USER'S GUIDE
InfraStruXure Manager

Contents

Introduction 1
- Before You Start 1
- Overview 2
- Supported devices 4
- APC and User Local Area Networks (LANs) 5
- Network Time Protocol (NTP) server feature 5
- How to restore access to the InfraStruXure Manager server 6

Initial configuration requirements 7
- Overview 7
- InfraStruXure Manager Setup Wizard 8

Status and event severity levels 10

"Device Status" display 11

Device groups 12
- Overview 12
- "Device Groups" frame 12
- Device group management 13
- "Configure Notifications for Group" display 15

"Device List" frame 16
- Overview 16
- Right-click menus 17
- "Set Rack Properties" display 19
- "Device Identification" display 19
- "View Group Membership" display 19

"Device Details" display 20
- Overview 20
- HTML "Device Details" display 21
- "HTTP Properties" display 22

InfraStruXure PDU details 23
Overview 23
Branch Breakers 25
Bypass Input 27
Main Input 27
Output Current 28
Output Voltage 29
Q-Breaker Modes 30
Metered Rack PDU details 31
"Recommended Actions" frame 34
"Power Zones" display 35
Power zones 36
Overview 36
"Power Zones" frame 36
Power zone management 38
InfraStruXure PDU diagrams 40
Overview 40
Power zone example 42
InfraStruXure PDU diagram example 43
Diagram legend 46
Device diagrams 47
Overview 47
Power zone example 48
Diagram examples 48
"Reports" display 52
"Logs" display 53
File menu 54
Overview 54
Backup Server 55
Restore Server 56
"Server Log On" display 57

Edit menu 58

Overview 58
Add Devices 59
Disable Notifications for Maintenance 61

View menu 63

Overview 63
"Configure Columns" display 64

Event Management menu 65

Overview 65
Global Device Thresholds 66
Overview 66
UPS tab 67
Environmental Monitor tab 67
Metered Rack PDU tab 67
Schedule tab 68
SNMP Trap Forwarding 69
Building Management System 70
Overview 70
"Configure Slave Addresses" display 71
"Select BMS Slave Devices" display 72
Pinout for the RS-485 port connector 73
Remote Monitoring Service 74

System Management menu 75

Overview 75
Authentication Settings 77
Overview 77
Administrator versus General access 78
Configure local users 78
Configure RADIUS settings 79
"Test RADIUS Access" display 80
Device Access 81
Overview 81
Community names 82
Timeout settings 83
Trap receiver feature 84
FTP Settings 85
Failed to register as a trap receiver for a device 86

Mass Configuration 87
Overview 87
Configuration procedure 87
"Send Configuration to Selected Devices" display 88
"One or More Settings Failed" display 91
Available mass configuration settings 92
Excluded configuration settings 92
Racks 94
Overview 94
Configure Racks 96
Default Power Settings 97
Modify Rack 98
Edit Power Settings 99
Rack kWatt values 100
Power factor values 101
Server Time 103
Shut Down or Reboot Server 104
Overview 104
Duplicate IP addresses assigned on the APC LAN 104
Setup Wizard 104
Network Settings 105
Notification Settings 106
Overview 106
Settings tab 107
Recipients tab (no incident management) 108
Recipients tab (incident management) 108
Error messages during notification tests 109
"Add Recipients" display 109
SMS notifications 110
"Configure Notifications for Recipient" display 111
"Add Recipients" and "Modify Recipients" displays (incident management) 112
Availability settings 113
FTP Server Settings 114
System Identification 114
Proxy Settings 115
Log Settings 116

License Keys 117
Overview 117
"License Keys" display 118
"Evaluation Period" display 119
"Update License Keys" display 120
"Product Activation" display 121
"Insufficient License Keys" display 121
Using the "License Keys" display to update license keys 122
Client Preferences 123

Updates menu 124

Overview 124
Check for Updates 125
Apply Firmware Updates 126
Overview 126
Configure Update tab 126
Last Update Results tab 127
Apply Server Updates 130
Import the product update file to the InfraStruXure Manager server 131
Overview 131
Enable FTP at the InfraStruXure Manager server 131
Download the update file to the InfraStruXure Manager client 132
Use FTP to transfer the update file to the InfraStruXure Manager server 133

Help menu 134

Reports 135

Overview 135
Common report and log features 136
"Select Report Filter" display 137
Environmental report 137
Exceptions reports 138
Overview 138
Bad Battery report 138
Downtime report 138
Exceptions Summary report 140
Rack PDU reports 142
UPS reports 143

Data logs 144

Event log 147

Overview 147

Events 149

Overview 149
APC InfraStruXure Manager events 150
ATS events 151
Environmental events 153
InfraStruXure PDU events 157
MasterSwitch events 162
MasterSwitch Plus events 163
MasterSwitch VM events 164
<Other APC Device> events 166
Rack PDU events 168
System events 170
UPS events 175

InfraStruXure Manager Power Zones Wizard 189

Overview 189

"Define the Power Zone Name" display 190

"Power on all Power Sources" display 190

"Select the Source Power Devices" display 190

"Select the InfraStruXure Manager Rack" display 191

"Power off the Device Racks" display 192

"Define The Server Rack Name" display 192

"Select the Server Rack Devices" display 193

"Select Another Rack" display 193

"Define the Device Rack Name" display 193

"Power on the Rack Devices" display 194

"Select the Rack Devices" display 194

"Finish" display 194

Incident management module 195

Overview 195
Incident management notifications 196
Escalation process 198
Overview 198
Acknowledging incidents 200
Initial configuration 201
Setup Wizard 201
"Incident Management" display 202
Overview 202
Display filters 203
Display columns 204
"Incident History" display 205
Incident Management menu 207
Default Escalation Policy 207
Group Escalation Policy 208
Escalation display features 208
Overview 208
Add Recipient to Policy 209
Edit Time Delay 210
Coverage Schedule 210
How to define an escalation policy 211
"Recipient Incident Actions" display 212

Third-party software 214

Copyrights 214
Copyright (c) 1998-2003, The OpenSSL Project. All rights reserved. 215

APC Worldwide Customer Support 225

Copyright 226

Introduction

Before You Start

Review the following sections before you start using the APC® InfraStruXure™ Manager server:

- Overview provides a brief description of the main InfraStruXure Manager functions and features.
- Initial configuration requirements provides information about how to configure the InfraStruXure Manager server after it is installed.
- Backup Server describes how to save InfraStruXure Manager configuration settings to a backup (*.apc) file.
- Restore Server describes how to import configuration settings from a backup (*.apc) file.
- Incident management module provides information about a separately-licensed feature that the InfraStruXure Manager server can use to make sure that warning and critical status incidents are acknowledged.
- Network Time Protocol (NTP) server feature provides information about using the InfraStruXure Manager server as an NTP server on its APC and User Local Area Networks (LANs).
- How to restore access to the InfraStruXure Manager server provides information about accessing the server if the Administrator username or password becomes unknown, or if **RADIUS only** is selected in the "Authentication Settings" display and a RADIUS server is unavailable.

See also

Also review the release notes, which provide information about requirements and known issues. A copy is available on the installation CD, and as a free download at the bottom of the InfraStruXure Manager product page at the APC Web site.

Overview

An InfraStruXure Manager server can monitor the status of Supported devices on its APC and User Local Area Networks (LANs), and generate reports about those devices.

- Two main displays provide status and other information about monitored devices, including access to device management applications.
  - The "Device Status" display allows you to assign monitored devices to Device groups which provide status and other information about those devices, and allow you to control the content of reports and logs.
  - The "Power Zones" display allows you to create diagrams that identify how the devices assigned to Power zones relate to each other, and to the available power sources.

    For information about the icons used to identify the severity of conditions that exist at monitored devices, see Status and event severity levels.
- The "Logs" display allows you to generate logs (Data logs and an Event log) for monitored devices.
- The "Reports" display allows you to generate Reports for the devices the InfraStruXure Manager server monitors.
- The "Incident Management" display reports information about warning and critical status incidents that occur at monitored devices when the license for the Incident management module has been purchased and activated.

- A menu bar, located above the main displays, provides seven menus that allow you to configure and use the InfraStruXure Manager server:
  - File menu
  - Edit menu
  - View menu
  - Event Management menu
  - System Management menu
  - Updates menu
  - Incident Management menu

    Note

    The **Incident Management** menu is present only when the license for the Incident management module was purchased and activated.
  - Help menu

    For information about how whether you log on as the Administrator or as a General user affects access to menus and options, see Administrator versus General access.

Supported devices

An InfraStruXure Manager server can monitor any APC device that it can discover on its APC and User Local Area Networks (LANs). This includes any device that uses the following APC hardware and software SNMP agents:

Use the Add Devices option in the Edit menu to discover User LAN (corporate network) devices. APC LAN devices are discovered automatically.

- A PowerChute® Business Edition Agent at a NetWare®, Windows® 2000, Windows 2003, Windows NT®, or Windows XP computer

SNMP service must be enabled at the PowerChute Business Edition Agent's host computer.

- Network Management Card (all versions)
- AP9606, AP9617, AP9618, or AP9619 Web/SNMP Management Card

An InfraStruXure Manager server can also monitor the following APC devices:

New APC devices can be added to the list of devices an InfraStruXure Manager server can monitor without requiring a server update. For more information, see <Other APC Device> events.

- MasterSwitch™, MasterSwitch VM, and MasterSwitch Plus units
- Environmental Monitoring Cards, Environmental Monitoring Units, and Environmental Management Systems
- NetworkAIR™ FM or PA units
- InfraStruXure Power Distribution Unit (PDU)
- Metered or Switched Rack Power Distribution Unit (Rack PDU)

- Automatic Transfer Switch (ATS)
- Other InfraStruXure Manager servers

InfraStruXure Manager v4.0-v4.1.x servers can be monitored, but not accessed directly. They require a compatible version of the InfraStruXure Manager client; APC PowerStruXure Information Controllers cannot be monitored.

APC and User Local Area Networks (LANs)

An InfraStruXure Manager server can monitor the Supported devices (APC devices that provide power and environmental protection) on two LANs:

- APC LAN: Monitors the APC devices for the local InfraStruXure zone.
- User LAN: Monitors APC devices on the corporate network.

For information about using the InfraStruXure Manager server as an NTP server on the APC and User LANs, see Network Time Protocol (NTP) server feature.

Network Time Protocol (NTP) server feature

When the InfraStruXure Manager server discovers the Supported devices on its APC LAN, it automatically defines itself as the NTP server for those devices. Those devices will send periodic NTP requests to the InfraStruXure Manager server, which provides the time defined in its "Server Time" display to each requesting device.

The InfraStruXure Manager server can also provide its server time to any device that connects to its User LAN. However, the InfraStruXure Manager server must be manually defined as the NTP server at that device.

How to restore access to the InfraStruXure Manager server

If the username or password used for local, **Administrator** access becomes unknown, use the following procedure to restore access.

Note

If a logoff occurs while **RADIUS only** is selected in the "Authentication Settings" display, and the "Configure local users" display does not have a valid RADIUS server defined, access to the InfraStruXure Manager server cannot be restored. The InfraStruXure Manager Appliance will need to be replaced. For more information, contact APC Support.

1. Connect a computer to the hub on the APC LAN.
2. Reboot the InfraStruXure Manager server.

   Note

   This may require physically disconnecting and reconnecting InfraStruXure Manager at its input power source.

3. Use the InfraStruXure Manager client (step 1) to connect to the InfraStruXure Manager server.
4. When the "Server Log On" display appears, use **admin** (lowercase) as the **Username**, and **apc** (lowercase) as the **Password**, to log on.

   Note

   If the logon fails, try again; the InfraStruXure Manager server may not have finished rebooting. After the "Server Log On" display appears, you must log on within about eight minutes, or you must repeat steps 2 through 4.

5. Select Authentication Settings in the System Management menu.
6. Click the Configure local users button to define the **Administrator** values.

Initial configuration requirements

Overview

Use the following procedure to configure a newly-installed InfraStruXure Manager server.

1	Use the InfraStruXure Manager Setup Wizard	The InfraStruXure Manager Setup Wizard accesses the configuration options that are most important to the InfraStruXure Manager operation. **NOTE:** When you log on to an newly-installed InfraStruXure Manager server, click **Yes** to run the wizard immediately. If you click **No**, you can select the Setup Wizard option in the System Management menu to run the wizard at any time.
2	Review configuration settings the InfraStruXure Manager Setup Wizard cannot access	Select the Client Preferences option in the System Management menu to define whether **Fahrenheit** (the default) or **Celsius** will be used to report temperatures, or to enable (disabled by default) the periodic sending of information to APC about how you use the InfraStruXure Manager features. **NOTE:** No personal information is sent about any user, server, network, system, etc., only general information about how the InfraStruXure Manager features are used.
		Select the System Identification option in the System Management menu to define the InfraStruXure Manager **System Name**, **Contact**, and **Location** values.
		Select the Log Settings option in the System Management menu to define how often data is stored in the data logs, as well as the age at which entries will be deleted from the event or data logs.
3	Create the device groups	See Device groups for information about this InfraStruXure Manager feature.
4	Create the power zones	See "Power Zones" display for information about this InfraStruXure Manager feature.

InfraStruXure Manager Setup Wizard

The following table provides an overview of the configuration settings that can be accessed using this wizard.

Network Settings	The settings for the APC and User Local Area Networks (LANs): By default, the APC LAN uses **192.168.0.*** as its IP address, and a DCHP server provides the settings needed for the User LAN (corporate) network access. **NOTE:** If you change a APC LAN or User LAN setting, the InfraStruXure Manager server must reboot to apply the change.
Server Time	The **Date**, **Time**, and **Time Zone** settings the InfraStruXure Manager server will use. **NOTE:** Any change to the settings will require the InfraStruXure Manager server to reboot. After it reboots, log on and access this wizard again.
Proxy Settings	The **Proxy Host** (IP address or host name), **Port Number**, and access (**Username** and **Password**) settings needed to use a proxy server for HTTP communication.
License Keys	The licence list that determines how many devices the InfraStruXure Manager server can monitor. **NOTE:** A license key must be listed in this display before the InfraStruXure Manager server can monitor the number of devices allowed by that key.
Authentication Settings	The settings that select the authentication method used to log on to the InfraStruXure Manager server and configure the settings used by that method.
Notification Settings	The settings the InfraStruXure Manager server uses to send notifications for events, device group summaries, and firmware updates. **NOTE:** The SMTP settings must be defined before the InfraStruXure Manager server can send notifications to an identified recipient.

Global Device Thresholds	The global thresholds the InfraStruXure Manager server monitors for possible warning conditions. **NOTE:** The global threshold settings do not affect monitored device thresholds, and monitored device thresholds do not affect the global threshold settings.
Device Access	Define settings the InfraStruXure Manager server uses to discover and monitor devices, and to perform firmware updates and mass configurations.
Remote Monitoring Service	The settings used to register the InfraStruXure Manager server to use APC Remote Monitoring Service (RMS) support.
Add Devices	The settings used to discover the User LAN (corporate network) devices the InfraStruXure Manager server will monitor.

Status and event severity levels

The InfraStruXure Manager server, and the devices it monitors, generate events that represent status changes. Each event has a severity level assigned: **Critical**, **Warning**, or **Informational** (or **Normal**).

By default, all events are recorded in the Event log.

The severity levels also apply to status reported by the InfraStruXure Manager server.

Critical	Indicates a condition that requires immediate attention. Left unresolved, the condition may damage the load equipment, or result in the loss of UPS protection during a power failure. In the event log, the following icon identifies critical events; this icon is used in InfraStruXure Manager displays to indicate a critical status: 
Warning	Indicates a condition that may require attention to make sure it does not deteriorate into a critical state. In the event log, the following icon identifies warning events; this icon is used in InfraStruXure Manager displays to indicate a warning status: 
Informational (or Normal)	In the event log, the Informational severity level identifies events which report that the device has performed a normal operation, or that a critical or warning condition has been cleared. In InfraStruXure Manager displays, the following icon indicates a device is operating normally: 

"Device Status" display

This display appears when you log on to the InfraStruXure Manager server, or select the **Device Status** option in the navigation bar or View menu. It has three frames:

"Device Groups" frame	The left frame lists the Device groups and allows you to select which group has its devices displayed in the "Device List" frame. **NOTE:** Device groups also allow you to tailor reports. See "Select Report Filter" display.
"Device List" frame†	The top-right frame displays status and "Configure Columns" display information for the devices assigned to the group selected in the "Device Groups" frame. You can select a device to view more detail about its status in the "Recommended Actions" frame. **NOTE:** Double-clicking a device accesses its management application, or a display that provides more information about that device. See "Device Details" display.
"Recommended Actions" frame†	The bottom-right frame provides more detailed status for the device selected in the "Device List" frame.
† Also appears in the **Devices** tab of the "Power Zones" display.	

Device groups

Overview

Use the Device group management procedures to create and manage the device groups. These device groups, which allow you to assign devices to groups based on your criteria (for example, device locations), are listed in the left frame of the "Device Status" display, and provide the following functions:

- The "Device Groups" frame allows you to select which device group has its devices displayed in the "Device List" frame.
- A "Select Report Filter" display allows you to create Reports that include all the device groups identified in the filter, or just the groups you select.
- An "Configure Notifications for Group" display allows you to customize how the InfraStruXure Manager server uses notifications for a selected group.
- The InfraStruXure Manager server generates System events when specific power problems occur at the UPS systems assigned to a device group.

"Device Groups" frame

This frame lists the Device groups you create, and two groups which cannot be renamed or deleted. When selected, the following device group display their devices in the "Device List" frame:

- **All Devices**: All monitored devices.
- **Unassigned**: All devices that are not assigned to a created group.
- **Created Group**: The devices assigned to the selected group.

All groups, including **All Devices** and **Unassigned**, use icons to indicate whether device problems exist. See Status and event severity levels.

Device group management

Two menus can be used to manage the device groups:

Unless you log on as the Administrator, the menu options are disabled. See Administrator versus General access.

- Right-click menu: Right-click a device group to access up to four options: **Add Device Group**, **Remove Device Group**, **Rename Group**, and **Configure Notifications**.
- Edit menu: **Add Device Group** and **Remove Device Group**.

When **All Devices** is selected, only the **Add Device Group** option is active; when **Unassigned** is selected, only the **Configure Notifications** option is active.

Create a Group	Select **All Devices,** and use the **Add Device Group** option.
Create a Sub-group	Use the **Add Device Group** option at a group that has no devices. **NOTE:** An error message appears if you attempt to create a sub-group for a group (or sub-group) that has devices assigned.
Assign or Move Devices	1. Select the group from which the devices will be moved. 2. In the "Device List" frame, select and drag the devices you want moved to the new group. **NOTE:** You can move devices to a group (or sub-group) that has no sub-group assigned only. Otherwise, the move will fail.
Assign Devices to Multiple Groups	1. Select a group in which the devices are assigned. 2. In the "Device List" frame, select the devices you want assigned to both the selected group and to a new group. 3. Hold the CTRL key down and drag the selected devices into the new group. **NOTE:** You can move devices to a group (or sub-group) that has no sub-group assigned only. Otherwise, the move will fail.

Remove Devices from a Group	1. Select the group from which you want to remove devices. 2. In the "Device List" frame, select the devices you want removed. 3. Right-click a selected device and use one of the following **Group** options: • **Remove Device from All Assigned Groups**: Moves the devices to the **Unassigned** group from all groups to which they are assigned. • **Remove Device from Selected Group**: Removes the devices from the selected group only. Devices that are not assigned to another group move to the **Unassigned** group. **NOTE:** The InfraStruXure Manager server still monitors the removed devices.
Remove a Group	Select the group and use the **Remove Device Group** option. **NOTE:** The InfraStruXure Manager server still monitors the deleted group's devices. Devices that are not assigned to another group move to the **Unassigned** group.
Rename a Group	Right-click the group and use the **Rename Group** option.
Configure Notifications for a Group	1. Right-click the group, and use the **Configure Notifications** option. 2. Use the "Configure Notifications for Group" display (or a "Group Escalation Policy" display, if the Incident management module is activated) to define how notifications are used for events that occur at a selected group's devices. **NOTE:** You can only configure notifications for a group (or sub-group) that has no sub-group assigned. Otherwise, the **Configure Notifications** option is disabled.

"Configure Notifications for Group" display

Use this display for the right-click **Configure Notifications** option in the "Device Groups" frame, to customize how the InfraStruXure Manager server uses notifications for a device group.

When the Incident management module is activated, the **Configure Notifications** option accesses the "Group Escalation Policy" display for the selected device group.

To define the recipients and SMTP settings required for notifications, see Notification Settings.

1. Double-click a listed recipient, or, to configure multiple recipients using identical settings, select those recipients and click **Configure**.
2. Select only the items for which you want to send notifications and click **Apply**.

   For information about the available selections, see Events, Updates menu, and Schedule tab (a "Global Device Thresholds" display tab).
3. Configure any other recipients, as needed.

"Device List" frame

Overview

This frame displays status and other information about the devices assigned to the device group selected in the "Device Groups" frame. This frame also appears in the "Power Zones" display when the **Device** tab is selected.

Select **All Devices** to have the "Device List" frame display information about all the Supported devices the InfraStruXure Manager server is monitoring on its APC and User Local Area Networks (LANs).

To access additional information about a listed device:

- Select a device to display information about that device in the "Recommended Actions" frame.
- Double-click a device to access a "Device Details" display that provides more detail about the device, or direct access to the device's management application.

The following menus provide options you use with the "Device List" frame:

- Two Right-click menus provide column and device-management options.
- A View menu option accesses the "Configure Columns" display that defines what columns of information the "Device List" frame displays.
- A File menu option (**Print Device List**) prints a copy of the displayed list of devices.

Right-click menus

Two right-click menus are available in the "Device List" frame.

- Right-click any column heading to enable or disable individual columns, or to access the "Configure Columns" display.
- Right-click a device to use the options described in the following table.

Unless you log on as the Administrator, these menu options are disabled. See Administrator versus General access.

Device Details	Accesses the "Device Details" display. **NOTE:** This option is disabled if multiple devices are selected.
Device Identification	Accesses the "Device Identification" display. **NOTE:** This option is disabled if multiple devices are selected.
Group	**View Group Membership**: Accesses the "View Group Membership" display. **NOTE:** This option is disabled if multiple devices are selected. **Remove Device from Selected Group**: Removes selected devices from the group (or sub-group) highlighted in the "Device Groups" frame. **NOTE:** Unless a device is assigned to another group it is moved to the **Unassigned** group. **Remove Device from All Assigned Groups**: Moves selected devices to the **Unassigned** group from any groups (or sub-groups) to which they are assigned.
HTTP Properties	Accesses the "HTTP Properties" display.
Rack Properties	Accesses the "Set Rack Properties" display. **NOTE:** This option is disabled if multiple devices are selected.

Remove Devices	The InfraStruXure Manager server will no longer monitor the selected devices. **NOTE:** This option is disabled during a discovery. See Add Devices.
Register as a Trap Receiver **Unregister as a Trap Receiver**	These options control whether the InfraStruXure Manager server will receive SNMP traps from a selected device. When multiple devices are highlighted, one of these options will be enabled if all selected devices can use the same option (**Register** or **Unregister)**. Otherwise, both are disabled. **NOTE:** The trap receiver options are disabled for InfraStruXure PDUs and for some Metered Rack PDUs. To use the InfraStruXure Manager server as a trap receiver for other devices, see Trap receiver feature.
Notification	Accesses the options involved in the Disable Notifications for Maintenance feature. **NOTE:** All **Notification** options are disabled during a discovery. See Add Devices.
Mass Configuration	Accesses the options involved in the Mass Configuration feature.
View Data Log	Creates a data log for the selected device. **NOTE:** If a data log cannot be generated for the type of device selected, an error message appears. For information about the available logs, see Data logs.

"Set Rack Properties" display

Use this display to do the following:

Edit the **Power Settings** only when they are known to be inaccurate. For information about how these settings are initially assigned to a Metered or Switched Rack PDU, and how the settings are used to determine the kWatt values for the racks, see Rack kWatt values.

Rack Name	Select the rack name to be assigned. **NOTE:** Use **New** to add a rack name to the list.
Power Settings (Metered and Switched Rack PDUs only)	
Voltage	Edit the AC voltage (VAC) rating.
Power Factor	Edit the power factor.

"Device Identification" display

Use this display to define the **System Name**, **Contact**, and **Location** values for the selected device.

"View Group Membership" display

Use this display to view the list of device groups and sub-groups to which the selected device is assigned.

"Device Details" display

Overview

To access more details for a monitored device:

- Double-click a device in the "Device List" frame.
- Highlight a device in the "Device List" frame and select the **Device Details** option in the View menu.
- Right-click a device in the "Device List" frame and select the **Device Details** option in the right-click menu.
- Double-click a device in an Event log, or in the Reports and Data logs.

The type of details display that appears depends on the selected device:

- For monitored InfraStruXure Manager servers, the "Server Log On" display appears.
- For InfraStruXure PDUs, an InfraStruXure PDU details display appears.
- For some Metered Rack Power Distribution Unit (Rack PDU) versions, a Metered Rack PDU details display appears.
- For all other devices, an HTML "Device Details" display allows direct access to the management application at the device.

HTML "Device Details" display

With the exception of the devices identified in the Overview, the InfraStruXure Manager server uses this display to directly accesses the management application for its monitored devices.

- If the device uses a PowerChute Business Edition (PCBE) Agent to connect to the network, that agent's logon display appears for all users, including the Administrator.
- If the device uses a management card to connect to the network, and the settings in the "HTTP Properties" display are properly defined, the following occurs:
  - For the Administrator, the management application for the device is displayed automatically in the HTML frame.
  - For a General user, a logon display appears.

For more information about Administrator and General access, see Administrator versus General access.

In addition to displaying a **Refresh** button, the HTML frame identifies whether the InfraStruXure Manager server is reporting a **Normal**, **Warning** or **Critical** status for the device. You can click a drop-down menu to identify the warning or critical conditions that exist. Typically this status matches the status the device is reporting. However, the status can report violations of the InfraStruXure Manager Global Device Thresholds, thresholds which have no direct effect on the device.

See also

To use a management application that appears in the HTML frame, see the help for that application, as well as any documentation, such as a users guide, that may be available.

"HTTP Properties" display

Use this display to define the parameters the InfraStruXure Manager server uses to access the management card at a monitored device using the HTML "Device Details" display.

Username and **Password**	Identifies the values the InfraStruXure Manager server uses to log on to a device's management card automatically. The automatic logon occurs only for the InfraStruXure Manager Administrator, and not for a General user. To use the HTML "Device Details" display to access a device, the username or password must match the access values required for administrative access to that device's management card. **NOTE:** For more information about the two levels of access, see Administrator versus General access.
Port Number	Identifies the port used for HTTP (80, by default) or HTTPS (443, by default) communication with the device's management card. To use the HTML "Device Details" display to access a device, this port number must match the port number used at that device's management card. **NOTE:** To access the logon display for a PCBE agent, this port number must be 3052.
Protocol	Identifies the protocol used to communicate with the device's management card. To use the HTML "Device Details" display to access a device, this protocol must match the protocol used at that device's management card. **NOTE:** To access the logon display for a PCBE agent, HTTP must be the selected protocol.

InfraStruXure PDU details

Overview

This "Device Details" display includes device information, and up to ten **Status** options, depending on the InfraStruXure Power Distribution Unit (PDU) type. Except for **Output Power**, **System Breakers**, and **System Components**, the **Status** options provide thresholds and other configurable settings.

One **Status** option, **Bypass Input,** is available only for a dual-input InfraStruXure PDU.

Device Information (General option)	Identifies the device by its **Model Name**, **Model Number**, **Serial Number**, **Manufacture Date**, **Firmware Revision**, and **Hardware Revision**.
Branch Breakers	Accesses four tabs that each display 21 breakers, and that provide settings that describe those breakers.
Bypass Input	Accesses information about the bypass input voltage for a dual-input InfraStruXure PDU, as well as settings for three thresholds.
Contact Closures	**Contact**: Identifies each contact zone by number.
	Name: Identifies the user-configurable description assigned to each zone.
	Normal State: Identifies either **Open** or **Closed** as the normal position for each contact.
	Current State: Identifies the status of each contact.

Ground Monitor	**Current**: Identifies the ground wire current.
	Threshold: Identifies the ground current, in amps, at or above which a threshold violation occurs.
	Alarm: Identifies whether a violation of the ground-current threshold exists.
Main Input	Accesses information about the main input voltage, and settings for the input voltage thresholds.
Output Current	Accesses information about the output current, and settings for the output current thresholds.
Output Power	**Maximum Power**: Identifies the maximum power output rating for the InfraStruXure PDU.
	Load (kVA): Identifies the maximum load, in kVA, that each phase can support.
	Load (kWatts): Identifies the maximum load, in kilowatts, that each phase can support.
	Power Factor: Identifies the power factor for each phase, as well as the overall power factor for all phases.
	Total kWatts: Identifies the total kilowatts for all phases.
	Total kVA: Identifies the total kVA for all phases.
Output Voltage	Accesses information about the output voltage, and settings for the output voltage thresholds.

System Breakers	**Input Breakers**: Identifies the **Main Input Breaker Position** (**Open** or **Closed**) and **Main Input Breaker Rating**. For a dual-input InfraStruXure PDU, the **Bypass Input Breaker Position** (**Open** or **Closed**) and **Cross Tie Breaker Position** (**Open**, **Closed**, or **Not Installed**) are identified. **NOTE:** A single-input InfraStruXure PDU reports **Not Installed** for both the **Bypass Input Breaker Position** and **Cross Tie Breaker Position**.
	Q Breakers: Identifies the **Q-Breaker Mode**, and the position and rating for the Q1, Q2, and Q3 breakers, for InfraStruXure PDUs that have these breakers. **NOTE:** See Q-Breaker Modes.
	Panel Feed Breaker: Identifies the **Panel Feed** status for InfraStruXure PDUs that have this breaker (no Q breakers).
System Components	Identifies the components that the InfraStruXure PDU includes, and whether the **Emergency Power Off (EPO) Mode** is armed.

