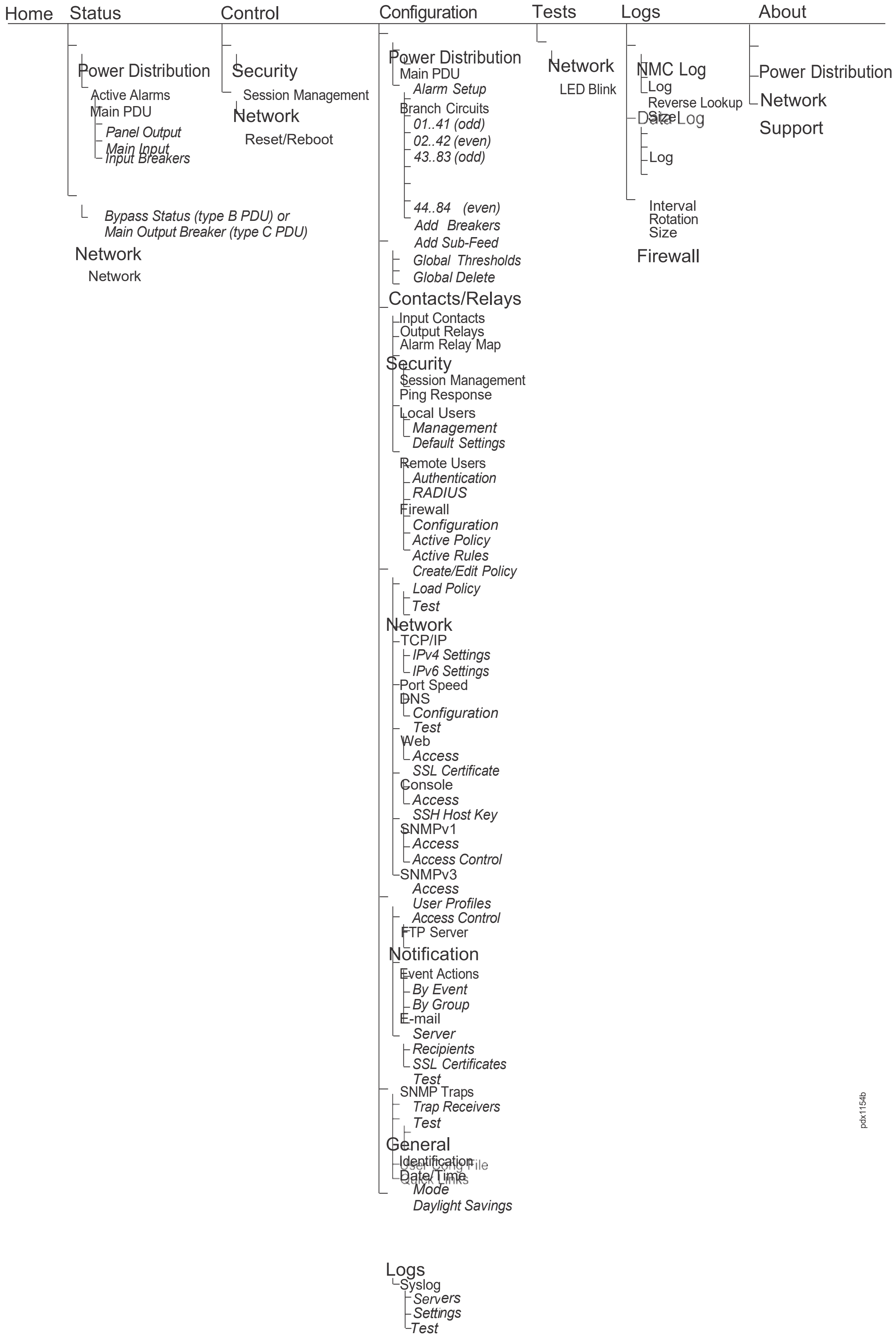
- **Link 1:** The home page of the APC by Schneider Electric web site
- **Link 2:** Demonstrations of Schneider Electric web-enabled products.
- **Link 3:** Information on Schneider Electric Remote Monitoring Services.

**Tabs:** Select a tab to display listed menus and sub-menus:

- **Home:** This is the default tab when you log on. (To change the login page to a different page, click the push-pin button 📌 at the top right of the browser window while on the desired page). View active alarms; voltage, current, and power; and the most recent device events. See “Home Page” on page 56 for more information.
- **Status:** Gives the user the status of the **Power Distribution** and **Network**. The **Power Distribution** menu covers the status of Active Alarms and the Main PDU. Main PDU covers more information which will be described in “Status Tab” on page 57**.** The **Network** menu covers just the network. See “Status Tab” on page 57 for more information.
- **Control:** The **Control** tab covers **Security** and **Network**. Much more information is covered under each of these menus and will be described in “Control Tab” on page 60.
- **Configuration:** The **Configuration** tab covers **Power Distribution**, **Contacts/Relays, Security**, **Network**, **Notification**, **General** and **Logs**. Much more information is covered under each of these menus and will be described in the “Configuration Tab” on page 61.
- **Tests:** The **Tests** tab covers **Network**. The **Network** menu covers LED Blink.

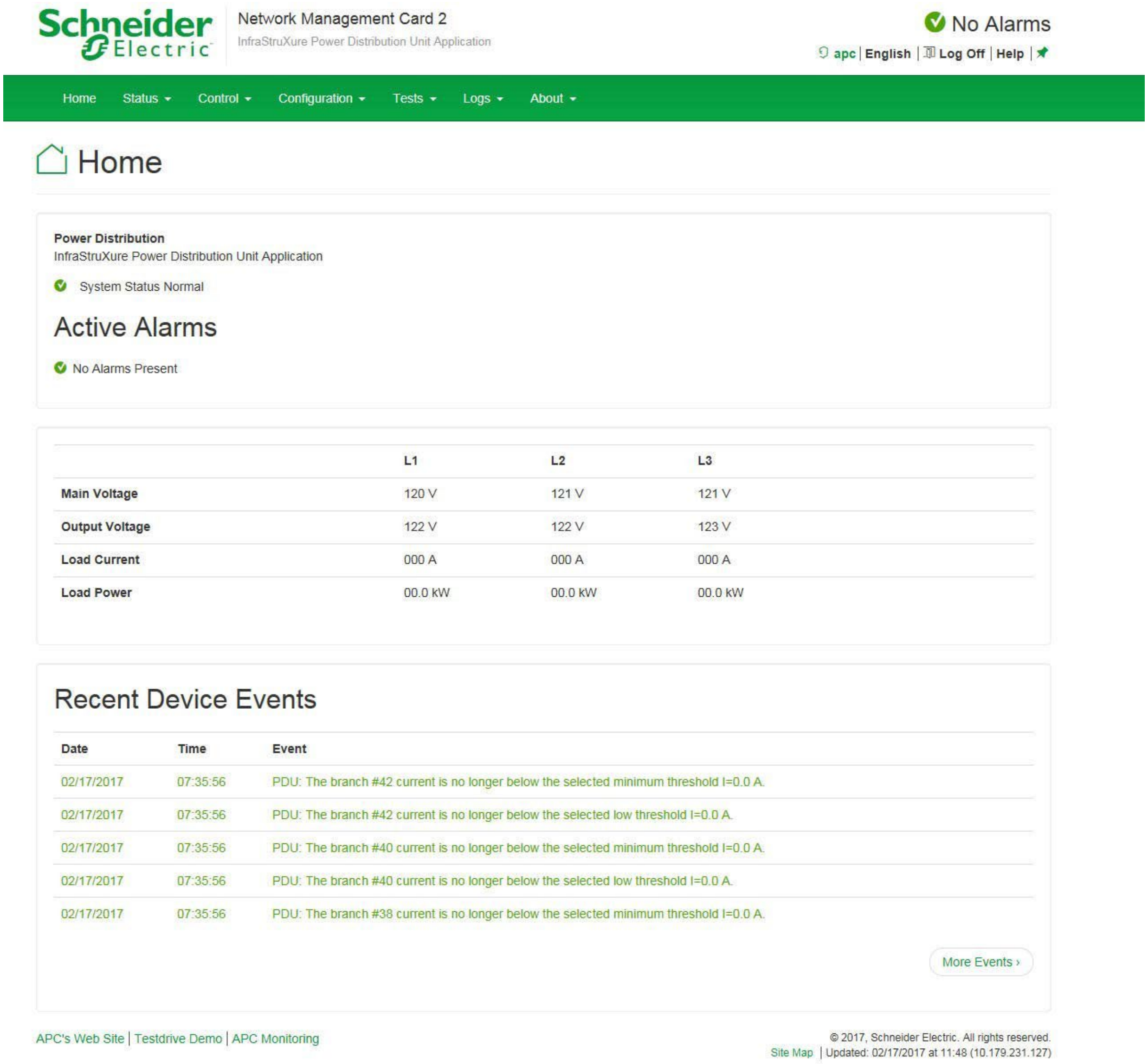
- **Logs:** The **Logs** section covers **NMC Log**, **Data Log**, and **Firewall**. The **NMC Log** and **Data Log** menus cover more information which will be further discussed in the "Logs Tab" on page 89.
- **About:** The **About** tab covers **Power Distribution**, **Network** and **Support**. See "About Tab" on page 94 for more information.

## Device menu tree



# Home Page

The **Home** page contains the following information: Active Alarms, Load information (voltage, current, and power), and Recent Device Events. Active Alarms will show if any alarms exist. If no alarms exist, a green check mark with the words “No Alarms Present” will show. If you want to see more events, select the **More Events** link at the bottom of the list to view the Event Log, which lists the most recent events by Date, Time, User and Event.(See “NMC log/event log” on page 89 for more information.)



Network Management Card 2
InfraStruXure Power Distribution Unit Application

✓ No Alarms

Home

**Power Distribution**
InfraStruXure Power Distribution Unit Application

✓ System Status Normal

Active Alarms

✓ No Alarms Present

| | L1 | L2 | L3 |
|---|---|---|---|
| **Main Voltage** | 120 V | 121 V | 121 V |
| **Output Voltage** | 122 V | 122 V | 123 V |
| **Load Current** | 000 A | 000 A | 000 A |
| **Load Power** | 00.0 kW | 00.0 kW | 00.0 kW |

Recent Device Events

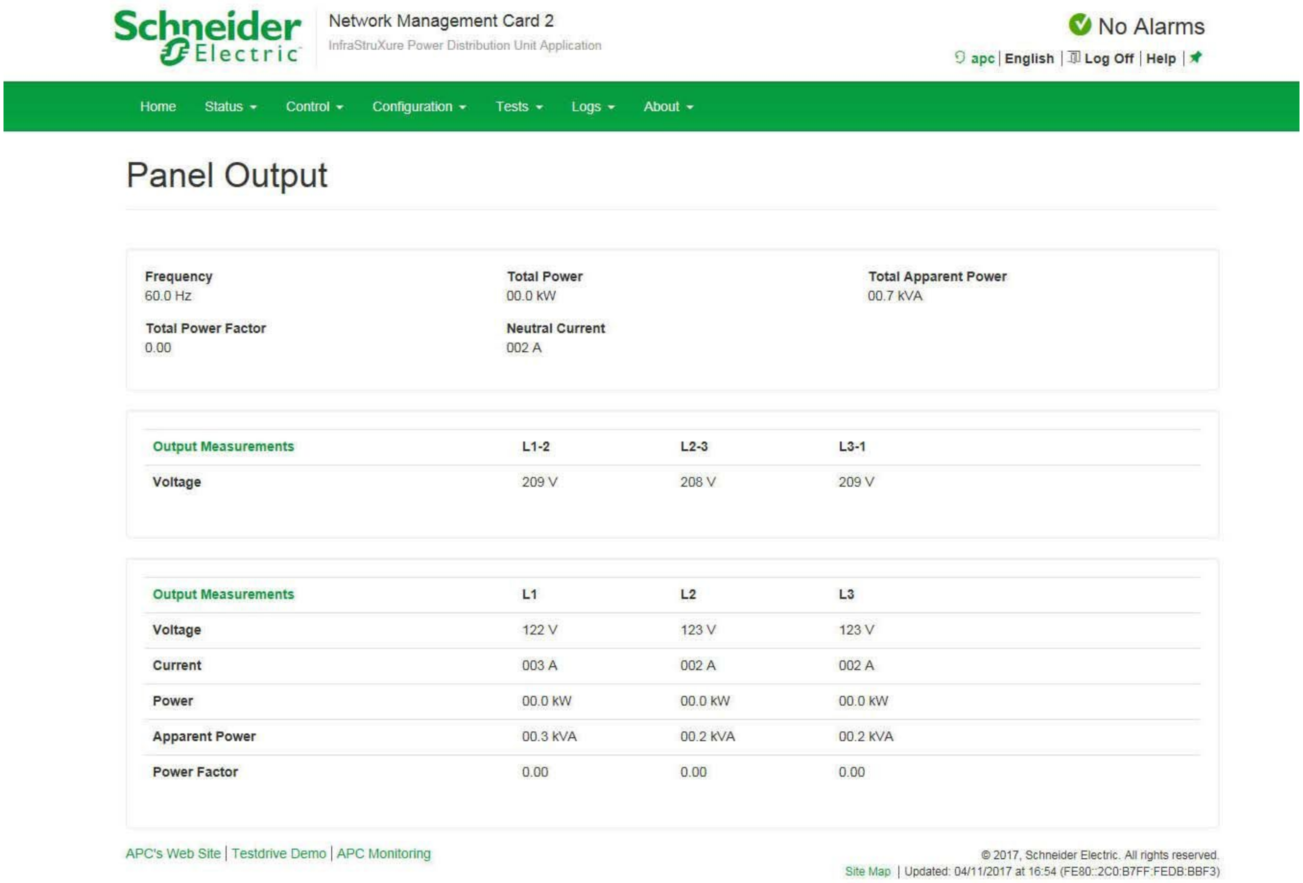
| Date | Time | Event |
|---|---|---|
| 02/17/2017 | 07:35:56 | PDU: The branch #42 current is no longer below the selected minimum threshold I=0.0 A. |
| 02/17/2017 | 07:35:56 | PDU: The branch #42 current is no longer below the selected low threshold I=0.0 A. |
| 02/17/2017 | 07:35:56 | PDU: The branch #40 current is no longer below the selected minimum threshold I=0.0 A. |
| 02/17/2017 | 07:35:56 | PDU: The branch #40 current is no longer below the selected low threshold I=0.0 A. |
| 02/17/2017 | 07:35:56 | PDU: The branch #38 current is no longer below the selected minimum threshold I=0.0 A. |

APC's Web Site | Testdrive Demo | APC Monitoring

© 2017, Schneider Electric. All rights reserved.
Site Map | Updated: 02/17/2017 at 11:48 (10.179.231.127)

# Status Tab

Select **Power Distribution** to view the status of the unit and its breakers. Select **Network** to view the current IPv4, IPv6 settings, Domain Name System Status, and Port Speed


Schneider Electric
Network Management Card 2
InfraStruXure Power Distribution Unit Application
No Alarms
apc | English | Log Off | Help
Home
Status
Control
Configuration
Tests
Logs
About

Panel Output

|  |  |  |
|---|---|---|
| **Frequency**<br>60.0 Hz | **Total Power**<br>00.0 kW | **Total Apparent Power**<br>00.7 KVA |
| **Total Power Factor**<br>0.00 | **Neutral Current**<br>002 A |  |

| Output Measurements | L1-2 | L2-3 | L3-1 |
|---|---|---|---|
| Voltage | 209 V | 208 V | 209 V |

| Output Measurements | L1 | L2 | L3 |
|---|---|---|---|
| Voltage | 122 V | 123 V | 123 V |
| Current | 003 A | 002 A | 002 A |
| Power | 00.0 kW | 00.0 kW | 00.0 kW |
| Apparent Power | 00.3 kVA | 00.2 kVA | 00.2 kVA |
| Power Factor | 0.00 | 0.00 | 0.00 |

APC's Web Site | Testdrive Demo | APC Monitoring

© 2017, Schneider Electric. All rights reserved.