Branch Breakers

Up to four tabs representation the InfraStruXure PDU breaker panels. Each tab illustrates 21 breaker positions:

- **Positions 1-41**: Displays odd-numbered breakers from 1 through 41
- **Positions 2-42**: Displays even-numbered breakers from 2 through 42
- **Positions 43-83**: Displays odd-numbered breakers from 43 through 83
- **Positions 44-84**: Displays even-numbered breakers from 44 through 84

Each tab provides the following information about its positions:

RDP Feed	Identifies whether a breaker supports a remote distribution panel (RDP).
Current (Amps)	Identifies the output current for each breaker.
Alarm	Identifies whether an overcurrent or undercurrent threshold violation exists at a breaker.
Description	Identifies a description for each breaker which typically identifies the racks or devices that connect to each breaker for power.
Breaker Rating	Identifies the maximum current each breaker can support without being tripped.
Undercurrent (%)	Identifies, as a percentage of the **Breaker Rating**, the current that will result in an undercurrent alarm for each breaker.
Overcurrent (%)	Identifies, as a percentage of the **Breaker Rating**, the current that will result in an overcurrent alarm for each breaker.

The **Rating (Amps)**, **Description**, **Overcurrent (%)**, and **Undercurrent (%)** columns report information defined by settings in the "PDU Breaker Panel Settings" display for each position.

Unless a current monitoring sensor board is installed at the breaker panel, no values are displayed for the **Current (Amps)**, **Overcurrent (%)**, **Undercurrent (%)**, and **Alarm** columns, and the **Overcurrent** and **Undercurrent** thresholds are disabled in the "PDU Breaker Panel Settings" display.

The "PDU Breaker Panel Settings" display, accessed by double-clicking a listed position, includes a **Tied to Next Panel Position** option to identify whether the breaker position is linked to the next position at the breaker panel.

Any change made to a **Breaker Rating** or threshold setting for a position in the "PDU Breaker Panel Settings" display will change that setting at any positions tied to the changed position.

Bypass Input

Use this InfraStruXure PDU details **Status** option to view information about the bypass input power at a dual-input InfraStruXure PDU, and to set voltage thresholds.

Voltage Table	Identifies the phase-to-phase (**L-L**) and phase-to-neutral (**L-N**) voltages for each phase, and identifies whether a phase has an alarm.
Undervoltage Threshold	Defines the percentage of the phase-to-neutral (**L-N**) voltage to be used to determine if an undervoltage exists at any phase.
Overvoltage Threshold	Defines the percentage of the phase-to-neutral (**L-N**) voltage to be used to determine if an overvoltage exists at any phase.

Main Input

Use this InfraStruXure PDU details **Status** option to view information about the main input power, and to set voltage thresholds.

Nominal Input Voltage	Identifies the voltage rating for the main input.
Input Voltage Table	Identifies the line-to-line voltages present for **L1-2**, **L2-3**, and **L3-1**, when a transformer is part of the InfraStruXure PDU, and identifies whether a phase has an alarm. **NOTE:** When a transformer is not present, the **L1**, **L2**, and **L3** voltages are reported.
Undervoltage Threshold	Defines a percentage of the **Nominal Input Voltage** to be used to determine if an undervoltage exists at any phase.
Overvoltage Threshold	Defines a percentage of the **Nominal Input Voltage** to be used to determine if an overvoltage exists at any phase.

Output Current

Use this InfraStruXure PDU details **Status** option to view information about the output current, and to set current thresholds.

Current Information	**Panel Breaker Rating**: Identifies the total Amps the branch breaker panel is rated to support.
	Current (Amps): Identifies the current present on each phase.
	Alarms: Identifies whether a violation of an overcurrent or undercurrent threshold exists at a phase.
	Undercurrent Threshold: Defines a percentage of the rated current that will be used to determine if an undercurrent exists at an output phase.
	Overcurrent Threshold: Defines a percentage of the rated current that will be used to determine if an overcurrent exists at an output phase.
Neutral Current	**Current (Amps)**: Identifies the rated neutral current.
	Threshold: Defines a percentage of the rated neutral current that will be used to determine if an overcurrent exists.
	Alarms: Identifies whether a violation of the neutral overcurrent threshold exists.

Output Voltage

Use this InfraStruXure PDU details **Status** option to view information about the output voltage, and to set voltage thresholds.

Output Information	**Voltage Table**: Identifies the phase-to-phase (**L**-**L**) and phase-to-neutral (**L**-**N**) voltages for each phase, and identifies whether a phase has an alarm.
	Undervoltage Threshold (L-N): Defines the percentage of the phase-to-neutral (**L**-**N**) voltage to be used to determine if an undervoltage exists at any phase.
	Overvoltage Threshold (L-N): Defines the percentage of the phase-to-neutral (**L**-**N**) voltage to be used to determine if an overvoltage exists at any phase.
Frequency	**Frequency**: Identifies the frequency, in Hz, of the output voltage.
	Threshold Range (+/-): Defines the variance, in Hz, from the rated frequency that will cause a threshold violation.
	Alarms: Identifies whether a violation of the frequency threshold exists.

Q-Breaker Modes

The **Q-Breaker Mode** is determined by the open and closed conditions of the **Q1**, **Q2**, and **Q3** circuit breakers, as described in the following table.

Each of the modes represents an informational, warning, or critical InfraStruXure PDU event. The table identifies the severity level for each mode.

System Off (Critical)	All three Q breakers open. If the UPS is on, it switches to battery operation due to the loss of input voltage (**Q1** open); however, **Q2** open prevents any output from the UPS from reaching the breaker panel, and **Q3** open prevents the InfraStruXure PDU input voltage from being routed to the breaker panel.
On Battery (Warning)	**Q1** and **Q3** open, **Q2** closed. The UPS switches to battery operation due to the loss of input voltage (**Q1** open); **Q2** closed allows the battery-generated output power from the UPS to be passed to the breaker panel; **Q3** open prevents the InfraStruXure PDU from routing its input voltage to the breaker panel.
Maintenance Bypass (Informational)	**Q1** and **Q2** open, **Q3** closed. Maintenance at the UPS can be performed while the UPS is isolated from the InfraStruXure PDU (**Q1** and **Q2** open); **Q3** closed routes the InfraStruXure PDU input voltage to the breaker panel.
Q1 Atypical Bypass (Warning)	**Q1** open, **Q2** and **Q3** closed. The UPS switches to battery operation due to the loss of input voltage (**Q1** open); the battery-generated output power from the UPS (**Q2** closed) and the InfraStruXure PDU input voltage (**Q3** closed) are both routed to the breaker panel.

No Panel Feed (Critical)	**Q2** and **Q3** open, **Q1** closed. The InfraStruXure PDU input voltage is routed to the UPS (**Q1** closed), but no power is provided to the breaker panel by either the UPS (**Q2** open) or the InfraStruXure PDU input voltage (**Q3** open). **NOTE:** For an InfraStruXure PDU without Q breakers, this mode indicates that the panel feed breaker is open.
UPS Operation (Informational)	**Q3** open, **Q1** and **Q2** closed. The InfraStruXure PDU input voltage is routed to the UPS (**Q1** closed), and the output from the UPS is routed to the breaker panel (**Q2** closed); **Q3** open prevents the InfraStruXure PDU from routing its input voltage to the breaker panel.
Q2 Atypical Bypass (Warning)	**Q2** open, **Q1** and **Q3** closed. The InfraStruXure PDU input voltage is routed to the UPS (**Q1** closed), but no power is provided to the breaker by the UPS (**Q2** open); the InfraStruXure PDU input voltage is routed to the breaker panel (**Q3** closed).
Forced Bypass (Critical)	All three Q breakers closed. The InfraStruXure PDU input voltage is routed to the UPS (**Q1** closed) and to the breaker panel (**Q3** closed); output power from the UPS is also routed to the breaker panel (**Q2** closed).

Metered Rack PDU details

The InfraStruXure Manager server can use the HTML “Device Details” display to access the management application for most Metered Rack PDUs. This Metered Rack PDU “Device Details” display provides device information, **Configuration** (**Settings**), and **Status** options for the Metered Rack PDU models that cannot be accessed using the HTML “Device Details” display.

Device Information (General option)	Identifies the device by its **Model Name**, **Model Number**, **Serial Number**, **Manufacture Date**, **Firmware Revision**, and **Hardware Revision**.
Settings (Configuration option)	Defines **L1**-through-**L3** current and load thresholds for 3-phase Metered Rack PDUs, or **L1**, for single-phase models: **Overload**: If the available current is at or above the defined Amps, an overload event occurs. **Overcurrent**: If the available current is at or above the defined Amps, an overcurrent event occurs. **Undercurrent**: If the available current falls below the defined Amps, an undercurrent event occurs. **NOTE:** If the **Undercurrent** threshold is **0**, an undercurrent event occurs when the current falls to 0 Amps. The threshold settings must follow this rule: **0** <= **Undercurrent** < **Overcurrent** <=**Overload** <=**22 Amps** Attempts to define threshold values that violate this rule will fail: • If the **Undercurrent** threshold is **5**, to change the **Overcurrent** threshold to **5** or less you must first change the **Undercurrent** threshold to a value that is less than the **Overcurrent** threshold you want to set, and click **Apply** to save that change. • If the **Overcurrent** threshold is **12**, to change the **Overload** threshold to less than **12** you must first change the **Overcurrent** threshold to a value that it is equal to or less than the **Overload** threshold you want to set, and click **Apply** to save that change.
	Enable Audible Alarm: Enables (the default setting) or disables the audible alarm at the Metered Rack PDU.

Outlet Status (Status option)	Uses a icon to report the status of each available phase, and provides the following information for a phase: **Current**: Identifies the output current, in Amps **Threshold**: Identifies the acceptable current range, as defined by the **Undercurrent** and **Overcurrent** threshold settings in the **Settings** option. **Overload**: Identifies the current, in Amps, that represents an overload, as defined by the **Overload** threshold setting in **Settings** option. **Status**: Reports **Normal**, for no threshold violations, or identifies a violated threshold (**Undercurrent**, **Overcurrent**, or **Overload**).

"Recommended Actions" frame

This frame displays information about the device selected in the "Device List" frame:

Note

No information is displayed when multiple devices are highlighted.

- **Hostname**, **Model Name**, **Contact**, and **Location** values for the device
- A title that identifies the current condition, and a status icon that identifies its severity

For more information about status icons and the conditions they represent, see Status and event severity levels.

- A description of the condition
- The recommended actions

Note

If multiple warning or critical conditions exist, each condition is listed.

"Power Zones" display

This display appears when you select the **Power Zones** option in the navigation bar or View menu. It has three main elements:

"Power Zones" frame	The left frame lists the Power zones and allows you to select which Power Zone or Power Source is displayed in the **Devices** or **Diagram** tabs.
Devices tab	This tab has two frames: • The "Device List" frame provides status and "Configure Columns" display information for the devices assigned to the zone or source selected in the "Power Zones" frame. • The "Recommended Actions" frame provides more detail about the status of the device selected in the "Device List" frame. **NOTE:** Double-clicking a device accesses its management application, or a display that provides more information about that device. See "Device Details" display.
Diagram tab	This tab displays the diagrams for the Power zones you created. **NOTE:** For information about the two basic types of diagrams, see InfraStruXure PDU diagrams and Device diagrams.

Power zones

Overview

The power zones feature allows you to create diagrams that represent the path that power travels, from a power source, through the APC power distribution devices, to the load equipment those devices support.

You create the diagrams by assigning the power sources and the monitored devices to a power zone in the "Power Zones" frame; you use the procedures provided in Power zone management to manage those power zones.

"Power Zones" frame

This frame lists the power zones you create, as well as two selections which cannot be deleted or renamed:

- **All Devices**: When selected, all the devices the InfraStruXure Manager server monitors are listed in the **Devices** tab.
- **Unassigned**: When selected, all the devices not currently assigned to a power zone are listed in the **Devices** tab.

For more information about the **Devices** tab, see "Device List" frame.

No diagrams appear in the **Diagrams** tab when **All Devices** or **Unassigned** is selected. The type of diagram that appears for a power zone depends on the following:

- InfraStruXure PDU diagrams: Illustrate power zones that have one of the following InfraStruXure PDUs assigned to at least one power source:
  - 60 kW or 150 kW InfraStruXure PDU: A PDU with a panel feed breaker that is typically used with a large, remote 3-phase UPS (Symmetra or Silcon) to provide power to the power zone breaker panels.
  - 40 kW or 80 kW InfraStruXure PDU: A PDU that typically provides input power to a 3-phase UPS (Symmetra or Silcon) assigned to the same power source as the PDU. The PDU and its associated UPS must both be assigned to the same power source before an InfraStruXure PDU diagram for that power source can be displayed in the **Diagrams** tab.
- Device diagrams: Illustrate the power relationship of devices assigned to a power zone that does not have an InfraStruXure PDU, or that has an InfraStruXure PDU with system breakers, but a 3-phase UPS (Symmetra or Silcon) has not yet been assigned to the same power source as that InfraStruXure PDU. For these power zones, a device diagram appears when a device is selected; no diagram appears when the power zone or a power source is selected.

For information about the icons used to indicate status conditions, see Status and event severity levels.

Power zone management

Two menus provide the options you use to manage the power zones when the "Power Zones" display is selected:

- Right-click menu: **Add Power Zone**, **Add Power Source**, **Rename**, and **Remove**
- Edit menu: **Add Power Zone**, **Add Power Source**, and **Remove Selected Zone or Source**

Unless you log on as the Administrator, these menu options are disabled. See Administrator versus General access.

You use the procedures described in the following table to create a power zone, as follows:

1. Add the power zone.
2. Add the power sources (at least one, but no more than two).
3. Assign the devices to the appropriate power source.
4. Arrange the devices in the order in which they connect with each other.
5. Assign the appropriate rack names to devices.

When the "Power Zones" display is selected, you can use the **Power Zones Wizard** option in the Edit menu to launch the InfraStruXure Manager Power Zones Wizard. This wizard automates the process of creating power zones for the devices the InfraStruXure Manager server monitors on its APC LAN.

To Add a Power Zone	1. Select **All Devices**. 2. Select the **Add Power Zone** option in the right-click or Edit menu.
To Add a Power Source	1. Select the power zone. 2. Select the **Add Power Source** option in the right-click or Edit menu.

To Assign Devices to a Power Source	1. Select the **Unassigned** device group. 2. In the **Devices** tab, select the devices you want to assign to the power source. 3. Drag the devices to the power sources.
To Arrange Devices	1. Select a device in the power zone and drag it to the device to which it connects for its power. 2. Repeat until all devices are connected in the order in which they receive power. **NOTE:** This procedure is critical to creating the diagrams described in Device diagrams; it has no affect on the diagrams described in InfraStruXure PDU diagrams except to represent the relationship of the devices assigned to a power zone, as displayed in the "Power Zones" frame.
To Set Rack Names	1. In the **Devices** tab, select all the devices to be assigned the same rack name. 2. Right-click any highlighted device and select the **Set Rack Name** option. 3. Assign the rack name, if the appropriate name is not already assigned. 4. Repeat the preceding steps to assign a different rack name to other devices. **NOTE:** This procedure is critical to creating the diagrams described in InfraStruXure PDU diagrams; it has no affect on the diagrams described in Device diagrams.
To Remove a Power Source or Power Zone	1. Select the zone or source. 2. Select the **Remove Selected Zone or Source** option in the right-click or Edit menu. **NOTE:** Any devices assigned to the deleted zone or source are moved to **Unassigned**; they are not deleted.
To Rename a Power Zone or Source	Right-click the power zone or power source, and select the **Rename** option.

InfraStruXure PDU diagrams

Overview

When a power zone contains a 60 kW or 150 kW InfraStruXure PDU, or a 40 kW or 80 kW InfraStruXure PDU that has its associated 3-phase UPS (Symmetra or Silcon) assigned to the same power source, a single diagram is created that identifies the following power zone components:

- The InfraStruXure PDUs
- The UPS associated with a system-bypass InfraStruXure PDU, when this type of PDU is assigned to the power zone
- The racks that have been identified as containing the devices assigned to the power zone
- The power path from the InfraStruXure PDUs to the racks.

In addition, the InfraStruXure PDU diagram does the following:

- For an InfraStruXure PDU:
  - Uses an icon to identify the severity associated with the identified InfraStruXure PDU breaker mode.
  - Includes status information for the InfraStruXure PDU contact closures.
  - Allows you to click an InfraStruXure PDU graphic to access the InfraStruXure PDU details for that PDU.
- For a 3-phase UPS (Symmetra or Silcon):
  - Uses an icon to identify the status of any UPS associated with a 40 kW or 80 kW InfraStruXure PDU.
  - Allows you to click a UPS graphic to access the HTML “Device Details” display for that UPS.

- For device racks:
  - Uses icons to report whether a warning or critical condition exists at one or more of the devices assigned to a rack. No icon appears for a rack when all of its devices are operating normally.
  - Allows you to click a rack graphic to access a list of the devices assigned to that rack, as well as information about the status and kWatts for the rack.

Double-clicking a rack's name accesses more information about that rack. See Configure Racks.

  - Allows you to click a listed device to access the "Device Details" display for that device.

For InfraStruXure PDU diagrams to accurately portray a power zone, each device assigned to that power zone must have its rack name defined: a rack appears in the diagram only when at least one device assigned to the power zone uses that rack name. See "Set Rack Properties" display.

For an example of what a power zone that uses an InfraStruXure PDU can look like in the "Power Zones" frame, see Power zone example; for an example of an InfraStruXure PDU diagram, see InfraStruXure PDU diagram example.

Power zone example

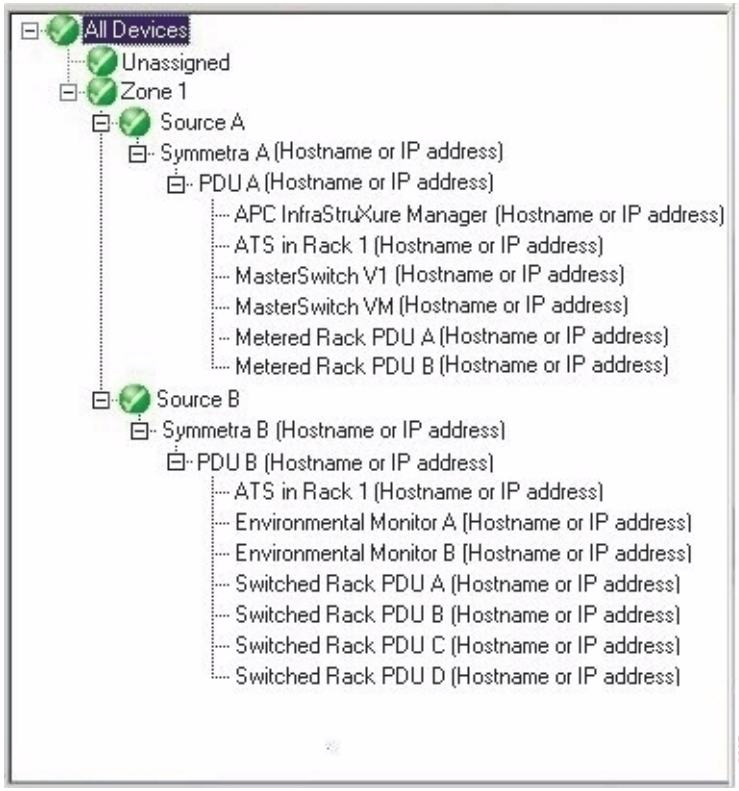
This example is for a dual-source power zone with a 40 kW or 80 kW InfraStruXure PDU and 3-phase Symmetra UPS for each power source. This example shows how the power zone would appear in the "Power Zones" frame.

Each device is identified in the "Power Zones" frame by its system name (if a system name has been defined), with its hostname (or IP address if no hostname is defined) in parentheses.

A power zone that uses an InfraStruXure PDU typically has more devices, and more device racks, than this example.

The power zone in this example was created using the InfraStruXure Manager Power Zones Wizard. Once a power zone is created, you can click and drag devices to arrange the devices in the order in which they receive power.

Arranging the devices has no affect on the power zone diagram. It only represents the power relationship of the devices as shown in the "Power Zones" frame.

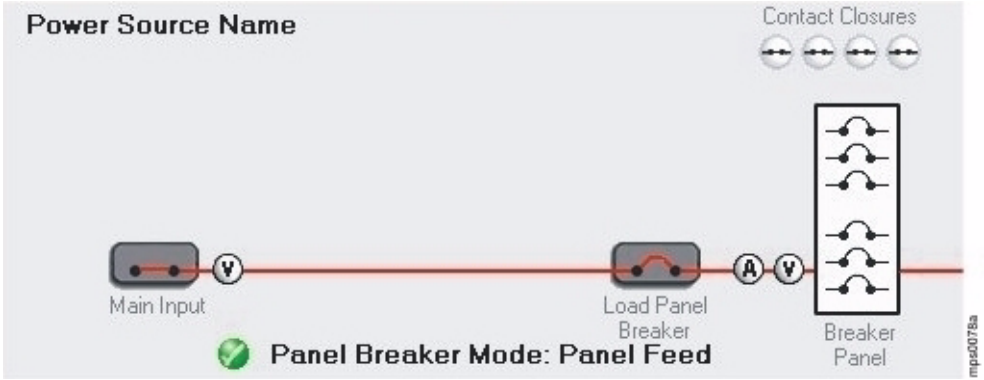


InfraStruXure PDU diagram example

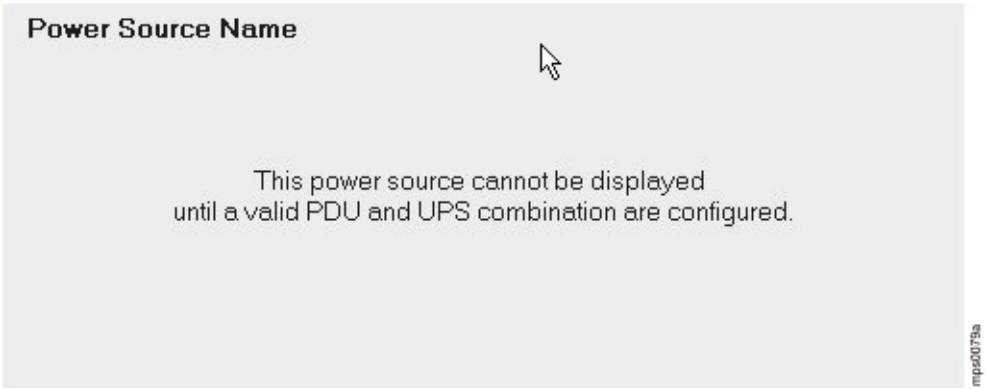
The example provided is for a power zone with a 40 kW or 80 kW InfraStruXure PDU and 3-phase Symmetra UPS for each power source. The following conditions would change the appearance of the InfraStruXure PDU diagram as described:

- For a power zone with only one power source, only one InfraStruXure PDU graphic appears in an InfraStruXure PDU diagram.

- For a power source with a 60 kW or 150 kW InfraStruXure PDU, the InfraStruXure PDU diagram uses this graphic to represent that power source:



- When two power sources are assigned to a power zone, and one of those sources does not have either a 60 kW or 150 kW InfraStruXure PDU, or a 40 kW or 80 kW InfraStruXure PDU and its associated 3-phase UPS (Symmetra or Silcon), assigned to it, the InfraStruXure PDU diagram uses this graphic to represent that power source:



For information about the legend that appears in the upper-right corner of all diagrams, see Diagram legend.

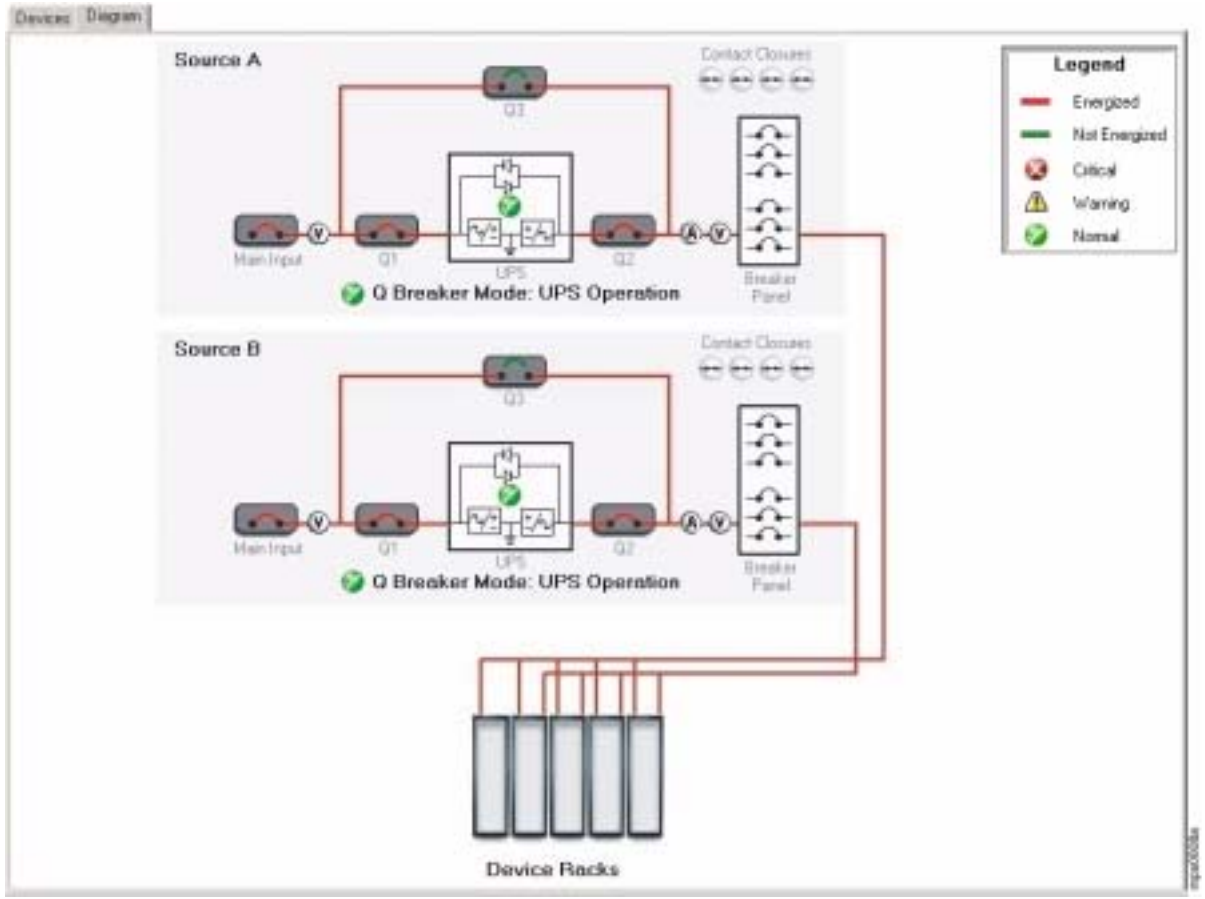

Devices
Diagram
Source A
Contact Closures
Q3
Main Input
Q1
UPS
Q2
Breaker Panel
Q Breaker Mode: UPS Operation
Source B
Contact Closures
Q3
Main Input
Q1
UPS
Q2
Breaker Panel
Q Breaker Mode: UPS Operation
Legend
Energized
Not Energized
Critical
Warning
Normal
Device Racks

Diagram legend

Every diagram, including the Device diagrams, includes a legend in the upper-right corner. This legend identifies the icons used to indicate **Critical**, **Warning**, and **Normal** conditions, as well as the power status of the power paths:

- Red lines illustrate power paths that have power present (**Energized**).
- Green lines illustrate power paths that have no power present (**Not Energized**).

For more information about the warning, critical, and normal conditions, see Status and event severity levels.

Device diagrams

Overview

When a power zone does not contain a power source that has either a 60 kW or 150 kW InfraStruXure PDU, or a 40 kW or 80 kW InfraStruXure PDU and the 3-phase UPS (Symmetra or Silcon) associated with that PDU, a set of diagrams is created. Each diagram identifies the power relationship for one of the devices assigned to that power zone.

Typically such a power zone would have only one source, but it could have two. The diagrams created for each source are independent of the other source, and only illustrate the devices assigned to that power source.

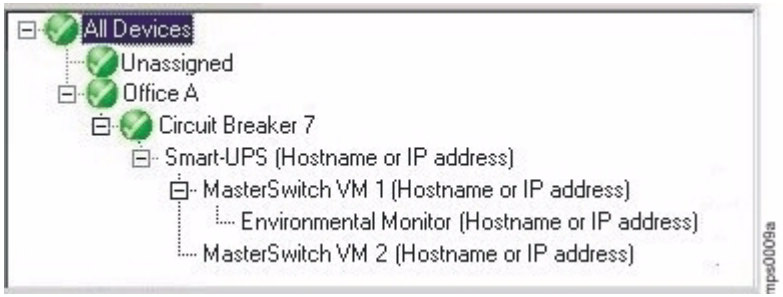
Each device that appears in a diagram is identified by model and system name, and an icon identifies the status of the device. You can click a device to access the "Device Details" display for that device. For these diagrams to accurately portray the power relationship of the devices within a power zone, the devices must be assigned to each other in the order in which they receive power. For example:

- In a power zone with a Smart-UPS that provides power to two MasterSwitch VM devices, the MasterSwitch VM devices must be assigned to the Smart-UPS.
- If one of the MasterSwitch VM devices provides power to another APC device, such as an Environmental Monitoring Unit, that APC device must be assigned to that MasterSwitch VM device.

For information about how the power zone described above would look, see Power zone example; for information about the types of diagrams that would appear for this example, see Diagram examples; for information about how to create power zones, including information about assigning devices, see Power zone management.

Power zone example

The following is power zone would appear in the "Power Zones" frame for the example cited in Device diagrams. Each device is identified in the "Power Zones" Frame by its system name (if a system name has been defined), with its hostname (or IP address if no hostname is defined) in parentheses:



The diagram that appears in the **Diagram** tab depends on the device you select in the power zone (no diagram appears when you select a power zone or power source). However, as shown in the Diagram examples, all diagrams show the selected device, any devices that receive power directly from that device, and all of the devices through which the selected device connects to the power source.