Site Map | Updated: 04/11/2017 at 16:54 (FE80::2C0:B7FF:FEDB:BBF3)

## View power distribution Status

**Path: Status > Power Distribution**

**> Active Alarms:** Lists active device alarms by severity.

**> Main PDU > Panel Output:** If an alarm caused by voltage or current variation exists, a status icon and accompanying text display at the top of the page.

| Measurement | Description |
|---|---|
| Frequency | The frequency, in Hz, of the output |
| Total Power | The active power, in kW, provided for the total of three phases |
| Total Apparent Power | The apparent power, in kVA, provided for the total of three phases. |
| Total Power Factor | The ratio between active power and apparent power (kW/kVA) for all three phases. This ratio affects the power available to the load |
| Neutral Current | The load supported by the neutral line, in A |
| **Output Measurements** | |
| Voltage | The phase-to-phase output voltage (e.g., L1-2 for phase L1 to phase L2) and the phase-to-neutral output voltage (e.g., L1 for phase 1 to neutral) |
| Current | The load, in A, supported by each phase |
| Power | The active power, in kW, provided for each phase |
| Apparent Power | The apparent power, in kVA, provided for each phase |
| Power Factor | The ratio between active power and apparent power (kW/kVA) for each phase. This ratio affects the power available to the load |

**> Main PDU > Main Input:** Shows **Main Voltage**, the phase-to-phase input voltage (e.g., L1-2 for phase L1 to phase L2) for a 3-wire connection, or the phase-to-neutral voltage (e.g., L1 for phase 1 to neutral) for a 4-wire connection. If an alarm caused by voltage or current variation exists, a status icon and accompanying text display at the top of the page.

**> Main PDU > Input Breakers**

| Setting | Description |
|---|---|
| Main Input Breaker | When the PDU is operating normally, this breaker is closed. |
| Bypass Breaker | When the PDU is operating normally, this breaker is closed. The Bypass Input Switch is available on select PDU models only, and it provides a connection for a second power source |
| Cross Tie Breaker | When the PDU is operating normally, this breaker is closed. The output of this breaker feeds the Bypass Input Switch of another PDU. This feature is available on select PDU models only. |

**> Main PDU > Bypass Status (type B PDU)**

| Setting | Description |
|---|---|
| UPS Input Breaker (Q1) | When the PDU is operating normally, this breaker is closed. During Maintenance Bypass Operation, this breaker is open |
| UPS Output Breaker (Q2) | When the PDU is operating normally, this breaker is closed. During Maintenance Bypass Operation, this breaker is open |
| Maintenance Bypass (Q3) | When the PDU is operating normally, this breaker is open. During Maintenance Bypass Operation, this breaker is closed |

### > Main PDU > Main Output (type C PDU)

| Setting | Description |
|---|---|
| Main output breaker | When the PDU is operating normally, this breaker is closed. During Maintenance Bypass Operation, this breaker is open |

## View network status

### Path: Status > Network

### > Network

| Setting | Description |
|---|---|
| **Current IPv4 Settings** | |
| System IP | The IP address of the unit |
| Subnet Mask | The IP address of the sub-network |
| Default Gateway | The IP address of the router used to connect to the network |
| MAC Address | The Media Access Control address of the unit |
| Mode | How the IPv4 settings are assigned: **Manual**, **DHCP**, or **BOOTP** |
| DHCP Server* | The IP address of the DHCP server. |
| Lease Acquired* | The date/time that the IP address was accepted from the DHCP server. |
| Lease Expires* | The date/time the IP address from the DHCP server expires and will need to be renewed. |
| **Current IPv6 Settings** | |
| Type | How the IPv6 settings are assigned |
| IP Address | The IP address of the unit |
| Prefix Length | The range of addresses for the sub-network |
| **Domain Name System Status** | |
| Active Primary DNS Server | The IP address of the primary DNS server |
| Active Secondary DNS Server | The IP address of the secondary DNS server |
| Active Host Name | The host name of the active DNS server |
| Active Domain Name (IPv4/IPv6) | The IPv4/IPv6 domain name that is currently in use |
| Active Domain Name (IPv6) | The IPv6 domain name that is currently in use |
| **Port Speed** | |
| Current Speed | The current speed assigned to the Ethernet port |

*These fields are only displayed if the **Mode** is **DHCP**.

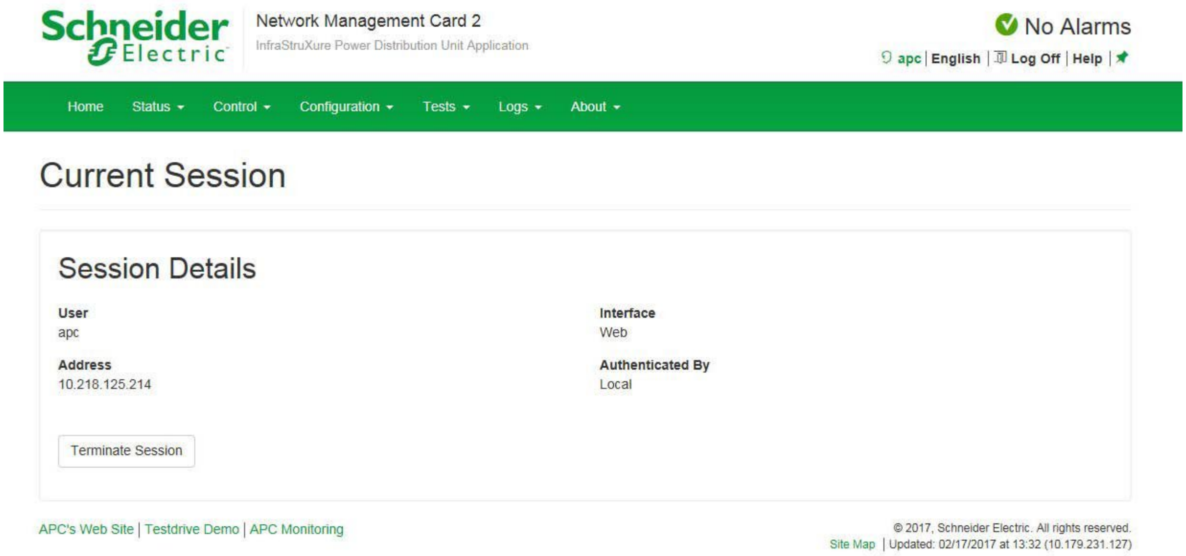
# Control Tab

The **Control** tab options enable you manage active users and the security of your network.

## Manage user sessions

### Path: Control > Security

**> Session Management:** The **Session Management** menu displays all users currently connected to the unit. Select a user name to open the **Session Details** screen, which displays basic information about the user including the user name, the interface they are logged into, their IP address, and their authentication type. To end a user's session, click the **Terminate Session** button.


Schneider Electric
Network Management Card 2
InfraStruXure Power Distribution Unit Application
No Alarms
apc | English | Log Off | Help |
Home
Status
Control
Configuration
Tests
Logs
About
Terminate Session
APC's Web Site | Testdrive Demo | APC Monitoring
Site Map

Current Session

Session Details

User
apc

Interface
Web

Address
10.218.125.214

Authenticated By
Local

© 2017, Schneider Electric. All rights reserved.
Updated: 02/17/2017 at 13:32 (10.179.231.127)

## Reset the network interface

### Path: Control > Network

**> Reset/Reboot:** This menu gives you the option to reset and reboot various components of the network interface.

| Setting | Description |
|---|---|
| Reboot Management Interface | Restart the PDU's network interface, but not the PDU. This function does not affect the ON/OFF status of the PDU. |
| Reset All | Clear the **Exclude TCP/IP** check box to reset all configuration values; select the **Exclude TCP/IP** check box to reset all values except TCP/IP. |
| Reset Only | Resetting may take up to a minute. Options include<br>• **TCP/IP settings:** Set TCP/IP Configuration to **DHCP**, its default setting, which requires the InfraStruxure PDU to receive its TCP/IP settings from a DHCP or BOOTP server. See "View the result of the test DNS in the Last Query Response field."<br>• **Event configuration:** Reset all changes to event configuration, by event and by group, to their default settings. |

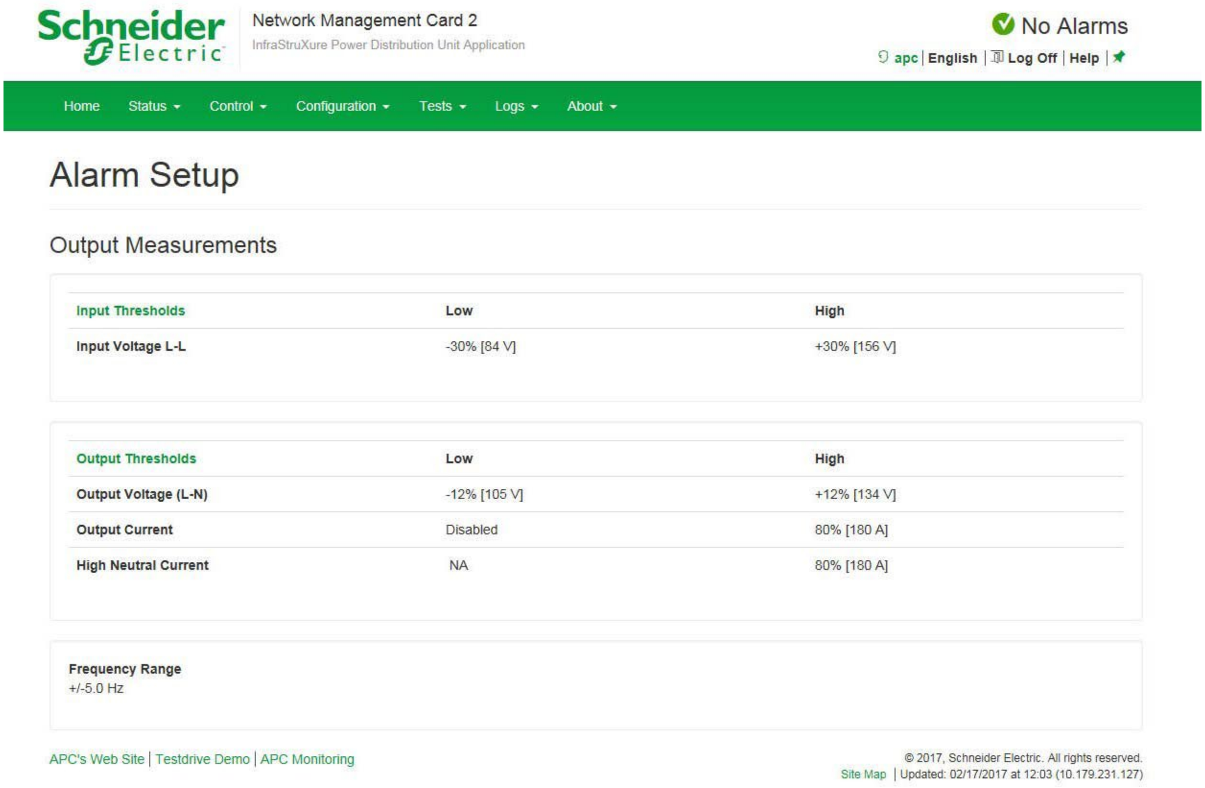
Click **Apply** to save your changes or **Cancel** to leave without saving.

# Configuration Tab

Use the Configuration tab to change PDU settings.

## Configure alarm thresholds

### Path: Configuration > Power Distribution > Main PDU> Alarm Setup



Network Management Card 2
InfraStruXure Power Distribution Unit Application
No Alarms
apc | English | Log Off | Help |
Home
Status
Control
Configuration
Tests
Logs
About

Alarm Setup

Output Measurements

| Input Thresholds | Low | High |
|---|---|---|
| Input Voltage L-L | -30% [84 V] | +30% [156 V] |

| Output Thresholds | Low | High |
|---|---|---|
| Output Voltage (L-N) | -12% [105 V] | +12% [134 V] |
| Output Current | Disabled | 80% [180 A] |
| High Neutral Current | NA | 80% [180 A] |

Frequency Range
+/-5.0 Hz

APC's Web Site | Testdrive Demo | APC Monitoring
© 2017, Schneider Electric. All rights reserved.
Site Map | Updated: 02/17/2017 at 12:03 (10.179.231.127)

For each measurement, a value below the **Low** threshold or above the **High** threshold generates an alarm. Select **Input Thresholds** or **Output Thresholds** to configure alarms**:**

| **Setting** | **Description** |
|---|---|
| **Input Thresholds** | |
| Input Voltage L-L | The acceptable range for the voltage entering the PDU |
| **Output Thresholds** | |
| Output Voltage (L-N) | The acceptable range for the voltage that the PDU provides to the load |
| Output Current | The acceptable range for the output current. The PDU monitors the output current on each phase, and a threshold violation on any phase generates an alarm |
| High Neutral Current | The acceptable range for the current on the output neutral line |
| Frequency Range | The acceptable frequency variation for the output current, in Hertz (Hz). |

## Configure branch circuit breaker settings

**Path: Configuration > Power Distribution**

**> Branch Circuits:** To view branch circuit breaker settings, select a group of circuit breakers (**01..41 [odd]**, **02..42 [even]**, **43..83 [odd]**, or **44..84 [even]**). The following information is displayed for each group:

| **Setting** | **Description** |
|---|---|
| Position | The position of the breaker on the circuit breaker panel. Position numbers correspond to numbers on the physical breaker panel |
| Branch Rating | The rating of the breaker in Amperes (A). For special connections, enter ELCB (for Earth Leakage Circuit Breakers) or NEUT (for Neutral Connections). |
| Status | The state of the breaker.<br>• Normal: The breaker is operating normally.<br>• Warning: The low or high rating threshold has been violated.<br>• Critical: The minimum or maximum rating threshold has been violated. |
| Name | A descriptive name for the breaker |
| Current | The measured current of the breaker in A |
| Location | A user-configured description of the location of the breaker (for example, the physical location of the PDU in which it is installed) |

To edit the branch rating, name, or location of a breaker:

1. Select the **Branch Rating**, **Name**, or **Location** of the breaker. A configuration page opens.
2. Type your changes in the appropriate text fields.
3. Click **Apply** to save, **Delete Group** to delete the breaker group, or **Cancel** to leave the page without saving.

To edit threshold settings for a breaker:

1. Select the **Branch Rating**, **Name**, or **Location** of the breaker group. A configuration page opens.
2. Select **Percent Rating**. A configuration page opens.
3. Select or clear the check box for each threshold to define whether that threshold will generate breaker alarms. Define each threshold as a percentage of the rated current.
4. Click **Apply** to save or **Cancel** to leave the page without saving.

### > Add Breakers

| Setting | Description |
|---|---|
| Panel Position | Type in the breaker's position number. This value is listed on the circuit breaker panel |
| Number of Poles | Select the number of poles in the breaker from the drop-down menu. For a branch breaker, valid values are 1-pole, 2-pole, or 3-pole. Select the value that matches the type of load (1-phase, 2-phase, or 3-phase) that is receiving power. |
| Breaker Rating | Set the rating of this breaker, in A. For special connections, enter ELCB (for Earth Leakage Circuit Breakers) or NEUT (for Neutral Connections). |
| Breaker Identification | Type a descriptive **Name** and **Location** (up to 19 characters each) for the breaker. If you have added a neutral connection or Earth-leakage circuit breaker, you can identify it here. |
| Branch Current Thresholds | Select any **Enable** check box to generate an alarm when the electric current violates the Maximum, High, Low, or Minimum threshold. Clear any check box to disable the associated alarm. Define each threshold as a percentage of the **Breaker Rating** |

Click **Add Branch Breaker** to save or **Cancel** to leave the page without saving.