Diagram examples

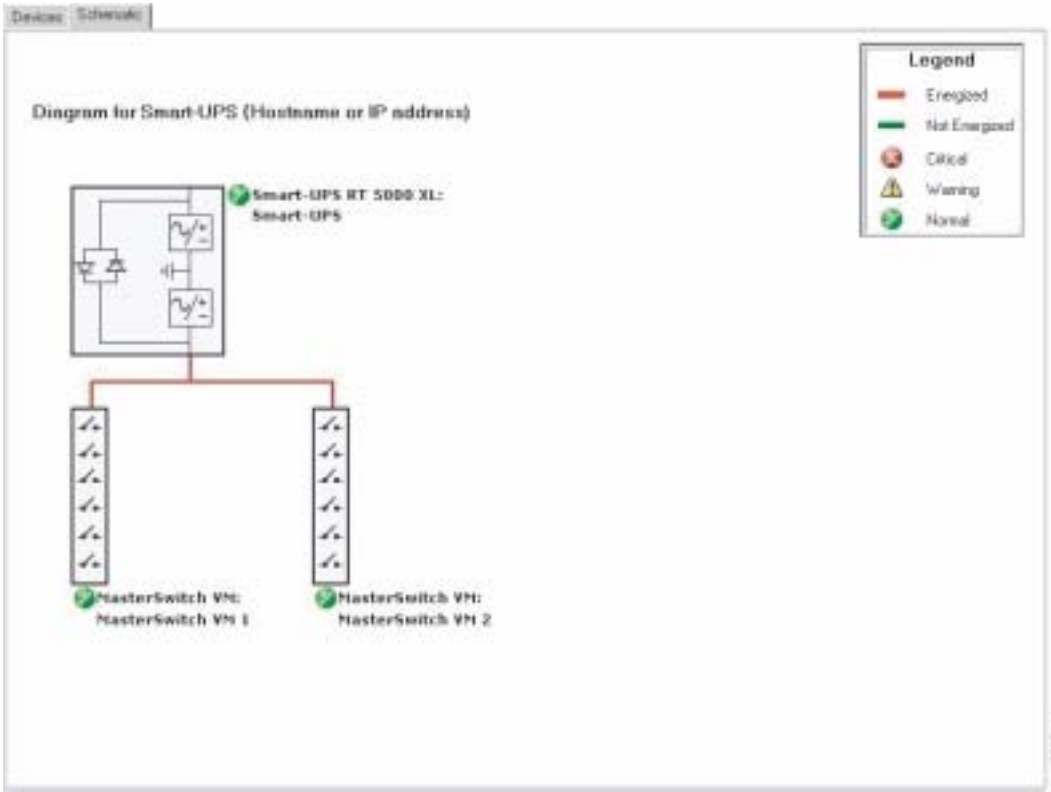
You can click a device graphic to access its "Device Details" display.

- Smart-UPS diagram
- MasterSwitch VM 1 (or Environmental Monitor) diagram
- MasterSwitch VM 2 diagram

For information about the legend in the upper-right corner of each diagram, see Diagram legend.

Smart-UPS diagram. The Smart-UPS in the Power zone example was selected.

- The Smart-UPS provides the power for the power source.
- The only APC devices that obtain power directly from the Smart-UPS are two MasterSwitch VM devices.

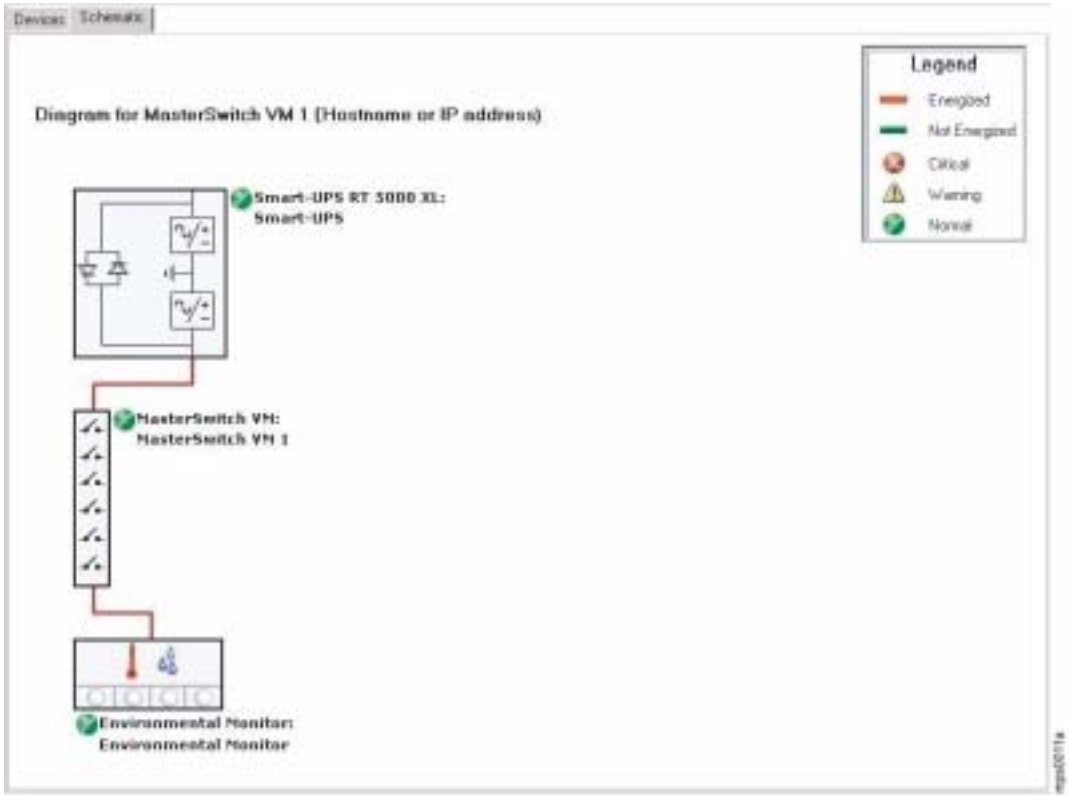


MasterSwitch VM 1 (or Environmental Monitor) diagram. The MasterSwitch VM 1 device in the Power zone example was selected.

- The Smart-UPS provides the power for the power source.
- The MasterSwitch VM device, which obtains its power from the Smart-UPS, provides power to the environmental monitoring device.

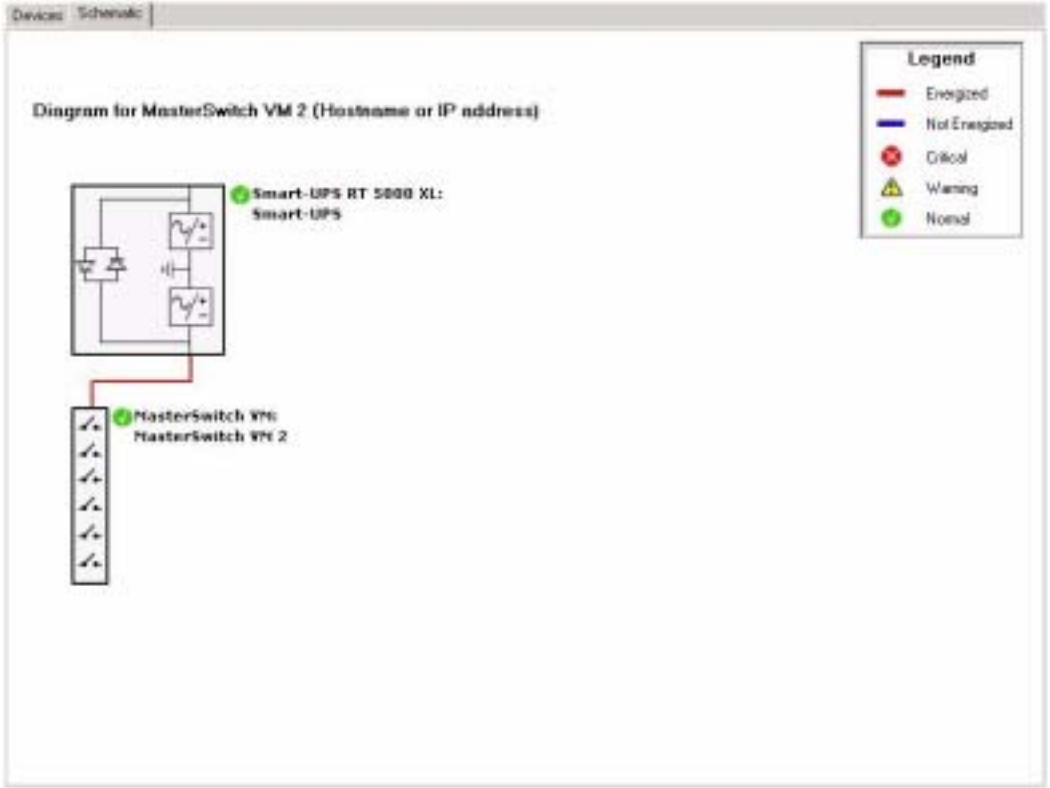
Note

The same basic diagram (but with a different name) would appear if the Environmental Monitoring Unit was selected, since all diagrams show the APC devices through which a selected device obtains its power.



MasterSwitch VM 2 diagram. The MasterSwitch VM 2 device in the Power zone example was selected.

- The Smart-UPS is the source of power for the other
- The MasterSwitch VM device, obtains its power from the Smart-UPS, provides no power to other APC devices.



"Reports" display

This display appears when you select the **Reports** option in the navigation bar or View menu.

The left frame groups the available reports by main report type: **Environmental**, **Exceptions**, **Rack PDU**, and **UPS**. When you select a report from the left frame, a "Select Report Filter" display allows you to identify the device groups to include in the report. For one report, **Downtime**, this filter also allows you to define the date range covered by the report.

See Reports.

"Logs" display

This display appears when you select the **Logs** option in the navigation bar or View menu.

Use the **Log Type** options to select the type of log you want to create:

- An Event log records information about status changes that occur at the monitored devices, as well as system information about the InfraStruXure Manager server.
- Data logs record information about the monitored ATS, InfraStruXure PDU, Rack PDU, Symmetra UPS, Silcon UPS, and environmental devices.

File menu

Overview

Use the menu options to do the following:

Change Server	Log on to a different InfraStruXure Manager v4.4 server using the "Server Log On" display. **NOTE:** You cannot use this option to log on to any other InfraStruXure Manager version.
Backup Server	Save InfraStruXure Manager configuration settings, including the definitions for the Device groups and Power zones, to a backup (*.apc) file. **NOTE:** The settings for the Client Preferences option in the System Management menu are not saved in the *.apc file. These settings are specific to each InfraStruXure Manager client.
Restore Server	Import settings from a backup (*.apc) file.
Print Device List	Print a copy of the devices listed in the "Device List" frame. **NOTE:** Which devices are listed depends on the group selected in the "Device Groups" frame, including the **All Devices** or **Unassigned** selections.
Exit	End the InfraStruXure Manager session.

Backup Server

Use the display for this File menu option to export InfraStruXure Manager configuration settings, including the definitions for the Device groups and Power zones, to an InfraStruXure Manager backup (*apc) file.

The settings for the Client Preferences option in the System Management menu are not saved in the *.apc file. These preferences are specific to each InfraStruXure Manager client.

The Restore Server option is used to import *.apc file settings at an InfraStruXure Manager server, or its replacement.

1. Click **Browse**.
2. Navigate to an *.apc file or to the folder in which a new file will be created.
3. Select an existing file, or create a new one, and click **Save**.
4. Enter the **FTP Username** and **FTP Password**, and click **Backup**.

To change the FTP values (lowercase **apc**, by default, for both), see FTP Server Settings.

Restore Server

Use the display for this File menu option to import configuration settings from an *.apc file that contains configuration settings that were saved using the Backup Server option:

1. Use **Browse** to navigate to the *.apc file.
2. Select the file and click **Open**.
3. Enter the **FTP Username** and **FTP Password**, and click **Restore**.

To change the FTP values (lowercase **apc**, by default, for both), see FTP Server Settings.

"Server Log On" display

To log on to an InfraStruXure Manager server:

Note

The InfraStruXure Manager server and client versions must be compatible, or the logon will fail. For example, you cannot use a v4.2 client to log on to a v4.0-v4.1.x server.

1. Identify the **Server**.

   Note

   The server is already identified when you access this display using the listing for a monitored InfraStruXure Manager server in the "Device List" frame.

2. Enter the server's **Password** and **Username**.
3. Click **Connect**.

   Note

   A "Could not log on" error occurs if the username or password is invalid, or the InfraStruXure Manager client and server versions are not compatible. A "Could not connect" error occurs if the InfraStruXure Manager client fails to connect to the server, the server you identified does not exist, the client is disconnected from the network, or the server is not operating normally.

Edit menu

Overview

Use the menu options to do the following:

Unless you log on as the Administrator, these menu options are disabled. See Administrator versus General access.

Add Devices	Access the "Add Devices" display to discover new devices for the InfraStruXure Manager server to monitor.
Remove Selected Devices	Remove devices from the list of devices the InfraStruXure Manager server monitors. **NOTE:** This option is disabled during a discovery. See Add Devices.
Set Rack Properties for Selected Device	Access the "Set Rack Properties" display for the device selected in the "Device List" frame.
Set HTTP Properties for Selected Devices	Access the "HTTP Properties" display for the device or devices selected in the "Device List" frame.
Notification	Access the options involved in the Disable Notifications for Maintenance feature.
Add or Remove Device Group	Manage the device groups, as described in Device group management.
Add Power Zone	Add a power zone, as described in Power zone management. **NOTE:** This option is active only when **All Devices** is selected in the "Power Zones" frame.
Add Power Source	Add a power source to a selected power zone, as described in Power zone management. **NOTE:** A power zone must have one or two power sources assigned.
Remove Selected Zone or Source	Remove a selected power source or power zone.
Power Zones Wizard	Launch the InfraStruXure Manager Power Zones Wizard.

Add Devices

Use the display for this Edit menu option to discover and add Supported devices on the User LAN (corporate network) to the list of devices the InfraStruXure Manager server monitors.

Supported devices on the APC LAN are discovered automatically. For more information about the two LANs, see APC and User Local Area Networks (LANs).

You cannot remove devices or use any **Notification** options during a discovery.

During a discovery, only the IP addresses you define are searched for APC devices.

Before an APC device can be discovered, its read community name must be listed in the "Device Access" display (**SNMP** tab); for a Switched Rack PDU or newer Metered Rack PDU version, the username and password used for administrator access must also be listed in the "Device Access" display (**Administrator Accounts** tab). In addition, some devices use an initialization file to provide the information the InfraStruXure Manager server needs to fully monitor that file's device. For such devices, the administrator access settings must be defined in the FTP Settings tab before the InfraStruXure Manager can download an initialization file from those devices.

1. Select a tab:
   - **Network Address**: To define a single IP address.
   - **Network Segment**: To define all IP addresses for a specified network segment.
   - **Network Address Range:** To define a dedicated range of IP addresses that can include multiple network segments. For example, to search a User LAN that reserves 100 through 200 on the XXX.XXX.14.* through XXX.XXX.17.* network segments for APC devices, do the following:
     - Use **XXX.XXX.14.100** for the **IP Range Start** value.
     - Use ***.*.17.200** for the **IP Range End** value.
   - **Import**: To import a user-defined list of network IP addresses from a *.csv or *.txt file.

     Note: This user-defined file, which can use a DOS or UNIX format, must contain numerical IP addresses only (255.255.255.1, for example). The IP addresses can be delimited by tab, space, comma, line-feed or end-of-line characters.

     - Use **Browse** to locate and select the file.
     - When the file appears in the **Import** tab, click **Import Now**.
2. Click **Add** to list the IP addresses in the **Network Addresses to Search** box.

   Note: Right-click an address and click **Delete** to remove it from the **Network Addresses to Search** list.
3. Repeat step 1 and step 2 to list all the IP addresses to be searched.

4. Disable the **Configure SNMP Agents to Send Traps to Server** option if you do not want the InfraStruXure Manager server to be a trap receiver for any discovered devices.

   For more information about whether monitored devices will use the InfraStruXure Manager server as a trap receiver, see Trap receiver feature.

5. Click **Apply**.
6. Click **Yes** to initiate the discovery process.

   Note

   Discovered devices are listed under **Unassigned** in the "Device Groups" frame.

Disable Notifications for Maintenance

Use the display for this **Notification** option in the Edit menu (or in a device's right-click menu) to disable notifications for any device or devices selected in the "Device List" frame.

Notification options are disabled during a discovery. See Add Devices.

- Identify why notifications were disabled (**Reason**).
- Define how long notifications will be disabled:
  - The **Duration** settings define how long notifications will be disabled before they are enabled automatically.
  - The **Disable notification indefinitely** option disables notifications until the **Enable Notifications** option is used.

When notifications are disabled:

- Event log entries for affected devices identify when the notifications were disabled and when they were enabled again.
- In the "Device List" frame, the information for affected devices is italicized and the regular status icons are replaced.

	If a critical condition was reported for a device when its notifications were disabled, a wrench with a red circle appears; if the device status was normal, or a warning condition existed, a wrench with a yellow triangle appears. You can click a device to view its status in the "Recommended Actions" frame: a warning or critical condition is reported along with the disabled-notifications condition; only the disabled-notifications condition is reported when the status is normal.

The following table describes the other **Notification** options.

Enable Notifications	Manually enables notifications again. **NOTE:** This option is enabled only when at least one device with disabled notifications is selected.
Notification Settings for Selected Device	Views information about why the notifications were disabled, and when they will be enabled again. **NOTE:** This option is disabled if multiple devices are selected, or notifications are enabled for the selected device.

View menu

Overview

Use the menu options to do the following:

Device Status	Access the "Device Status" display.
Power Zones	Access the "Power Zones" display.
Reports	Access the "Reports" display.
Logs	Access the "Logs" display.
Incidents	Access the "Incident Management" display. **NOTE:** This option, the **Incident Management** option in the navigation bar, and the Incident Management menu, appear only when the Incident management module is activated.
Device Details	Access the "Device Details" display for the device selected in the "Device List" frame.
Device Identification	Access the "Device Identification" display for the device selected in the "Device List" frame.
View Group Membership	Access the "View Group Membership" display that lists all the device groups to which the device selected in the "Device List" frame is assigned.
Refresh	Refresh the "Device Status" display or "Power Zones" display.
Configure Columns	Access the "Configure Columns" display.

"Configure Columns" display

This display defines what type of information appears for devices listed in the "Device List" frame, as well as the columns displayed for a selected log or report. How this display is used depends on the selected feature:

- When the "Device Status" display (or **Devices** in the "Power Zones" display) is selected: Use **Configure Columns** in the View menu (or in the right-click menu for any column heading in the "Device List" frame) to select what type of information will appear in the device list.
- When any log or report is displayed: Use **Configure Columns** in the View menu to select which columns will appear in the displayed, printed, or filed versions of a report or log.
  - The "Configure Columns" display lists only the columns that are specific to the selected report or log.
  - Only enabled columns are included in saved, printed, or displayed versions of the selected report or log.
- When the Incident management module is enabled: Right-click a column in the "Incident Management" display to select which columns will appear in that display.

Event Management menu

Overview

Use the menu options to do the following:

Unless you log on as the Administrator, these menu options are disabled. See Administrator versus General access.

Global Device Thresholds	Define values for thresholds the InfraStruXure Manager server applies to devices it monitors.
SNMP Trap Forwarding	Enable the InfraStruXure Manager server to forward SNMP traps to the identified IP addresses.
Building Management System	Define settings that allow the Building Management System (BMS) to get data from devices that the InfraStruXure Manager server monitors.
Remote Monitoring Service	Register to use the APC Remote Monitoring Service (RMS).

Global Device Thresholds

Overview

Use the display tabs for this Event Management menu option to define the global device thresholds the InfraStruXure Manager server applies to devices it monitors, and to schedule notifications for device group summaries, summaries which include information about any global threshold violations.

The global device thresholds allow the InfraStruXure Manager server to change a single threshold setting that is used to monitor every device that uses that threshold, without the need to change the local threshold setting at the monitored devices. Global device threshold settings are independent of the local device thresholds, so that changes to the InfraStruXure Manager global device thresholds will not change the local threshold settings at monitored devices.

If a value violates the local threshold at a device and the global device threshold at the InfraStruXure Manager server, both threshold-violation events will be reported.

- UPS tab
- Environmental Monitor tab
- Metered Rack PDU tab
- Schedule tab

An Exceptions Summary report includes information about existing global device threshold violations and certain status events (lost-communication, bad-battery, and self-test failed).

UPS tab

Defines values the InfraStruXure Manager server monitors for all UPS systems in its device list. The Global Device Thresholds and corresponding local device thresholds are independent of each other.

Battery Age Exceeds	The maximum age for a UPS battery, from 1 to 150 months.
UPS Age Exceeds	The maximum age for a UPS, from 1 to 150 months.
Runtime Remaining Less Than	The minimum amount of runtime remaining, from 1 to 999 minutes.
UPS Load Exceeds	The maximum load, as a percentage of full capacity, from 0% to 100%.

Environmental Monitor tab

Defines values the InfraStruXure Manager server monitors for the humidity and temperature sensors at all environmental monitoring devices and UPS systems in its device list. The Global Device Thresholds and corresponding local device thresholds are independent of each other.

Temperature Below **Temperature Above**	The boundaries of the normal temperature range, from 32 F to 140 F (0 C to 60 C).
Humidity Below **Humidity Above**	The boundaries of the normal relative humidity range, from 32 F to 140 F (0 C to 60 C).

Metered Rack PDU tab

Defines values the InfraStruXure Manager server monitors for the load at all Switched Rack PDUs, Metered Rack PDUs, and MasterSwitch VM units in its device list. The Global Device Thresholds and corresponding local device thresholds are independent of each other.

Load Exceeds <*n*> Percent	The maximum load, as a percentage of full capacity, from 0% to 100%.

Schedule tab

Use this tab to define how often summary notifications are sent, or to disable these notifications (enabled by default).

Summary notifications can be sent for any device group that has a recipient configured to receive these notifications. The notifications identify any global threshold violations that exist within a device group, as well as other status exceptions (communication-lost, UPS self-test failed, or UPS bad-battery conditions).

For the recipient and SMTP settings required for notifications, see Notification Settings; to define which recipients receive summary notifications, see "Configure Notifications for Recipient" display.

Send Periodic Exceptions Summary Notifications	Enables notifications.
Date and **Time**	Identifies when the next notifications will be sent.
Recurrence	Defines how often notifications will be sent.
NOTE: No summary notification is sent for any device group that has no global threshold violations or other status exceptions (communication-lost, UPS self-test failed, or UPS bad-battery conditions).	

SNMP Trap Forwarding

Use the display for this Event Management menu option to enable the InfraStruXure Manager server to forward SNMP traps it receives from monitored devices, and to identify the IP addresses for the trap receivers.

The InfraStruXure Manager server can forward SNMP traps it receives from a monitored device only when the server is defined as a trap receiver at that device. For more information, see Trap receiver feature.

To enable SNMP trap forwarding	Checkmark the **Enable SNMP Trap Forwarding** option.
To add a trap receiver	1. Click **Add** to access the "Add SNMP Trap Destination" display. 2. Define the IP address of the **Trap Destination**. 3. Define the **Community Name** needed to send the SNMP traps to the **Trap Destination**.
To remove a trap receiver	Select any listed IP addresses and click **Remove**.

Building Management System

Overview

Use the display for this Event Management menu option to enable the InfraStruXure Manager server's Building Management System (BMS) support. This support allows a BMS to use the Modbus Remote Terminal Unit (RTU) protocol to access data from monitored devices through the InfraStruXure Manager server's RS-485 port.

See also

For information about how the InfraStruXure Manager server uses Modbus for BMS support, see *InfraStruXure Manager v4.x Addendum: Building Management System Integration*. A copy is available on the installation CD, or in the document list accessed by the **User Manuals & Installation Guides** link at the InfraStruXure Manager product page.

Enable BMS Modbus RTU option	Enables or disables BMS support through the RS-485 port.
Port Settings	Selects the baud rate for the RS-485 port: 19200 (default rate) or 9600. This port also uses Data Bits (8), Stop Bits (1), and Parity (even) settings that cannot be changed. **NOTE:** To wire a connector for use with the RS-485 port, see Pinout for the RS-485 port connector.
Configure Slave Addresses button	Accesses the "Configure Slave Addresses" display used to manage the list of devices with which the BMS can communicate. **NOTE:** This button is only enabled when BMS support is enabled.

"Configure Slave Addresses" display

BMS personnel can use this display to manage a list of devices with which the BMS can communicate.

Caution

This display should be used by BMS personnel only. Improper or failed communication will result if the display settings do not exactly match the corresponding BMS settings.

Each device is identified by **Hostname** (or IP address, if no hostname is available), **Model Name**, **System Name**, and **Slave Address** (the address the BMS can use to access data from that device using the Modbus RTU protocol). The InfraStruXure Manager server is always listed, and its slave address (**1**) can never change. Up to 246 other devices can be listed.

For information about the types of devices that can be listed, see "Select BMS Slave Devices" display.

Add button	Accesses the "Select BMS Slave Devices" display used to add devices to the device list.
Modify button	Accesses a list of available slave addresses you can use to assign a new address to a selected device. **NOTE:** Only slave addresses that are currently unassigned are listed. If you want to change the slave address for a device to one that is assigned to another device, you must either change the address assigned to the other device, or remove that other device from the device list.
Remove button	Removes a selected device from the list. **NOTE:** The slave address for the removed device becomes available for use at another device.
Print button	Prints a copy of the device list.

"Select BMS Slave Devices" display

Use this display to select the devices you want to add to the device list in the "Configure Slave Addresses" display. The devices you add are assigned unique slave addresses the BMS can use to access data at those devices.

The "Select BMS Slave Devices" display lists only the monitored devices that support MODBUS monitoring.

The InfraStruXure Manager server may monitor new or updated APC products without the need to be updated itself. When these devices provide BMS support, they may appear in the "Select BMS Slave Devices" display list. For more information, see <Other APC Device> events.

You can select devices individually, or use the **Select/Deselect All** option.

The number of devices you select, along with the number of devices already listed in the "Configure Slave Addresses" display, including the InfraStruXure Manager server, cannot exceed 247. If the total exceeds 247 when you click **OK,** a message instructs you to deselect some of those devices. You will be unable to exit the "Add Slave Address Devices" display until you reduce the total to no more than 247, or click **Cancel**.

Pinout for the RS-485 port connector

The following table identifies the active pins for a 9-pin, female (DB9-F) connector used to connect to the RS-485 port.

DB9-F Pin	RS-485 Signal
1	-
2	-
3	RxD/TxD+
4	GND
5	-
6	GND
7	-
8	RxD/TxD-
9	-
Shell	Chassis GND

Remote Monitoring Service

Use the display for this Event Management menu option to register for the Remote Monitoring Service (RMS) support available from APC, and to disable or enable this service, once you register.

To use a proxy server for HTTP-based communication with the remote RMS server, see Proxy Settings.

To register for APC RMS support	1. Click **RMS Settings**. 2. Click **New RMS Customer** in the "Access RMS Settings" display. **NOTE**: A message will inform you if the InfraStruXure Manager server is already registered for RMS support. 3. Provide the required company and contact information in the "RMS Settings" display, and click **Save**. 4. Checkmark the **Enable APC's Remote Monitoring Service** option, and click **Apply**. 5. Click **http://rms.apc.com** to go to the RMS Web page. 6. Log on to the RMS Web site using the logon values (address and password) you created. 7. Follow the on-screen instructions to finish configuring the RMS support.
To enable or disable RMS support	Check or uncheck the **Enable APC's Remote Monitoring Service** option, and click **Apply**.
To change customer or contact information	1. Click **RMS Settings**. 2. Use the RMS logon values for the **E-mail** and **Password** settings in the "Access RMS Settings" display, and click **Ok**. **NOTE**: If you have not finished registering the InfraStruXure Manager server, click **New RMS Customer** to access the company and contact information settings. 3. Modify the company and contact information in the "RMS Settings" display, and click **Save**.

System Management menu

Overview

Use the menu options to do the following:

All options except **Client Preferences** are disabled unless you log on as the Administrator. See Administrator versus General access.

Authentication Settings	Select the authentication method used to log on to the InfraStruXure Manager server, and configure the settings used by that method.
Device Access	Define settings the InfraStruXure Manager server uses to discover and monitor devices, and to perform firmware update and Mass Configuration procedures.
Mass Configuration	Apply configuration settings to multiple devices.
Racks	Define settings the InfraStruXure Manager server uses to calculate, monitor, and report the power used at monitored racks.
Server options	Server Time: Define the time and date settings used by the InfraStruXure Manager server.
	Shut Down or Reboot Server: Shut down or reboot the InfraStruXure Manager server. **NOTE:** You can use this option to reset the server to its factory-default settings.
	Setup Wizard: Access the wizard that is used for part of the Initial configuration requirements.

Network options	Network Settings: Define the settings the InfraStruXure Manager server needs to operate on its APC and User Local Area Networks (LANs).
	Notification Settings: Define the settings that enable the InfraStruXure Manager server to send notifications. **NOTE:** This option also appears in the Incident Management menu when the Incident management module is activated.
	FTP Server Settings: Start or stop the FTP service, and define the FTP logon settings.
	System Identification: Define the **System Name**, **Contact**, and **Location** values for the InfraStruXure Manager server.
	Proxy Settings: Define the settings the InfraStruXure Manager server must use to communicate with the APC Web site over a network that uses a proxy server. **NOTE:** The InfraStruXure Manager server uses the Web to communicate with the APC Remote Monitoring Service (RMS), to download firmware updates, and to authenticate license keys.
Log Settings	Define settings that affect how long data remains in the event and data logs, and how often data is sampled and saved in the data logs.
License Keys	Manage the license requirements.
Client Preferences	Define client-specific preferences.

Authentication Settings

Overview

Use the display for this System Management menu option to select the authentication method used to log on to the InfraStruXure Manager server, and to configure the settings used by that method: Local, Remote Authentication Dial In User Service (RADIUS), or both.

Caution

When **RADIUS only** is selected as the **Authentication Method**, failure to make sure the InfraStruXure Manager server can access at least one of the servers defined in the "Configure RADIUS settings" display can result in the permanent loss of access to the InfraStruXure Manager server when you log off. For information about testing this access, see "Test RADIUS Access" display; for information about setting up a RADIUS server to work with the InfraStruXure Manager server, see Configure a RADIUS server to validate logon attempts.