### > Add Sub-Feed

| Setting | Description |
|---|---|
| Panel Position | Select the three numbers that match the selected panel's sub-feed position. These values are listed on the breaker panel. |
| Number of Poles | For sub-feed breakers, 3-pole is the only valid value |
| Breaker Rating | Set the rating of this breaker in A |
| Breaker Identification | Type a descriptive **Name** and **Location** (up to 19 characters each) for the breaker |
| Branch Current Thresholds | Select the **Enable** check box to generate an alarm when the electric current violates a threshold, or clear the check box to disable alarms. Define each threshold as a percentage of the **Breaker Rating**. |

Click **Add Sub-Feed** to save, or **Cancel** to leave the page without saving.

**> Global Thresholds:** Change threshold settings for all branch circuit breakers

1. Select the check box associated with a threshold to apply this configuration to all of the branch breakers, or clear the check box to disable threshold configuration.
2. Define the **Maximum**, **High**, **Low**, and **Minimum** thresholds as a percentage of the rated current.
3. Click **Apply** to save or **Cancel** to leave the page without saving.

**> Global Delete:** Delete all branch circuit breaker settings

Select the check box for each range of breakers you want to delete. Click **Delete All Checked** to delete the breakers or **Cancel** to undo your changes.

## Configure contacts and relays

### Path: Configuration > Contacts/Relays

**> Input Contacts:** View and configure input contacts

View the name of each input contact, its alarm status (Normal, Warning, or Critical), and its current state (Open or Closed). Up to 4 inputs can be connected to the PDU. Select a contact **Name** to open its configuration page.

| Setting | Description |
|---|---|
| Name | Type a descriptive user name (up to 14 characters). |
| Alarm Status | When the input contact is not in a **Normal State**, an alarm will be generated. |
| State | Shows whether the input contact is open or closed at this moment. |
| Normal State | Select whether the input contact is open or closed when the PDU is operating normally. |

Click **Apply** to save or **Cancel** to leave the page without saving.

**> Output Relays:** View the state (open or closed) of all 4 output relays. To configure an output relay

1. Select an output relay's **Name** to open its configuration page.
2. In the **Name** field, type a descriptive name (up to 14 characters).
3. Under **Normal State**, select **Open** or **Closed**. See "> Alarm Relay Map:" on this page to define alarms that will cause the relay to change from its normal state.
4. Click **Apply** to save or **Cancel** to leave the page without saving.

**> Alarm Relay Map:** Use the alarm relay map to set actions that will cause a relay to change its state. To configure a relay to react to an alarm condition, select the check box that corresponds to the alarm condition and the relay:

| Setting | Description |
|---|---|
| Any Load | Change the relay state when an over-current or under-current alarm is detected for a circuit breaker panel or branch circuit. |
| Overload | Change the relay state when an over-current alarm is detected for a circuit breaker panel, branch circuit, or system ground. |
| Input Voltage | Change the relay state when an input voltage alarm is active. |
| Output Voltage | Change the relay state when an output voltage alarm is active. |
| PDU in Bypass | Change the relay state when the Q3 breaker on the PDU is closed. |
| Any Breaker | Change the relay state when the input, bypass input, or cross-tie output breaker is not in its normal state, or a system state alarm (such as System Off, On Battery Only, Bypass Alarm, No Panel Feed, Bypass Alarm, or Forced Bypass) is active. |
| Contact 1–4 Alarms | Change the relay state when the input is not in its normal state. |

Click **Apply** to save or **Cancel** to leave the page without saving.

## Manage user sessions, ping response, and user accounts

**Path: Configuration > Security**

**> Session Management**

- **Allow Concurrent Logins:** Select **Enable** to let two or more users log on at the same time. Each user has equal access and each interface (HTTP, FTP, telnet console, serial console, etc.) counts as a logged-in user.
- **Remote Authentication Override:** RADIUS storage of passwords on a server is supported. However, if you enable this override, the unit will allow a local user to log on using locally stored password on the unit. For more information on RADIUS, see “Manage remote access to the web interface” on page 68.

**> Ping Response:** Select the **Enable** check box for **IPv4 Ping Response** to allow the unit to respond to network pings. Clear the check box to disable a unit response. This does not apply to IPv6.

**> Local Users > Management:** The Super User or an Administrator can set access permissions for other users. Select a **User Name** to configure individual user settings, or click **Add User** to create a new account.

- **Access:** Select the **Enable** check box to allow access to the web interface.
- **User name:** User names are case sensitive and can be up to 10 characters long.
- **Password, New Password, and Confirm Password:** Passwords are case sensitive and can be up to 32 characters long. Blank passwords are not allowed. To change an Administrator/Super User setting, you must enter all three password fields.

  **NOTE:** Values greater than 64 bytes in **User Name** and **Password** fields may be truncated.

- **User Type:** Levels of access are protected by user name and password requirements. During authentication, the user's credentials are compared against the Local User Database and/or are validated against a RADIUS server (depending on configuration). If valid, access with appropriate permissions is granted.

  **NOTE:** This option is only available on the **Add User** configuration page.

| User Type | Default User Name | Interface Access | Read/Write permission |
|---|---|---|---|
| Administrator | apc | web and command line | Read/write for all menus |
| Device | device | web and command line | Read/write for device-related menus authorized by Super User or Administrator |
| Read-Only | readonly | web only | Read-only for device-related menus authorized by Super User or Administrator |
| Network-Only | n/a | web and command line | Read/write for network menus |

- **User Description:** Type additional identification details in this field.

- **Session Timeout:** Set the time (3 minutes by default) that the PDU waits before logging off an inactive user. If you change this value, you must log off for the change to take effect.

  **NOTE:** This timer continues to run if a user closes the browser window without first logging off by clicking **Log Off** on the upper right of your screen. Because that user is still considered to be logged on, no user can log on until the specified timeout (minutes of inactivity) expires. For example, with the default **Session Timeout** (3 minutes), if a user closes the browser window without logging off, no user can log on for 3 minutes.

- **Serial Remote Authentication Override:** Select the **Enable** check box to allow the user to bypass RADIUS by using the serial console (CLI) connection. This screen enables Serial Remote Authentication Override for the selected user, but it must also be enabled globally to work, (see “Manage user sessions, ping response, and user accounts” on page 65).

**> Local Users > Default Settings:** Determine the default values to populate in each field when the Super User or Administrator-level account creates a new user. These values can be changed before the settings are applied to the system.

- **Access:** Select the **Enable** check box to allow access to the web interface.
- **User Type:** Levels of access are protected by user name and password requirements. During authentication, the user's credentials are compared against the Local User Database and/or are validated against a RADIUS server (depending on configuration). If valid, access with appropriate permissions is granted.

| User Type | Default User Name | Interface Access | Read/Write permission |
|---|---|---|---|
| Administrator | apc | web and command line | Read/write for all menus |
| Device | device | web and command line | Read/write for device-related menus authorized by Super User or Administrator |
| Read-Only | readonly | web only | Read-only for device-related menus authorized by Super User or Administrator |
| Network-Only | n/a | web and command line | Read/write for network-related menus |

- **User Description:** Type the user description in the box.
- **Session Timeout:** Configure the time (3 minutes by default) that the PDU waits before logging off an inactive user.
- **Bad Login Attempts:** Set the number of failed login attempts the user can have (0 to 99 attempts; 0 = unlimited).

### User Preferences

- **Event Log Color Coding:** Select the check box to enable color-coding of alarm text recorded in the event log. System event entries and configuration change entries do not change color.

| Text Color | Alarm Severity |
|---|---|
| Orange | **Critical:** A critical alarm exists, which requires immediate action. |
| Yellow | **Warning:** An alarm condition requires attention and could jeopardize your data or equipment if its cause is not addressed. |
| Green | **Alarm Cleared:** The conditions that caused the alarm have improved. |
| Black | **Normal:** No alarms are present. The PDU and all connected devices are operating normally. |

- **Export Log Format:** Configure which format the event log should be displayed in when exported (downloaded). Tab (default) allows fields to be tab-delimited whereas CSV is comma-separated.
- **Temperature scale:** Select the temperature scale, **US Customary** (Fahrenheit) or **Metric** (Celsius), in which to display all temperature measurements in this user interface.
- **Date Format:** Select the numerical format in which to display all dates in this user interface. Each letter—m (for month), d (for day), and y (for year)—represents one digit. Single-digit days and months are displayed with a leading zero.

### Password Requirements

- **Strong Passwords:** When enabled, new passwords require at least one lowercase character, one uppercase character, one number, and one symbol.
- **Password Policy:** Enter the number of days after which users will be required to change their passwords. A value of 0 days disables this feature.

## Manage remote access to the web interface

**Path: Configuration > Security > Remote Users**

**> Authentication:** Specify how you want remote users to be authenticated at log on. Schneider Electric supports the authentication and authorization functions of RADIUS (Remote Access Dial-In User Service).

- When a user accesses a PDU that has RADIUS enabled, an authentication request is sent to the RADIUS server to determine the user's permission level.
- RADIUS user names used with the PDU are case-sensitive, and have a 64 byte maximum, supporting up to 64 ASCII characters; less for multi-byte languages. Passwords with no characters (blank passwords) are not allowed.

Select one of the following:

| Setting | Description |
|---|---|
| Local Authentication Only | RADIUS is disabled. Local authentication is enabled. For information about local authentication (not using the centralized authentication of a RADIUS server), see the *Security Handbook*, available at **www.apc.com**. |
| RADIUS, then Local Authentication | RADIUS and local authentication are enabled. Authentication is requested from the RADIUS server first. If the RADIUS server fails to respond, local authentication is used. |
| RADIUS Only | RADIUS is enabled. Local authentication is disabled. |
| **NOTE:** If **RADIUS Only** is selected and the RADIUS server is unavailable, improperly identified, or improperly configured, you must use a serial connection to the CLI and change the Access setting to **Local Authentication Only** or **RADIUS, then Local Authentication** to regain access. See "Manage user sessions, ping response, and user accounts" on page 65 to enable users to override RADIUS authentication in the case of an unresponsive server. | |

**> RADIUS:** Specify up to two properly configured RADIUS servers. To add a server, click **Add Server**. To modify an existing server, select the server name.

| Setting | Description |
|---|---|
| RADIUS Server | The name or IP address of the RADIUS server |
| Port | The port (1812 by default) that the RADIUS server listens on<br>**NOTE:** You can change the port setting to any unused port from 5000 to 32768. |
| Secret | The shared secret between the RADIUS server and the InfraStruxure PDU. |
| Reply Timeout | The time (in seconds) the PDU waits for a response from the RADIUS server. |
| Test Settings | Enter the Administrator user name and password to test the RADIUS server path that you have configured. |
| Skip Test and Apply | Do not test the RADIUS server path (not recommended). |
| Switch Server Priority | Change which RADIUS server will authenticate users if two configured servers are listed and **RADIUS, then Local Authentication** or **RADIUS Only** is the enabled authentication method. |

**Summary of the Configuration Procedure:** You must configure your RADIUS server to work with the PDU. For examples of the RADIUS users file with the Vendor Specific Attributes (VSAs) and an example of an entry in the dictionary file on the RADIUS server, see the *Security Handbook* (available online at **www.apc.com**).

1. Add the IP address of the unit to the RADIUS server client list (file).
2. Users must be configured with Service-Type attributes unless Vendor Specific Attributes (VSAs) are defined. If no Service-Type attributes are configured, users will have read-only access (on the web interface only).

   **NOTE:** See your RADIUS server documentation for information about the RADIUS users file.
3. Vendor Specific Attributes (VSAs) can be used instead of the Service-Type attributes provided by the RADIUS server. VSAs require a dictionary entry and a RADIUS users file. In the dictionary file, define the names for the ATTRIBUTE and VALUE keywords, but not for the numeric values. If you change numeric values, RADIUS authentication and authorization will fail. VSAs take precedence over standard RADIUS attributes.

## Configure a RADIUS server on UNIX® with shadow passwords

If UNIX shadow password files are used (/etc/passwd) with the RADIUS dictionary files, the following methods can be used to authenticate users:

– If all UNIX users have administrative privileges, add the following to the RADIUS “user” file. To allow only Device Users, change the Service-type to `Device`.

```
DEFAULTAuth-Type = System
APC-Service-Type = Admin
```

– Add user names and attributes to RADIUS “user” file. Verify passwords against `/etc/passwd`. The following example is for users `bconners` and `thawk`:

```
bconnersAuth-Type = System
APC-Service-Type = Admin
thawkAuth-Type = System
APC-Service-Type = Device
```

## Supported RADIUS servers

FreeRADIUS v1.x and v2.x, and Microsoft Server 2008 and 2012 Network Policy Server (NPS) are supported. Other commonly available RADIUS applications may work, but may not have been fully tested.

## Firewall

### Path: Configuration > Security > Firewall

A configurable network firewall is provided. The firewall can allow or deny network traffic to and from the device, based on user-configured rules that are ordered by priority. A sample firewall policy (.fwl) is provided in the file system for reference. It is available for download via FTP or SCP from the /fwl directory of the file system. In the web interface, you can use the firewall policy editor to create or edit a custom firewall policy.

**NOTE:** The firewall is disabled by default.

**> Configuration:** Enable or disable the overall firewall functionality. Any configured policy is also listed, even if the firewall is disabled.

**> Active Policy:** Select an active policy from the available firewall policies and view policy validity.

**> Active Rules:** When a firewall is enabled, this lists the individual rules that are being enforced by a current active policy. You can add rules, delete rules, or edit existing rules here.

**> Create/Edit Policy:** Create a new policy or edit an existing one. Multiple firewall policies can be stored, but only one policy can be active at once.

**> Load Policy:** Load a policy (with the .fwl suffix) from a source external to this device.

**NOTE:** When a firewall is enabled and a custom policy file is applied, the policy is checked for syntax errors. If an error is found, the policy will not be loaded.

**> Test:** Test and verify a custom firewall policy by specifying a number of minutes to enforce the rules of the chosen policy. It is recommended that a firewall policy is tested before it is applied to a production environment.

## Configure network settings

**Path: Configuration > Network**

**> TCP/IP > IPv4 Settings:** View the current IPv4 address, subnet mask, default gateway, MAC address, and boot mode of the unit. For information on DHCP and BOOTP options, see **RFC2131** and **RFC2132**.

Configure the following IPv4 Settings

| Setting | Description |
|---|---|
| Enable | Select the check box to enable IPv4 |
| Manual | Configure IPv4 manually by entering the IP address, subnet mask, and default gateway. |
| BOOTP | A BOOTP server provides the TCP/IP settings. At 32-second intervals, the unit requests network assignments from any BOOTP server:<br>• If the unit receives a valid response, it starts the network services.<br>• If the unit finds a BOOTP server, but a request to that server fails or times out, the unit stops requesting network settings until it is restarted.<br>• By default, if previously configured network settings exist, and the unit receives no valid response to five requests (the original and four retries), it uses the previously configured settings so that it remains accessible.<br><br>Click **Next>>** to access the BOOTP Configuration page and change the number of retries allowed or the action to take if all retries fail:<br>• **Maximum retries:** Enter the number of retries that will occur when no valid response is received, or zero (0) for an unlimited number of retries.<br>• **If retries fail:** Select **Use prior settings** (the default) or **Stop BOOTP request**.<br><br>**NOTE:** The default values for these three settings on the configuration pages generally do not need to be changed:<br>• **Vendor Class:** APC<br>• **Client ID:** The MAC address of the NMC, which uniquely identifies it on the local area network (LAN)<br>• **User Class:** The name of the application firmware module |
| DHCP | The default setting. At 32-second intervals, the PDU requests network assignments from any DHCP server.<br>• If the PDU receives a valid response, it does not (as previously) require the APC cookie from the DHCP server in order to accept the lease and start the network services.<br>• If the PDU finds a DHCP server, but the request to that server fails or times out, it stops requesting network settings until it is restarted.<br>• **Require vendor specific cookie to accept DHCP Address:** Select this check box to require the DHCP server to provide a cookie, which supplies information to the InfraStruxure PDU. |

### DHCP response options

Each valid DHCP response contains options that provide the TCP/IP settings the unit needs to operate on a network, and other information that affects the operation of the unit.

**Vendor Specific Information (option 43):** The unit uses this option in a DHCP response to determine whether the DHCP response is valid. This option contains an APC-specific option in a TAG/LEN/DATA format, called the APC Cookie. This is disabled by default.

- APC Cookie. Tag 1, Len 4, Data “1APC”

Option 43 communicates to the InfraStruxure PDU that a DHCP server is configured to service devices. Following, in hexadecimal format, is an example of a Vendor Specific Information option that contains the APC cookie:

- Option 43 = `0x01 0x04 0x31 0x41 0x50 0x43`

**TCP/IP options:** The unit uses the following options within a valid DHCP response to define its TCP/IP settings. All of these options except the first are described in **RFC2132**.

| **Option** | **Description** |
|---|---|
| IP Address | From the **yiaddr** field of the DHCP response, described in RFC213: The IP address that the DHCP server is leasing to the unit |
| Subnet Mask (option 1) | The Subnet Mask value that the unit needs to operate on the network |
| Router, i.e., Default Gateway (option 3) | The default gateway address that the unit needs to operate on the network |
| IP Address Lease Time (option 51) | The time duration for the lease of the IP Address to the unit |
| Renewal Time, T1 (option 58) | The time that the unit must wait after an IP address lease is assigned before it can request a renewal of that lease |
| Rebinding Time, T2 (option 59) | The time that the unit must wait after an IP address lease is assigned before it can seek to rebind that lease |

**Other options:** The unit also uses these options within a valid DHCP response. All of these options, except **Boot File Name**, are described in **RFC2132**.

| **Option** | **Description** |
|---|---|
| Network Time Protocol Servers (option 42) | Up to two NTP servers (primary and secondary) the unit can use |
| Time Offset (option 2) | The offset of the unit subnet, in seconds, from Coordinated Universal Time (UTC) |
| Domain Name Server (option 6) | Up to two Domain Name System (DNS) servers (primary and secondary) the unit can use |
| Host Name (option 12) | The host name the unit will use (32-character maximum length) |
| Domain Name (option 15) | The domain name the unit will use (64-character maximum length) |
| Boot File Name | From the **file** field of the DHCP response, described in **RFC2131**: The fully qualified directory-path to a user configuration file (.ini file) to download. The **siaddr** field of the DHCP response specifies the IP address of the server from which the InfraStruxure PDU will download the .ini file. After the download, the .ini file is used as a boot file to reconfigure the settings. |

**> TCP/IP > IPv6 settings:** Configure the following IPv6 settings:

| Setting | Description |
|---|---|
| IPv6 | Enable or disable IPv6 with this check box. |
| Manual Configuration | Select the **Enable** check box, then enter the IP address and default gateway. |
| Auto Configuration | When the **Auto Configuration** check box is selected, the system obtains addressing prefixes from the router (if available). It uses those prefixes to automatically configure IPv6 addresses. |
| DHCPv6 Mode | **Router Controlled:** Selecting this option means that DHCPv6 is controlled by the Managed (M) and Other (O) flags received in IPv6 router advertisements (as opposed to being controlled by the user). When a router advertisement is received, the NMC checks whether the M or the O flag is set. The NMC interprets the state of the M (Managed Address Configuration Flag) and O (Other Stateful Configuration Flag) "bits" for the following cases:<br>• *Neither is set*: Indicates the local network has no DHCPv6 infrastructure. The NMC uses router advertisements and manual configuration to get addresses that are not link-local and other settings.<br>• *M, or M and O are set*: In this situation, full DHCPv6 address configuration occurs. DHCPv6 is used to obtain addresses AND other configuration settings. This is known as `DHCPv6 stateful`. Once the M flag has been received, the DHCPv6 address configuration stays in effect until the interface in question has been closed. This is true even if subsequent router advertisement packets are received in which the M flag is not set.<br>If an O flag is received first, then an M flag is received subsequently, the NMC performs full address configuration upon receipt of the M flag<br>• *Only O is set*: In this situation, the NMC sends a DHCPv6 Info-Request packet. DHCPv6 will be used to configure “other” settings (such as location of DNS servers), but NOT to provide addresses. This is known as `DHCPv6 stateless`.<br>**Address and Other Information:** With this selected, DHCPv6 is used to obtain addresses AND other configuration settings. This is known as `DHCPv6 stateful`.<br>**Non-Address Information Only:** With this selected, DHCPv6 will be used to configure "Other" settings (such as location of DNS servers), but NOT to provide addresses. This is known as `DHCPv6 stateless`.<br>**Never:** Select **Never** to disable DHCPv6. |

**> Port Speed:** Define the communication speed of the TCP/IP port.

- For **Auto-negotiation** (the default), Ethernet devices negotiate to transmit at the highest possible speed. If the supported speeds of two devices are unmatched, the slower speed is used.
- Choose 10 Mbps or 100 Mbps, with the option of half-duplex (communication in only one direction at a time) or full-duplex (communication in both directions simultaneously).

**> DNS > Configuration:** Use these options to manually configure DNS settings:

| Setting | Description |
|---|---|
| Override Manual DNS Settings | Select this option to make configuration data from other sources (typically DHCP) take precedence over manual configurations. |
| Primary DNS Server or Secondary DNS Server | Type the IPv4 or IPv6 addresses of the primary and optional secondary DNS server in these fields. For the InfraStruxure PDU to send e-mail, you must at least define the IP address of the primary DNS server.<br>• The system waits up to 15 seconds for a response from the primary DNS server or secondary DNS server (if specified). If the InfraStruxure PDU does not receive a response within that time, e-mail cannot be sent. Use DNS servers on the same segment as the InfraStruxure PDU or on a nearby segment (but not across a wide-area network [WAN]).<br>• To look up the IP address for that computer and verify correct operation, define the IP addresses of the DNS servers, then enter the DNS name of a computer on your network. |
| System Name Synchronization | Allow the system name to be synchronized with the host name so both fields automatically contain the same value. Select **System Name** to open the Identification page (See "General Options" on page 85).<br>**NOTE:** When enabling this feature, the system name identifier can no longer contain a space character (since it will be synchronized to the host name field).<br>• **Host Name:** Enter a host name here. When you have configured both a host name and a domain name (in either **Domain Name** field), users can enter a host name in any field in the interface (except e-mail address fields) that accepts a domain name.<br>**NOTE:** To override the expansion of a specific host name entry, include a trailing period. The NMC recognizes a host name with a trailing period (such as *mySnmpServer.*) as if it were a fully-qualified domain name and does not append the domain name.<br>• **Domain Name (IPv4/IPv6)** or **Domain Name IPv6:** Configure the domain name in one of these fields. In all other fields in the interface (except e-mail address fields) that accept domain names, the unit adds this domain name when only a host name is entered.<br>To override every instance where a host name is appended to the domain name, set the domain name field to its default, `example.com`, or to `0.0.0.0`. |

Click **Apply** to save your changes or **Cancel** to leave the page without saving.

**> DNS > Test:** Use this option to send a DNS query that tests the setup of your DNS servers by looking up the IP address. View the result of a test in the **Last Query Response** field.

| Setting | Description |
|---|---|
| Query Type | Select the method to use for the DNS query:<br>• **by Host:** the URL name of the server<br>• **by FQDN:** the fully qualified domain name<br>• **by IP:** the IP address of the server<br>• **by MX:** the Mail Exchange used by the server |
| Query Question | Identify the value to be used for the selected query type:<br>• **by Host:** the URL<br>• **by FQDN:** The fully qualified domain name, *`my_server.my_domain`*<br>• **by IP:** the IP address<br>• **by MX:** the Mail Exchange address |

Click **Apply** to send a query or **Cancel** to leave the page without sending a query.

### > Web > Access

Use the following options to configure access to the web interface:

| Setting | Description |
|---|---|
| Enable HTTP | Enable Hypertext Transfer Protocol (HTTP), which provides web access by user name and password, but does not encrypt user names, passwords, and data during transmission. |
| Enable HTTPS | Enable Hypertext Transfer Protocol (HTTP) over Secure Sockets Layer (SSL)/Transport Layer Security (TLS). SSL/TLS encrypts user names, passwords, and data during transmission, and authenticates the InfraStruxure PDU by digital certificate. When HTTPS is enabled, your browser displays a small lock icon. (See “Creating and Installing Digital Certificates” in the *Security Handbook*, available at **www.apc.com**.) |
| HTTP Port | The TCP/IP port (80 by default) used by HTTP to communicate with the unit. |
| HTTPS Port | The TCP/IP port (443 by default) used by HTTPS to communicate with the unit.<br>For either port, you can change the port setting to any unused port from 5000 to 32768 for additional security. Users must then use a colon (:) in the address field of the browser to specify the port number. For example, for a port number of 5000 and an IP address of 152.214.12.114:<br>`http://152.214.12.114:5000`<br>`https://152.214.12.114:5000` |
| Minimum Protocol | The minimum HTTPS protocol to use. Select SSL 3.0, TLS 1.0, TLS 1.1 or TLS 1.2. |
| Require Authentication Cookie | Select the check box to enable this feature. |
| Limited Status Access | Select **Enable** to display a read-only, public web page with basic device status. Select **Use as default page** to show this page when a user accesses the device with just the IP/hostname (before logon). |

Click **Apply** to save your changes or **Cancel** to leave without saving.

**> Web > SSL Certificate:** Add, replace, or remove a security certificate.

| Setting | Description |
|---|---|
| Status | View the SSL certificate status<br>• **Not installed:** A certificate is not installed, or was installed by FTP or SCP to an incorrect location. Using **Add or Replace Certificate File** installs the certificate to the correct location, **/ssl** on the unit.<br>**NOTE:** If you install an invalid certificate, or if no certificate is loaded when you enable SSL, the unit generates a default certificate, which delays access to the interface for up to one minute. You can use the default certificate for basic encryption-based security, but a security alert message displays whenever you log on.<br>• **Generating:** The unit is generating a certificate because no valid certificate was found.<br>• **Loading:** A certificate is being activated on the unit.<br>• **Valid certificate:** A valid certificate was installed or was generated by the unit. Select this link to view the contents of the certificate. (See the *Security Handbook* on **www.apc.com** for more information about SSL Certificates.) |
| Add or Replace Certificate File | Enter or browse to the certificate file created with the Security Wizard.See “Creating and Installing Digital Certificates” in the *Security Handbook,* available at **www.apc.com***,* to choose a method for using digital certificates created by the Security Wizard or generated by the unit. |
| Remove | Delete the current certificate |

Click **Apply** to save your changes or **Cancel** to leave without saving.

**> Console > Access:** Configure access to the CLI:

| Setting | Description |
|---|---|
| Telnet | Select the check box to enable telnet or clear the check box to disable it. Telnet transmits user names, passwords, and data without encryption. |
| SSH | Select the check box to enable SSH or clear the check box to disable it. SSH transmits user names, passwords, and data in encrypted form, providing protection from attempts to intercept, forge, or alter data during transmission. |
| Telnet Port | The Telnet port used to communicate with the unit (23 by default). You can change the port setting to any unused port from 5000 to 32768 for additional security. Users must then use a colon (:) or a space, as required by your Telnet client program, to specify the non-default port. For example, for port 5000 and an IP address of 152.214.12.114, your Telnet client requires one of the these commands:<br>`telnet 152.214.12.114:5000`<br>`telnet 152.214.12.114 5000` |
| SSH Port | The SSH port used to communicate with the unit (22 by default). You can change the port setting to any unused port from 5000 to 32768 for additional security. See the documentation for your SSH client for the command line format required to specify a non-default port. |

Click **Apply** to save your changes or **Cancel** to leave without saving.

**> Console > SSH Host Key:** View the status of an installed SSH host key. Add, replace, or remove a host key:

| Setting | Description |
|---|---|
| Status | Indicates whether the current SSH host key is valid.<br>• **SSH Disabled: No host key in use:** When disabled, SSH cannot use a host key.<br>• **Generating:** The InfraStruxure PDU is creating a host key because no valid host key was found.<br>• **Loading:** A host key is being activated on the InfraStruxure PDU.<br>• **Valid:** A 2048-bit host key generated by the NMC. (See the *Security Handbook* on **www.apc.com** for more information on SSH host keys.) |
| Add or Replace | To use a host key you created with the Security Wizard, load the host key before you enable SSH. Browse to or enter the path name of the host key file created with the Security Wizard, and click **Apply.**<br>If the host key has been removed, or if no host key was loaded, and you enable SSH, the device restarts and generates a host key. Allowing the device to generate its own host key could make the SSH server unavailable for use for up to1 minute. |
| Host Key Fingerprint | A fingerprint helps authenticate a server. If the Security Wizard is used to generate the host key, it also generates the fingerprint, which is displayed here when SSH is enabled and the host key is in use. When you first connect to the device using SSH, compare the fingerprint presented by the SSH client to the fingerprint that the Security Wizard generated to ensure that they match. (Almost all SSH clients display the fingerprint.) |
| Remove | Remove the current host key. |

Click **Apply** to save your changes or **Cancel** to leave without saving.

**NOTE:** To use SSH, you must have an SSH client installed. Most Linux and other UNIX platforms include an SSH client, but Microsoft Windows operating systems do not. Clients are available from various vendors.

## SNMP

All user names, passwords, and community names for SNMP are transferred over the network as plain text. If your network requires the high security of encryption, disable SNMPv1 and enable SNMPv3 instead.

When using StruxureWare to manage a unit on the public network, you must have the same version of SNMP enabled in the interface and in StruxureWare Data Center Expert. Read access will allow StruxureWare to receive traps from the InfraStruxure PDU, but Write access is required while you use the interface to set StruxureWare as a trap receiver.

For detailed information on enhancing and managing the security of your system, see the *Security Handbook*, available at **www.apc.com.**

## SNMPv1

### Path: Configuration > Network > SNMPv1

**> Access:** Select **Enable SNMPv1 Access** to enable SNMP version 1 as a method of communication with this device.

**> Access Control:** Configure up to four access control entries to specify which NMSs have access to this device. The access control opening page, by default, assigns one entry to each of the four SNMPv1 communities. If you leave a default entry unchanged, that community will have access from anywhere on the network. You can also edit the access control settings to apply more than one entry to any community to grant access by several specific IP addresses, host names, or IP address masks.

**NOTE:** Multiple access control entries for one community name means one or more of the other communities will have no access control entry. If no access control entry is listed, that community has no access to the device.

To edit a community's access control settings, select the **Community Name** and use the following options:

| Setting | Description |
|---|---|
| Community Name | The name that a NMS uses to access the community. The maximum length is 15 ASCII characters. The default names are `public`, `private`, `public2`, and `private2`. |
| NMS IP/Host Name | The IP address, IP address mask, or host name that controls access by NMSs. A host name or a specific IP address allows access only by the NMS at that location. IP addresses that contain 255 restrict access as follows:<br>• 149.225.12.**255**: Access only by an NMS on the 149.225.12 segment.<br>• 149.225.**255.255**: Access only by an NMS on the 149.225 segment.<br>• 149.**255.255.255**: Access only by an NMS on the 149 segment.<br>• 0.0.0.0 (default) can also be expressed as 255.255.255.255: Access by any NMS on any segment. |
| Access Type | The actions an NMS can perform through the community.<br>• **Read:** GETs only, at any time.<br>• **Write:** GETs at any time, and SETs when no user is logged onto the web interface.<br>• **Write+:** GETs and SETs at any time.<br>• **Disabled:** No GETs or SETs at any time. |

## SNMPv3

### Path: Configuration > Network > SNMPv3

For SNMP GETs, SETs, and trap receivers, SNMPv3 uses a system of user profiles to identify users. An SNMPv3 user must have a user profile assigned in the MIB software program to perform GETs and SETs, browse the MIB, and receive traps.

You must have a MIB program that supports SNMPv3. The NMC supports only MD5 authentication and DES encryption.