Authentication Method	Select the method used to verify log on attempts: • **Local only**: Check the logon values against the "Configure local users" display settings. • **Local, then RADIUS**: If the logon values do not match the "Configure local users" display settings, check the settings stored at the RADIUS server. • **RADIUS, then Local**: If the logon values do not match the settings stored at the RADIUS server, check the "Configure local users" display settings. • **RADIUS only**: Check the logon values against the settings stored at the RADIUS server.
Configure local users	Configure the **Administrator** and **General** settings used for local access.
Configure RADIUS settings	Configure the settings used to access the RADIUS server.
Allow users to save their logon settings	Allow the **Save Logon Settings** option in the "Server Log On" display to be used for local access to this server.

Administrator versus General access

The **Administrator** has full access. A **General** user can generate reports and logs, access status, and use only the following menu options:

- All Help menu options
- The **Change Server** and **Exit** options in the File menu
- The Client Preferences option in the System Management menu

Configure local users

Use the display for this Authentication Settings button to manage the case-sensitive **Administrator** and **General** usernames and passwords used for local access.

The initial settings include the **Administrator** (**apc**, lowercase, for the default username and password) and a **General** user (**guest** [username] and **apc** [password], both lowercase, for the default values). To help prevent unauthorized access, change the default values as soon as possible.

There can be only one **Administrator** and up to 24 **General** users, each with its own username and password. For information about how the type of user affects which features are available, see Administrator versus General access.

To add a **General** user	Click **Add** and define the **Username** and **Password** for the new user.
To delete a **General** user	Select the user, and click **Remove**.
To change the **Username** or **Password** for any user	Select the **Administrator** or **General** user, and click **Modify** to change the **Username** or **Password**.

Configure RADIUS settings

Use the display for this Authentication Settings button to identify the settings used to communicate with the primary and secondary RADIUS servers to authenticate the settings used to log on to the InfraStruXure Manager server.

Note

A secondary server authenticates settings only when the primary server is unavailable. It will not verify settings the primary server rejects.

Server Address	The IP address or hostname to be used to access the server.
Port Number	The port the InfraStruXure Manager server will use to communicate with the RADIUS server.
Shared Secret	The phrase used to validate a logon attempt.
Test RADIUS Access	Accesses the "Test RADIUS Access" display used to verify the InfraStruXure Manager server can access at least one of the defined RADIUS servers.

Configure a RADIUS server to validate logon attempts. Before a RADIUS server can validate logon attempts, it must be configured as follows:

- It must be enabled to use the Password Authentication Protocol (PAP).
- Administrator username and password combinations must be configured to support the following Service-Type attribute:
  Console Access Level Administrator: Service-Type = Administrative
- General username and password combinations must be configured to support the following Service-Type attribute:
  Console Access Level General: Service-Type = Login

For information about how the type of user affects which features are available, see Administrator versus General access.

"Test RADIUS Access" display

Use this display to make sure the InfraStruXure Manager server can access at least one of the RADIUS servers defined in the "Configure RADIUS settings" display.

Enter a **Username** and **Password** and click **Test**. If the test fails, one of the following results can be reported:

- **Incorrect Username and Password**: The test successfully accessed at least one of the defined RADIUS servers, but that server determined that an invalid **Username** or **Password** was used.

  For information about how to define the InfraStruXure Manager logon values when a RADIUS server is used, see Configure a RADIUS server to validate logon attempts.

- **Receive timed out**: The defined RADIUS servers are unavailable, or both server definitions have an incorrect **Server Address** or **Port Number**.

  The "Configure RADIUS settings" display must correctly define at least one RADIUS server. Otherwise, no RADIUS server can validate InfraStruXure Manager logon attempts, and if **RADIUS only** is selected in the "Authentication Settings" display when you log off, InfraStruXure Manager server access is permanently lost.

- **Authentication** failure: The **Server Address** and **Port Number** is correctly defined for at least one RADIUS server, but the **Shared Secret** definition does not match the value that RADIUS server expects. The exact text used for these failures may vary based on the RADIUS server used.

  If you log off while the authentications do not match, the RADIUS servers cannot validate logon attempts until the authentication values are edited at those servers to match the **Shared Secret** definitions in the "Configure RADIUS settings" display.

Device Access

Overview

Use the display tabs for this System Management menu option to define the settings the InfraStruXure Manager server uses to communicate with Supported devices. If the following settings are not all properly defined, the server may not be able to monitor or communicate with some APC devices.

SNMP tab	Define the Community names and Timeout settings the InfraStruXure Manager server uses for its SNMP communications. **NOTE:** For information about how the InfraStruXure Manager server controls whether it receives SNMP traps from monitored devices, see Trap receiver feature.
Administrator Accounts tab	Define administrator username and password combinations the InfraStruXure Manager server uses to discover and add a Switched Rack PDU or newer version of the Metered Rack PDU to the list of monitored devices.
FTP Settings tab	Define the FTP Settings used during a firmware update or Mass Configuration. **NOTE:** The InfraStruXure Manager server also uses FTP to download an initialization file from some devices. Each initialization file provides all the information the InfraStruXure Manager server needs to fully monitor that device.

Community names

The InfraStruXure Manager server uses the community names in the Device Access **SNMP** tab to do the following:

- Read community names are used to access devices for status and other information: the InfraStruXure Manager server cannot add a device to the list of devices it monitors if that device uses a read community name that is not listed in the **SNMP** tab.

  The username and password combinations in the Device Access **Administrator Accounts** tab are used to discover and add any Switched Rack PDU or newer version of the Metered Rack PDU to the list of devices the InfraStruXure Manager server monitors.

- Write community names are used to perform SNMP SETs that change settings at monitored devices. This includes using SETs to define itself as a trap receiver at those devices: if a device uses a write community name that is not listed in the **SNMP** tab, the InfraStruXure Manager server cannot define itself as a trap receiver or change thresholds and settings at that device.

  For more information about how the InfraStruXure Manager server controls whether it is defined as a trap receiver, see Trap receiver feature.

To add a **Read Community Name** or **Write Community Name**	Click the appropriate **Add** button and define the new community name.
To remove a **Read Community Name** or **Write Community Name**	Select the community name and click **Remove**.

Timeout settings

The InfraStruXure Manager server uses the following settings in the Device Access **SNMP** tab when it attempts to communicate with a device using SNMP.

Retries	How many times the InfraStruXure Manager server will attempt to establish SNMP communication after an initial attempt fails (the default is **1**). **CAUTION:**The InfraStruXure Manager server uses SNMP to discover devices and to poll monitored devices for status information. The **Timeout (ms)** and **Retries** values can dramatically increase the time it takes to discover devices, particularly when a large number of the IP addresses to be searched are for unsupported devices (see Supported devices); these values can also increase the time needed to poll monitored devices for status when a network problem exists. This is because the timeout value doubles for each retry. For example, if the **Timeout (ms)** used for the initial attempt is the default setting of **1000** ms (1 second), the timeout value for the first retry is **2000** ms (2 seconds), **4000** ms (4 seconds) for a second retry, and so on. Thus, for a **Retries** setting of **5**, the InfraStruXure Manager server can take 63000 ms (63 seconds) to determine that it cannot connect to one device: 1000 ms for the initial attempt, and 62000 ms for the five retries (2000+4000+8000+16000+32000 = 62000).
Timeout (ms)	The amount of time, in milliseconds (ms), the InfraStruXure Manager server waits when it first tries to communicate with an SNMP agent before it considers the attempt failed (the default is **1000**).

Trap receiver feature

You can use the SNMP Trap Forwarding option in the Event Management menu to enable the InfraStruXure Manager server to forward SNMP traps it receives from it monitored devices to the trap receivers you define. However, the InfraStruXure Manager server can receive SNMP traps only from devices at which it is defined as a trap receiver.

For a Matrix-UPS, a Smart-UPS, and some Environmental Monitoring Units, some events can be reported and logged only when the InfraStruXure Manager server is defined as a trap receiver at those devices. See UPS events and Environmental events.

The InfraStruXure Manager server uses SNMP SET commands to define itself as a trap receiver at monitored devices:

- If the **Configure SNMP Agents to Send Traps to Server** option is enabled when you use the "Add Devices" display to discover new devices to be monitored, the InfraStruXure Manager server can register itself as a trap receiver at the added devices.
- The "Device List" frame has **Register as a trap receiver** and **Unregister as a trap receiver** options in a right-click menu you can use to control whether the InfraStruXure Manager server is defined as a trap receiver at any selected devices.

The InfraStruXure Manager server cannot be defined as a trap receiver at an InfraStruXure PDU or at some Metered Rack PDU models. For information about what can cause the InfraStruXure Manager server to fail to register itself at other devices, see Failed to register as a trap receiver for a device.

FTP Settings

Use this Device Access tab to define the FTP access values the InfraStruXure Manager server uses to log on to devices during a firmware update or Mass Configuration.

The InfraStruXure Manager server also uses FTP to download an initialization file from some devices. Each initialization file provides all the information the InfraStruXure Manager server needs to fully monitor that device.

FTP must be enabled at a device, and the correct FTP username and password for that device must be used, before firmware can be downloaded to that device. By default, the InfraStruXure Manager server can download firmware only to devices that use **apc** (lowercase) for the FTP username and FTP password.

Use **Add** and **Remove** to modify the list of usernames and passwords the InfraStruXure Manager server can use for FTP access to the devices it monitors.

Username	The usernames the InfraStruXure Manager server can use during logon attempts.
Password	The passwords the InfraStruXure Manager server can use during logon attempts.
FTP Port	The port used for FTP communication at the devices.
Update Retries	How many times the InfraStruXure Manager server will attempt to log on to a device before a failure occurs.

Failed to register as a trap receiver for a device

The InfraStruXure Manager server cannot be defined as a trap receiver at the following devices:

- An InfraStruXure PDU
- Some older Metered Rack PDU models
- Any device that uses a PowerChute Business Edition agent to communicate with the InfraStruXure Manager server
- Any device that reports <Other APC Device> events only

The InfraStruXure Manager server fails to register itself as a trap receiver at other devices under the following circumstances:

- The device uses a write community name that is not listed in the write "Device Access" display's write community name list.
  a. Select the Device Access option in the System Management menu.
  b. Use the Community names section of the Device Access **SNMP** tab to add the write community name.
  c. Right-click the device in the "Device List" frame and select the **Register as a trap receiver** option.
- All of the device's trap receiver definitions are assigned to other trap receivers.
  a. Double-click the device in the "Device List" frame to access its management application.
  b. Change a trap receiver definition to the InfraStruXure Manager server's IP address.
- Communication with the device's agent, or with the device, was lost. Try again, after communication is established.
- Someone is logged on to a management application at the device. Try again, after the user logs off.

Mass Configuration

Overview

The mass configuration feature allows you to configure multiple devices using the same configuration settings. Except for direct current (DC) products, any device that uses an internal or external network management card with an APC operating system (AOS) of 2.5.0 or higher can be mass configured.

- Configuration procedure
- "Send Configuration to Selected Devices" display
- "One or More Settings Failed" display
- Available mass configuration settings
- Excluded configuration settings

Configuration procedure

To configure multiple devices with the same settings, do the following in the "Device List" frame:

1. Highlight the device that has the configuration settings to be used for the mass configuration and select the **Use Configuration from Selected Device** option in the right-click or System Management menu.
2. Highlight the devices at which the configuration settings will be applied, and select the **Send Configuration to Selected Devices** option in the right-click or System Management menu.

Select devices that match the model and firmware revision of the device selected in step 1. Only compatible, shared settings are applied at a device. See Available mass configuration settings.

3. Click **Yes** to start the configuration process.

Note

The process, which takes about six minutes for every ten devices, is reported in the "Send Configuration to Selected Devices" display.

"Send Configuration to Selected Devices" display

The display for this Mass Configuration option reports the configuration progress, including the status at each device.

Note

You can use the **View Mass Configuration Status** option in the right-click or System Management menu to access status information for the last mass configuration process, unless the InfraStruXure Manager server reboots.

After the settings are successfully applied at a device, **Completed** is reported as the status for that device. The following table describes the error status that can be reported.

Aborted or **Deleted**	**Description**: The device was removed from the list of monitored devices before the InfraStruXure Manager server could apply the settings. **Recommended Action**: Use the Add Devices option in the Edit menu to rediscover the device. Then use the Configuration procedure to apply the settings at the device.

FTP Logon Failed or **FTP Transfer Failed**	**Description**: The InfraStruXure Manager server could not log on to the device (**FTP Logon Failed**) or the FTP connection was lost before the configuration settings could be applied (**FTP Transfer Failed**). **Recommended Action**: • Make sure the device is turned on and connected to the network. • Correct any network connection problem. • Make sure the FTP service is enabled at the device, and the Device Access option (FTP Settings) in the System Management menu identifies the username, password, and FTP port needed to access the device. • If the problem persists, contact APC Customer Support. Once the problem is corrected, use the Configuration procedure to apply the configuration settings at the device.
Initialization Failure	**Description**: The InfraStruXure Manager server could not find the configuration file to be used for the mass configuration. **Recommended Action**: Use the Configuration procedure to select the initialization file you want to use (**Use Configuration from Selected Device** option) and apply the settings (**Send Configuration to Selected Devices** option). If it fails again, contact *APC Customer Support*.
Interrupted	**Description**: The device was removed from the list of monitored devices before the InfraStruXure Manager server finished applying the configuration settings. **Recommended Action**: Use the Add Devices option in the Edit menu to rediscover the device. Then use the Configuration procedure to apply the settings at the device.

Not Supported	**Description**: The device does not support the mass configuration process. **Recommended Action**: • If the device connects to the network through a PowerChute Business Edition agent, it cannot support mass configuration. • If the device uses network management firmware earlier than v2.5.0, it must be updated using the Updates menu or configured individually. • If the device cannot use any of the configuration settings being applied, you must configure that device individually.
One or More Settings Failed	**Description**: At least one of configuration settings was not changed because the applied setting's value was incompatible with the values the device has available for that setting. **NOTE:** See "One or More Settings Failed" display. **Recommended Action**: Double-click the listed device (or highlight and click **Details**) to view information about the configuration settings that do not match.

"One or More Settings Failed" display

To access this display, double-click a device that reports **One or More Settings Failed** as its status in the "Send Configuration to Selected Devices" display, or select that device and click **Details**.

This display provides information about any attempt to apply a configuration setting value that is incompatible with the values the device has available for that setting: For example:

- Not all Smart-UPS configuration values match the values a Matrix UPS uses. Use a mass configuration process only with identical models (for example, Smart-UPS 1000 to Smart-UPS 1000).
- The devices use different firmware versions. Use the Updates menu to update all Configuration procedure devices to use the same firmware.

For information about the configuration settings that can be applied, see Available mass configuration settings.

The following table describes the information provided for failed settings:

Section Name	The section of the device's initialization (*.ini) file which contains the affected setting.
Key Name	The name the setting uses in the *.ini file.
Expected Value	The value that the InfraStruXure Manager server expected the setting would have after the configuration was completed.
Actual Value	The value that the setting has at the device.

Available mass configuration settings

During a Mass Configuration, the InfraStruXure Manager server uses the settings contained in the initialization (config.ini) file of the last device selected by the **Use Configuration from Selected Device** option, as follows:

- Excluded configuration settings are not applied at any device.
- Only shared settings that are applied at a device. For example, if the configuration settings are from a Smart-UPS 1000, few of those settings would be applied at a Metered Rack PDU.

Some devices can share a configuration setting, but not the values available for that setting. See "One or More Settings Failed" display.

Excluded configuration settings

The following settings are not applied during a Mass Configuration.

Section Name	Key Name	Description
NetworkTCP/IP	Entire Section	Network settings
PowerChute	Entire Section	PowerChute Network Shutdown settings
FTPServer	Entire Section	FTP server settings
SystemID	Entire Section	System identification settings
NetworkAirFMInputs Outputs	Entire Section	Input and output settings
NetworkAirFMGroup	Entire Section	Group settings
NetworkAirFMModules	Entire Section	Module settings
NetworkAirFMOutput Mapping	Entire Section	Output mapping settings
NetworkAirFMShutdown Events	Entire Section	Shutdown settings
NetworkAirFMSystem	Entire Section	System settings

UPS	UPSName	Name used by the UPS
UPS	BatteryDate	Date the battery was last replaced
UPS	ExternalBatteries	Number of external batteries
Modbus	UniqueTargetID	Modbus address assigned to the device
RackPDUOutlet	Outlet Names	Names assigned to outlets
Environment	Probe Names	Names assigned to sensors at an environmental monitoring device
InputContacts	Contact Names	Names assigned to contacts
OutputRelays	Relay Names	Names assigned to output relays
Sensors	Sensor Names	Names assigned to sensors at an Environmental Management System
Outlets	Outlet Names	Names assigned to outlets
External	Probe Names	Names assigned to external environmental sensors at a UPS
Integrated	Probe Names	Names assigned to integrated environmental sensors at a UPS

Racks

Overview

The racks feature allows the InfraStruXure Manager server to do the following:

- Monitor the power (in kWatts) and status for racks that receive power from Metered and Switched Rack PDUs monitored by the InfraStruXure Manager server.
- Report the rack power and status information for monitored racks in a "Configure Racks" display, and in any InfraStruXure PDU diagrams that include racks in the "Power Zones" display.

Two **Racks** options in the System Management menu define how the InfraStruXure Manager server calculates, monitors, and reports the power that Metered and Switched Rack PDUs provide at the monitored racks.

The InfraStruXure Manager server cannot report the power provided by MasterSwitch, MasterSwitch Plus, or MasterSwitch VM devices.

Configure Racks	Use to manage a list of monitored racks that reports the kWatts and status for those racks. **NOTE:** For information about how the kWatts value is determined for a rack, see Rack kWatt values.
Default Power Settings	Use to define the default power settings that may be assigned to Rack PDU models. These values will be used if the InfraStruXure Manager does not have specific values for a Rack PDU model. Typically, this occurs for new Rack PDU models that were released after the InfraStruXure Manager server was last updated. **NOTE:** The power settings assigned to any Rack PDU can be edited using either the "Edit Power Settings" display, or the "Set Rack Properties" display.

Configure Racks

Use the display for this Racks option to manage a list that identifies the monitored racks by name, and the kWatt power and status for each rack.

For information about how the rack kWatt values are defined, see Rack kWatt values.

- Use **Add** and **Remove** to manage the rack list.
- Use **Modify** to access the "Modify Rack" display.
- Use **Print** to print a copy of the rack list.

The following status conditions can be reported for a listed rack:

Normal	At least one Rack PDU is identified as providing power at the rack, all Rack PDUs are communicating normally, and no power threshold violation exists (or those thresholds are disabled).
Device not communicating	Communication has been lost with at least one of the Rack PDUs identified as providing power at the rack.
Device initializing	Communication is initializing with at least one of the Rack PDUs identified as providing power at the rack.
No power devices selected	No Rack PDU is identified as providing power at the rack. **NOTE:** Use the **Modify** button to select which Rack PDUs provide power at a rack. See Devices tab.
Violates the low-power threshold	These Thresholds tabsettings define the high and low limits of an acceptable power range that provides a means to discover problems that can adversely affect the devices that receive their power at the rack. For example, an overload can violate the high threshold, while turning off an outlet at a Switched Rack PDU can violate the low threshold. **NOTE:** If communication is lost with a Rack PDU at a rack that has a threshold violation, the rack status changes to **Device not communicating**, and the event that indicates the violation no longer exists cannot occur until after the communication problem clears.
Violates the high-power threshold	

Default Power Settings

When you use the Devices tab in the "Modify Rack" display to assign a Rack PDU to a rack, the Racks feature uses the **Nominal Voltage** and **Power Factor** assigned to that Rack PDU to compute how much kWatts that Rack PDU provides at the rack.

For information about how the power settings are used to determine the kWatt values for the racks, see Rack kWatt values.

Use the display for this **Default Power Settings** option to define the values that will be assigned to a Rack PDU when both of the following circumstances exist:

- The InfraStruXure Manager server cannot assign the **Nominal Voltage** and **Power Factor** associated with the Rack PDU, because it does not recognize the Rack PDU model number. This typically occurs because the Rack PDU model was released after the InfraStruXure Manager server version was last updated.
- Neither the "Edit Power Settings" display nor the "Set Rack Properties" display was used to define the values for the Rack PDU.

The "Default Power Settings" display's **Nominal Voltage** and **Power Factor** values are set to **120V** and **1.0** respectively. These values are based on power settings that are common to models used in the United States. You can edit these settings to match your local requirements.

Once these settings are assigned to a Rack PDU, you can use the "Edit Power Settings" display, or the "Set Rack Properties" display, to edit the assigned settings.

Modify Rack

The display for the **Modify** button in the "Configure Racks" display has two tabs:

- Devices tab
- Thresholds tab

Devices tab. Use this tab to do the following:

- Redefine the rack's name.
- Use check marks to identify which of the listed Rack PDUs provide power at the selected rack. The list includes all monitored Rack PDUs that are not assigned to another rack.

  Caution For the racks feature to work properly, only the Rack PDUs that provide power to the equipment installed in a rack should be assigned to the rack, and those Rack PDUs must provide power to that rack's equipment only.

- Select a listed Rack PDU and click Edit Power Settings to modify the **Voltage (VAC)** or **Power Factor** for that Rack PDU.

  For information about how the power settings are used to determine the kWatt values for the racks, see Rack kWatt values.

Thresholds tab. Use this tab to define the upper and lower power thresholds, in kWatts, for the identified rack's normal power consumption range, and to define how long a threshold violation must exist before the InfraStruXure Manager server acts on that violation. These thresholds help measure how planned and unplanned equipment changes impact a rack's power and heat management.

When a threshold is violated for the defined period of time, the following occurs:

- The violation is reported as the rack's status in the "Configure Racks" display list, and in any InfraStruXure PDU diagrams that include the rack.
- A notification is sent to the recipients configured to receive warning notifications for System events, or if the Incident management module is enabled, to the recipients identified by the "Warning" tab in the Default Escalation Policy display.
- The violation is recorded in the Event log when it occurs and when it no longer exists.

If the rack changes to the Device not communicating status while a threshold violation exists, the event that indicates the violation no longer exists cannot occur until after the communication problem clears. For information about the possible causes and corrective actions for these threshold violations, see System: The power consumed by rack <rack name> has violated the <high or low> power threshold of <n> kWatts for over <time>.

Edit Power Settings

Use the display for this button in the Devices tab of the "Modify Rack" display to change the voltage and power factor settings assigned to a listed Metered or Switched Rack PDU only when those settings are known to be inaccurate.

For information about how the power settings are used to determine the kWatt values for the racks, see Rack kWatt values.

Rack kWatt values

The Configure Racks option reports the total power consumed at each monitored rack. This figure is the sum of the power values reported for each Rack PDU identified as providing power at the rack.

- Each Metered or Switched Rack PDU is assigned a voltage and power factor value when it is assigned to a rack. These power values can be viewed using the "Edit Power Settings" display, or the "Set Rack Properties" display, and edited under the following circumstances:
  - The Default Power Settings were assigned to a Rack PDU, and more accurate values have since been determined.
  - The voltage assigned to a Rack PDU model that can use different input voltages (only one voltage value can be assigned to a Rack PDU) does not match the input voltage actually used.
  - A measurement of a Rack PDU's input voltage shows the value is within the range a Rack PDU supports, but the difference between the actual voltage and the assigned nominal voltage affects the accuracy of the kWatt calculation.
  - A detailed analysis indicates that the efficiency of the load equipment does not match the power factor assigned to the Rack PDU.

    Before you edit the power factor for a Rack PDU, see Power factor values.
- The output current at a Metered or Switched Rack PDU is combined with that Rack PDU's voltage and power factor to calculate the kWatts that the Rack PDU provides at the rack.

  For information about how the Rack PDUs that provide power to a rack are identified, see Modify Rack.

Power factor values

The power factor is the ratio between the kW (kilowatts) and the kVA (kilo-Volt Amperes) drawn by an electrical load, where kW is the actual load power and kVA is the apparent load power. It is a measure of how effectively the current is converted into useful work output and is a good indicator of the effect the equipment load current has on the efficiency of the supply system.

An equipment load with a power factor of 1.0 indicates the most effective use of voltage and current by the connected load (the voltage and current are in phase with each other and have the same wave shape), while a power factor of 0.5 indicates a less effective use of voltage and current (the voltage and current are not in phase with each other, and do not have the same wave shape). Either of the following can cause a poor power factor:

- The voltage and current are out of phase with each other, resulting in the kW drawn having a lower value than the kVA.
- A high harmonic content or distorted/discontinuous current waveform.

The power factor directly affects the kW drawn from a Rack PDU.

- When equipment with a power factor of 1.0 is drawing 10 amps of current at 208 volts from a 3-phase Switched Rack PDU, 2.1kW will be drawn from the Rack PDU.

  For a 3-phase Rack PDU, the InfraStruXure Manager server assigns a power factor value to the Rack PDU when it is configured to power equipment in a rack. This single power factor value applies to the equipment powered by all three banks of the Rack PDU (e.g. groups of sockets identified as B1, B2 and B3). If the equipment connected to the three banks have various power factors, it may result in an inaccurate power calculation for that Rack PDU. Care should be taken to match, as much as possible, the power factor of the load equipment on each bank.

- When equipment with a power factor of 0.8 is drawing 10 amps of current at 208 volts from a 3-phase Switched Rack PDU, 1.7kW will be drawn from the Rack PDU.

  1.0, the default power factor assigned to a Rack PDU, represents the most effective use of the Rack PDU's current and voltage by its load equipment. Do not change a Rack PDU's power factor unless the manufacturer's specifications for its load equipment indicates that the equipment has a less effective power factor.

Server Time

Use the display for this System Management menu option to define the date and time settings for the InfraStruXure Manager server.

Note

When these settings are enabled (the settings are disabled while a 30-day evaluation period is in effect), the InfraStruXure Manager server must reboot before a change to any setting can take effect.

Server Date	The date the server is currently using.
Server Time	The time the server is currently using. **NOTE:** Click **Use Client Time** to set the time to match the client.
Time Zone	The time zone in which the server is located.

Shut Down or Reboot Server

Overview

Use the display for this System Management menu option to shut down or reboot the server.

Caution

Using the **Reset to Factory Defaults** option during a shutdown or reboot, deletes all report and log data, and resets all configuration settings to their default values. Also, if a computer that connects to the APC LAN is not turned off, its IP address could be inadvertently assigned to another APC LAN device. See Duplicate IP addresses assigned on the APC LAN.

Shutdown	Shuts down the server.
Reboot	Reboots the server.
Reset to Factory Default Settings	When checked, resets the InfraStruXure Manager server to its factory default settings during a shutdown or reboot procedure.

Duplicate IP addresses assigned on the APC LAN

If a computer that connects to the APC LAN is not turned off when the Shut Down or Reboot Server option is used with **Reset to Factory Defaults** enabled (or the InfraStruXure Manager server is replaced), the computer's IP address may inadvertently be assigned to another APC device. To clear this problem, release and renew the computer's IP address. For example, use `ipconfig /release` and `ipconfig /renew` at the command prompt of a Windows-based computer.

Setup Wizard

Use this System Management menu option to launch the InfraStruXure Manager Setup Wizard.

Network Settings

Use the display for this System Management menu option to define the settings the InfraStruXure Manager server uses to communicate over the APC and User Local Area Networks (LANs).

The InfraStruXure Manager server must reboot before a change to any network setting can take effect.

Hostname	Defines the name for the InfraStruXure Manager server.
MAC Address	Identifies the Media Access Control (MAC) address assigned to the InfraStruXure Manager User LAN card.
APC LAN	Accesses the display that identifies the **192.168.*.*** or **10.0.*.*** address range the InfraStruXure Manager server uses on its APC LAN. The available settings select address ranges that allow the InfraStruXure Manager server to monitor up to 1000 devices on the APC LAN. For example, the default settings (**192.168** as the network and **0** as the segment) select **192.168.0.2** though **192.168.3.254** as the network address range. **NOTE:** Select a different **192.168.*.*** or **10.0.*.*** address range only when the default setting conflicts with another network segment.
DHCP Network Address	Selects to use the TCP values provided by the User LAN's Dynamic Host Configuration Protocol (DHCP) server. **NOTE:** When DHCP is used, a permanent IP address must be reserved for the InfraStruXure Manager server at the DHCP server.

Static Network Address	Selects to use the following manually defined address values for the User LAN: **IP Address**: The network address of the InfraStruXure Manager server. **Subnet Mask**: The TCP/IP subnet address for the local segment. **Gateway**: The IP address of the gateway. **Domain Name**: The name of the network domain on which the InfraStruXure Manager server resides. **Primary DNS Server**: The IP address of the primary Domain Name Service (DNS) server used to map IP addresses to domain names. **Secondary DNS Server**: The IP address of the DNS server used when the primary DNS server is busy or off-line.

Notification Settings

Overview

Use the display for this System Management menu and Incident Management menu option to define the recipients and SMTP settings the InfraStruXure Manager server uses to send notifications for events, exceptions summaries, and firmware updates.

The **Incident Management** menu appears only when the Incident management module is activated.

The “Notification Settings” display has a Settings tab and two versions of a **Recipients** tab:

- Recipients tab (no incident management)
- Recipients tab (incident management)

Settings tab

Use this tab to define the SMTP server settings the InfraStruXure Manager server needs for notifications. These settings must be properly defined before the InfraStruXure Manager server can send notifications.

The SMTP server settings are the same, with or without the Incident management module activated.

SMTP Server	The hostname (or IP address) of the server.
Secondary SMTP Server	The hostname (or IP address) of the server that will be used only when the primary server is unavailable.
E-Mail From Address	A properly formatted address (xxxx@xxxx.xxx) to be used as the **From** address in e-mail notifications.

Recipients tab (no incident management)

Use this tab to manage the recipients the InfraStruXure Manager server uses for e-mail or SMS notifications when the Incident management module is not activated.

Recipients are listed by the **Address** used for notifications, and **Recipient Type** (**SMS** or **E-Mail**).

Add button	Accesses the "Add Recipients" display used to define a new recipient.
Remove button	Deletes the selected recipient from the list.
Configure button	Accesses the "Configure Notifications for Recipient" display used to define which notifications the selected recipient will receive.
Test button	Sends a test notification to the selected recipient. **NOTE:** For information about error messages that may occur, see Error messages during notification tests.