**> Access:** Select **SNMPv3 Access** to enable SNMPv3 as a method of communication with this device.

**> User Profiles:** By default, this page lists the settings of four user profiles, configured with the user names **apc snmp profile1** through **apc snmp profile4**, no authentication, and no privacy (no encryption). To edit the following settings for a user profile, select a **User Name** in the list.

| **Setting** | **Description** |
|---|---|
| User Name | The identifier of the user profile. SNMP version 3 maps GETs, SETs, and traps to a user profile by matching the user name of the profile to the user name in the data packet being transmitted. A user name can have up to 32 ASCII characters. |
| Authentication Passphrase | A phrase of 15 to 32 ASCII characters (`hidden auth. phrase`, by default) that verifies that the NMS communicating with this device through SNMPv3 is the NMS it claims to be, that the message has not been changed during transmission, and that the message was communicated in a timely manner, indicating that it was neither delayed nor copied and sent again later at an inappropriate time. |
| Privacy Passphrase | A phrase of 15 to 32 ASCII characters `(hidden crypt. phrase`, by default) that ensures the privacy of the data (by means of encryption) an NMS is sending to this device or receiving from this device through SNMPv3. |
| Authentication Protocol | Supports SHA or MD5 authentication. Authentication will not occur unless SHA or MD5 is selected as the authentication protocol. |
| Privacy Protocol | Supports AES or DES as the protocol for encrypting and decrypting data. Privacy of transmitted data requires that AES or DES is selected. |

**> Access Control:** Configure up to four access control entries to specify which NMSs have access to this device. The access control opening page, by default, assigns one entry to each of the four user profiles. If you leave a default entry unchanged, all NMSs using that profile will have access to this device. You can also edit the access control settings to apply more than one entry to any user profile to grant access by several specific IP addresses, host names, or IP address masks.

**NOTE:** If there are multiple access control entries for one user profile, one or more of the other user profiles will have no access control entry. If no access control entry is listed, NMSs using that profile have no access to the device.

To edit the access control settings for a user profile, select its **User Name**:

| **Setting** | **Description** |
|---|---|
| Access | Select the **Enable** check box to activate access control. |
| User Name | Select the user profile to which access control will apply. The choices are the four user names configured in the **User Profiles** page (see "> User Profiles:" on page 79). |
| NMS IP/Host Name | The IP address, IP address mask, or host name that controls access by the NMS. A host name or a specific IP address allows access only by the NMS at that location. An IP address mask that contains 255 restricts access as follows:<br>• 149.225.12.**255**: Access only by an NMS on the 149.225.12 segment.<br>• 149.225.**255.255**: Access only by an NMS on the 149.225 segment.<br>• 149.**255.255.255**: Access only by an NMS on the 149 segment.<br>• 0.0.0.0 (the default) or 255.255.255.255: Access by any NMS on any segment. |

## FTP server configuration

### Path: Configuration > Network > FTP Server

The **FTP Server** settings enable or disable access to the FTP server and specify the TCP/IP port (21 by default) that the FTP server uses to communicate with the unit. The FTP server uses both the specified port and the port one number lower than the specified port.

You can change the **Port** setting to the number of any unused port from 5001 to 32768 for added security. Users must then use a colon (:) to specify the non-default port number. For example, for port 5001 and IP address 152.214.12.114, the command would be `ftp 152.214.12.114:5001`.

**NOTE:** FTP transfers files without encryption. For higher security, disable the FTP server, and transfer files with SCP. Selecting and configuring Secure SHell (SSH) enables SCP automatically.

**NOTE:** To configure and update the PDU with StruxureWare, you must enable the same protocol (FTP or SCP) on both the PDU and StruxureWare Data Center Expert.

For detailed information on enhancing and managing the security of your system, see the *Security Handbook*, available at **www.apc.com**.

## Configure notifications

### Path: Configuration > Notification > Event Actions

**Types of notification:** You can configure event actions to occur in response to an event or group of events. These actions notify users of the event in any of several ways:

- Automatic notification. Specified users or monitoring devices are contacted directly.
  - E-mail notification
  - SNMP traps
  - Remote Monitoring Service
  - Syslog notification
- Indirect notification
  - **Event log:** If no direct notification is configured, users must check the log to determine which events have occurred.
  - You can also log system performance data to use for device monitoring. See “Configure Syslog servers, settings, and tests” on page 87 for information on how to configure and use this data logging option.
  - **Queries (SNMP GETs):** SNMP enables an NMS to perform informational queries. For SNMPv1, which does not encrypt data before transmission, configuring the most restrictive SNMP access (READ) enables informational queries without the risk of allowing remote configuration changes. (See “SNMP” on page 77.)

**> By Event:** To define event actions for an individual event:

- Find an event: select a column heading to see the lists under the **InfrastruXure Power Distribution** or **System Events** categories. You can also select a sub-category under these headings, such as **Security** or **Temperature**.
- Possible events for the selected category are listed by severity. Select the event name to view or change the current configuration:
  - **Event Log:** Select the check box for events to appear in the Event Log. (See “NMC log/event log” on page 89.)
  - **Syslog:** Select a Syslog server to log events and send alerts.

- **E-mail:** Select users to be notified by e-mail.
- **Traps:** Configure Network Management Systems (NMSs) as recipients to be notified by SNMP traps.

**NOTE:** If no Syslog server is configured, items related to Syslog configuration are not displayed.

**NOTE:** When viewing details of an event configuration, you can enable or disable event logging or Syslog, or disable notification for specific e-mail recipients or trap receivers, but **you cannot add or remove recipients or receivers. To add or remove recipients or receivers, see the following:**

- “Configure Syslog servers, settings, and tests” on page 87
- “> Recipients:” on page 82
- “Path: Configuration > Notification > SNMP Traps” on page 84

**> By Group:** To configure a group of events simultaneously:

1. Select how to group events for configuration:
   - Select **Events by Severity**, and then select one or more severity levels. You cannot change the severity of an event.
   - Select **Events by Category**, and then select events in one or more pre-defined categories.
2. Click **Next** to select an event action. To select any action except **Logging** (the default), you must first have at least one relevant recipient or receiver configured.
3. Click **Next** to do one of the following:
   - If you selected **Logging** on the previous screen and *have not* configured a Syslog server, select the **Configure Event Log** check box.
   - If you selected **Logging** on the previous screen and *have* configured a Syslog server, select **Event Log** or **Syslog**. To configure a Syslog server, see “Configure Syslog servers, settings, and tests” on page 87.
   - If you selected **E-mail Recipients** on the previous screen, select the e-mail recipients to configure.
   - If you selected **Trap Receivers** on the previous screen, select the trap receiver to configure.
4. Click **Next** to configure notification parameters. These configuration fields define e-mail parameters for sending notifications of events:
   - If you are configuring **Logging** settings, select **Enable Notification** or **Disable Notification**.
   - If you are configuring **E-mail Recipients** or **Trap Receivers,** select **Enable Notification** or **Disable Notification** and set the notification timing settings (see “Configure notifications” on page 80 for more information on these settings).
5. Click **Next** to move to the next screen, and do one of the following:
   - View the pending actions and click **Apply** to accept the changes.
   - Click **Cancel** to revert to the previous settings.

## Configure e-mail notifications

### Path: Configuration > Notification > E-mail

Use Simple Mail Transfer Protocol (SMTP) to send e-mail to a maximum of four recipients when an event occurs. To use the e-mail feature, you must define the following settings:

- The IP addresses of the primary and, optionally, the secondary Domain Name System (DNS) servers. (See “> DNS > Configuration:” on page 74.)
- The From Address and IP address or DNS name for the SMTP Server.
- A maximum of four recipient e-mail addresses.

You can use the **To Address** setting of the **Recipients** option to send e-mail to a text-based screen.

**> Server:** View and configure the following fields:

| Setting | Description |
|---|---|
| Active Primary and Secondary DNS Server | Select either server to go to its configuration page (see “> DNS > Configuration:” on page 74). |
| From Address | The contents of the From field in e-mail messages sent by the unit:<br>• Use the format user@ [IP_address] (if an IP address is specified as Local SMTP Server).<br>• Use the format user@domain (if DNS is configured and the DNS name is specified as Local SMTP Server) in the e-mail messages.<br>**NOTE:** The local SMTP server may require that you use a valid user account on the server for this setting. See the server documentation. |
| SMTP Server | The IPv4/IPv6 address or DNS name of the local SMTP server.<br>**NOTE:** This definition is required only when the SMTP server is set to **Local**. |
| Port | The SMTP port number, with a default of 25. Acceptable ports include 25, 465, 587, 2525, and 5000 to 32768. |
| Authentication | Enable this if the SMTP server requires authentication.<br>**User Name, Password, and Confirm Password:** If your mail server requires authentication, enter your user name and password here. This performs simple authentication, not SSL/TLS. |
| Use SSL/TLS | Select when encryption is used from the drop-down list.<br>• **Never:** The SMTP server neither requires nor supports encryption.<br>• **If Supported:** The SMTP server advertises support for STARTTLS but doesn't require the connection to be encrypted. The STARTTLS command is sent after the advertisement is given.<br>• **Always:** The SMTP server requires the STARTTLS command to be sent on connection to it.<br>• **Implicitly:** The SMTP server only accepts connections that begin encrypted. No STARTTLS message is sent to the server. |
| Require CA Root Certificate | This should only be enabled if the security policy of your organization does not allow for implicit trust of SSL/TLS connections. If this is enabled, a valid root CA certificate must be loaded onto the unit for encrypted e-mails to be sent. |
| File Name | This field is dependent on the root CA certificates installed on the unit and whether or not a root CA certificate is required. Select the file name to upload or configure a new SSL/TLS certificate (see “> SSL Certificates:” on page 84). |

**> Recipients:** Specify up to four e-mail recipients. Click **Add Recipient** or select a name to configure the following settings:

- **Generation:** Enables (default) or disables sending e-mail to the recipient.
- **To Address:** The user name and domain name of the recipient. To use e-mail for paging, use the e-mail address for the recipient’s pager gateway account (for example, `myacct100@skytel.com`). The pager gateway will generate the page.

  To bypass the DNS lookup of the IP address of the mail server, use the IP address in brackets instead of the e-mail domain name, e.g., use jsmith@[xxx.xxx.x.xxx] instead of jsmith@company.com. This is useful when DNS lookups are not working correctly.

- **Format:** The long format contains name, location, contact, IP address, serial number of the device, date and time, event code, and event description. The short format provides only the event description.
- **Language:** The language which the e-mail notification will be sent in. This is dependent on the installed language pack (if applicable).
- **Port:** The SMTP port number, with a default of 25. The range is 25, 465, 587, 5000 to 32768.
- **Server:** Select one of these methods for routing e-mail:
  - **Local:** This is through the site-local SMTP server. This recommended setting ensures that the e-mail is sent using the site-local SMTP server. Choosing this setting limits delays and network outages and retries sending e-mail for many hours. When selecting the Local setting, you must also enable forwarding at the SMTP server of your device and set up a special external e-mail account to receive the forwarded e-mail. Check with your SMTP server administrator before making these changes.
  - **Recipient:** This is the SMTP server of the recipient. The unit performs an MX record look-up on the recipients e-mail address and uses that as its SMTP server. The e-mail is only sent once, so it can be lost more easily than with Local or Custom settings.
  - **Custom:** This enables each e-mail recipient to have its own server settings. These settings are independent of the settings given under "Configure e-mail notifications" on page 81.

| Setting | Description |
|---|---|
| From Address | The contents of the **From** field in e-mail messages sent by the unit:<br>• If an IP address is specified as Local SMTP Server, use the format user@ [IP_address].<br>• If DNS is configured and the DNS name is specified as Local SMTP Server, use the format user@domain.<br>**NOTE:** The local SMTP server may require that you use a valid user account on the server for this setting. See the server documentation. |
| SMTP Server | The IPv4/IPv6 address or DNS name of the local SMTP server.<br>**NOTE:** This definition is required only when the SMTP server is set to **Local**. |
| Port | The SMTP port number, with a default of 25. The range is 25, 465, 587, 5000 to 32768. |
| Authentication | Enable this if the SMTP server requires authentication. |
| User Name, Password, and Confirm Password | If your mail server requires authentication, enter your user name and password here. This performs simple authentication, not SSL/TLS. |
| Use SSL/TLS | Select when encryption is used from the drop-down list.<br>• **Never:** The SMTP server neither requires nor supports encryption.<br>• **If Supported:** The SMTP server advertises support for STARTTLS but doesn't require the connection to be encrypted. The STARTTLS command is sent after the advertisement is given.<br>• **Always:** The SMTP server requires the STARTTLS command to be sent on connection to it.<br>• **Implicitly:** The SMTP server only accepts connections that begin encrypted. No STARTTLS message is sent to the server. |
| Require CA Root Certificate | This should only be enabled if the security policy of your organization does not allow for implicit trust of SSL/TLS connections. If this is enabled, a valid root CA certificate must be loaded onto the unit for encrypted e-mails to be sent. |
| File Name | This field is dependent on the root CA certificates installed on the unit and whether or not a root CA certificate is required. Select the file name to upload or configure a new SSL/TLS certificate (see "> SSL Certificates:" on page 84). |

**> SSL Certificates:** Load a mail SSL certificate on the unit for greater security. The file must have an extension of `.crt` or `.cer`. Up to five files can be loaded at any given time.

When installed, the certificate details are displayed on this page. An invalid certificate will display "n/a" for all fields except **File Name**.

Certificates can be deleted using this screen. Any e-mail recipients using deleted certificates should be manually modified to remove reference to the deleted certificates.

**> E-mail > Test:** Send a test message to a configured recipient, and view the result under **Last Test Result** and **Last Server Response**.\

## Configure SNMP traps

### Path: Configuration > Notification > SNMP Traps

With Simple Network Management Protocol (SNMP) traps, you can generate automatic notifications for significant unit events. These notifications, or Traps, are a useful tool for monitoring devices on your network.

**> Trap Receivers:** The trap receivers are displayed by **NMS IP/Host Name**, where NMS stands for Network Management System. You can configure up to six trap receivers.

To configure a new trap receiver, click **Add Trap Receiver**. To edit (or delete) one, select its IP address/host name.

| Setting | Description |
|---|---|
| Trap Generation | Enable (the default) or disable trap generation for this trap receiver. |
| NMS IP/Host Name | The IPv4/IPv6 address or host name of this trap receiver. The default, 0.0.0.0, leaves the trap receiver undefined. |
| Language | Select a language from the drop-down list. This can differ from the web or command line interfaces and from other trap receivers. |
| SNMPv1 or SNMPv3 | Select an SNMP version to specify the trap type. For an NMS to receive both types of traps, you must separately configure two trap receivers for that NMS, one for each trap type.<br>**SNMPv1** settings:<br>• **Community Name:** The name ("public" by default) used as an identifier when SNMPv1 traps are sent to this trap receiver.<br>• **Authenticate Traps:** When this option is enabled (the default), the NMS identified by the NMS IP/Host Name setting will receive authentication traps (traps generated by invalid attempts to log on to this device).<br>**SNMPv3** settings:<br>• **User Name:** Select the user profile for this trap receiver. |

If you delete a trap receiver, all notification settings configured under "Configuring event actions" for the deleted trap receiver are set to their default values.

Click **Apply** to save your changes or **Cancel** to leave without saving.

**> Test**

| Setting | Description |
|---|---|
| Last Test Result | The result of the most recent SNMP trap test. A successful SNMP trap test verifies only that a trap was sent; it does not verify that the trap was received by the selected trap receiver. A trap test succeeds if all of the following are true:<br>• The SNMP version (SNMPv1 or SNMPv3) configured for the selected trap receiver is enabled on this device.<br>• The trap receiver itself is enabled.<br>• If a host name is selected for the **To** address, that host name can be mapped to a valid IP address. |
| To | Select the IP address or host name to which a test SNMP trap will be sent. If no trap receiver is configured, a link to the **Trap Receiver** configuration screen is displayed. |

Click **Apply** to test the selected trap or **Cancel** to leave without testing.

## General Options

### Path: Configuration > General

**> Identification:** Configure NMC identification.

| Setting | Description |
|---|---|
| Host Name Synchronization | When enabled, this allows the host name to be synchronized with the system name so both fields automatically contain the same value.<br>**NOTE:** When enabling this feature, the system name identifier can no longer contain a space character (since it will be synchronized to the host name field). |
| Name, Contact, and Location | Define values for **Name** (the device name), **Contact** (the person responsible for the device), and **Location** (the physical location) used by the InfraStruxure PDU's SNMP agent. These settings are the values used for the MIB-II **sysName**, **sysContact**, and **sysLocation** Object Identifiers (OIDs). |
| System Message | When defined, a custom message will appear on the logon screen for all users. |

Click **Apply** to save your changes or **Cancel** to leave without saving.

**> Date/Time > Mode**: Set the time and date used by the InfraStruxure PDU. You can change the current settings manually or through a Network Time Protocol (NTP) Server:

| **Setting** | **Description** |
|---|---|
| Time Zone | Select your local time difference from Coordinated Universal Time (UTC), also known as Greenwich Mean Time (GMT). |
| Manual Mode | Do one of the following<br>• Enter the date and time for the PDU<br>• Select the **Apply Local Computer Time** check box to apply the date and time settings of the computer you are using |
| Synchronize with NTP Server | Have an NTP (Network Time Protocol) server define the date and time for the PDU. By default, any PDU on the private side of a StruxureWare server obtains its time settings by using StruxureWare as an NTP server.<br>• **Override Manual NTP Settings:** If you select this, data from other sources (typically DHCP) take precedence over the NTP configurations you set here.<br>• **Primary NTP Server:** Enter the IP address or domain name of the primary NTP server.<br>• **Secondary NTP Server:** Enter the IP address or domain name of the secondary NTP server if a secondary server is available.<br>• **Update Interval:** Define, in hours, how often the PDU accesses the NTP server for an update. Minimum: 1; Maximum: 8760 (1 year).<br>• **Update Using NTP Now:** Initiate an immediate update of the date and time by the NTP Server. |

Click **Apply** to save your changes or **Cancel** to leave without saving.

**> Date/Time > Daylight Savings:** Enable traditional United States daylight saving time (DST), or enable and configure a customized daylight saving time to match how daylight saving time is implemented in your local area. DST is disabled by default.

When customizing daylight saving time (DST):

- If the local DST always starts or ends on the fourth occurrence of a specific weekday of a month (the fourth Sunday of June, for example), select **Fourth/Last** from the first **Date** drop-down list. If a fifth Sunday occurs in that month in a subsequent year, the time setting still changes on the fourth Sunday.
- If the local DST always starts or ends on the last occurrence of a specific weekday of a month, whether it is the fourth or the fifth occurrence, choose **Fifth/Last**.

**> User Config File:** Use the settings from one InfraStruxure PDU to configure another. Retrieve the config.ini file from the configured PDU, customize that file (e.g., to change the IP address), and upload the customized file to the new PDU. The file name can be up to 64 characters, and must have the.ini suffix.

- **Status:** Reports the progress of the upload. The upload succeeds even if the file contains errors, but a system event reports the errors in the event log.
- **Upload:** Browse to the customized file and upload it so the current InfraStruxure PDU can use it to set its configuration.
- **Download:** Download a configuration file (config.ini) directly through the web browser to your computer.

Instead of uploading the file to one InfraStruxure PDU, you can export the file to multiple InfraStruxure PDUs by using an FTP script or a batch file and the APC .ini file utility, available from **www.apc.com/tools/download**. Click **Apply** to save your changes or **Cancel** to leave without saving.

**> Quick Links:** View and change the URL links displayed at the bottom left of each page of the interface.

By default, these links access the following web pages:

- **Lin**k 1: The home page of the APC by Schneider Electric web site.
- Link 2: A page where you can use samples of web-enabled products.
- **Link 3:** The home page for Schneider Electric Remote Monitoring Service.

Select a link **Name** to go to the Quick Links configuration page. There, enter a new link **Name** and **Address**, or click **Reset to Defaults** to restore the default links.

## Configure Syslog servers, settings, and tests

### Path: Configuration > Logs > Syslog

**> Servers:** Select a server to change it's configuration, or click **Add Server** to configure a new Syslog server.

| **Setting** | **Description** |
|---|---|
| Syslog Server | Use IPv4/IPv6 addresses or host names to identify up to four servers that will receive Syslog messages sent by the unit. |
| Port | The port the unit will use to send Syslog messages. The default UDP port assigned to Syslog is 514. |
| Language | Select the language for any Syslog messages. |
| Protocol | Select either UDP or TCP. |

Click **Apply** to save your changes or **Cancel** to leave without saving.

**> Settings**

| **Setting** | **Description** |
|---|---|
| Message Generation | Enable the generation and the logging of Syslog messages for events that have Syslog configured as a notification method. |
| Facility Code | Selects the facility code assigned to the Syslog messages of the unit (User, by default).<br>**NOTE: User** best defines the Syslog messages sent by the unit. Do not change this selection unless advised to do so by the Syslog network or system administrator. |
| Severity Mapping | This section maps each severity level of the unit or environment events to available Syslog priorities. The local options are **Critical**, **Warning**, and **Informational**. You should not need to change severity mappings.<br>• **Critical** is mapped to **Critical** (critical conditions)<br>• **Warning** is mapped to **Warning** (warning conditions)<br>• **Informational** is mapped to **Info** (informational messages)<br><br>Other options include<br>• **Emergency:** The system is unusable.<br>• **Alert:** Action must be taken immediately.<br>• **Error:** Error conditions<br>• **Notice:** Normal but significant conditions<br>• **Debug:** Debug-level messages |

Click **Apply** to save your changes or **Cancel** to leave without saving.

### > Test

Send a test message to the Syslog servers. The result will be sent to all configured Syslog servers.

Select a severity to assign to the test message, and then define the test message. Format the message to consist of the event type (for example: APC, System, or Device) followed by a colon, a space, and the event text. The message can have a maximum of 50 characters.

Example: `APC: Test Syslog.`

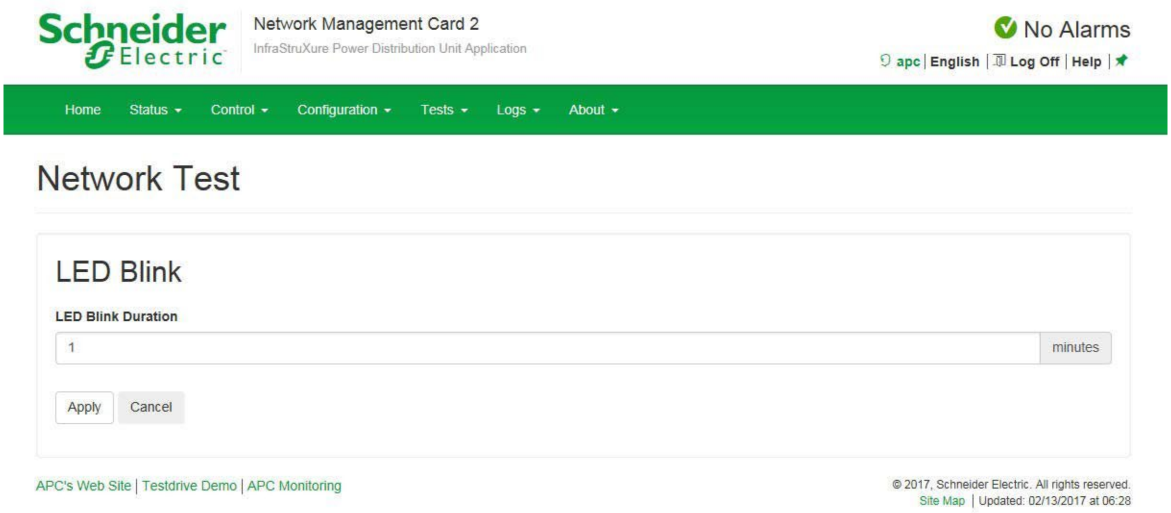
The test message should have the following fields:

- The priority (PRI): the Syslog priority assigned to the message event, and the facility code of messages sent by the unit.
- The Header: a time stamp and the IP address of the unit.
- The message (MSG) part:
- The **TAG** field, followed by a colon and space, identifies the event type.
- The **CONTENT** field is the event text, followed (optionally) by a space and the event code.

Example: `APC: Test Syslog is valid.`

# Tests Tab

**Path: Tests > Network > LED Blink**


Schneider Electric
Network Management Card 2
InfraStruXure Power Distribution Unit Application
No Alarms
apc | English | Log Off | Help
Home
Status
Control
Configuration
Tests
Logs
About
Apply
Cancel
APC's Web Site | Testdrive Demo | APC Monitoring
© 2017, Schneider Electric. All rights reserved.
Site Map | Updated: 02/13/2017 at 06:28

Network Test

LED Blink

LED Blink Duration: 1 minutes

If you are having trouble finding your unit, enter a number of minutes in the **LED Blink Duration** field, and then click **Apply**. The Status LED on the Ethernet port will blink for the specified number of minutes. (The Ethernet port is on the user connection plate; see the *Operation Manual* on **www.APC.com**).

# Logs Tab

## NMC log/event log

**Path: Logs > NMC Log**

The NMC Log, or Event Log, displays all events recorded during the past few days, including events that send SNMP traps (with the exception of SNMP authentication failures and abnormal internal system events).

**> Log:** By default, the event log displays the most recent events first. To see the events listed together on a web page, click **Launch Log in New Window**. To open the log in a text file or save the log to your computer, click the floppy disk icon(💾) on the same line as the **Event Log** heading.

**NOTE:** You can also use FTP or Secure CoPy (SCP) to view the event log. See “Use FTP or SCP to retrieve log files” on page 92.

**NOTE:** You can enable color coding for events. See “> Local Users > Default Settings:” on page 66.

**Filter event logs:** Use filtering to omit information you don’t want to display.

- Filter the log by date or time: Use the **Last** or **From** buttons. (The filter configuration is saved until the PDU restarts.)
- Filter the log by event severity or category:
  a. Click **Filter Log**.
  b. Clear a check box to remove events of a certain severity or category from view.
  c. Do one of the following:
     - Click **Apply** to activate your filter. After you click **Apply**, text at the upper right corner of the **Event Log** page indicates that a filter is active. The filter is active until you clear it or until the PDU restarts.
     - Click **Cancel** to leave the page without activating your filter.
     - Click **Clear Filter** (**Show All**) to deactivate any filters in use.
     - Click **Save As Default** to make your filter the default setting for all users.
       **NOTE:** This option is only available for Administrators.

Important points on filtering:

- Events are processed through the filter using OR logic. If you apply a filter, it works regardless of the other filters.
- Events that you cleared in the **Filter By Severity** list never display in the filtered Event Log, even if selected in the **Filter by Category** list. Similarly, events that you clear in the **Filter by Category** list never display in the filtered Event Log.

To delete all events, click **Clear Log**. Deleted events cannot be retrieved.

To disable the logging of events based on their assigned severity level or their event category, see “> By Event:” on page 80.

**> Reverse Lookup:** With **reverse lookup** enabled, when a network-related event occurs, both the IP address and the domain name for the networked device are logged in the event log. If no domain name entry exists for the device, only its IP address is logged with the event.

Since domain names generally change less frequently than IP addresses, enabling reverse lookup can improve the ability to identify addresses of networked devices that are causing events.

Reverse lookup is disabled by default. You should not need to enable it if you have no DNS server configured or have poor network performance because of heavy network traffic.

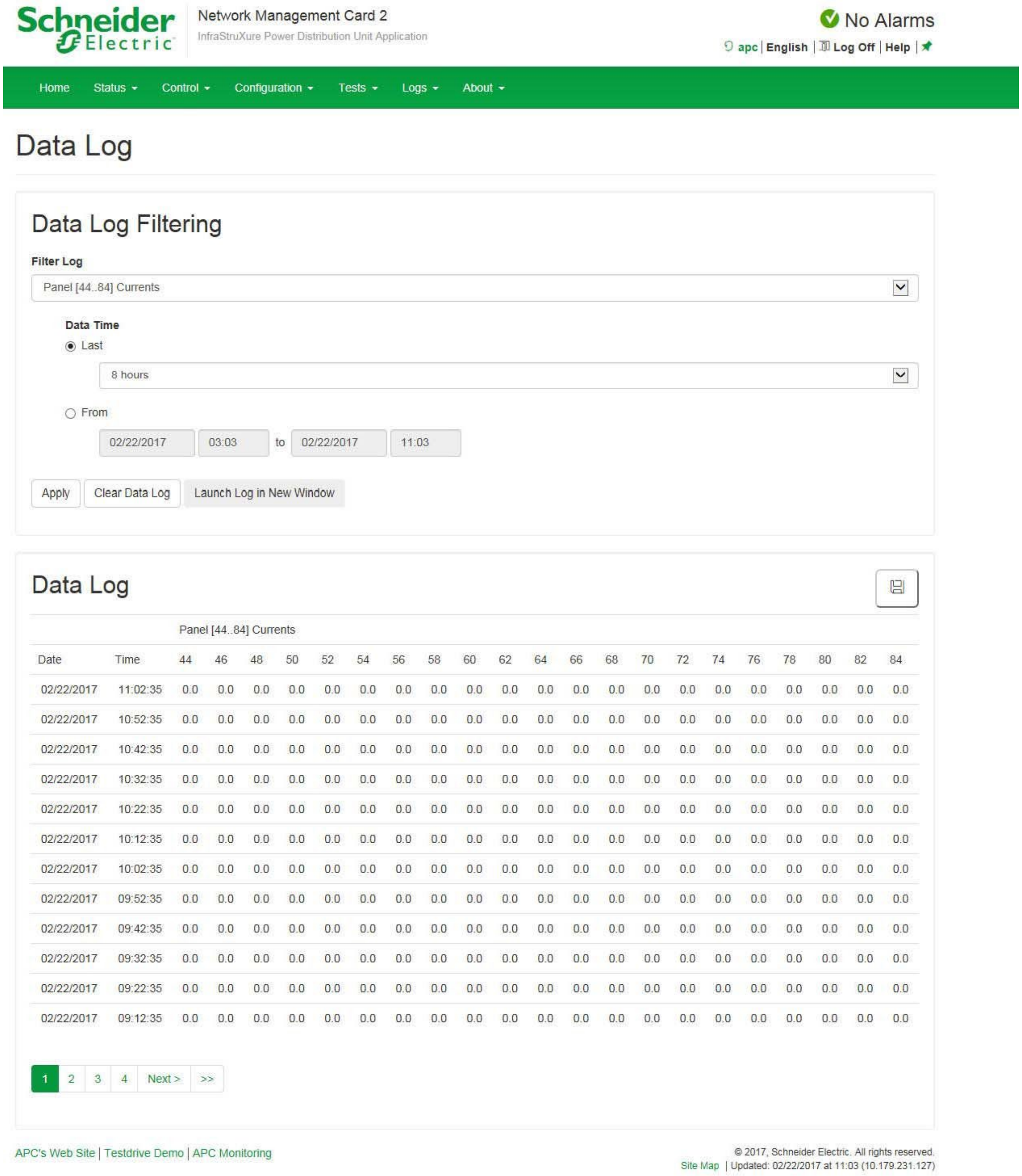
**> Size:** Specify the maximum number of log entries: type a number between 25 and 1500 into the **Event Log Size** field. Click **Apply** to save your changes or **Cancel** to leave the page without saving.

**NOTE:** When you resize the event log in order to specify a maximum size, all existing log entries are deleted. When the log subsequently reaches the maximum size, the oldest entries are deleted.

## Data log

### Path: Logs > Data Log

Use the data log to display measurements about the unit, the power input to the unit, and the ambient temperature of the unit.