Recipients tab (incident management)

Use this tab to manage the recipients the InfraStruXure Manager server uses for e-mail or SMS notifications when the Incident management module is activated.

Recipients are listed by **Name**, the **Address** used for notifications, and **Recipient Type** (**SMS** or **E-Mail**).

Add button **Modify** button	Access the "Add Recipients" and "Modify Recipients" displays (incident management) used to define or edit a recipient, including the Availability settings.
Remove button	Deletes the recipient selected in the list.
Test button	Sends a test notification to the selected recipient. **NOTE:** For information about error messages that may occur, see Error messages during notification tests.

Error messages during notification tests

If an SMTP error message appears when you send a test notification:

- Make sure the **SMTP Server** and **E-Mail From Address** values are defined correctly in the Settings tab.
- Make sure the SMTP server is configured to allow the InfraStruXure Manager server to send notifications.
- Consult the SMTP server documentation to make sure the server is properly configured to receive and send notifications.

The error message may contain an SMTP error code (for example, 550 5.7.1) that can help identify the setting to investigate at the SMTP server.

- Make sure a properly configured SMS gateway is available for a test sent to an address used for SMS notifications.

"Add Recipients" display

Use this display for the **Add** button in the Recipients tab (incident management) to define a new recipient:

- The **Address** defines the recipient by an e-mail address, or by the address of a text-messaging device, such as a cell phone, for SMS notifications.
- The **Short Message Service (SMS) address** option selects whether e-mail notifications (disabled) or SMS notifications (enabled) will be sent to the recipient.

SMS notifications

E-mail notifications, which include a subject line and body text that provides more detail about the event, are not an effective format for notifications sent to text-messaging devices, such as a cell phones. The **Short-Message Service (SMS) address** option allows notifications that are specifically designed for text-messaging devices to be sent to a recipient's address (for example, 4015551212@<service_provider>). These SMS messages use a maximum of 160 characters, and have a <*system_name*> at <*location*>: <*message*> format.

When a text-messaging device address is used, the **Short Message Service (SMS) address** option must be enabled for optimal text-messaging.

<*system_name*>	Identifies the monitored device associated with the event. **NOTE:** If no system name is defined, the hostname is used; if no hostname is defined, the IP address is used.
<*location*>	Identifies the device location. **NOTE:** If no location is defined for the device, only the <*system_name*> is used for the message prefix.
<*message*>	Identifies the event that occurred. **NOTE:** The title that identifies a warning or critical event in the "Recommended Actions" frame is used for the SMS message.
NOTE: For InfraStruXure Manager system events, <*system_name*> and <*location*> identify the InfraStruXure Manager server that sent the notification.	

"Configure Notifications for Recipient" display

Use this display for the **Configure** button in the Recipients tab (no incident management) to customize the Device group notifications and System event notifications for a selected recipient.

Note

This display is not available when the Incident management module is activated.

Device group notifications. Configure which notifications are enabled or disabled for each device group:

1. Double-click a **Device Group**, or to configure multiple device groups, select those groups and click **Configure**.
2. In the "Select Notifications" display, select the items you want enabled for notifications for the selected device group:
   - **Critical**, **Warning**, and **Informational Events**: Send a notification when an event with a selected severity occurs at a device.

     See Status and event severity levels.

   - **Firmware Update Available**: Send a notifications when a firmware update is available for a device.

     See Apply Firmware Updates.

   - **Exceptions Summary**: Send scheduled notifications for each device group that has global device threshold violations or status exceptions (communication lost, UPS failed self-test, or UPS bad-battery).

     To enable and schedule these notifications, see Schedule tab.
3. Configure any other device groups, as needed.

System event notifications. In the box near the bottom of the Schedule tab, double-click the **System Events** listing and use the "Select Notifications" display to identify the severity levels that will result in notifications.

For more information about **Critical**, **Warning**, and **Informational Events**, see Status and event severity levels.

"Add Recipients" and "Modify Recipients" displays (incident management)

The **Add** and **Modify** buttons in the Recipients tab (incident management) open displays which use the same elements: only the display names are different.

Name	Identifies the name of the recipient.
Address	Identifies the address to which notifications will be sent.
Short Message Service (SMS) address option	Selects whether e-mail notifications (disabled) or SMS notifications (enabled) will be sent.
Availability settings	Identifies when the recipient will be available for notifications.
Receive Summary Events option	Selects whether summary notifications will be sent for any device group that includes the recipient in its warning policy. **NOTE:** No notification is sent for any device group at which no global device threshold violations or status exceptions (communication-lost, UPS self-test failed, or bad-battery conditions) exist when a notification is scheduled to occur. See Schedule tab.
Receive Firmware Events option	Selects whether firmware notifications will be sent for devices in any device group that includes the recipient in its warning policy. **NOTE:** For more information, see Apply Firmware Updates.

Availability settings

Use these settings in the "Add Recipients" and "Modify Recipients" displays (incident management) to identify when the selected recipient is available for incident notifications:

The time settings are based on the InfraStruXure Manager server's time. If the recipient is in a different time zone from the server, adjust the time settings to meet the recipient's availability requirements.

1. Select the **Day of the Week** to edit.
2. Disable the **Available on Selected Day** option, if the recipient is unavailable during the selected day, or use the **Start Time** and **End Time** settings to define when the recipient is available.

   To define an availability range that starts on one day and ends on the next, use the **Start** and **End Time** settings for the day on which the availability starts.
3. Repeat steps 1 and 2 to edit another **Day of the Week**.

FTP Server Settings

Use the display tabs for this System Management menu option to do the following:

FTP must be enabled before you can download software updates using the Apply Server Updates option in the Updates menu.

Status tab	Start or stop FTP access to the InfraStruXure Manager server.
Username/Password tab	Define the **Username** and **Password** used for FTP access (apc, lowercase, is the default value for both).

System Identification

Use the display for this System Management menu option to define the InfraStruXure Manager **System Name**, **Contact**, and **Location** values.

Proxy Settings

Use the display for this System Management menu option to enable the InfraStruXure Manager server to communicate with the APC Web site over a network that uses a proxy server.

Select the **Proxy Enabled** option and define the following values:

Note

Click **Test** to make sure the InfraStruXure Manager server can access the identified proxy server using the proxy settings you define.

Proxy Host	The IP address or hostname of the proxy server
Port Number	The port at the proxy server the InfraStruXure Manager server will use to communicate with that server
Username and **Password**	The username and password used to access the proxy server. **NOTE:** If the proxy server does not require a username and password, leave these fields blank.

Log Settings

Use the display for this System Management menu option to define settings that affect the event and data logs.

When the Incident management module is activated, the **Clear Event Log** option becomes **Clear Event and Incident Logs**. When used, this option clears all event log entries, as well as the data used by two incident management displays: "Incident History" display and "Recipient Incident Actions" display.

Event Log	**Clear events after**: The age, in days, at which events are deleted automatically from the event log. **Clear Event Log**: Clears all events from the log.
Data Log	**Clear data after**: The age, in days, at which data are deleted automatically from any data log. **Log data every**: How often, in minutes, data is recorded in the data logs. **Clear Data Log**: Clears all data from all data logs.

License Keys

Overview

When a new InfraStruXure Manager server is installed, its features and functions can be used for 30 days without any license keys. When an existing InfraStruXure Manager server is updated to at least version 4.3, the new version can be used for 30 days without updating the previous version's license keys.

The 30-day evaluation process allows you to identify how many supported APC power and environmental protection devices you want the InfraStruXure Manager server to monitor (up to 1000) on the InfraStruXure Manager server's APC and User Local Area Networks (LANs). Once you add or update license keys at the server, the evaluation period ends, and the ability to monitor devices is limited to the number of devices allowed by those license keys.

The following displays are involved in adding or updating license keys at a new or updated InfraStruXure Manager server:

- "License Keys" display
- "Evaluation Period" display
- "Update License Keys" display
- "Product Activation" display
- "Insufficient License Keys" display

"License Keys" display

Use this display to manage (add or remove) InfraStruXure Manager license keys. This display identifies the total nodes allowed by the existing licenses, and lists those licenses in the **Entered Keys** section.

When an InfraStruXure Manager server is updated, the previous version's license keys must be updated. Until they are, the "License Keys" display description includes a **Click here to update the license keys online** link. To use this link to update the license keys, even if your InfraStruXure Manager client has no internet access, see Using the "License Keys" display to update license keys.

Add a license key. Identify the license key in the **New Key** field at the bottom of the "License Keys" display, and click **Add**. The InfraStruXure Manager server will send the license key identification to an activation server. If the activation server validates the license key, that license is added in the **Entered Keys** section of the display.

For information about how to validate a license key when the InfraStruXure Manager server cannot access the activation server, see "Product Activation" display.

Remove a license key. Select the license in the **Entered Keys** section of the "License Keys" display and click **Remove**, or right-click that license and select **Remove Key**.

You can remove a license key only if the total of the remaining keys at least equals the number of Supported devices being monitored by the InfraStruXure Manager server.

"Evaluation Period" display

This display appears when you log on at a recently installed InfraStruXure Manager server at which no license keys have been added. It informs you whether the evaluation period has expired, or how much of the evaluation period remains. Use this display to do the following:

- Continue to use the InfraStruXure Manager server without adding any license keys, if the evaluation period has not expired (click **Close**).
- Purchase license keys for the InfraStruXure Manager server:
  a. Click **Purchase a license key online**, if your InfraStruXure Manager client has internet access, or use the following URL to open the InfraStruXure Manager product page at a client that has internet access:
  www.apc.com/products/family/index.cfm?id=56
  b. Select the appropriate country from the drop-down list at the top of the page.
  c. Use the cart icons, and follow the on-screen instructions, to purchase the needed licenses.
- Add license keys that have been purchased to the "License Keys" display (click **Enter a License Key**).

"Update License Keys" display

This display appears when you log on at an updated version of the InfraStruXure Manager server at which none of the previous version's license keys have been updated. Use this display to do the following:

- Continue to use the InfraStruXure Manager server without updating the license keys for the previous server version, if the evaluation period has not expired (click **Close**).
- Identify the new license keys for the updated InfraStruXure Manager server.
  - **At a client with internet access**:
    a. Click **Update license keys online**.
    b. Follow the instructions on the Update Licenses Web page to identify the e-mail address to which you want the license key identifications sent.
  - **At a client without internet access**:
    a. Right-click **Update license keys online** and select **Copy**.
    b. Paste the copied link information into a text file. This link information is a URL address for the Update Licenses Web page that includes the identification of the licenses that need to be updated.
    c. At a computer with internet access, use the link information as the Web browser's URL address.
    d. Follow the instructions on the Update Licenses Web page to identify the e-mail address to which you want the license key identifications sent.
- Add updated license keys to the "License Keys" display (click **Enter a License Key**).

"Product Activation" display

This display appears when you attempt to add a license key in at the "License Keys" display when the InfraStruXure Manager server cannot access the activation server. Use this display as follows:

- **At a client with internet access:**
  a. Click the provided Web link.
  b. Follow the on-screen instructions in the Customer Activation page.
  c. When the activation code appears in the text box, click **Activate**.
- **At a client without internet access:**
  a. Contact APC Worldwide Customer Support and provide the identified License Key and Serial Number.
  b. Type the activation code that APC provides into the text box.
  c. Click **Activate**.

"Insufficient License Keys" display

This display appears when not enough licenses have been added or updated in the "License Keys" display to allow the InfraStruXure Manager server to continue to monitor the devices it has been monitoring during the 30-day evaluation period. For example, if the InfraStruXure Manager server was monitoring 540 devices during the evaluation period, and the license total equals 500, you must do one of the following before you can start using the InfraStruXure Manager server:

- Add license keys until the total reported in the "License Keys" display equals or exceeds the number of monitored devices.
- Access the "Device List" frame and delete devices until the number of monitored devices does not exceed the license keys total reported in the "License Keys" display.

Using the "License Keys" display to update license keys

If your InfraStruXure Manager client has internet access, use **Click here to update the license keys online** to update the existing license keys online.

If your client has no internet access, do the following:

1. Right-click **Click here to update the license keys online** and select **Copy**.
2. Paste the copied link information into a text file. This link information is a URL address for the Update Licenses Web page that includes the identification of the licenses that need to be updated.
3. At a computer with internet access, use the link information as the Web browser's URL address.
4. Follow the instructions on the Update Licenses Web page to identify the e-mail address to which you want the license key identifications sent.
5. Use the "License Keys" display to add the new license keys, one key at a time.

Client Preferences

Use the display tabs for this System Management menu option to do the following:

Temperature Units	Select whether **Fahrenheit** (the default setting) or **Celsius** will be used to report temperatures.
Data Collection	Enable the periodic sending of information to APC about how you use the InfraStruXure Manager features. **NOTE:** No personal information is sent about any user, server, network, system, etc., only general information about how the InfraStruXure Manager features are used.

Updates menu

Overview

Use the menu options to do the following:

Unless you log on as the Administrator, these menu options are disabled. See Administrator versus General access.

Check for Updates	Schedule how often the InfraStruXure Manager server checks for available updates, or check for updates immediately. **NOTE:** To check for updates, the InfraStruXure Manager server must be able to use the internet to access the APC auto-update server.
Apply Firmware Updates	Apply firmware updates to devices monitored by the InfraStruXure Manager server. **NOTE:** After a firmware update is applied, use the **Refresh** option in the View menu to refresh the InfraStruXure Manager server displays.
Apply Server Updates	Apply an update to the InfraStruXure Manager server.

Check for Updates

Use the display for this Updates menu option to schedule when, if ever, the InfraStruXure Manager server automatically checks for firmware updates, or to immediately check for those updates.

To check for updates, the InfraStruXure Manager server must be able to use the internet to access APC's auto-update server:

- When device firmware updates are discovered, the InfraStruXure Manager server automatically downloads those files. You can then use the Apply Firmware Updates option to update the firmware at monitored devices.
- When an InfraStruXure Manager update is available, you must manually Import the product update file to the InfraStruXure Manager server before you can use the Apply Server Updates option to apply the update.

The InfraStruXure Manager server can send a notification when a firmware update is available for a monitored device. See Notification Settings.

Automatically Check for Updates	Use the **Date** and **Time** settings to identify when the first check occurs, and the **Recurrence** setting to define how often checks will occur.
I want to know when server or client updates are available	Enable a pop-up to appear whenever you log on after an available InfraStruXure Manager update has been discovered. The pop-up provides a link to the update. You must Import the product update file to the InfraStruXure Manager server before you use the Apply Server Updates option. **NOTE:** This setting is client-specific. It will not affect any other InfraStruXure Manager clients.
Check for Updates Now	Click to immediately check for available updates.

Apply Firmware Updates

Overview

Use the display tabs for this Updates menu option to do the following:

FTP must be enabled at a device, and the correct FTP username and password for that device must be used, before firmware can be updated at that device. For information about adding FTP username and password settings or changing the **FTP Port** and **Retries** settings, see FTP Settings.

Configure Update tab	Apply available firmware updates.
Last Update Results tab	View the firmware update results.

Configure Update tab

Use this tab to apply an available update to monitored devices:

1. Select an update from the **Available Firmware Updates** list.
2. Select the devices to be updated from the list in the lower, right-hand box of the display.

   Only devices that use a management card to which the available firmware update can be applied are listed.
3. Click **Update Now**.
4. Click **Yes** to start the update process.
5. When the update finishes, select the **Refresh** option in the View menu to refresh the InfraStruXure Manager server displays.

The **Configure Update** tab also includes the following elements.

Next Update Check field	Identifies when the InfraStruXure Manager server will check for updates, as defined by the Check for Updates option.
Update details box	Provides information about the update selected in the **Available Firmware Updates** list.

Last Update Results tab

Use this tab to view the results of the last firmware update.

Aborted	**Description**: The device was removed from the list of monitored devices after **Update Now** was clicked in the Configure Update tab, but before the InfraStruXure Manager server could schedule the update for that device. **Recommended Action**: Use the Add Devices option in the Edit menu to rediscover the device, and apply the update.
AOS Connection Failed **AOS Download Failed** **App Connection Failed** **App Download Failed**	**Description**: The InfraStruXure Manager server had the password, username, and FTP port it needed to log on to the device, but the FTP connection was lost before it could log on (connection failed) or update (download failed) the APC operating system (AOS) or APC application layer (App) file at the device. **CAUTION:**The device may not function correctly until this problem is corrected. **Recommended Action**: • Make sure the device is turned on and connected to the network. • Correct any network connection problem. • If the problem persists, contact APC Customer Support. Once the problem is corrected, use the Configure Update tab to apply the update to the device.

Cancelled	**Description**: The device was removed from the list of monitored devices after the update was selected in the **Available Firmware Updates** list (Configure Update tab), but before **Update Now** was clicked. **Recommended Action**: Use the Add Devices option in the Edit menu to rediscover the device, and apply the update to that device.
File Verification Failed	**Description**: The APC operating system (AOS) or APC application layer (App) files at the device do not match the files the InfraStruXure Manager server used for the update. The APC operating system (AOS) or APC application layer (App) file name may have changed or a file is corrupted. **CAUTION:**The device may not function correctly until this problem is corrected. **Recommended Action**: Contact APC Customer Support to verify that the correct AOS and application files are available at the APC server, and then use the Configure Update tab to apply the update after you download the update again.
FTP Logon Failed	**Description**: The InfraStruXure Manager server could not log on to the device. **Recommended Action**: • Make sure the FTP service is enabled at the device, and the Device Access option (FTP Settings) identifies the username, password, and FTP port needed to access the device. • Make sure the device is turned on and connected to the network. • Correct any network connection problem. • If the problem persists, contact APC Customer Support. Once the problem is corrected, use the Configure Update tab to apply the update to the device.

Initialization Failure	**Description**: The InfraStruXure Manager server could not find one or both of the files it downloaded from APC for the selected update. **Recommended Action**: Use the Check for Updates option to schedule a new update check, and after the firmware files are downloaded, use the Configure Update tab to apply the update to the devices.
Update Verification Failed	**Description**: The update was completed, but the InfraStruXure Manager server could verify that it was successful. In addition to the network and FTP issues that can cause this problem, the APC application layer (App) file may have caused an unrecoverable problem at the device. **CAUTION:**The device may not function correctly until this problem is corrected. **Recommended Action**: See the recommended actions for FTP Logon Failed.

Apply Server Updates

Use the display for this Updates menu option to update the InfraStruXure Manager server and client when a product update is available.

1. Import the product update file to the InfraStruXure Manager server.
2. Select the InfraStruXure Manager server update in the **Available Product Updates list** section, and click **Apply**.

Installed Products	Identifies the current firmware for the InfraStruXure Manager Server and Operating System (OS).
Available Product Updates	Lists available updates.
Apply	Installs the update selected in the **Available Firmware Updates** list.

3. Click **Yes** to reboot the server.
4. When a message informs you the connection has been lost, click **OK**.
5. Follow any on-screen instructions that appear while the update progress is displayed.
6. When the “Server Log On” display appears, log on to the server.
7. Select the **About** option in the Help menu to verify that the **Server Version** and **Client Version** match the version for the applied update.

Import the product update file to the InfraStruXure Manager server

Overview

To import an available product update to the InfraStruXure Manager server:

1. Enable FTP at the InfraStruXure Manager server
2. Download the update file to the InfraStruXure Manager client
3. Use FTP to transfer the update file to the InfraStruXure Manager server

To apply the update once it is imported to the InfraStruXure Manager server, see Apply Server Updates.

Enable FTP at the InfraStruXure Manager server

The FTP service must be enabled before the InfraStruXure Manager server can import an update file.

1. Log on to the InfraStruXure Manager server to be updated.
2. Select FTP Server Settings, a System Management menu **Network** option.
3. In the "FTP Settings" display, check the **FTP Server Status** in the "Status" tab.
   - **Started**: The FTP service is enabled.
   - **Not Started**: Click **Apply** (**Start service** is selected when the service is disabled).

You can use the "Username/Password" tab to define the username and password used for FTP access to the InfraStruXure Manager server. By default, both settings use **apc** (lowercase).

Download the update file to the InfraStruXure Manager client

Before you can transfer an update file to the InfraStruXure Manager server, that file must be downloaded from APC.

1. Go to the download page at the APC Web site (www.apc.com/tools/download/).
2. If necessary, select your country or region from the drop-down list at the top of the page.
3. In the InfraStruXure Manager section, click the update's **Free Download** button.
4. Follow the links to download the update (*.upd) file to a directory at the InfraStruXure Manager client.
5. Import the update (*.upd) file to the InfraStruXure Manager server.

See Use FTP to transfer the update file to the InfraStruXure Manager server

Use FTP to transfer the update file to the InfraStruXure Manager server

Once you Download the update file to the InfraStruXure Manager client, import that file to the InfraStruXure Manager server:

1. At a command prompt, use the cd command to navigate to the directory that contains the update (*.upd) file.
2. Type `ftp` and the IP address of the InfraStruXure Manager server.
3. At the `User` prompt, type the server's FTP username (the default is lowercase `apc`) and press ENTER.
4. At the `Password` prompt, type the server's FTP password (the default is lowercase `apc`) and press ENTER.
5. At the `ftp>` prompt, type `bin` (or `binary`) and press ENTER.
6. At the next `ftp>` prompt, type `put <filename.upd>`, where `<filename.upd>` is the name of the update (*.upd) file, and press ENTER.
7. At the next `ftp>` prompt, type `bye` and press ENTER to exit FTP.
8. See Apply Server Updates to update the InfraStruXure Manager server.

Help menu

Use the menu options to do the following:

Contents	Open the help at the Introduction.
Context Help	Open the help for the currently selected main display: "Device Status" display, "Power Zones" display, "Reports" display, or "Logs" display.
About	View the **Server Version, Console Version**, **Server Up-time,** and **Server Hardware** information (**Serial Number**, **Model Number**, **Hardware Revision**, and **Manufacture Date**).

Reports

Overview

Use the "Reports" display to generate reports about devices the InfraStruXure Manager server monitors. Reports list devices by their IP addresses, and can include some or all of the following information about the report's devices: **Hostname**, **Serial Number**, **Model**, **Firmware**, **Hardware**, **Manufactured**, **Contact**, **Location**, and **Device Name**.

- Environmental report
- Exceptions reports
- Rack PDU reports
- UPS reports

To customize the columns displayed, saved, or printed for the reports, see "Configure Columns" display; for information about the features the reports share, see Common report and log features; for information about the display that appears when you initiate a report, see "Select Report Filter" display.

Common report and log features

Reports and logs share the following features:

Feature	Description
Export Report button: 	Use to save a report or log to a file.
Print Report button: 	Use to print a report or log.
Filter Data button:  **(Reports only)**	Use to access the "Select Report Filter" display to generate a new version of the current report.
Next Page and **Previous Page** buttons  **(Logs only)**	Use to move through a log, one day at a time.
Double-click a listed device to access more information about that device	For a monitored APC InfraStruXure Manager server, the "Server Log On" display appears with that server selected in the **Server** field. For an InfraStruXure PDU, an InfraStruXure PDU details display appears. For some Metered Rack Power Distribution Unit (Rack PDU) versions, a Metered Rack PDU details display appears. For all other devices, an HTML "Device Details" display accesses the management application at the device.
Sort by column headings	Click a column heading to sort the report or log in ascending or descending order, based on that column's data.
Reports only: Select the devices to be included	Use the "Select Report Filter" display to select the devices.

"Select Report Filter" display

Use this display to customize a report:

- "Groups" tab: Click **Selected Groups** to limit the report to the groups you select. By default, **Select All Groups** is enabled.

  Note: This display lists the Device groups that have a relevant device. For example, for a **UPS 3-Phase Load** report, only groups with a 3-phase UPS are listed.

- "Date Range" tab (**Downtime** report only): Use **Begin** and **End** (by default, **Selected Date Range** is enabled) to define a date range for the report, or click **Select All Dates** to include all available data.

Once you select the tab settings, click **Generate Report**.

Environmental report

A **Model** report provides information about the monitored Environmental Monitoring Units, Environmental Monitoring Cards, and Environmental Management Systems.

Devices are listed, by **IP address**, within **Model Name** categories (for example, Environmental Management System). Each device listing can include information about the number of local (**Probe Count**) and remote (**Remote Probe Count**) probes, and Air Replacement Units (**ARU Count**).

Exceptions reports

Overview

The following **Exceptions** reports are available:

- Bad Battery report
- Downtime report
- Exceptions Summary report

Bad Battery report

Identifies by IP address, the UPS systems that are reporting at least one faulty battery.

Downtime report

Overview. Two tabs provide information about the downtime, on-battery, and lost-communication events that occurred at the monitored UPS systems:

The downtime status reports information about any UPS that turned off while the InfraStruXure Manager server was polling that UPS to monitor an on-battery condition. The downtime status lasts until InfraStruXure Manager polling indicates the UPS turned on again.

For information about how a **Downtime** report's date range is defined, see "Select Report Filter" display.

- "Detail" tab
- "Summary" tab

"Detail" tab. Lists, by IP address, the UPS systems at which downtime, on-battery, or lost-communication events occurred, and identifies the following information for those events:

Event	The type of event that occurred: Lost Communication, On Battery, or Downtime.
Event Start	When the event started, by date and time.
Event End	When the event ended, by date and time.
Event Duration	How long the event lasted.

"Summary" tab. Provides information about power and communication problems that occurred during the **Reporting Period Start** to **Reporting Period End** date range.

Number of UPS systems reporting Downtime events	How many UPS systems shut down due to a low-battery condition while on battery.
Number of reported Downtime Events	How many times the UPS systems shut down due to a low-battery condition while on battery.
Estimated total time for all Downtime events (all instances/all UPS systems)	The estimated total time power was shut down for all Downtime events at all UPS systems.
Average time for each reported Downtime event	The average amount of time a UPS was shut down in response to a power problem.
Number of UPS systems reporting On Battery events	How many UPS systems switched to battery operation in response to a power problem.
Number of reported On Battery Events	How many times the UPS systems switched to battery operation in response to power problems.

Estimated total time for all On Battery events (all instances/all UPS systems)	The estimated total time the UPS systems were switched to battery operation for all On Battery events.
Average time for each reported On Battery event	The average amount of time a UPS was switched to battery operation in response to a power problem.
Number of UPS systems reporting Lost Communication events	How many UPS systems lost communication with the InfraStruXure Manager server.
Number of reported Lost Communication events	How many times the UPS systems lost communication with the InfraStruXure Manager server.
Estimated total time for all Lost Communication events (all instances/all UPS systems)	The estimated total time communication was lost for all Lost Communication events at all UPS systems.
Average time for each reported Lost Communication event	The average amount of time communication was lost between a UPS and the InfraStruXure Manager server.

Exceptions Summary report

Identifies devices that are violating the InfraStruXure Manager Global Device Thresholds, or that have status exceptions (**Communication Lost**, **Bad Battery**, and **Failed Self-Test**).

If none of the exceptions listed in the table exist at any device group or groups selected for an Exceptions Summary report, the report that appears will have no entries.

Violation: UPS Age	Identifies UPS systems that violate the UPS age threshold in the UPS tab.
Violation: UPS Load	Identifies UPS systems violate the load threshold in the UPS tab.
Violation: Rack PDU Load	Identifies Metered Rack PDU, Switched Rack PDU, and MasterSwitch devices that violate the load threshold in the Metered Rack PDU tab.
Violation: Battery Age	Identifies UPS systems that violate the battery age threshold in the UPS tab.
Violation: High Temperature	Identifies devices with probes that violate the identified threshold in the Environmental Monitor tab.
Violation: Low Temperature	
Violation: High Humidity	
Violation: Low Humidity	
Violation: Lost Communication	Identifies devices that have lost communication with the InfraStruXure Manager server.
Violation: Bad Battery	Identifies UPS systems that have faulty batteries.
Violation: Failed Self-Test	Identifies UPS systems that failed their last self-test.
Violation: Minimum Runtime	Identifies UPS systems that violate the runtime threshold in the UPS tab.

Rack PDU reports

Three reports provide information about the monitored Metered Rack PDUs, Switched Rack PDUs, and MasterSwitch devices.

1-Phase Load	Lists devices, by **IP address**, in **Load Range** categories (for example, **0-10 Amps**). **NOTE:** A device is listed under **Unknown** when the **Load Range** cannot be determined.
3-Phase Load	Lists devices, by **IP address**, without categories, since the load can vary for each output phase at a device.
Model	Lists devices, by **IP address**, within **Model Name** categories (for example, **MasterSwitch VM**). **NOTE:** A device is listed under **Unknown** when the **Model Name** cannot be determined.

UPS reports

The following reports provide information about the monitored UPS systems.

1-Phase Load	Lists UPS systems, by **IP address**, in **Output Load**-range categories (for example, **0-20%**). **NOTE:** A UPS is listed under **Unknown** when the **Output Load** cannot be determined.
3-Phase Load	Lists UPS systems, by **IP address**, without categories, since the load can vary for each output phase at a UPS.
Battery Age	Lists UPS systems, by **IP address**, within **Battery Age**-range categories (for example, **0-1 years old**). **NOTE:** A UPS is listed under **Unknown** when the **Battery Age** cannot be determined.
Model	Lists UPS systems, by **IP address**, within **UPS Type** categories (for example, **Smart-UPS**). **NOTE:** A UPS is listed under **Unknown** when the **UPS Type** cannot be determined.
Runtime	Lists UPS systems, by **IP address**, within available **Runtime Range** categories (for example, **0-10 Minutes**). **NOTE:** A UPS is listed under **Unknown** when the **Runtime Range** cannot be determined.
UPS Age	Lists UPS systems, by **IP address**, within **UPS Age**-range categories (for example, **0-1 years old**). **NOTE:** A UPS is listed under **Unknown** when the **UPS Age** cannot be determined.

Data logs

Use the "Device List" frame or "Logs" display to generate a data log for any of the types of monitored devices typically used in InfraStruXure zones:

For information about how to define how often log data is sampled, see Log Settings.

- "Device List" frame: Right-click a listed ATS, InfraStruXure PDU, Rack PDU, Symmetra UPS, Silcon UPS, or environmental device and select **View Data Log** (**View Data Log** is disabled for other devices).
- "Logs" display: Do the following in the left frame:
  a. Select **Data Log** as the **Log Type**.
  b. Select the **Date** you want the log to display initially.
  c. Select the IP address of the device for which you want to create a data log from the **Select a Device** list.
  d. Click **Generate Report**.