Schneider Electric
Network Management Card 2
InfraStruXure Power Distribution Unit Application
No Alarms
apc | English | Log Off | Help
Home
Status
Control
Configuration
Tests
Logs
About
Apply
Clear Data Log
Launch Log in New Window
1
2
3
4
Next >
>>
APC's Web Site | Testdrive Demo | APC Monitoring
Site Map

Data Log

Data Log Filtering

Filter Log

Panel [44..84] Currents

Data Time

● Last

8 hours

○ From

02/22/2017 03:03 to 02/22/2017 11:03

Data Log

| | | Panel [44..84] Currents | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Date | Time | 44 | 46 | 48 | 50 | 52 | 54 | 56 | 58 | 60 | 62 | 64 | 66 | 68 | 70 | 72 | 74 | 76 | 78 | 80 | 82 | 84 |
| 02/22/2017 | 11:02:35 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 |
| 02/22/2017 | 10:52:35 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 |
| 02/22/2017 | 10:42:35 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 |
| 02/22/2017 | 10:32:35 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 |
| 02/22/2017 | 10:22:35 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 |
| 02/22/2017 | 10:12:35 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 |
| 02/22/2017 | 10:02:35 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 |
| 02/22/2017 | 09:52:35 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 |
| 02/22/2017 | 09:42:35 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 |
| 02/22/2017 | 09:32:35 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 |
| 02/22/2017 | 09:22:35 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 |
| 02/22/2017 | 09:12:35 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 |

© 2017, Schneider Electric. All rights reserved.

| Updated: 02/22/2017 at 11:03 (10.179.231.127)

**> Log:** By default, the most recent data is displayed first. To see data listed on a separate web page, click **Launch Log in New Window**.

To open the log in a text file or to save the log to disk, click the floppy disk icon(💾) on the same line as the **Data Log** heading.

**NOTE:** You can also use FTP or Secure CoPy (SCP) to view the data log. See “Use FTP or SCP to retrieve log files” on page 92.

**Filter data logs:** Use filtering to omit unneeded information from view.

- Filter by breaker group: In the **Filter Log** drop-down list, select the desired range of breaker positions.
- Filter by data time: Use the **Last** or **From** buttons to define the time in which the data was logged. (The filter configuration is saved until the unit restarts.)
  - **Last:** Select the number of recent hours, days, or weeks to show recorded data for.
  - **From:** Specify a range of time to show recorded data for.

To delete all data log records, click **Clear Data Log**. Deleted data log records cannot be retrieved.

**> Interval:** Define, in the **Log Interval** fields, how frequently data is searched for and stored in the data log. When you click **Apply**, the number of possible storage days is recalculated and displays at the top of the screen. When the log is full, the oldest entries are deleted.

**NOTE:** Because the interval specifies how often the data is recorded, smaller intervals cause the log to fill more quickly.

**> Rotation:** Rotation causes the contents of the data log to be appended to a file you specify by name and location. To enable rotation, select the **Data Log Rotation** check box. Use the following options to set up password-protection and other parameters:

| Setting | Description |
|---|---|
| FTP Server | The IP address or host name of the server where the file will reside. |
| User Name/ Password | The user name and password required to send data to the repository file. This user must also be configured to have read and write access to the data repository file and the directory (folder) in which it is stored. |
| File Path | The path to the repository file. |
| Filename | The name of the repository file (an ASCII text file), e.g. datalog.txt. Any new data is appended to this file; it does not overwrite the file. |
| Unique Filename | Select this check box to save the log as *mmddyyyy_<filename>.txt*, where *filename* is what you specified in the **Filename** field above. Any new data is appended to the file, but each day has its own file. |
| Delay n hours between uploads | The number of hours between uploads of data to the file (max. 24 hours). |
| Upon failure, try uploading every n minutes | The number of minutes between attempts to upload data to the file after a failed upload.<br>• **Maximum attempts:** The maximum number of times the upload will be attempted after it fails initially.<br>• **Until upload succeeds:** Attempt to upload the file until the transfer is completed. |

Click **Apply** to save your changes, **Cancel** to leave without saving, or **Upload Now!** to rotate data immediately.

**> Size:** Specify the maximum number of log entries.

**NOTE:** When you re-define the maximum log size, all existing log entries are deleted. When the log subsequently reaches the maximum size, the oldest entries are deleted.

## Firewall logs

### Path: Logs > Firewall

If you create a firewall policy, firewall events will be logged here.

The information in the firewall policy log can help the technical support team solve problems. Log entries contain information about the traffic and the rules action (allowed, discarded). When logged here, these events are not logged in the main Event Log (see “NMC log/event log” on page 89).

A firewall log contains up to 50 of the most recent events. The firewall log is cleared when the management interface reboots.

## Use FTP or SCP to retrieve log files

A Super User, Administrator, or Device User can use FTP or SCP to retrieve a tab-delineated event log file `(event.txt)` or data log file `(data.txt)` and import it into a spreadsheet.

- The file reports all events or data recorded since the log was last deleted or (for the data log) truncated because it reached maximum size.
- The file includes information that the event log or data log does not display.
  - The version of the file format (first field)
  - The date and time the file was retrieved
  - The **Name**, **Contact**, and **Location** values and IP address of the InfraStruxure PDU
  - The unique **Event Code** for each recorded event (*event.txt* file only)

  **NOTE:** The file uses a four-digit year for log entries. You may need to select a four-digit date format in your spreadsheet application to display all four digits.

If you are using the encryption-based security protocols for your system, use SCP to retrieve the log file. If you are using unencrypted authentication methods for the security of your system, use FTP to retrieve the log file.

See the *Security Handbook*, available at **www.apc.com,** for information on available protocols and methods for setting up the type of security you need.

### Use SCP to retrieve the files

To retrieve the `event.txt` file, use the following command:

```
scp username@hostname_or_ip_address:event.txt ./event.txt
```

To use SCP to retrieve the `data.txt` file, use the following command:

```
scp username@hostname_or_ip_address:data.txt ./data.txt
```

### Use FTP to retrieve the files

To retrieve the `event.txt` or `data.txt` files

1. At a command line, type `ftp` and the IP address of the InfraStruxure PDU, and press ENTER.

   If the Port setting for the FTP Server option (set through the ftp -p command in the CLI or **Configuration > Network > FTP server** on the web interface) has been changed from its default (21), you must use the non-default value in the FTP command. For Windows FTP clients, use the following command, including spaces. (For some FTP clients, you must use a colon instead of a space between the IP address and the port number.)

   ```
   ftp>open ip_address port_number
   ```

   To set a non-default port value to enhance security for the FTP Server, see “FTP server configuration” on page 80. You can specify any port from 5001 to 32768.

2. Use the case-sensitive **User Name** and **Password** for a Super User, Administrator, or Device User to log on. The default **User Name** for a Super User and Administrator is **apc**. For a Device User, the default **User Name** is **device.**

3. Use the **get** command to transmit the text of a log to your local drive.

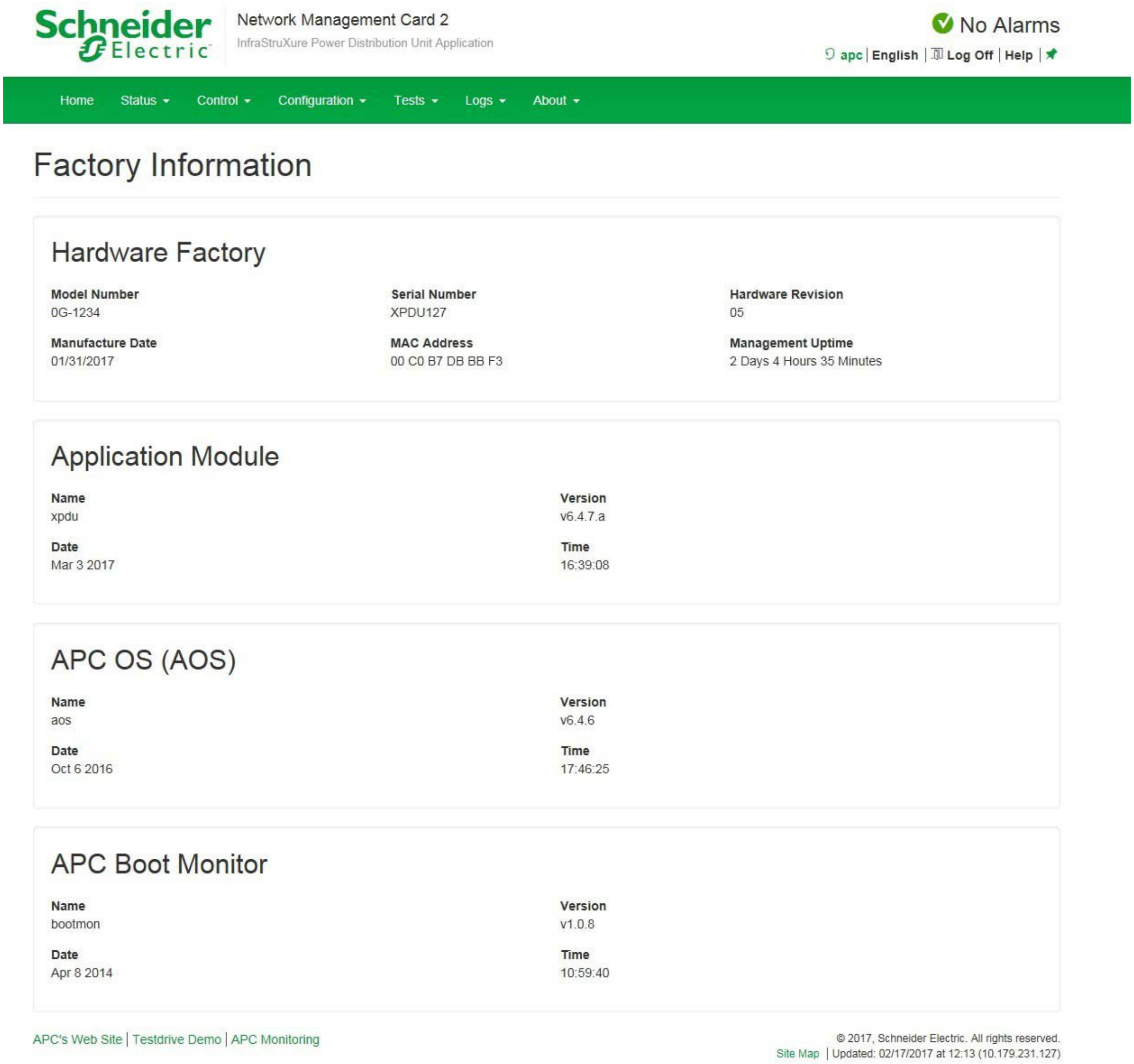
   ```
   ftp>get event.txt
   ```

   or

   ```
   ftp>get data.txt
   ```

4. Type `quit` at the `ftp>` prompt to exit FTP.

# About Tab


Schneider Electric
Network Management Card 2
InfraStruXure Power Distribution Unit Application
No Alarms
apc | English | Log Off | Help
Home
Status
Control
Configuration
Tests
Logs
About

Factory Information

Hardware Factory

| Model Number | Serial Number | Hardware Revision |
|---|---|---|
| 0G-1234 | XPDU127 | 05 |
| **Manufacture Date** | **MAC Address** | **Management Uptime** |
| 01/31/2017 | 00 C0 B7 DB BB F3 | 2 Days 4 Hours 35 Minutes |

Application Module

| Name | Version |
|---|---|
| xpdu | v6.4.7.a |
| **Date** | **Time** |
| Mar 3 2017 | 16:39:08 |

APC OS (AOS)

| Name | Version |
|---|---|
| aos | v6.4.6 |
| **Date** | **Time** |
| Oct 6 2016 | 17:46:25 |

APC Boot Monitor

| Name | Version |
|---|---|
| bootmon | v1.0.8 |
| **Date** | **Time** |
| Apr 8 2014 | 10:59:40 |

APC's Web Site | Testdrive Demo | APC Monitoring

© 2017, Schneider Electric. All rights reserved.
Site Map | Updated: 02/17/2017 at 12:13 (10.179.231.127)

## About power distribution

### Path: About > Power Distribution

Power distribution information shows ratings for main breakers and panel breakers, which optional features have been installed, and the installed version of power-metering firmware.

## About your PDU model

### Path: About > Network

The Hardware Factory information is useful to Schneider Electric Customer Support for troubleshooting problems with the unit. The serial number and MAC address are also available on the PDU.

**Management Uptime** is the length of time the web interface has been running continuously.

Factory information for the Application Module, APC OS (AOS), and APC Boot Monitor indicates the name, the firmware version, and the date and time each firmware module was created. This information is also useful in troubleshooting and enables you to determine if updated firmware is available at **www.apc.com**.

## About support

### Path: About > Support

This page provides links to **Support Resources** including:

- Knowledge Base
- Company Contact Information
- Firmware Downloads

The **Technical Support Debug Information Download** feature is provided at the bottom of the page. This feature captures an assortment of debug data into a single file and then allows the user to download that file to a local computer intended for technical support use.

# Device IP Configuration Wizard

The APC by Schneider Electric Device IP Configuration Wizard configures the IP address, subnet mask, and default gateway of one or more units. You can use the Wizard in either of the following ways:

- Remotely over your TCP/IP network: discover and configure unconfigured units on the same network segment as the computer running the Wizard.
- Through a direct connection from a serial port: configure or reconfigure the unit.

## System requirements

The Device IP Configuration Wizard runs on Microsoft® Windows® 2000, Windows Server® 2003, Windows Server® 2012, and on 32- and 64-bit versions of Windows XP, Windows Vista, Windows 2008, Windows 7, Windows 8, and Windows 10 operating systems.

## Installation

Install the Wizard from a downloaded executable file:

1. Go to **www.apc.com**.
2. Download the latest version of the Device IP Configuration Wizard.
3. Run the executable file (DeviceIPConfigurationWizard.exe).

## Launch the Wizard

The installation creates a shortcut link in the Windows **Start** menu to launch the Wizard. Most software firewalls must be temporarily disabled for the Wizard to discover unconfigured units.

# Export Configuration Settings

## Retrieve and Export the .ini File

### Summary of the procedure

A Super User/Administrator can retrieve the .ini file of a unit and export it to another unit or to multiple units. The steps are below; see details in the following sections.

1. Configure a unit with the desired settings and export them.
2. Retrieve the .ini file from that unit.
3. Customize the file to change the TCP/IP settings at least.
4. Use a file transfer protocol supported by the unit to transfer a copy to one or more other units. For a transfer to multiple units, use an FTP or SCP script or the .ini file utility.

Each receiving unit uses the file to reconfigure its own settings and then deletes it.

**NOTE:** Users are no longer managed via the config.ini in any form. Users are now managed via a separate file with the .csf extension. For further information on this topic, refer to article ID FA176542 in the Knowledge Base at **www.apc.com**.

### Contents of the .ini file

The config.ini file you retrieve from a unit contains the following:

- Section headings and keywords (only those supported for the particular device from which you retrieve the file): **Section headings** are category names enclosed in brackets ([ ]). **Keywords**, under each section heading, are labels describing specific unit settings. Each keyword is followed by an equals sign and a value (either the default or a configured value).
- The `Override` keyword: With its default value, this keyword prevents the exporting of one or more keywords and their device-specific values. For example, in the `[NetworkTCP/IP]` section, the default value for `Override` (the MAC address of the PDU) blocks the exporting of values for the `SystemIP`, `SubnetMask`, `DefaultGateway`, and `BootMode`.

### Detailed procedures

**Retrieving:** To set up and retrieve an .ini file to export:

1. If possible, use the interface of a unit to configure it with the settings to export. (Directly editing the .ini file risks introducing errors).
2. To use FTP to retrieve *config.ini* from the configured unit:

   a. Open a connection to the unit using its IP address:

   ```
   ftp> open ip_address
   ```

   b. Log on using the Super User/Administrator user name and password.

   c. Retrieve the *config.ini* file containing the settings of the unit:

   ```
   ftp> get config.ini
   ```

   The file is written to the folder from which you launched the FTP.
   To retrieve configuration settings from multiple InfraStruxure PDUs and export them to other units, see *Release Notes: ini File Utility, version 2.0,* available at **www.apc.com**.