The following table identifies the information the different data logs provide.

For information about features the data logs share, see Common report and log features; to customize the columns used in displayed, saved, or printed data log, see "Configure Columns" display.

Automatic Transfer Switch (ATS)	• The source (**Active Source**) selected when the data was sampled • The voltage (**L1 (VAC)** - **L3 (VAC)**) and **Frequency (Hz)** at each source (**Source A** and **Source B**) • The **Output Current (Amps)** at each output phase (**L1**-**L3**)

Environmental	• The **Model Name** of each device • The **Name**, **Temp** (**°F** or **°C**), and **Humidity** from up to ten probes (**Probe 1** - **Probe 10**) **Note**: The **Symmetra/Silcon** data log provides probe data for environmental devices that connect to the network through a Symmetra or Silcon UPS. • The **Name** and three **Temp** (**°F** or **°C**) values from up to eight Air Removal Units (**ARU 1** - **ARU 8**) at environmental devices that support these units **Note**: To select the temperature unit (**°F** or **°C**) for reports and displays, see Client Preferences.
InfraStruXure PDU	• The **Main Input Voltage (VAC)** at each input (**L1**-**L3**) and transformer phase (**Trans L1**-**Trans L3**) • The **Bypass Input Voltage** at each phase (**L1**-**L3**) of a dual-input InfraStruXure PDU • The phase-to-phase **Output Voltage L-L (VAC)** at each output phase (**L1**-**L3**) • The phase-to-neutral **Voltage L-N (VAC)** at each output phase (**L1**-**L3**) • The **Output Current (Amps)** at each output phase and the neutral wire (**L1**-**L3** and **N**) • The **Output Power (kW)** and **Output Power (kVA)** values at each output phase (**L1**-**L3**), and the **Total** for each output type • The **Output Frequency (Hz)** and **Ground Current (Amps)** **Note**: For more information about the log values, see InfraStruXure PDU details.
Rack PDU (see note in description)	• The unit number (**Unit #**) for each device • The **Current (Amps)** at each output phase (**L1**-**L3**). **NOTE:** A data log can be created for any Metered Rack PDU, Switched Rack PDU, or MasterSwitch VM device; data logs are unavailable for MasterSwitch V1, MasterSwitch V2, or MasterSwitch Plus devices.

Symmetra/Silcon	• The **Input Voltage (VAC)** and **Input Current (Amps)** at each input phase (**L1**-**L3**) • The **Output Voltage (VAC)**, **Output Current (Amps)**, **Output Load (VA)**, and **Output Power (W)** (as a percentage of full load capacity) at each output phase (**L1**-**L3**) • The **Input Frequency (Hz)** and **Output Frequency (Hz)** • **Battery Data**: The **Capacity**, **Voltage (VDC)**, **Temp** (**°F** or **°C)**, and **Current (Amps)** that was available • **Environmental Data**: The **Temp** (**°F** or **°C**) and **Humidity** values that were available from each probe **Note**: To select the temperature unit (**°F** or **°C**) used in reports and displays, see Client Preferences.

Event log

Overview

Use the left frame of the "Logs" display to generate an event log:

1. Select **Event Log** as the **Log Type**.
2. Select the **Date** you want the log to display initially (use the arrow buttons to move back and forth through the log, one day at a time).
3. Select the **Event Type** options to include in the log.
   - **System**: Events that occurred at the InfraStruXure Manager server.
   - **Status**: Events that occurred at monitored devices.

   You must select at least one option.
4. Select the **Severity** entries to include in the log:
   - **Critical**, **Warning**, or **Informational**: **System** (InfraStruXure Manager server) or **Status** (monitored device) events for any selected severity.
   - **Summary**: A notification that was sent summarizing power-related events at a device group.
   - **Firmware**: Entries related to firmware updates for the monitored devices.

   You must select at least one option. For more information about the **Critical**, **Warning**, and **Informational** selections, see Status and event severity levels; for more information about the **Summary** and **Firmware** selections, see System events.

The following table describes the information an event log provides.

To disable columns in a displayed, saved, or printed event log, see "Configure Columns" display.

Log Time	The date and time at which the event occurred.
IP Address	The IP address of the device at which the event occurred, or blank, if the event is for the InfraStruXure Manager server itself. **NOTE:** Except for System events, you can double-click an event to access more information about the device associated with the event.
Severity Level	The event severity level (**Critical**, **Warning**, **Informational**, **Summary**, or **Firmware**). **NOTE:** For more information about **Critical**, **Warning**, and **Informational** events, see Status and event severity levels; for more information about **Summary** or **Firmware** events, see System events.
Event Text	The event that occurred.

Events

Overview

The following sections list the events that can appear in the Event log for the identified devices. For each device, events are listed alphabetically, by severity, and recommended actions are provided, where appropriate.

For information about events that use a different prefix than those listed below, see <Other APC Device> events.

- APC InfraStruXure Manager events
- ATS events
- Environmental events
- InfraStruXure PDU events
- MasterSwitch events
- MasterSwitch Plus events
- MasterSwitch VM events
- Rack PDU events
- System events
- UPS events

System events report operational and status events directly related to the operation of the InfraStruXure Manager server.

APC InfraStruXure Manager events

The Event log can report general-status and communication events for a monitored InfraStruXure Manager server.

Note

When communication with a monitored InfraStruXure Manager server is lost, the fact that it is a monitored InfraStruXure Manager server can no longer be determined. Therefore, APC Device is used as the prefix for lost-communication events.

Critical Events	Recommended Actions
APC InfraStruXure Manager: A critical condition exists	Access the management application at the device to identify and correct the problem.
APC Device: The agent lost communication with the device	Make sure the device and its agent are connected properly to the network and that normal power is available to both. If the problem persists, contact APC Support.
APC Device: The InfraStruXure Manager server lost communication with the agent	
Warning Events	
APC InfraStruXure Manager: A warning condition exists	Access the management application at the device to identify and correct the problem.
APC InfraStruXure Manager: Notifications disabled for maintenance	If necessary, use “Enable Notifications” in the “Notification” menu once the reason for disabling notifications no longer exists.
Informational Events (No Action Required)	
APC InfraStruXure Manager: Notifications now enabled	
APC InfraStruXure Manager: The agent established communication with the device	
APC InfraStruXure Manager: The InfraStruXure Manager server established communication with the agent	
APC InfraStruXure Manager: This device is now operating normally	

ATS events

The Event log can report the following Automatic Transfer Switch (ATS) events:

Critical Events	Recommended Actions
ATS: A fault exists at the 5V power supply	The ATS cannot provide power to its hardware SNMP Agent while a 5V power supply failure exists. Contact APC Support.
ATS: A fault exists at the 24V power supply	The ATS cannot switch its power source while a power supply failure exists. Contact APC Support.
ATS: An output overcurrent threshold violation exists	Make sure the threshold is set correctly at the device. Reduce the load, if necessary. If the problem persists, contact APC Support.
ATS: The ability to switch between power sources was lost	Correct the problem at the power source that lost its AC input power. If the problem persists, contact APC Support.
ATS: The agent lost communication with the device	Make sure the device and its agent are connected properly to the network and that normal power is available to both. If the problem persists, contact APC Support.
ATS: The InfraStruXure Manager server lost communication with the agent	
Warning Events	
ATS: Lost input power	Correct the AC input power problem. If the problem persists, contact APC Support.
ATS: Notifications disabled for maintenance	If necessary, use “Enable Notifications” in the “Notification” menu once the reason for disabling notifications no longer exists.

Firmware Events (No Action Required Except as Noted)	
ATS: Agent firmware is being updated	
ATS: Agent firmware update failed	Make sure FTP is enabled at the device, and try to update the firmware again. If the problem persists, contact APC Support.
ATS: Agent firmware update is available or succeeded	
Informational Events (No Action Required)	
ATS: A fault no longer exists at the 5V power supply	
ATS: A fault no longer exists at the 24V power supply	
ATS: A reset was performed	
ATS: An output overcurrent threshold violation no longer exists	
ATS: Notifications now enabled	
ATS: Switched to Source A	
ATS: Switched to Source B	
ATS: The ability to switch between power sources was regained	
ATS: The agent established communication with the device	
ATS: The InfraStruXure Manager server established communication with the agent	

Environmental events

The Event log can report the events for environmental devices (Environmental Monitoring Cards, Environmental Monitoring Units, and Environmental Management Systems) that do not connect to the network through a UPS. For information about the temperature, humidity, contact, and relay events that occur at an environmental monitoring device that connects to the network through a UPS, see UPS events.

Unless the InfraStruXure Manager server is defined as a trap receiver at some environmental monitoring devices, only Global Device Thresholds events can be logged for those devices. See Trap receiver feature.

Critical Events	Recommended Actions
Environmental: A fan <*n*> failure exists at air removal unit <*n*> (<*unit name*>)	A hardware failure exists. Contact APC Support.
Environmental: A fault exists at contact <*n*> (<*contact name*>)	Correct the fault condition. If the problem persists, contact APC Support.
Environmental: A fault exists at outlet <*n*> (<*outlet name*>)	Correct the fault condition. Make sure the outlet was not switched to its fault position using the management card's Outlet Control feature. If the problem persists, contact APC Support.
Environmental: A fault exists at output relay <*n*> (<*relay name*>)	Correct the fault condition. Make sure the output relay was not switched to its fault position using the management card's Output Relay Control feature. If the problem persists, contact APC Support.
Environmental: A fault exists at sensor <*n*> (<*sensor name*>)	Correct the fault condition. If the problem persists, contact APC Support.

Environmental: A high-temperature violation exists at air removal unit <*n*> (<*unit name*>)	Correct the temperature problem. If the problem persists, contact APC Support.
Environmental: A Major alarm exists	Check the device's status and correct the fault that caused the alarm
Environmental: A Minor alarm exists	
Environmental: An A-Link power overload exists	Make sure the A-Link device is installed correctly and that terminators are not connected to both A-Link ports on the Environmental Management System. If the problem persists, contact APC Support.
Environmental: An exhaust-temperature violation exists at air removal unit <*n*> (<*unit name*>)	Correct the temperature problem. If the problem persists, contact APC Support.
Environmental: A sensor connection error exists	Make sure the sensor is installed correctly, with the sensor connected securely to the correct port on the Environmental Management System. If the problem persists, contact APC Support.
Environmental: A smoke violation exists at air removal unit <*n*> (<*unit name*>)	Correct the smoke problem. If the problem persists, contact APC Support.
Environmental: Lost communication with air removal unit <*n*> (<*unit name*>)	Make sure the air removal unit is connected correctly to the environmental monitoring device. If the problem persists, contact APC Support.
Environmental: The agent lost communication with the device	Make sure the device and its agent are connected properly to the network and that normal power is available to both. If the problem persists, contact APC Support.
Environmental: The InfraStruXure Manager server lost communication with the agent	

Environmental: Violates a <*humidity or temperature*> threshold for sensor <*n*>	Make sure the threshold is set correctly at the device, and the central air conditioning system is functioning properly. If the problem persists, see the APC Cooling Solutions product page for information about air conditioning equipment designed specifically for UPS and IT environments. Otherwise, contact APC Support.
Environmental: Violates the InfraStruXure Manager global device <*humidity or temperature*> threshold for sensor <*n*>	Make sure the <*humidity or temperature*> threshold is set correctly in the Environmental Monitor tab of the "Global Device Thresholds" display. Also, make sure the central air conditioning system is functioning properly. See the APC Cooling Solutions product page for information about air conditioning equipment designed specifically for UPS and IT environments. If the problem persists, contact APC Support.
Warning Events	
Environmental: Notifications disabled for maintenance	If necessary, use "Enable Notifications" in the "Notification" menu once the reason for disabling notifications no longer exists.
Environmental: The alarm beacon is on	Correct the fault condition. Make sure the beacon was not switched to its fault position using the management card's Beacon Control feature. If the problem persists, contact APC Support.
Environmental: The Check Event Log Light is on	Check the device's event log and correct the fault that caused the event log light to go on.
Firmware Events (No Action Required Except as Noted)	
Environmental: Agent firmware is being updated	
Environmental: Agent firmware update failed	Make sure FTP is enabled at the device, and try to update the firmware again. If the problem persists, contact APC Support.
Environmental: Agent firmware update is available or succeeded	

Informational Events (No Action Required)
Environmental: A fan <*n*> failure no longer exists at air removal unit <*n*> (<*unit name*>)
Environmental: A fault no longer exists at <*device*> <*n*> (<*device name*>)
Environmental: A high-temperature violation no longer exists at air removal unit <*n*> (<*unit name*>)
Environmental: A major alarm no longer exists
Environmental: A minor alarm no longer exists
Environmental: An A-Link power overload no longer exists
Environmental: An exhaust-temperature violation no longer exists at air removal unit <*n*> (<*unit name*>)
Environmental: A sensor connection error no longer exists
Environmental: A smoke violation no longer exists at air removal unit <*n*> (<*unit name*>)
Environmental: <*Connected or Disconnected*> sensor <*n*>
Environmental: No longer violates the <*humidity or temperature*> threshold for sensor <*n*>
Environmental: No longer violates the InfraStruXure Manager global device <*humidity or temperature*> threshold for sensor <*n*>
Environmental: Notifications now enabled
Environmental: Restored communication with air removal unit <*n*> (<*unit name*>)
Environmental: The agent established communication with the device
Environmental: The alarm beacon is now off
Environmental: <*Connected or Disconnected*> the alarm beacon
Environmental: The Check Event Log Light is now off
Environmental: The InfraStruXure Manager server established communication with the agent

InfraStruXure PDU events

The Event log can report the following InfraStruXure Power Distribution Unit (PDU) events:

Critical Events	Recommended Actions
InfraStruXure PDU: A fan failure exists	Replace the fan. Contact APC Support.
InfraStruXure PDU: A fault exists at contact <*n*> (<*name*>)	Identify and correct the problem that activated this fault. If the problem persists, contact APC Support.
InfraStruXure PDU: Bypass input breaker is open	Close the bypass breaker if no UPS maintenance is being performed. If UPS maintenance is being performed, close the breaker as soon as that maintenance is completed to avoid dropping the load if a main input power problem occurs.
InfraStruXure PDU: Lost the phase L<*n*> input to the UPS	Correct any problem that is external to the PDU, such as a tripped circuit breaker. If the problem persists, contact APC Support.
InfraStruXure PDU: Q breakers set for no panel feed mode	For an 60 kW or 150 kW InfraStruXure PDU, close the Panel Feed breaker. For all other InfraStruXure PDUs, see Q-Breaker Modes for descriptions of the available modes and their breaker settings.
InfraStruXure PDU: Q breakers set for system off mode	See Q-Breaker Modes for descriptions of the available modes and their breaker settings.
InfraStruXure PDU: The InfraStruXure Manager server lost communication with this device	Make sure the InfraStruXure PDU is connected properly to the network. If the problem persists, contact APC Support.
InfraStruXure PDU: The input transformer is overheated	Make sure no overload exists, and the InfraStruXure PDU is not overheated. If the problem persists, contact APC Support.

InfraStruXure PDU: Violates the frequency threshold for the system output	Make sure the threshold is set correctly in the "InfraStruXure PDU details" display. Also, make sure no problem exists with the frequency of the power (UPS output or InfraStruXure PDU input) supplied to the breaker panel. If the problem persists, contact APC Support.
InfraStruXure PDU: Violates the ground current threshold	Make sure the threshold is set correctly in the "InfraStruXure PDU details" display, and the ground wire is connected securely. If the problem persists, contact APC Support.
InfraStruXure PDU: Violates the overcurrent threshold exists for panel breaker <*n*>	Make sure the threshold is set correctly in the "InfraStruXure PDU details" display, and no overload exists at the breaker. If the problem persists, contact APC Support.
InfraStruXure PDU:Violates the overcurrent threshold for the system output neutral wire	Make sure the threshold is set correctly in the "InfraStruXure PDU details" display, and the neutral wire is connected securely. If the problem persists, contact APC Support.
InfraStruXure PDU: Violates the overcurrent threshold for phase L<*n*> of the system output	Make sure the threshold is set correctly in the "InfraStruXure PDU details" display, and the loads are balanced on all output phases. Switch some equipment to different phases to balance the load, as needed. If the problem persists, contact APC Support.
InfraStruXure PDU: Violates the overvoltage threshold for phase L<*n*> of the bypass input	Make sure the threshold is set correctly in the "InfraStruXure PDU details" display, and no input-power problem exists. If the problem persists, contact APC Support.
InfraStruXure PDU: Violates the overvoltage threshold for phase L<*n*> of the main input	
InfraStruXure PDU: Violates the overvoltage threshold for phase L<*n*> of the system output	Make sure the threshold is set correctly in the "InfraStruXure PDU details" display, and no problem exists with the voltage (UPS output or PDU input) supplied to the breaker panel. If the problem persists, contact APC Support.

InfraStruXure PDU: Violates the undercurrent threshold for panel breaker <*n*>	Make sure the threshold is set correctly in the "InfraStruXure PDU details" display, and all load equipment is operational and plugged in securely. If the problem persists, contact APC Support.
InfraStruXure PDU: Violates the undercurrent threshold for phase L<*n*> of the system output	Make sure the threshold is set correctly in the "InfraStruXure PDU details" display. Also, make sure all breaker loads are operational and connected properly, and no problem exists with the voltage (UPS output or PDU input) supplied to the breaker panel. If the problem persists, contact APC Support.
InfraStruXure PDU: Violates the undervoltage threshold for phase L<*n*> of the bypass input	Make sure the threshold is set correctly in the "InfraStruXure PDU details" display. Also, make sure the circuit breaker is closed, and no input-power problem exists. If the problem persists, contact APC Support.
InfraStruXure PDU: Violates the undervoltage threshold for phase L<*n*> of the main input	
InfraStruXure PDU: Violates the undervoltage threshold for phase L<*n*> of the system output	Make sure the threshold is set correctly in the "InfraStruXure PDU details" display, and no problem exists with the voltage (UPS output or PDU input) supplied to the breaker panel. If the problem persists, contact APC Support.
Warning Events	
InfraStruXure PDU: Notifications disabled for maintenance	If necessary, use "Enable Notifications" in the "Notification" menu once the reason for disabling notifications no longer exists.
InfraStruXure PDU: Q breakers set for atypical bypass mode	See Q-Breaker Modes for descriptions of the available modes and their breaker settings.
InfraStruXure PDU: Q breakers set for forced bypass mode	
InfraStruXure PDU: Q breakers set for maintenance bypass mode	
InfraStruXure PDU: Q breakers set for on battery mode	

Informational Events (No Action Required)
InfraStruXure PDU: A contact fault no longer exists
InfraStruXure PDU: A fan failure no longer exists
InfraStruXure PDU: Breakers set for panel feed mode
InfraStruXure PDU: Bypass breaker is no longer open
InfraStruXure PDU: No longer violates the frequency threshold no longer exists for the system output neutral wire
InfraStruXure PDU:No longer violates the frequency threshold no longer exists for the system output
InfraStruXure PDU: No longer violates the ground current threshold no longer exists
InfraStruXure PDU:No longer violates the overcurrent threshold for panel breaker <*n*>
InfraStruXure PDU: No longer violates the overcurrent threshold for the system output neutral wire
InfraStruXure PDU: No longer violates the overcurrent threshold for phase L<*n*> of the system output
InfraStruXure PDU: No longer violates the overvoltage threshold for phase L<*n*> of the bypass input
InfraStruXure PDU: No longer violates the overvoltage threshold for phase L<*n*> of the main input
InfraStruXure PDU: No longer violates the overvoltage threshold for phase L<*n*> of the system output
InfraStruXure PDU: No longer violates the undercurrent threshold for the circuit panel's breaker <*n*>
InfraStruXure PDU: No longer violates the undercurrent threshold for phase L<*n*> of the system output
InfraStruXure PDU: No longer violates the undervoltage threshold for phase L<*n*> of the bypass input
InfraStruXure PDU: No longer violates the undervoltage threshold for phase L<*n*> of the main input

InfraStruXure PDU: No longer violates the undervoltage threshold for phase L<*n*> of the system output
InfraStruXure PDU: Notifications now enabled
InfraStruXure PDU: Q breakers set for UPS operation mode
InfraStruXure PDU: Restored the phase L<*n*> input to the UPS
InfraStruXure PDU: The InfraStruXure Manager server established communication with this device
InfraStruXure PDU: The input transformer is no longer overheated

MasterSwitch events

The Event log can report the following events for a MasterSwitch V2 unit; a MasterSwitch V1 unit can only report the lost and established communication events:

Critical Events	Recommended Actions
MasterSwitch: The agent lost communication with the device	Make sure the device and its agent are connected properly to the network and that normal power is available to both. If the problem persists, contact APC Support.
MasterSwitch: The InfraStruXure Manager server lost communication with the agent	
Warning Events	
MasterSwitch: Notifications disabled for maintenance	If necessary, use “Enable Notifications” in the “Notification” menu once the reason for disabling notifications no longer exists.
Firmware Events (No Action Required Except as Noted)	
MasterSwitch: Agent firmware is being updated	
MasterSwitch: Agent firmware update failed	Make sure FTP is enabled at the device, and try to update the firmware again. If the problem persists, contact APC Support.
MasterSwitch: Agent firmware update is available or succeeded	
Informational Events (No Action Required)	
MasterSwitch: Notifications now enabled	
MasterSwitch: Outlet <*n*> was turned off	
MasterSwitch: Outlet <*n*> was turned on	
MasterSwitch: The agent established communication with the device	
MasterSwitch: The InfraStruXure Manager server established communication with the agent	

MasterSwitch Plus events

The Event log can report the following MasterSwitch Plus events:

Critical Events	Recommended Actions
MasterSwitch Plus: The agent lost communication with the device	Make sure the device and its agent are connected properly to the network and that normal power is available to both. If the problem persists, contact APC Support.
MasterSwitch Plus: The InfraStruXure Manager server lost communication with the agent	
Warning Events	
MasterSwitch Plus: Lost Communication with unit <*n*> (<*unit name*>)	Make sure the unit is operational and connected properly to any other units, and to the network. If the problem persists, contact APC Support.
MasterSwitch Plus: Notifications disabled for maintenance	If necessary, use “Enable Notifications” in the “Notification” menu once the reason for disabling notifications no longer exists.
Firmware Events (No Action Required Except as Noted)	
MasterSwitch Plus: Agent firmware is being updated	
MasterSwitch Plus: Agent firmware update failed	Make sure FTP is enabled at the device, and try to update the firmware again. If the problem persists, contact APC Support.
MasterSwitch Plus: Agent firmware update is available or succeeded	
Informational Events (No Action Required)	
MasterSwitch Plus: Notifications now enabled	
MasterSwitch Plus: Outlet <*n*> (<*name*>) on unit <*n*> (<*name*>) was turned off	
MasterSwitch Plus: Outlet <*n*> (<*name*>) on unit <*n*> (<*name*>) was turned on	
MasterSwitch Plus: Restored communication with unit <*n*> (<*unit name*>)	
MasterSwitch Plus: The agent established communication with the device	
MasterSwitch Plus: The InfraStruXure Manager server established communication with the agent	
MasterSwitch Plus: The number of units was increased	
MasterSwitch Plus: The number of units was decreased	

MasterSwitch VM events

The Event log can report the following MasterSwitch VM events:

Critical Events	Recommended Actions
MasterSwitch VM: An overload exists at unit <*n*> (<*unit name*>)	Reduce the load on the unit until it is within an acceptable range. If the problem persists, contact APC Support.
MasterSwitch VM: The agent lost communication with the device	Make sure the device and its agent are connected properly to the network and that normal power is available to both. If the problem persists, contact APC Support.
MasterSwitch VM: The InfraStruXure Manager server lost communication with the agent	
MasterSwitch VM: Violates the InfraStruXure Manager global device load threshold at unit <*n*>	Make sure the "Load Exceeds <n> Percent" threshold is set correctly in the Metered Rack PDU tab of the "Global Device Thresholds" display. Reduce the load, if necessary. If the problem persists, contact APC Support.
Warning Events	
MasterSwitch VM: A low load exists at unit <*n*> (<*unit name*>)	Make sure the threshold is set correctly at the unit, and all load equipment is operational and plugged in securely. If the problem persists, contact APC Support.
MasterSwitch VM: Lost Communication with unit <*n*> (<*unit name*>)	Make sure the unit is operational and connected properly to any other units, and to the network. If the problem persists, contact APC Support.
MasterSwitch VM: Notifications disabled for maintenance	If necessary, use "Enable Notifications" in the "Notification" menu once the reason for disabling notifications no longer exists.
MasterSwitch VM: The load is approaching an overload at unit <*n*> (<*unit name*>)	Make sure the threshold is set correctly at the unit. Reduce the load, if necessary.

Firmware Events (No Action Required Except as Noted)	
MasterSwitch VM: Agent firmware is being updated	
MasterSwitch VM: Agent firmware update failed	Make sure FTP is enabled at the device, and try to update the firmware again. If the problem persists, contact APC Support.
MasterSwitch VM: Agent firmware update is available or succeeded	
Informational Events (No Action Required)	
MasterSwitch VM: A load problem no longer exists at unit <*n*> (<*unit name*>)	
MasterSwitch VM: No longer violates the InfraStruXure Manager global device load threshold at unit <*n*>	
MasterSwitch VM: Notifications now enabled	
MasterSwitch VM: Outlet <*n*> (<*outlet name*>) on unit <*n*> (<*unit name*>) was turned off	
MasterSwitch VM: Outlet <*n*> (<*outlet name*>) on unit <*n*> (<*unit name*>) was turned on	
MasterSwitch VM: Restored communication with unit <*n*> (<*unit name*>)	
MasterSwitch VM: The agent established communication with the device	
MasterSwitch VM: The InfraStruXure Manager server established communication with the agent	

<Other APC Device> events

Not all APC devices currently support being monitored by an InfraStruXure Manager server. However, as these APC devices are updated, they can be added to the list of Supported devices the InfraStruXure Manager server can monitor without the need to update the server.

Two types of InfraStruXure Manager support can be provided for these newly supported devices:

- For some, the InfraStruXure Manager support may be limited initially to only the general status (critical, warning, or normal device status) and other events described in this section's table.
- For others, the InfraStruXure Manager support will include the ability to report on a full range of device-specific status events.

When communication is lost with a newly supported device, the InfraStruXure Manager server can no longer determine the device type. Therefore, APC Device is the prefix used for the lost-communication events.

For both types of support, you can access a device's network management application for more information about the current status. For devices that can report a full range of status events, you can also do the following:

- Use the **Notifications** option in the management application's **Administration** tab to identify the status events that can occur at the device.
- Highlight the device in the "Device Status" display to view information about any active critical and warning events in the "Recommended Actions" frame.

Critical Events	Recommended Actions
<*Other APC Device*>: A critical condition exists	Access the management application at the device to identify and correct the problem.
APC Device: The InfraStruXure Manager server lost communication with the agent	Make sure the device and its agent are connected properly to the network and that normal power is available to both. If the problem persists, contact APC Support.
APC Device: The InfraStruXure Manager server lost communication with the device	If the device turned or rebooted, wait for it to finish initializing. Otherwise, make sure the device and its agent are connected properly to the network and that normal power is available to both. If the problem persists, contact APC Support.
Warning Events	
<*Other APC Device*>: A warning condition exists	Access the management application at the device to identify and correct the problem.
<*Other APC Device*>: Notifications disabled for maintenance	If necessary, use “Enable Notifications” in the “Notification” menu once the reason for disabling notifications no longer exists.
Firmware Events (No Action Required Except as Noted)	
<*Other APC Device*>: Agent firmware is being updated	
<*Other APC Device*>: Agent firmware update failed	Make sure FTP is enabled at the device, and try to update the firmware again. If the problem persists, contact APC Support.
<*Other APC Device*>: Agent firmware update is available or succeeded	
Informational Events (No Action Required)	
<*Other APC Device*>: Notifications now enabled	
<*Other APC Device*>: The InfraStruXure Manager server established communication with the <*agent or device*>	
<*Other APC Device*>: This device is now operating normally	

Rack PDU events

The Event log can report the following Metered or Switched Rack Power Distribution Unit (Rack PDU) events:

Critical Events	Recommended Actions
Rack PDU: A low load exists at output phase L<*n*>	Make sure the threshold is set correctly at the device, and all load equipment is operational and plugged in securely. If the problem persists, contact APC Support.
Rack PDU: A problem exists at power supply <*n*>	A hardware failure exists. Contact APC Support.
Rack PDU: An overcurrent exists at output phase L<*n*>	Make sure the threshold is set correctly at the device. Reduce the load, if necessary. If the problem persists, contact APC Support.
Rack PDU: An overload exists at output phase L<*n*>	
Rack PDU: An undercurrent exists at output phase L<*n*>	Make sure the threshold is set correctly at the device, and all load equipment is operational and plugged in securely. If the problem persists, contact APC Support.
Rack PDU: The agent lost communication with the device	Make sure the device and its agent are connected properly to the network and that normal power is available to both. If the problem persists, contact APC Support.
Rack PDU: The InfraStruXure Manager server lost communication with the agent	
Rack PDU: Violates the InfraStruXure Manager global device load threshold	Make sure the “Load Exceeds <n> Percent” threshold is set correctly in the Metered Rack PDU tab of the “Global Device Thresholds” display. Reduce the load, if necessary. If the problem persists, contact APC Support.
Rack PDU: Violates the InfraStruXure Manager global device load threshold for output phase L<*n*>	

Warning Events	
Rack PDU: Notifications disabled for maintenance	If necessary, use “Enable Notifications” in the “Notification” menu once the reason for disabling notifications no longer exists.
Rack PDU: The load is approaching an overload on output phase L<*n*>	Make sure the threshold is set correctly at the device. Reduce the load, if necessary.
Firmware Events (No Action Required Except as Noted)	
Rack PDU: Agent firmware is being updated	
Rack PDU: Agent firmware update failed	Make sure FTP is enabled at the device, and try to update the firmware again. If the problem persists, contact APC Support.
Rack PDU: Agent firmware update is available or succeeded	
Informational Events (No Action Required)	
Rack PDU: A low load no longer exists at output phase L<*n*>	
Rack PDU: A problem no longer exists at power supply <*n*>	
Rack PDU: An overcurrent no longer exists at output phase L<*n*>	
Rack PDU: An overload no longer exists at output phase L<*n*>	
Rack PDU: An undercurrent no longer exists at output phase L<*n*>	
Rack PDU: No longer violates the InfraStruXure Manager global device load threshold for output phase L<*n*>	
Rack PDU: Notifications now enabled	
Rack PDU: Outlet <*n*> (<*outlet name*>) was turned off	
Rack PDU: Outlet <*n*> (<*outlet name*>) was turned on	
Rack PDU: The agent established communication with the device	
Rack PDU: The InfraStruXure Manager server established communication with the agent	
Rack PDU: The load is no longer approaching an overload at output phase L<*n*>	

System events

The Event log can report events which are directly associated with the InfraStruXure Manager status and operation. This includes four Firmware events, and one Summary event.

Critical Events	Recommended Actions
System: A shutdown occurred because the CPU temperature exceeded 80 degrees C (176 degrees F)	Make sure no vents are blocked, and that the internal fan is operating. Also, make sure sufficient cooling is available and that the cooling solutions are operating properly. If the problem persists, contact APC Support. **NOTE:** See the APC Cooling Solutions product page for information about air conditioning equipment designed specifically for UPS and IT environments.
System: Disk usage exceeds the critical threshold of 80 percent	The system will delete the oldest data and event log entries until disk usage decreases to 75% or less.
System: The number of devices connected to the APC LAN exceeds the DHCP lease limit of 1005	Reduce the number of devices on the APC LAN.
Warning Events	
System: An attempt to use the NTP servers to set the server time settings failed	Make sure the NTP server settings are properly defined in the Settings tab, and the NTP servers are connected to the network and operating properly. If the problem persists, contact APC Support.
System: At least 50% of the UPS systems in the <*name*> device group are compensating for a <*high or low*> input voltage	Correct the power problem for the UPS systems at the identified device group.
System: At least 50% of the UPS systems in the <*name*> device group are on battery	

System: An attempt was made to add more devices than the license key limit allows	Add a new license key to increase the number of devices the InfraStruXure Manager can monitor.
System: Disk usage exceeds the warning threshold of 60 percent	Use the "Log Settings" display to change the maximum age allowed for data or event log entries, or save the logs to files. **NOTE:** When disk usage reaches the critical threshold of 80%, the system automatically deletes the oldest data and event log entries until disk usage decreases to 75% or less.
System: Some UPS systems (less than 50%) in the <*name*> device group are compensating for a <*high or low*> input voltage	Correct the power problem for the UPS systems at the identified device group.
System: Some UPS systems (less than 50%) in the <*name*> device group are on battery	
System: The CPU temperature exceeds the warning threshold of 60 degrees C (140 degrees F)	Make sure none of the vents are blocked, and the internal fan is operating. Also, make sure sufficient cooling is available and the cooling solutions are operating properly. If the problem persists, contact APC Support. **NOTE:** When the CPU temperature reaches the critical threshold of 80 degrees C (176 degrees F), the InfraStruXure Manager server will shut down. See APC Cooling Solutions for information about air conditioning equipment designed specifically for UPS and IT environments
System: The InfraStruXure Manager evaluation period expires in <*n*> days	Update any existing version 4.2 licenses, or add new ones.

System: The power consumed by rack <*rack name*> has violated the <*high or low*> power threshold of <*n*> kWatts for over <*time*>	**For high power threshold violations**: • If equipment was recently added at the rack, change the thresholds to reflect the rack's higher kWatt requirements, or move the equipment to a rack that can better handle the increased power and heat. • Make sure the Rack PDUs that provide power at the rack are not providing power to equipment in any other rack. **For low power threshold violations**: • If equipment was recently removed from the rack, change the thresholds to reflect the rack's lower kWatt requirements. • Make sure that no equipment has been turned off. • Make sure that no equipment is receiving power from a Rack PDU assigned to another rack. **For high or low power threshold violations**: • Make sure the thresholds are set to account for the normal operating range for the rack equipment, and that enough time is allowed to prevent violations from being triggered by those operations. For example, if a Rack PDU allows for staggered reboots, the time allowed before a threshold violation occurs must exceed the time needed for the staggered reboots. • If the problem persists, contact APC Support.
Firmware Events (No Action Required)	
System: Checking for firmware updates	
System: Completed the firmware update requested by <*console username*>	
System: Firmware updates are available for monitored devices	
System: Started the firmware update requested by <*console username*>	
Summary Event (No Action Required)	
System: An exceptions summary notification was sent for the <*name*> device group	

Informational Events (No Action Required)
System: A hostname change initiated a reboot
System: A license key with a device limit of <*n*> was <*added or removed*>
System: Finished applying settings from an *.apc file at the server
System: A server time change initiated a reboot
System: A server update started
System: A user changed the frequency at which entries are logged in the data logs
System: A user changed the frequency at which entries are logged in the event log
System: A user changed the maximum age for <*data or event*> log entries
System: A user initiated a <*reboot or shutdown*>
System: A User LAN IP address change initiated a reboot
System: A user purged all the data logs
System: A user purged the event log
System: Added as a trap receiver at <*x*> of <*y*> selected devices
System: Added <*hostname*> to the list of hosts to which SNMP traps can be forwarded
System: An *.apc file was used to restore the configuration settings at the server
System: An APC LAN IP address change initiated a reboot
System: Applying settings from an *.apc file at the server
System: Completed the mass configuration requested by <*console username*>
System: Device discovery initiated
System: Disk usage no longer exceeds the critical threshold of 80 percent
System: Disk usage no longer exceeds the warning threshold of 60 percent
System: Discovery added <*x*> of <*y*> devices to the list of monitored devices
System: Discovery cancelled after <*x*> of <*y*> devices were added to the list of monitored devices
System: Entries older than <*n*> days were removed from the <*event log or data logs*>
System: Failed to import the source configuration file
System: Imported an *.apc file at the server

System: None of the UPS systems in the <*name*> device group are compensating for a <*high or low*> input voltage
System: None of the UPS systems in the <*name*> device group are on battery
System: Removed <*x*> of <*y*> selected devices from the list of monitored devices
System: Removed as a trap receiver at <*x*> of <*y*> selected devices
System: Removed <*hostname*> from the list of hosts to which SNMP traps can be forwarded
System: Started the mass configuration requested by <*console username*>
System: The CPU temperature no longer exceeds the warning threshold of 60 degrees C (140 degrees F)
System: The device limit has changed to <*n*>
System: The hardware watchdog initiated a reboot
System: The license key was not added because the device limit cannot exceed <*n*>
System: The number of devices connected to the APC LAN no longer exceeds the DHCP lease limit of 1005
System: The power consumed by rack <*rack name*> no longer violates the <*high or low*> power threshold
System: The software has started following a reboot or power-on event
System: The software watchdog initiated a reboot
System: User <*username*> failed to log on from <*hostname*>
System: User <*username*> has been <*added, modified, or removed*>
System: User <*username*> logged <*off or on*> from <*hostname*>

UPS events

The Event log can report the following UPS events, including events for an Integrated Environmental Monitor or an external environmental monitoring device that connects to the network through a UPS:

No UPS uses all the events identified in this table.

Critical Events	Recommended Actions
UPS: A base module fan failure exists (see footnote)	An internal hardware failure exists. Contact APC Support.
UPS: A battery charger failure exists (see footnote)	An internal hardware failure exists. Contact APC Support.
UPS: A battery monitor card failure exists	Remove and reinsert the card to make sure it is installed securely. If the problem persists, replace the card or contact APC Support.
UPS: A bypass power supply failure exists (see footnote)	An internal hardware failure exists. Contact APC Support.
UPS: A fault exists at *<external or Integrated>* Environmental Monitor contact *<n> (<name>)*	Access the device management application to identify and correct the problem that activated this fault. If the problem persists, contact APC Support.
UPS: A fault exists at *<external or Integrated>* Environmental Monitor output relay *<n> (<name>)*	
UPS: A graceful shutdown has started (see footnote)	Save and close any files at all devices that receive power from the UPS. The UPS will turn off as soon as the time defined by a shutdown delay at that UPS expires.
UPS: A hardware failure is causing an abnormal output voltage (see footnote)	An internal hardware failure exists. Contact APC Support.

UPS: A high battery temperature exists	Make sure the cooling solutions for the battery environment, and the central air conditioning system, are functioning properly. See the APC Cooling Solutions product page for information about air conditioning equipment designed specifically for UPS and IT environments. If the problem persists, contact APC Support.
UPS: A high isolation transformer temperature exists	An internal hardware failure exists. Contact APC Support.
UPS: A main intelligence module failure exists	An internal hardware failure exists. Contact APC Support.
UPS: An abnormal battery pack condition exists	Replace all faulty battery packs. You can use the APC Upgrade Selector page to order new battery packs.
UPS: An abnormal condition exists	For more detail about this problem, access the network management application or the interface at the UPS. Then correct the problem, or contact APC Support.
UPS: An automatic voltage regulation (AVR) relay failure exists	An internal hardware failure exists. Contact APC Support.
UPS: An extended run frame fault exists	Make sure the frame is connected properly to the UPS. If the problem persists, contact APC Support.
UPS: An external switch gear communication card failure exists	Remove and reinsert the card to make sure it is installed securely. If the problem persists, contact APC Support.
UPS: An input voltage or frequency problem occurred while on bypass due to a hardware failure, turning off the UPS	The "Drop Load" value is selected for the "UPS If UPS fails, and frequency or voltage is out of range" option at the management card, and a frequency or voltage deviation occurred while a hardware failure existed at the UPS. The UPS front panel display can be used to turn on the output power when the input power and hardware failure are both corrected. If the problem persists, contact APC Support.

UPS: An internal communications failure exists	An internal hardware failure exists. Contact APC Support.
UPS: An inverter failure is causing an abnormal output voltage	
UPS: A not-synchronized fault exists	Reboot the UPS. If the problem persists, contact APC Support.
UPS: An overload exists	Reduce the load on the UPS to a safe level (less than 100%), or upgrade to a unit that can support the existing load. You can use the APC Upgrade Selector page to identify the UPS that best meets your system requirements. If the problem persists, contact APC Support.
UPS: An XR communication card failure exists	Remove and reinsert the card to make sure it is installed securely. If the problem persists, replace the card or contact APC Support.
UPS: A power module failure exists	Replace all faulty power modules. If the problem persists, contact APC Support.
UPS: A redundant intelligence module failure exists	An internal hardware failure exists. Contact APC Support.
UPS: A site wiring fault exists (see footnote)	Have a licensed electrician ensure that the proper input wiring is connected to the UPS. This includes the proper phase rotation, a proper neutral connection, a proper ground connection, and a proper grounding electrode conductor connection. If the problem persists, contact APC Support.
UPS: A static bypass switch module failure exists	An internal hardware failure exists. Contact APC Support.
UPS: A system ID card failure exists	Remove and reinsert the card to make sure it is installed securely. If the problem persists, contact APC Support.
UPS: A system level fan failure exists	An internal hardware failure exists. Contact APC Support.
UPS: A system power supply card failure exists	

UPS: A system start up configuration failure exists	Reboot the UPS. If the problem persists, contact APC Support.
UPS: Battery power is too low to support the load if a power failure occurs	This condition typically exists following a runtime calibration, or when the UPS returns to online operation following a prolonged power failure. In both cases, monitoring the UPS should show that battery power is recharging. If the battery power is not recharging, and no event indicates that another battery problem exists, contact APC Support.
UPS: Cannot switch to bypass mode; the input voltage or frequency is not within its defined limits	Wait for the input power to return to normal before you attempt to switch the UPS to bypass mode. If the problem persists, contact APC Support.
UPS: Failed a self-test	Initiate a new self-test. If that test also fails, verify that no battery problems exist. If the problem persists, contact APC Support.
UPS: Lost communication with the battery packs (see footnote)	Make sure the battery packs are connected correctly. If the problem persists, contact APC Support.
UPS: No batteries installed	Make sure the *<batteries, battery packs, or power modules>* are installed and connected correctly. If the problem persists, contact APC Support.
UPS: No battery packs installed	
UPS: No power modules installed	
UPS: On bypass in response to a hardware failure	An internal hardware failure exists. Contact APC Support.
UPS: On bypass in response to an overload condition	Reduce the load on the UPS to a safe level (less than 100%) or upgrade to a unit that can support the existing load. You can use the APC Upgrade Selector page to identify the UPS that best meets your system requirements.
UPS: One or more faulty batteries exist	Replace all faulty batteries. You can use the APC Upgrade Selector page to order new batteries.

UPS: On forced bypass in response to the InfraStruXure PDU or UPS static switch	The InfraStruXure PDU Q breakers, or the UPS static switch, were used to force the UPS into bypass mode, typically for maintenance. Since the UPS cannot support its load if a power failure occurs, return the UPS to online operation as soon as possible.
UPS: Output power is off	When the load equipment is ready to use the output power from the UPS, turn on the UPS.
UPS: Output power is off for a user-defined period of time	A software command has been used to turn off the UPS for a user-defined period of time. The UPS will turn on its output power when that time elapses, or you can turn on the UPS manually at any time.
UPS: Output power is off until input power returns to normal	A low-battery condition caused the UPS to shut down during an extended power failure. When input power is restored, the UPS will restore output power to the load equipment.
UPS: Redundancy lost	The UPS can no longer detect any redundant power modules. Correct any power module problems (removed or failed), add power modules, or reduce the load. If the problem persists, contact APC Support.
UPS: The agent lost communication while the UPS was on battery	Save and close any files at all devices that receive power from the UPS, as it may turn off at any time. Make sure the UPS and its agent are connected properly to the network and that normal power is available to both. If the problem persists, contact APC Support.
UPS: The agent lost communication with the UPS	Make sure the proper communications cable is connected securely to the device and to the correct communications port at the agent's system. If the problem persists, contact APC Support.
UPS: The backfeed protection relay is open	An internal hardware failure exists. Contact APC Support.
UPS: The battery charger shut down externally	

UPS: The battery monitor card was removed	Reinsert the card.
UPS: The battery voltage exceeds the Nominal Battery Voltage rating	An internal hardware failure exists. Contact APC Support.
UPS: The bypass contactor is stuck in the bypass position	
UPS: The bypass contactor is stuck in the online position	
UPS: The bypass switch at the UPS fails to put the UPS on bypass	
UPS: The external DC disconnect switch is open	Contact APC Support.
UPS: The external switch gear communication card was removed	Reinsert the card.
UPS: The InfraStruXure Manager server lost communication with the UPS or its agent	Make sure the UPS and its agent are connected properly to the network and that normal power is available to both. If the problem persists, contact APC Support.
UPS: The InfraStruXure Manager server lost communication with the UPS or its agent while the UPS was on battery	Save and close any files at all devices that receive power from the UPS, as it may turn off at any time. Make sure the UPS and its agent are connected properly to the network and that normal power is available to both. If the problem persists, contact APC Support.
UPS: The input circuit breaker is open	Close the circuit breaker. If the problem persists, contact APC Support.
UPS: The internal DC disconnect switch is open	An internal hardware failure exists. Contact APC Support.
UPS: The InfraStruXure Manager server is not set as a trap receiver for this device	It is recommended that the InfraStruXure Manager server be defined as a trap receiver for this device. Until this is done, the server will be limited in the amount of information it can provide about the device.

UPS: The output voltage is not within its defined limits	An internal hardware failure exists. Contact APC Support.
UPS: The redundant intelligence module is in control	Correct the main intelligence module problem (it was removed or failed) that switched control to the redundant intelligence module. If the problem persists, contact APC Support.
UPS: The static bypass switch module was removed	Reinsert the module.
UPS: The system ID card was removed	Reinsert the card.
UPS: The system power supply card was removed	
UPS: The XR communication card was removed	
UPS: Unless input power returns, the UPS may shut down because its battery power is too low to continue supporting the load	The UPS cannot continue to use its battery power to support its load equipment. The remaining runtime equals, or is less than, the runtime defined by its "Low Battery" setting. Consider upgrading to a UPS that provides more runtime. You can use the APC Upgrade Selector page to identify the UPS that best meets your system requirements.
UPS: Violates a *<humidity or temperature>* threshold for external sensor *<n>* (see footnote)	Make sure the threshold is set correctly at the device, and the central air conditioning system is functioning properly. If the problem persists, see the APC Cooling Solutions product page for information about air conditioning equipment designed specifically for UPS and IT environments. Otherwise, contact APC Support.
UPS: Violates the *<low or high>* humidity threshold for <external or integrated> sensor *<n>*	
UPS: Violates the *<low or high>* temperature threshold for <external or Integrated> sensor *<n>*	

UPS: Violates the InfraStruXure Manager global device <*humidity or temperature*> threshold for <*external or integrated*> sensor <*n*>	Make sure the <*humidity or temperature*> threshold is set correctly in the Environmental Monitor tab of the "Global Device Thresholds" display. Also, make sure the central air conditioning system is functioning properly. See the APC Cooling Solutions product page for information about air conditioning equipment designed specifically for UPS and IT environments. If the problem persists, contact APC Support.
UPS: Violates the InfraStruXure Manager global device load threshold, as a percentage of available <*kWatts or kVA*>, for output phase L<*n*>	Make sure the "UPS Load Exceeds" threshold is set correctly in the UPS tab of the "Global Device Thresholds" display. Reduce the load, or upgrade to a unit that can support the existing load. You can use the APC Upgrade Selector page to identify the UPS that best meets your system requirements. If the problem persists, contact APC Support.
UPS: Violates the InfraStruXure Manager global device runtime threshold	Make sure the "Runtime Remaining Less Than" threshold is set correctly in the UPS tab of the "Global Device Thresholds" display. Reduce the load to conserve as much of the remaining runtime as needed to support critical systems. Consider adding additional batteries or upgrading to a UPS that provides more runtime. You can use the APC Upgrade Selector page to order new batteries or to identify the UPS that best meets your system requirements. If the problem persists, contact APC Support.
UPS: Violates the InfraStruXure Manager global device load threshold	Make sure the "UPS Load Exceeds" threshold is set correctly in the UPS tab of the "Global Device Thresholds" display. Reduce the load, or upgrade to a unit that can support the existing load. You can use the APC Upgrade Selector page to identify the UPS that best meets your system requirements. If the problem persists, contact APC Support.

UPS: Violates the internal battery temperature threshold	Make sure the cooling solutions for the battery environment, and the central air conditioning system, are functioning properly. See the APC Cooling Solutions product page for information about air conditioning equipment designed specifically for UPS and IT environments. If the problem persists, contact APC Support.
UPS: Violates the load (kVA) alarm threshold exists	Make sure the threshold is set correctly at the device. Reduce the load to a safe level (less than 100%), or upgrade to a unit that can support the existing load. You can use the APC Upgrade Selector page to identify the UPS that best meets your system requirements. If the problem persists, contact APC Support.
UPS: Violates the redundancy alarm threshold	Make sure the threshold is set correctly at the device. Add power modules, or reduce the load, if necessary. If the problem persists, contact APC Support.
UPS: Violates the runtime alarm threshold	Make sure the threshold is set correctly at the device. Reduce the load to conserve as much of the remaining runtime as needed to support critical systems. Consider adding additional batteries or upgrading to a UPS that provides more runtime. You can use the APC Upgrade Selector page to upgrade to a UPS that best meets your system requirements. If the problem persists, contact APC Support.
Warning Events	
UPS: A runtime calibration is in progress	Wait for the calibration to finish, or cancel it.
UPS: Compensates frequently for <*high or low*> input voltages	Contact APC Global Services for information about how to improve the quality of the UPS input power.

UPS: Compensating for a <*high or low*> input voltage	This event is logged, only. Information is provided in the "Device Status" display, and appropriate notifications sent, when a UPS: Compensating for a <*high or low*> input voltage for at least <*n*> seconds event occurs.
UPS: Compensating for a <*high or low*> input voltage for at least <*n*> seconds	Contact APC Global Services for information about how to improve the quality of the UPS input power.
UPS: No battery packs installed	Make sure the battery packs are installed and connected correctly. If the problem persists, contact APC Support.
UPS: Notifications disabled for maintenance	If necessary, use "Enable Notifications" in the "Notification" menu once the reason for disabling notifications no longer exists.
UPS: On battery for at least <*n*> seconds	Make sure the UPS is plugged in and that the circuit breaker is set properly. If the problem persists, contact APC Support.
UPS: On battery in response to a power failure	This event is logged, only. Information is provided in the "Device Status" display, and appropriate notifications sent, when a UPS: On battery for at least <*n*> seconds event occurs.
UPS: On bypass in response to a user-initiated command from a management application or UPS accessory	A user-initiated command from a management application or UPS accessory put the UPS into bypass mode, typically for maintenance. Since the UPS cannot support its load if a power failure occurs, return the UPS to online operation as soon as possible.
UPS: On bypass in response to the bypass switch at the UPS	The switch at the UPS was used to put the UPS into bypass mode, typically for maintenance. Since the UPS cannot support its load if a power failure occurs, return the UPS to online operation as soon as possible.
UPS: Power failures occur frequently	Contact APC Global Services for information about how to improve the quality of the UPS input power.

UPS: Rebooting the load equipment	The UPS is cycling its output power off and then on again to reboot its load equipment. Wait for the reboot to finish.
UPS: Violates the InfraStruXure Manager global device battery-age threshold	Make sure the "Battery Age Exceeds" threshold is set correctly in the UPS tab of the "Global Device Thresholds" display. You can use the APC Upgrade Selector page to order new batteries.
UPS: Violates the InfraStruXure Manager global device UPS-age threshold	Make sure the "UPS Age Exceeds" threshold is set correctly in the UPS tab of the "Global Device Thresholds" display. You can use the APC Upgrade Selector page to identify the UPS that best meets your system requirements.
Firmware Events (No Action Required Except as Noted)	
UPS: Agent firmware is being updated	
UPS: Agent firmware update failed	Make sure FTP is enabled at the device, and try to update the firmware again. If the problem persists, contact APC Support.
UPS: Agent firmware update is available or succeeded	
Informational Events (No Action Required)	
UPS: A base module fan failure no longer exists (see footnote)	
UPS: A battery charger failure no longer exists (see footnote)	
UPS: A battery monitor card failure no longer exists	
UPS: A battery was <*added or removed*>	
UPS: A bypass power supply failure no longer exists (see footnote)	
UPS: A fault no longer exists at an <*external or Integrated*> Environmental Monitor <*contact or relay*>	
UPS: A high battery temperature no longer exists	
UPS: A high isolation transformer temperature no longer exists	
UPS: A main intelligence module failure no longer exists	
UPS: An abnormal battery pack condition no longer exists	
UPS: An abnormal condition no longer exists	

UPS: An Automatic Voltage Regulation (AVR) relay failure no longer exists
UPS: An extended run frame fault no longer exists
UPS: An extended run frame was <*installed or removed*>
UPS: An <*external or Integrated*> Environmental Monitor was <*added or removed*>
UPS: An external switch gear communication card failure no longer exists
UPS: An internal communications failure no longer exists
UPS: A not-synchronized fault no longer exists
UPS: An overload no longer exists
UPS: An XR communication card failure no longer exists
UPS: A power module failure no longer exists
UPS: A power module was <*added or removed*>
UPS: A redundant intelligence module failure no longer exists
UPS: A runtime calibration ended
UPS: A site wiring fault no longer exists (see footnote)
UPS: A static bypass switch module failure no longer exists
UPS: A system ID card failure no longer exists
UPS: A system level fan failure no longer exists
UPS: A system power supply card failure no longer exists
UPS: A system start up configuration failure no longer exists
UPS: Batteries now installed
UPS: Battery power is no longer too low to support the load
UPS: Can switch to bypass; the input voltage or frequency is now within its defined limits
UPS: <*Connected or Disconnected*> sensor <*n*> at an <*external or Integrated*> Environmental Monitor
UPS: Faulty batteries no longer exist
UPS: Input power has returned to normal
UPS: No longer compensates frequently for a <*high or low*> input voltage
UPS: No longer compensating for a <*high or low*> input voltage

UPS: No longer on bypass in response to <*named cause*>
UPS: No longer on bypass
UPS: No longer on forced bypass
UPS: No Longer violates a <*humidity or temperature*> threshold for external sensor <*n*> (see footnote)
UPS: No longer violates the <*low or high*> <*humidity or temperature*> threshold for <*external or integrated*> sensor <*n*>
UPS: No longer violates the InfraStruXure Manager global device <*humidity or temperature*> threshold for <*external or integrated*> sensor <n>
UPS: No longer violates the InfraStruXure Manager global device load threshold for output phase L<*n*>
UPS: No longer violates the InfraStruXure Manager global device <*age or runtime*> threshold
UPS: No longer violates the load (kVA) alarm threshold
UPS: No longer violates the redundancy alarm threshold
UPS: No longer violates the runtime alarm threshold
UPS: Notifications now enabled
UPS: Output power has been turned on
UPS: Output power has returned to normal
UPS: Output power turned on after being off for a user-defined period of time
UPS: Passed a self-test
UPS: Power failures no longer occur frequently
UPS: Power modules now installed
UPS: Redundancy restored
UPS: Restored communication with the battery packs (see footnote)
UPS: The agent established communication with the device
UPS: The backfeed protection relay is no longer open
UPS: The battery charger is no longer shutdown externally
UPS: The battery monitor card was inserted

UPS: The battery voltage no longer exceeds the Nominal Battery Voltage rating
UPS: The bypass contactor problem no longer exists
UPS: The bypass switch at the UPS no longer fails to put the UPS on bypass
UPS: The external DC disconnect switch is no longer open
UPS: The external switch gear communication card was inserted
UPS: The external switch gear Q<*n*> is <*closed or open*>
UPS: The InfraStruXure Manager server is now set as a trap receiver for this device
UPS: The input circuit breaker is no longer open
UPS: The InfraStruXure Manager server established communication with the UPS or its agent
UPS: The power problem that caused the UPS to turn off while on bypass due to a hardware failure no longer exists
UPS: The internal DC disconnect switch is no longer open
UPS: The main intelligence module was <*inserted or removed*>
UPS: The output voltage is now within its defined limits
UPS: The redundant intelligence module is no longer in control
UPS: The redundant intelligence module was <*inserted or removed*>
UPS: The static bypass switch module was inserted
UPS: The system ID card was inserted
UPS: The system power supply card was inserted
UPS: The XR communication card was inserted
† For some Matrix-UPS or Smart-UPS models, this event can be reported only when the InfraStruXure Manager server is defined as a trap receiver at the UPS. See Trap receiver feature.

InfraStruXure Manager Power Zones Wizard

Overview

The InfraStruXure Manager Power Zones Wizard automates the process of creating diagrams for the InfraStruXure zones the InfraStruXure Manager server monitors on its APC LAN.

Although the power zones wizard can be adapted to help create diagrams for other types of power zones, you many find it easier to use the Power zone management procedures to create these other power zones.

The following displays are used in the power zones wizard:

- "Define the Power Zone Name" display
- "Power on all Power Sources" display
- "Select the Source Power Devices" display
- "Select the InfraStruXure Manager Rack" display
- "Power off the Device Racks" display
- "Define The Server Rack Name" display
- "Select the Server Rack Devices" display
- "Select Another Rack" display
- "Define the Device Rack Name" display
- "Power on the Rack Devices" display
- "Select the Rack Devices" display
- "Finish" display

"Define the Power Zone Name" display

Use up to 32 alphanumeric characters and spaces to define a name, and click **Next** to access the "Power on all Power Sources" display. The power zone now appears in the "Power Zones" frame.

"Power on all Power Sources" display

The power sources (at least one power source, but not more than two) must be providing power to the power zone before the wizard can discover the InfraStruXure PDU and any associated 3-phase UPS (Symmetra or Silcon) used by those sources.

Click **Next** to access the "Select the Source Power Devices" display.

"Select the Source Power Devices" display

Use the drop-down menus to select the InfraStruXure PDU, and any associated UPS, for each power source (**Source A** and **Source B**). The top menu for each source lists the available UPS selections, and the bottom menu lists the InfraStruXure PDUs, with each InfraStruXure PDU and UPS identified by model name and serial number, with the IP address provided in parentheses.

If the power zone uses only one power source, select the **Source A** components only:

- For a 60 kW or 150 kW InfraStruXure PDU, select the PDU for the power source, only. A local UPS is not associated with this PDU.
- For a 40 kW or 80 kW InfraStruXure PDU, select both the PDU and its associated UPS.

All monitored UPS systems are listed in the power source menus, regardless of whether they are on the User or APC LAN.

Click **Next** to access the "Select the InfraStruXure Manager Rack" display. Any power source for which you selected at least one component (an InfraStruXure PDU or a UPS) is added to the power zone in the "Power Zones" frame.

"Select the InfraStruXure Manager Rack" display

The devices that use the power available at a rack can be discovered by turning power off and then on again at any rack except the rack that provides power to the InfraStruXure Manager server.

- **PDU Rack**: No attempt will be made to identify any devices in this rack.
- **Device Rack**: The wizard will allow you to select any other devices in that rack without turning power off at that rack.

Click **Next** to access the "Power off the Device Racks" display.

"Power off the Device Racks" display

Never turn off power at an InfraStruXure PDU rack, at a rack that contains a UPS that provides power for a power source, at the InfraStruXure Manager rack, or at any rack that has load equipment turned on.

Unless you are using this wizard as part of the initial setup of an InfraStruXure zone, do not turn off power at any device rack. Turning off power risks turning off the equipment that the power zone you want to configure supports.

When you click **Next**, one of the following will happen:

- If the power-off display appeared after **Device Rack** was selected in the "Select the InfraStruXure Manager Rack" display, the "Define The Server Rack Name" display appears.
- If the power-off display appeared after you selected **PDU Rack** in the "Select the InfraStruXure Manager Rack" display, the "Define the Device Rack Name" display appears.
- If the power-off display appeared to begin the configuration of Source B, the "Power on the Rack Devices" display appears.

"Define The Server Rack Name" display

Use up to 32 alphanumeric characters and spaces to define a name, and click **Next** to access the "Select the Server Rack Devices" display.

"Select the Server Rack Devices" display

You must know the model and serial number of each device in the InfraStruXure Manager rack before you can use the following procedure to identify those devices:

1. Select the **Unassigned Devices** option.
2. Checkmark the devices that are known to be installed in the InfraStruXure Manager rack.
3. Click **Next** to access the "Select Another Rack" display. The selected devices are added to the power source in the "Power Zones" frame.