**Customizing:** You must customize the file before exporting it to other units.

1. Use a text editor to customize the file.
   - Section headings, keywords, and pre-defined values are not case-sensitive, but string values that you define are case-sensitive.
   - Use adjacent quotation marks to indicate no value. For example, `LinkURL1=""` indicates that the URL is intentionally undefined.
   - Enclose in quotation marks any values that contain leading or trailing spaces or are already enclosed in quotation marks.
   - To export scheduled events, configure the values directly in the .ini file.
   - To export a system time with the greatest accuracy, if the receiving units can access a Network Time Protocol server, configure `enabled` for `NTPEnable`:

     ```
     NTPEnable=enabled
     ```

     Alternatively, reduce transmission time by exporting the `[SystemDate/Time]` section as a separate .ini file.
   - To add comments, start each comment line with a semicolon (`;`).
2. Copy the customized file to another file name in the same folder:
   - The file name can have up to 64 characters and must have the .ini suffix.
   - Retain the original customized file for future use. **The file that you retain is the only record of your comments.**

**Exporting the file to a single unit:** To export the .ini file to another unit, do either of the following:

- From the web interface of the receiving unit, select **Configuration > General > User Config File**. Enter the full path of the file, or use Browse on your local PC.
- Use any file transfer protocol supported by units, i.e., FTP, FTP Client, SCP, or TFTP. The following example uses FTP:

  a. From the folder containing the copy of the customized .ini file, use FTP to log in to the unit to which you are exporting the .ini file:

  ```
  ftp> open ip_address
  ```

  b. Export the copy of the customized .ini file to the root directory of the receiving unit:

  ```
  ftp> put filename.ini
  ```

**Exporting the file to multiple units:** To export the .ini file to multiple units:

- Use FTP or SCP, but write a script that incorporates and repeats the steps used for exporting the file to a single unit.
- Use a batch processing file and the .ini file utility.
- To create the batch file and use the utility, see *Release Notes: ini File Utility, version 2.0*, available at **www.apc.com**.

# The Upload Event and Error Messages

The following event occurs when the receiving unit completes using the .ini file to update its settings.

```
Configuration file upload complete, with number valid values
```

If a keyword, section name, or value is invalid, the upload by the receiving unit succeeds, and additional event text states the error.

| **Event text** | **Description** |
|---|---|
| Configuration file warning: Invalid keyword on line *number*.<br>Configuration file warning: Invalid value on line *number*. | A line with an invalid keyword or value is ignored. |
| Configuration file warning: Invalid section on line *number.* | If a section name is invalid, all keyword/value pairs in that section are ignored. |
| Configuration file warning: Keyword found outside of a section on line *number*. | A keyword entered at the beginning of the file (i.e., before any section headings) is ignored. |
| Configuration file warning: Configuration file exceeds maximum size. | If the file is too large, an incomplete upload occurs. Reduce the size of the file, or divide it into two files, and try uploading again. |

## Messages in config.ini

A unit from which you download the config.ini file must be discovered successfully in order for its configuration to be included. If the unit is not present or is not discovered, the config.ini file contains a message under the appropriate section name instead of keywords and values.
For example: `xPDU not discovered`

If you did not intend to export the unit configuration as part of the .ini file import, ignore these messages.

## Errors generated by overridden values

The `Override` keyword and its value will generate error messages in the event log when it blocks the exporting of values. See “Contents of the .ini file” on page 97 for information about which values are overridden.

Because the overridden values are device-specific and not appropriate to export to other units, ignore these error messages. To prevent these error messages, delete the lines that contain the `Override` keyword and the lines that contain the values that they override. Do not delete or change the line containing the section heading.

# Related Topics

On Windows operating systems, instead of transferring .ini files, you can use the Device IP Configuration Wizard to update the basic TCP/IP settings of the unit and configure other settings through the web or command line interfaces. See “Device IP Configuration Wizard” on page 96.

# File Transfers

## Upgrading Firmware

### Benefits of upgrading firmware

When you upgrade the firmware on the NMC:

- You obtain the latest bug fixes and performance improvements.
- New features become available for immediate use.

Keeping the firmware versions consistent across your network ensures that all NMCs support the same features in the same manner.

### Firmware files (NMC)

A firmware version consists of two modules: An APC Operating System (AOS) module and an application module. Each module contains one or more Cyclical Redundancy Checks (CRCs) to protect its data from corruption during transfer.

The APC Operating System (AOS) and application module files used with the NMC share the same basic format:

`apc_hardware-version_type_firmware-version.bin`

- `apc`: Indicates that this is an APC file.
- `hardware-version: hw0`*`x`* identifies the version of the hardware on which you can use this binary file.
- `type:` Identifies whether the file is for the APC Operating System (AOS) or the application module for the NMC.
- `version:` The version number of the file.
- `bin`: Indicates that this is a binary file.

## Firmware File Transfer Methods

**NOTE:** Upgrade the bootmon module first, then the AOS module, and finally, the application module by placing them on the unit in that order.

Obtain the free, latest firmware version from the APC by Schneider Electric web site. To upgrade the firmware of one or more units, use 1 of these 5 methods:

- On a Windows operating system, use the **Firmware Upgrade Utility** downloaded from the web site **www.apc.com**.
- On any supported operating system, use **FTP** or **SCP** to transfer the individual AOS and application firmware modules.
- For a unit that is NOT on your network, use **XMODEM** through a serial connection to transfer the individual firmware modules from your computer to the unit.
- For upgrades to **multiple units**, see “Upgrade multiple units” on page 103.

## Use the Firmware Upgrade Utility

This Firmware Upgrade Utility is part of the firmware upgrade package available on **www.apc.com**. (*Never* use an Upgrade Utility designated for one product to upgrade the firmware of another product).

**Use the Utility for upgrades on Windows-based systems:** On any supported Windows operating system, the Firmware Upgrade Utility automates the transferring of the firmware modules *in the correct module order*.

Unzip the downloaded firmware upgrade file and double-click the .exe file. Then enter the IP address, the user name, and the password in the dialog fields and click **Upgrade Now**. You can use the **Ping** button to test your entered details.

**Use the Utility for manual upgrades, primarily on Linux:** On non-Windows operating systems, the Firmware Upgrade Utility extracts the individual firmware modules, but does not upgrade the unit.

To extract the firmware files:

1. After extracting files from the downloaded firmware upgrade file, run the **Firmware Upgrade Utility** (the .exe file).
2. At the prompts, click **Next**, and then specify the directory location to which the files will be extracted.
3. When the **Extraction Complete** message displays, close the dialog box.

## Use FTP or SCP to upgrade one unit

**FTP:** To use FTP to upgrade a unit over the network:

- The unit must be on the network, with its system IP, subnet mask, and default gateway configured.
- The FTP server must be enabled at the unit.

**NOTE:** The file-transfer procedure assumes the bootmon module does not need upgrading. However, it is always necessary to upgrade the AOS and application modules.

To transfer the files:

1. The firmware module files must be extracted.
2. At a computer on the network, open a command prompt window. Go to the directory that contains the firmware files, and list the files:

   ```
   C:\>cd apc
   ```

   ```
   C:\apc>dir
   ```

3. Open an FTP client session:

   ```
   C:\apc>ftp
   ```

4. Type `open` with the **IP address** of the unit, and press ENTER. If the **port** setting for the FTP Server has changed from its default of **21**, you must use the non-default value in the FTP command.

   - For Windows FTP clients, separate a non-default port number from the IP address by a space. For example (showing a space before 21000):
     ```
     ftp> open 150.250.6.10 21000
     ```
   - Some FTP clients require a colon instead before the port number.

5. Log on as Administrator (**apc** is the default user name).

6. Upgrade the AOS (always upgrade the AOS before the application module):
   `ftp> bin`
   `ftp> put apc_hw05_aos_`*`nnn`*`.bin` (where *`nnn`* is the firmware version number)
7. When FTP confirms the transfer, type `quit` to close the session.
8. After 20 seconds, repeat steps 3 through 7, using the application module file name from step 6.

**NOTE:** The following procedure assumes the bootmon module does not need upgrading. However, it is always necessary to upgrade the AOS and application modules.

**SCP:** To use Secure CoPy (SCP) to upgrade firmware for the unit:

1. Locate the firmware modules, see “Use the Utility for manual upgrades, primarily on Linux:” on page 101.
2. Use an SCP command line to transfer the AOS firmware module to the unit. The following example uses *`nnn`* to represent the version number of the AOS module:

```
scp apc_hw05_aos_nnn.bin apc@158.205.6.185:apc_hw05_aos_nnn.bin
```

3. Use a similar SCP command line, with the name of the application module, to transfer the application firmware module to the unit. (Always upgrade the AOS before the application module).

## Use XMODEM to upgrade one unit

To use XMODEM to upgrade one unit that is not on the network, you must extract the firmware files from the Firmware Upgrade Utility (see “Use the Firmware Upgrade Utility” on page 101).

**NOTE:** The following procedure assumes the bootmon module does not need upgrading. However, it is always necessary to upgrade the AOS and application modules

To transfer the files:

1. Select a serial port at the local computer and disable any service that uses the port.
2. Connect the provided serial configuration cable (part number 940-0144A) to the selected port and to the RJ-12 style serial port at the unit.
3. Run a terminal program such as HyperTerminal, and configure the selected port for 57600 bps, 8 data bits, no parity, 1 stop bit, and no flow control.
4. Press the pinhole **Reset** button on the PDU monitoring unit, then immediately press the **Enter** key twice, or until the Boot Monitor prompt displays: `BM>`
5. Type `XMODEM`, then press ENTER.
6. From the terminal program’s menu, select XMODEM, then select the binary AOS firmware file to transfer using XMODEM. After the XMODEM transfer is complete, the Boot Monitor prompt returns.

   (Always upgrade the AOS before the application module).
7. To install the application module, repeat steps 5 and 6. In step 6, use the application module file name.
8. Type `reset` or press the **Reset** button to restart the unit’s management interface.

## Upgrade multiple units

Use one of these methods:

- **Firmware Upgrade Utility:** Use this for multiple firmware updates in IPv4 if you have Windows. The utility records all upgrade steps in a log as a reference to validate the upgrade.The Utility is available from the Knowledge Base: **www.apc.com/support.**
- **Export configuration settings:** You can create batch files and use a utility to retrieve configuration settings from multiple units and export them to other units. See *Release Notes: ini File Utility, version 2.0,* available in the Knowledge Base at **www.apc.com**
- **Use FTP or SCP to upgrade multiple units:** To upgrade multiple units using an FTP client or using SCP, write a script which automatically performs the procedure.

### Use the Firmware Upgrade Utility for multiple upgrades

After downloading the Upgrade Utility, double click on the .exe file to run the utility (which ONLY works with IPv4) and follow these steps to upgrade your firmware:

1. Type in an IP address, a user name, and a password, and click **Ping** if you need to verify an IP address.
2. Click the **Device List** button to open the `iplist.txt` file. This should list any device IP, user name, and password.

   For example,
   ```
   SystemIP=192.168.0.1
   SystemUserName=apc
   SystemPassword=apc
   ```

   You can use an existing *iplist.txt* file if it already exists.
3. Select the **Upgrade From Device List** check box to use the `iplist.txt` file.
4. Click **Upgrade Now** to start the firmware version update(s).
5. Select **View Log** to verify any upgrade.

# Verify Upgrades and Updates

To verify a firmware upgrade succeeded, do one of the following:

- In the web interface, navigate to **Configuration > Network > FTP Server** to view **Last Transfer Result**.

| Last Transfer Result Code | Description |
|---|---|
| Successful | The file transfer was successful. |
| Result not available | There are no recorded file transfers. |
| Failure unknown | The last file transfer failed for an unknown reason. |
| Server inaccessible | The TFTP or FTP server could not be found on the network. |
| Server access denied | The TFTP or FTP server denied access. |
| File not found | The TFTP or FTP server could not locate the requested file. |
| File type unknown | The file was downloaded but the contents were not recognized. |
| File corrupt | The file was downloaded but at least one Cyclical Redundancy Check (CRC) failed. |

- Use an SNMP GET to the **mfiletransferStatusLastTransferResult** OID.

## Verify the version numbers of installed firmware

Verify the versions of the upgraded firmware modules: In the web interface, navigate to **Configuration > General > About >Network**, or use an SNMP GET to the MIB II **sysDescr** OID.

# Troubleshooting

## Access Problems

For problems that persist or are not described here, contact Schneider Electric Customer Care at **www.apc.com**.

| Problem | Solution |
|---|---|
| Unable to ping the unit | The unit supports the ability to disable IPv4 Ping Response for security reasons.<br>This setting is located in the web interface under **Configuration > Security > Ping Response** or can be located in the config.ini file. Check this setting or verify other access methods such as HTTPS, FTP, Telnet, or SSH.<br>If the unit's Status LED is green, try to ping another node on the same network segment as the unit. If that fails, it is not a problem with the unit. If the Status LED is not green, or if the ping test succeeds, perform the following checks:<br>• Verify all network connections.<br>• Verify the IP addresses of the unit and the NMS.<br>• If the NMS is on a different physical network (or subnetwork) from the unit, verify the IP address of the default gateway (or router).<br>• Verify the number of subnet bits for the unit's subnet mask. |
| Cannot allocate the communications port through a terminal program | Before you can use a terminal program to configure the unit, you must shut down any application, service, or program using the communications port. |
| Cannot access the command line interface through a serial connection | Make sure that the correct serial cable (part 940-0103) is connected to the serial port.<br>Make sure that you did not change the baud rate. Try 2400, 9600, 19200, or 38400. |
| Cannot access the command line interface remotely | • Make sure you are using the correct access method, Telnet or Secure SHell (SSH). These can be enabled or disabled independently. The Super User or an Administrator can enable these access methods.<br>• For SSH, the unit may create a host key. The unit can take up to one minute to create the host key, and SSH is inaccessible for that time. |
| Cannot access the web interface | • Verify that HTTP or HTTPS access is enabled.<br>• Make sure you are specifying the correct URL — one that is consistent with the security system used by the unit. SSL/TLS requires **https**, not **http**, at the beginning of the URL.<br>• Verify that you can ping the unit.<br>• Verify that you are using a web browser supported for the unit.<br>• If the unit has just restarted and SSL/TLS security is being set up, the unit may be generating a server certificate. The unit can take up to one minute to create this certificate, and the SSL/TLS server is not available during that time. |

# SNMP Problems

| Problem | Solution |
|---|---|
| Unable to perform a GET | • Verify the read (GET) community name (SNMPv1) or the user profile configuration (SNMPv3).<br>• Use the command line interface or web interface to ensure that the NMS has access. |
| Unable to perform a SET | • Verify the read/write (SET) community name (SNMPv1) or the user profile configuration (SNMPv3).<br>• Use the command line interface or web interface to ensure that the NMS has write (SET) access (SNMPv1) or is granted access to the target IP address through the access control list (SNMPv3). |
| Unable to receive traps at the NMS | • Make sure the trap type (SNMPv1 or SNMPv3) is correctly configured for the NMS as a trap receiver.<br>• For SNMP v1, query the **mconfigTrapReceiverTable** MIB OID to verify that the NMS IP address is listed correctly and that the community name defined for the NMS matches the community name in the table. If either is not correct, use SETs to the **mconfigTrapReceiverTable** OIDs, or use the command line interface or web interface to correct the trap receiver definition.<br>• For SNMPv3, check the user profile configuration for the NMS, and run a trap test. |
| Traps received at an NMS are not identified | See your NMS documentation to verify that the traps are properly integrated in the alarm/trap database. |

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
France
+ 33 (0) 1 41 29 70 00
www.se.com

As standards, specifications, and design change from time to time, please ask for confirmation of the information given in this publication.