"Select Another Rack" display

Select **Yes** and click **Next** to access the "Define the Device Rack Name" display; if you select **No** and click **Next**, one of the following occurs:

- If the power zone uses a single power source, or you finished defining the devices for both power sources, the "Finish" display appears.
- If the power zone uses two power sources, the "Power off the Device Racks" display appears.

"Define the Device Rack Name" display

Use up to 32 alphanumeric characters and spaces to define a name, and click **Next** to access the "Power on the Rack Devices" display.

"Power on the Rack Devices" display

A power-off and power-on sequence is used to discover the devices that obtain power at rack.

If the selected power source (**Source A** or **Source B**) is turned off at the rack, turn that power on. Click **Next** to access the "Select the Rack Devices" display.

"Select the Rack Devices" display

To select the devices, do the following:

1. Checkmark the devices the **New Devices** list, the **Unassigned Devices** list, or both.
   - **New Devices** option: Lists only the devices that were discovered by turning power off and then on again at the rack.
   - **Unassigned Devices** option: Lists any monitored devices that are not listed for the **New Devices** selection, and which are not assigned to another power zone, power source, or device rack.
2. Click **Next** to access the "Select Another Rack" display. The selected devices are added to the power source in the "Power Zones" frame.

"Finish" display

Click **Next** to create another power zone; click **Finish** to exit.

Incident management module

Overview

Incident management is a separately-licensed, optional feature that, when activated, replaces the standard notification process that the InfraStruXure Manager server uses to notify recipients when events occur.

For an overview of the changes to the notification processes that occur when the incident management module is activated, see Incident management notifications.

For more information about the incident management module, see the following:

- Escalation process
- Initial configuration
- Setup Wizard
- “Incident Management” display
- “Incident History” display
- Incident Management menu
- Default Escalation Policy
- Group Escalation Policy
- Escalation display features
- How to define an escalation policy
- “Recipient Incident Actions” display

Incident management notifications

The incident management module provides three benefits not available with the standard notifications:

- Settings (Availability settings) that allow you to define on what days notifications can be sent to a recipient, and at what time during those days.
- Escalation policies (Default Escalation Policy and Group Escalation Policy) that determine the order in which recipients will be notified, and how much time each recipient has to acknowledge an event before escalating to the next recipient or action, as described in Escalation process.
- An "Incident Management" display that reports the status of the notification process for the incidents.

When the incident management module is enabled, the following changes occur:

- The Notification Settings option in the System Management menu uses the Recipients tab (incident management) rather than the Recipients tab (no incident management) to manage the list of recipients for notifications.
- **Configure Notifications**, a "Device Groups" frame right-click option, accesses a "Group Escalation Policy" display instead of a "Configure Notifications for Group" display.

- Instead of the "Configure Notifications for Recipient" display that identifies whether a recipient will receive notifications when firmware or summary events occur, the "Add Recipients" and "Modify Recipients" displays (incident management) are used.

  When a firmware update is successfully applied at a device, any open incidents at that device are marked as **Cleared: Firmware Update**. For more information about firmware updates, see Apply Firmware Updates; for more information about summary notifications, see Schedule tab (a Global Device Thresholds tab).

- Warning or critical system (InfraStruXure Manager server) incidents are handled by the default policy (Default Escalation Policy). Information about these InfraStruXure Manager server incidents can appear in the "Incident Management" display only when you select **All Devices**.

  For information about the InfraStruXure Manager server events, see System events.

Escalation process

Overview

Each device group has two escalation policies, one for critical and one for warning status incidents that occur at the devices assigned to that group. These policies are defined specifically for a device group (Group Escalation Policy) or by the default policy (Default Escalation Policy).

Each policy defines the following:

- The recipients to notify when an incident occurs.
- The order in which those recipients will be notified.
- How long the InfraStruXure Manager server will wait for a recipient to acknowledge an incident before it notifies the next recipient.

For information about the two options that can be enabled for a policy (**If none of the recipients acknowledge an incident, notify all recipients again** and **When an incident is resolved, notify all previously-notified recipients**), see Escalation display features.

When an incident occurs, the InfraStruXure Manager server uses the escalation policy for that incident, as follows:

1. A notification is sent to the first available recipient. This notification identifies the incident that occurred, and provides a link that can be used to acknowledge the incident.

Each recipient has settings (Availability settings) that identify when that recipient can respond to incidents. If a recipient is unavailable, the InfraStruXure Manager server escalates to the next recipient immediately.

2. The InfraStruXure Manager server waits for the recipient to acknowledge the incident.
3. If the incident is not acknowledged within the identified wait time, the notification is sent to the next available recipient.

This process continues until the incident is acknowledged or cleared, or until all recipients have been notified, and no recipient acknowledged the incident within the allotted time. For information about how an incident can be acknowledged, see Acknowledging incidents.

During the escalation process, the InfraStruXure Manager server also does the following:

- Makes information about the incident available. See "Incident Management" display.
- Records information about the incident. See "Incident History" display.

Information about the incident actions associated with recipients for all incidents stored in the incidents log is available for reports generated using the "Recipient Incident Actions" display.

Acknowledging incidents

Active incidents can be acknowledged in the following ways (cleared incidents are not acknowledged):

- Right-click an incident listed in the "Incident Management" display, and select the **Acknowledge** option to change the incident's state to **Acknowledged: Console**.
- Use the link in an e-mail notification to change the incident's state to **Acknowledged: E-mail** unless one of the following has occurred:
  - The escalation process has moved to the next recipient.

    When a policy finishes escalating without the incident being acknowledged, and the **If none of the recipients acknowledge an incident, notify all recipients again** option is enabled, a notification is sent to all policy recipients, including unavailable recipients. Until the incident is acknowledged or cleared, any of those recipients can use the link that appears in the e-mail notification to acknowledge the incident.
  - The incident has been acknowledged by another recipient (**Acknowledged: E-mail**) or by the **Acknowledge** option in the "Incident Management" display (**Acknowledged: Console)**.

Initial configuration

Before you can start using the incident management module, you must do the following:

1. Enable the feature:
   a. Obtain a licence from APC for this feature.
   b. Activate the license by adding it to the list in the "License Keys" display.
2. Define the recipient and SMTP settings Notification Settings (Notification Settings) needed for notifications.
3. Define the default policy (Default Escalation Policy) used by any group, including **Unassigned**, that does not have a customized policy (Group Escalation Policy) defined.

You can use the Setup Wizard option in the Incident Management menu to define the notification settings and default policy.

Setup Wizard

Use this option in the Incident Management menu to access the "Incident Management Setup Wizard" that you can use to define the following:

- Notification Settings
- Default Escalation Policy

"Incident Management" display

Overview

When the incident management module is activated, the **Incident Management** option in the navigation bar accesses a display that provides information about the most recent status incidents that occurred at the monitored devices.

Note

When the incident management module has not been activated, the **Incident Management** option accesses a display that provides links to more information about this optional feature.

- The left frame of the "Incident Management" display lists the same device groups that appear in the "Device Status" display, but with the following differences in the "Incident Management" display:
  - You cannot edit the device groups.
  - Only one right-click option is available, **Configure Escalation Policy**. This option accesses the specific policy for any device group (Group Escalation Policy) except **All Devices**.
  - Folder icons use icons to indicate whether any critical (red x) or warning (yellow triangle) incidents exist at devices within a device group.

    For information about warning and critical status, see Status and event severity levels.
- The right frame provides information about the most recent active and cleared incidents that occurred at the devices assigned to the selected device group, including **All Devices**. The information provided depends on the selected columns (Display columns) and filters (Display filters).

Note

Right-click any incident to access its "Incident History" display.

Display filters

Two drop-down menus affect which incidents are displayed in the "Incident Management" display.

Status Filter	Selects which incidents are displayed, based on their severity (**All**, **Critical**, or **Warning**).
State Filter	Selects which incidents are displayed, based on their current state: • **All**: All incident states: **Escalating**: The escalation process is ongoing (**Escalate to**, **Escalate from**, and **Re-notify** actions are still occurring). **Finished Escalating**: The escalation policy finished without the incident being acknowledged or cleared. **Acknowledged**: The incident was acknowledged by using the console or the link available in e-mail notifications. **Cleared**: The incident is no longer active. • **Active**: All **Escalating**, **Finished Escalating**, and **Acknowledged** incidents. • **Cleared**: All **Cleared** incidents. • **Acknowledged**: All **Acknowledged** incidents. • **Unacknowledged**: All **Escalating** and **Finished Escalating** incidents. **NOTE:** For more information about incident states and actions, see "Incident History" display.

Display columns

Up to nine columns of information can be displayed.

- Click a column title to sort the incidents in ascending or descending order based on the selected column's data.
- Right-click a column title to enable or disable the display of any column, or to select **Configure Columns** to use the "Configure Columns" display to define which columns are displayed.
- Click and drag a column title to change the order in which that column appears.

All columns except **IP Address/Device Group** are optional.

Incident	The text that records the incident in the Event log.
Incident ID	The number assigned to the incident.
IP Address	The IP address of the device at which the incident occurred. **NOTE: System Events** is reported instead of an IP address, to identify incidents that are directly related to the operation of the InfraStruXure Manager server.
Owner	The recipient, if any, currently assigned to the incident.
Severity	The severity of the incident (**Warning** or **Critical**).
State	The current state of the incident's escalation process. **NOTE:** For information about the available states, see State Filter.
System Name	The system name of the device at which the incident occurred.
Time Active	The amount of time that the incident has been active. **NOTE: Not Active** is reported for cleared incidents.
Time Generated	The date and time when the incident initially occurred.

"Incident History" display

To access this display for any incident listed in the "Incident Management" display, right-click that incident and select the **Incident History** option. Use this display to view information about each **Incident Action**, by the **Date and Time** at which the action occurred. In addition to the incident's **Start** time, the following actions can be reported:

- **No Recipient Defined**: The incident's escalation policy had no recipients defined, or none of the recipients were available for notifications. In either case, **n/a** is reported for the **Recipient**.
- **Escalate to**: The escalation policy notified the identified **Recipient** about the incident.
- **Escalate from**: The escalation policy stopped waiting for the identified **Recipient** to acknowledge the incident.
- **Finished Escalating**: The escalation policy completed without the incident being acknowledged, with **Recipient** identifying the policy's final recipient.
- **Acknowledged: E-mail**: The identified **Recipient** used the link in the e-mail notification to acknowledge the incident.
- **Acknowledged: Console**: Someone who was logged on as the InfraStruXure Manager server's administrator right-clicked the incident and used the **Acknowledge** option.
- **Cleared**: The problem no longer exists. The last **Recipient** notified during the incident's escalation process is identified (or **n/a**, if no escalation policy was in effect).

- **Cleared: Firmware Update**: A firmware update was successfully applied at the device. The last **Recipient** notified during the incident's escalation process is identified (or **n/a**, if no escalation policy was in effect).

  Note

  If an incident is still active following the firmware update, a new incident is initiated for the device.

- **Cleared: Disabled Notifications**: The device at which the incident occurred had its notifications disabled while the incident was still active. The last **Recipient** notified during the incident's escalation process is identified (or **n/a**, if no escalation policy was in effect).

  For more information about the feature that allows you to disable device notifications, see Disable Notifications for Maintenance.

  Note

  Once device notifications are enabled again, view the device status in the "Device List" frame to verify that the incident is no longer active.

- **Re-notify**: One of the following occurred:
  - The If none of the recipients acknowledge an incident, notify all recipients again option was enabled for an escalation policy that completed without the incident being acknowledged or cleared, with **Re-notify** reported for every policy **Recipient.**
  - An incident cleared and the When an incident is cleared, notify all previously-notified recipients option was enabled for the escalation policy, with **Re-notify** reported for any **Recipient** who was notified of the incident.

Incident Management menu

Use the following menu options to configure the incident management module:

- Default Escalation Policy
- Group Escalation Policy
- Notification Settings

This **Notification Settings** option is shared by the **Incident Management** menu and the System Management menu.

- Setup Wizard

Another menu option accesses the "Recipient Incident Actions" display used to generate reports of the incident actions for individual recipients, or all recipients.

Default Escalation Policy

Use the display for this Incident Management menu to define the Escalation process to be used for the following incidents:

- Warning and critical incidents that occur at device groups, including **Unassigned**, that do not have a customized policy (Group Escalation Policy) defined.
- System (InfraStruXure Manager server) incidents always use the default policy.

For more information about the "Default Escalation Policy" display, see Escalation display features and How to define an escalation policy.

Group Escalation Policy

Use the display for this Incident Management menu to define a non-default Escalation process to be used for the critical or warning status incidents that occur at a selected device group.

A device group uses the default policy (Default Escalation Policy) until the "Group Escalation Policy" display is used to customize its escalation policies.

For more information about the "Group Escalation Policy" display, see Escalation display features and How to define an escalation policy.

Escalation display features

Overview

The Default Escalation Policy and the Group Escalation Policy displays have all the features described in the following table. For more information about these features, see How to define an escalation policy.

Critical and **Warning Escalation Policy** tabs	Lists the recipients assigned to the selected policy (**Warning** or **Critical**), in the order in which they will be notified. Each entry also identifies how long the InfraStruXure Manager server will wait for an incident to be acknowledged before it escalates to the recipient, or ends the process, if the wait time expires for the last recipient.
Add Recipient to Policy button	Accesses the "Add Recipient to Policy" display.
Remove Recipient from Policy button	Removes the selected recipient from the displayed policy.
Move Up and **Move Down** buttons	Reposition the selected recipient in the displayed policy.

Edit Time Delay button	Accesses the “Edit Time Delay” display. **NOTE:** This button is active only when a specific wait time for a listed recipient is selected.
Coverage Schedule button	Accesses the “Coverage Schedule” display.
If none of the recipients acknowledge an incident, notify all recipients again option	When enabled, a notification is sent to all policy recipients, even those who were unavailable, if an escalation process ends without an incident being acknowledged or cleared.
When an incident is cleared, notify all previously-notified recipients option	When enabled, a notification is sent to all recipients who were notified of an incident when that incident is cleared.

Add Recipient to Policy

Use the display for this escalation policy (Default Escalation Policy or Group Escalation Policy) button to add recipients to the selected policy.

Edit Time Delay

Use the display for this escalation policy (Default Escalation Policy or Group Escalation Policy) button to define how long the InfraStruXure Manager server must wait for the recipient associated with the selected time to acknowledge an incident before it can continue the Escalation process.

The defined time applies only to the wait time selected in the displayed policy. It does not affect wait times assigned to the associated recipient in the same or other policies.

Coverage Schedule

Use the display for this escalation policy (Default Escalation Policy or Group Escalation Policy) button to view the coverage provided by the policy's recipients.

The display provides a 24-hour graph for each day of the week that identifies when the policy's recipients are available, based on each recipient's Availability settings. This allows you to see any gaps in the coverage. You can then add recipients whose availability settings fill those gaps.

How to define an escalation policy

All escalation policies are defined in the same way, regardless of the incident severity (critical or warning) or the escalation display.

1. Select the **Critical** or **Warning** tab for the policy (Default Escalation Policy or Group Escalation Policy) you want to define.
2. Use the Add Recipient to Policy and **Remove Recipient from policy** buttons to define the recipients you want the selected policy to use.
3. Use the **Move Up** and **Move Down** buttons to identify the order in which you want the recipients to be notified.
4. Select a listed wait time and click the Edit Time Delay button to define how long the InfraStruXure Manager server must wait for the associated recipient to acknowledge an incident before it escalates to the next recipient or action. See Escalation process.
5. Enable or disable the If none of the recipients acknowledge an incident, notify all recipients again option.
6. Enable or disable the When an incident is cleared, notify all previously-notified recipients option.
7. Repeat step 1 through step 6 to define the other tab (**Critical** or **Warning**) for the selected policy (Default Escalation Policy or Group Escalation Policy).

"Recipient Incident Actions" display

Use this display to generate reports that identify how recipients were involved with incidents that occurred.

To generate a report, do the following in the left frame of the display:

1. Select a recipient in the **Recipient** menu, or select **All**, to include the incident actions for all recipients.

   Note: If you select **n/a**, only incidents that used an escalation policy that did not have a recipient defined will be included in the report.

2. Select a **Date** for the report. Only incidents that occurred on the selected date will be included.
3. Use the **Filters** options to select the actions the report will include.
4. Click **Generate Report** to create the report.

All reports have print and save buttons at the top of the report, as well as information about how many incident actions are included in the report. All reports include the information described in the following table.

Note: The report for **All Recipients** also has a column that identifies the recipient associated with an incident action. Click on any column heading to sort the report in ascending or descending order based on that column's data.

Time	When the reported Incident Action occurred, by date and time.
IP Address/Device Group	The device (by IP address) or device group (by name) to which the incident applied, or System Events, for InfraStruXure Manager server incidents.
Recipient	This column, included only in report for all recipients, identifies which recipient is associated with each of the listed incident actions: • For any incident action, the identified recipient can be any of the escalation policy's recipients. • For **Acknowledged**, the identified recipient can also be the InfraStruXure Manager server's administrator. • When an incident was resolved before anyone could acknowledge that incident, **n/a** is reported.
Incident Action	The incident action that occurred: **Escalate To**: The identified recipient was notified about the incident. **Escalate From**: The identified recipient failed to acknowledge the incident within the wait time defined for the incident's escalation policy. **Acknowledged: E-mail**: The identified recipient used the link in an e-mail notification to acknowledge the incident. **Acknowledged: Console**: The InfraStruXure Manager server's administrator right-clicked the incident in the "Incident Management" display and used the **Acknowledge** option. **Cleared**: Identifies the last recipient notified of an incident before that incident was cleared. If no recipient was notified before the incident cleared, **n/a** is reported. **Re-Notify**: Identifies the recipients who were re-notified about an incident after the escalation process ended without anyone acknowledging that incident (see If none of the recipients acknowledge an incident, notify all recipients again option) or when the incident was cleared (see When an incident is cleared, notify all previously-notified recipients option).
Message	The incident's event text.

Third-party software

Copyrights

Portions of this software are Copyright © 1993 - 2003, Chad Z. Hower (Kudzu) and the Indy Pit Crew - http://www.indyproject.org/License/BSD.iwp

Portions of this software are Copyright (c) 1996-2005, The PostgreSQL Global Development Group, Portions Copyright (c) 1994-6, Regents of the University of California - http://www.postgresql.org/about/licence.html

Portions of this software are <link>Copyright (c) 1998-2003, The OpenSSL Project. All rights reserved.

Copyright (c) 1998-2003, The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:
   “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)”
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:
   “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ‘‘AS IS’’ AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License ----------

/Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscape’s SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used.

This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)
   "The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related:-).
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:
   "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS’’ AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL

DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed, i.e., this code cannot simply be copied and put under another distribution license [including the GNU Public License.

Index

A

Aborted
- Firmware updates 127
- Mass configuration 88

Acknowledging incidents 200
Add devices 59
Administrator access settings 81
Alarms
- Current (InfraStruXure PDU) 28
- Frequency (InfraStruXure PDU) 29
- Icons 10

AOS
- Connection Failed 127
- Download Failed 127

APC LAN settings 105
App
- Connection Failed 127
- Download Failed 127

Apply
- Firmware Updates 126
- Server Updates 130

ATS
- Data log 144
- Events 151

Authentication settings 77
Availability settings 113
Available mass configuration settings 92

B

Backup Server 55
Bad Battery report 138
Battery Age report 143
Branch Breakers (InfraStruXure PDU) 25
Building Management System 70
Bypass input (InfraStruXure PDU) 27

C

Cancelled (Firmware updates) 128
Check for Updates 125
Circuit breaker description 26
Client preferences 122
Common report and log features 136
Community names (Device Access) 82
Components (InfraStruXure PDU system) 25
Configure
- Columns 64
- Local Users 78
- RADIUS Settings 79

Contact Closures (InfraStruXure PDU) 23
Critical status or severity level 10
Current (InfraStruXure PDU) 28

D

Data Log 144
- ATS 144
- Environmental 145
- InfraStruXure PDU 145
- Rack PDU 145
- Settings 116
- Symmetra/Silcon 146

Default
- Escalation Policy 207
- Gateway 106
- Power Settings display 97

Defining an escalation policy 211
Device
- Access settings 81
- Details display 20
  - InfraStruXure PDU 23
  - Metered Rack PDU 31

Groups 12
Frame 12
Management 13
Notifications for recipients 111
Report 13
Identification 19
Status display 11
Device List frame 16
DHCP 105
Disable Notifications for Maintenance 61
Domain Name 106
Downtime report 138
Duplicate IP addresses on the APC LAN 104

E

Edit
Menu 58
Power Settings display 99
E-mail
Device group configuration 15
Recipients configuration 111
Settings 106
Enable
Audible Alarm (Rack PDU) 32
Notifications 62
Environmental
Data log 145
Events 153
Monitor (Global Device Thresholds) 67
Report 137
Escalation
Default Policy 207
Defining a policy 211
Display features 208
Group Policy 208
Process 198
Evaluation Period display 119
Event Management menu 65
Events 149
APC InfraStruXure Manager 150
ATS 151
Environmental 153
InfraStruXure PDU 157
Log settings 116
MasterSwitch Plus 163
MasterSwitch V1/V2 162
MasterSwitch VM 164
Rack PDU 168
Severity levels 10
System 170
UPS 175
Exceptions reports 138
Excluded mass configuration settings 92

F

Failed to register as a trap receiver 86
File
Menu 54
Verification Failed 128
Frequency (InfraStruXure PDU) 29
FTP
Logon Failed (Firmware updates) 128
Logon Failed (Mass configuration) 89
Server Settings 114
Settings (Device Access) 85
Transfer Failed 89

G

General user 78
Global Device Thresholds 66
Ground Monitor 24
Group Escalation Policy 208

H

Help menu 134
Hostname (Network Settings) 105
HTML Device Details 21

I

Import a product update to the server 131
Incident 195
- Acknowledging 200
- Availability settings 113
- Default Escalation Policy 207
- Defining an escalation policy 211
- Escalation display features 208
- Escalation process 198
- Group Escalation Policy 208
- History display 205
- Initial configuration 201
- Management 195
  - Display 202
  - Menu 207
- Notifications 196
- Recipient Incident History 212

Informational severity level 10
InfraStruXure Manager
- Backup server settings 55
- Functions 2
- Importing a server update 131
- Power Zones Wizard 189
- psxconfig.xml file 57
- Reset to Factory Defaults 104
- Restore server access 6
- Restore server settings 56
- Setup Wizard 8
- System events 170

InfraStruXure PDU
- Branch Breakers 25
- Breaker Rating 26
- Bypass Input 27
- Circuit breaker description 26
- Contact Closures 23
- Current 28
- Data log 145
- Device Details display 23
- Events 157
- Frequency threshold 29
- Ground Monitor 24
- Main Input 27
- Neutral Current 28
- Panel Breaker Rating 28
- Power 24
- Q-Breaker mode 30
- System breakers 25
- Tied to Next Panel Position 26
- Voltage 29

Initial configuration
- Incidents 201
- Requirements 7

Initialization Failure
- Firmware updates 129
- Mass configuration 89

Input
- Bypass voltage (InfraStruXure PDU) 27
- Main voltage (InfraStruXure PDU) 27
- Nominal Voltage (InfraStruXure PDU) 27

Insufficient License Keys display 121
Interrupted (Mass configuration) 89
IP Address
- APC LAN setting 105
- User LAN (corporate network) setting 106

K

Known issues
- Duplicate IP addresses on the APC LAN 104
- Failed to register as a trap receiver 86

kWatt values for racks 100

L

Last Update Results tab 127
License keys 117
- Display 118
- Evaluation Period display 119
- Insufficient License Keys display 121
- Product Activation display 121
- Update License Keys display 120

Load
- InfraStruXure PDU 24
- Rack PDU reports 142
- UPS reports 143

Log Settings 116
Logs
Common features 136
Data 144
Display 53
Event 147
Settings 116

M

MAC Address 105
Main input (InfraStruXure PDU) 27
Mass configuration 87
Aborted 88
Available settings 92
Excluded configuration settings 92
FTP Logon Failed 89
FTP Transfer Failed 89
Initialization Failure 89
Interrupted 89
Not Supported 90
One or More Settings Failed display 91
Procedure 87
Send Configuration to Selected Devices 88
MasterSwitch Plus events 163
MasterSwitch V1/V2 events 162
MasterSwitch VM events 164
Maximum Power (InfraStruXure PDU) 24
Metered Rack PDU
Device Details 31
Events 168
Global Device Thresholds 67
Model report
Rack PDU 142
UPS 143
Modify Rack display 98

N

Network
Settings 105
Time Protocol (NTP) server feature 5
Neutral current (InfraStruXure PDU) 28
Nominal Input Voltage 27
Normal status 10
Not Supported (Mass configuration) 90
Notification Settings for Selected Device 62

O

One or More Settings Failed
Display 91
Status 90
Outlet Status (Rack PDU) 33
Overcurrent threshold
Branch Breakers (InfraStruXure PDU) 26
Output Current (InfraStruXure PDU) 28
Rack PDU 32
Overload threshold (Rack PDU) 32
Overvoltage threshold
Bypass Input (InfraStruXure PDU) 27
Main Input (InfraStruXure PDU) 27
Output (InfraStruXure PDU) 29

P

Panel Breaker Rating 28
Pinout for the RS-485 port (BMS support) 73
Power
Factor (InfraStruXure PDU) 24
Factor (Racks feature) 101
Zones 36
Display 35
Example 42, 48
Frame 36
Management 38
With an InfraStruXure PDU diagrams 40
Without an InfraStruXure PDU diagrams 47
Wizard 189
Primary DNS Server 106
Product
Activation display 121
Update importing 131
Proxy Settings 115

Q

Q-Breaker mode (InfraStruXure PDU) 30

R

Rack PDU
- Data log 145
- Enable Audible Alarm 32
- Events 168
- kWatt values 100
- Load reports 142
- Model report 142
- Outlet Status 33
- Settings 32
- Thresholds 32

Racks
- Configure Racks display 96
- Default Power Settings display 97
- Edit Power Settings display 99
- kWatt values 100
- Modify Rack display 98
- Options 94
- Power factor values 101

Recipients
- Incident History 212
- Tab (for incident management) 108
- Tab (no incident management) 108

Recommended Actions frame 34
Release Notes
- Overview 214
- Third-Party Software 214

Remote Monitoring Service 74
Reports 135
- Bad Battery 138
- Common features 136
- Display 52
- Downtime 138
- Environmental 137
- Exceptions 138
- Rack PDU 142
  - Load 142
  - Model 142
- Recipients Incident History 212
- Select Report Filter 137
- UPS 143
  - Age 143
  - Battery Age 143
  - Load 143
  - Model 143
  - Runtime 143

Reset to Factory Defaults 104
Restore
- InfraStruXure Manager server access 6
- Server settings 56

Right-click menus
- Device Group frame 13
- Device List frame 17
- Power Zones frame 38

RS-485 port pinout (BMS support) 73
Runtime report 143

S

Schedule (Global Device Thresholds) 68
Secondary DNS Server 106
Select Report Filter 137
Server
- Importing an update 131
- Log On 57
- Time 103

Set
- HTTP Properties for Selected Devices 22
- Rack Properties display 19

Settings
- Rack PDU 32
- Tab (E-mail) 107

Setup wizard
- Incident management 201
- InfraStruXure Manager server 104

Severity levels 10
Short Message Service (SMS) notifications 110
Shutdown or Reboot Server 104

SNMP
Settings 81
Trap Forwarding 69
Status icons and severity levels 10
Subnet Mask 106
Supported Devices 4
Switched Rack PDU
Events 168
Global Device Thresholds 67
Symmetra/Silcon Data log 146
System
Breakers 25
Components 25
Event notifications for recipients 112
Identification 114
Management menu 75

T

Third-Party Software 214
Thresholds
Branch Breakers (InfraStruXure PDU) 26
Bypass input (InfraStruXure PDU) 27
Current (InfraStruXure PDU) 28
Frequency (InfraStruXure PDU) 29
Global Device 66
Main input (InfraStruXure PDU) 27
Neutral Current (InfraStruXure PDU) 28
Rack PDU 32
Voltage (InfraStruXure PDU) 29
Tied to Next Panel Position option 26
Timeout settings (Device Access) 83
Total output power (InfraStruXure PDU) 24
Trap receiver feature 84

U

Undercurrent threshold
Branch Breakers (InfraStruXure PDU) 26
Output (InfraStruXure PDU) 28
Rack PDU 32
Undervoltage threshold
Bypass input (InfraStruXure PDU) 27
Main input (InfraStruXure PDU) 27
Output (InfraStruXure PDU) 29
Update tab (Apply Firmware Updates) 126
Updates
License Keys display 120
Menu 124
Verification Failed 129
UPS
Age report 143
Battery Age report 143
Events 175
Global Device Thresholds 67
Load reports 143
Model report 143
Reports 143
Runtime report 143
Symmetra/Silcon Data log 146
User LAN settings 105

V

View
Group Membership 19
Menu 63

W

Warning status or severity level 10
Wizard
Incident management 201
InfraStruXure Manager Setup 8
Power Zones 189

APC Worldwide Customer Support

Customer support for this or any other APC product is available at no charge in any of the following ways:

- Visit the APC Web site to access documents in the APC Knowledge Base and to submit customer support requests.
  - **www.apc.com** (Corporate Headquarters)

    Connect to localized APC Web sites for specific countries, each of which provides customer support information.
  - **www.apc.com/support/**

    Global support searching APC Knowledge Base and using e-support.
- Contact an APC Customer Support center by telephone or e-mail.
  - Regional centers:

Direct InfraStruXure Customer Support Line	(1)(877)537-0607 (toll free)
APC headquarters U.S., Canada	(1)(800)800-4272 (toll free)
Latin America	(1)(401)789-5735 (USA)
Europe, Middle East, Africa	(353)(91)702000 (Ireland)
Japan	(0) 35434-2021
Australia, New Zealand, South Pacific area	(61) (2) 9955 9366 (Australia)

  - Local, country-specific centers: go to **www.apc.com/support/contact** for contact information.
- Contact the APC representative or other distributor from whom you purchased your APC product for information on how to obtain local customer support.

Copyright

990-1394D ***9/2005***