Clio Care/CIO Fleetview Operation Manual

3731 Northridge Dr. N.W. Suite 1 | Walker, MI 49544 | 888.537.1311 | www.altus-inc.com | A55-00042-00002_REV.B

User Guide

ManageUPS® CIO

ALARM MONITORING

ASSET MANAGEMENT

FOR MPM POWERED CART S IN CAMPUS & REMOTE SITE INSTALLATIONS

Version: 2.0 MPM Fleetview Edition

A55-00049- ManageUPS CIO 2.0-MPM Fleet View ed. 17 July 2013
Also published as *913-601MPM Rev A 7 July 2013*

BEFORE YOU BEGIN

ManageUPS CIO . . . version 2.0, MPM Fleetview Edition

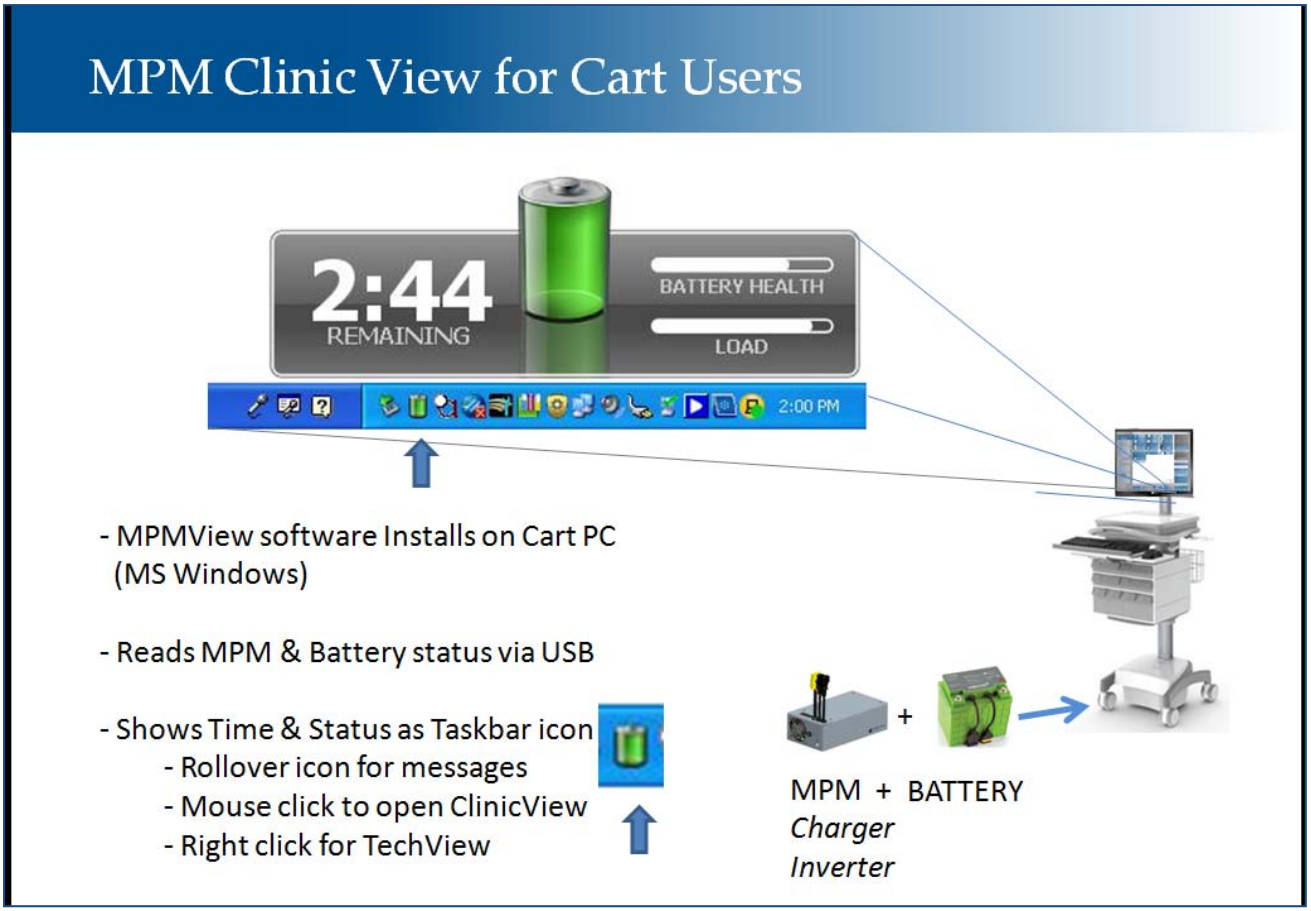
This edition of ManageUPS CIO will monitor a fleet of powered computer carts, each represented on a TCPIP network by:

- MPMView SOFTWARE

You can evaluate CIO on a workstation-class host computer.
If your cart inventory is greater than 5 carts, you should allocate a server-class host computer (VM or physical host) to run ManagegeUPS CIO in a production environment.

To evaluate ManageUPS CIO, you will also need at least one cart PC workstation running MPMView software. To download the install package and User Documentation for MPMView, go to:

http://connectivity.powervar.com/mpm



CONTENTS

SECTION I: GETTING STARTED – OVERVIEW AND QUICK START

OVERVIEW

WHO CAN USE MANAGEUPS CIO?

People who oversee a fleet of carts used for mobile or portable computer workstations that are powered by a POWERVAR mobile power unit can use this edition of CIO.

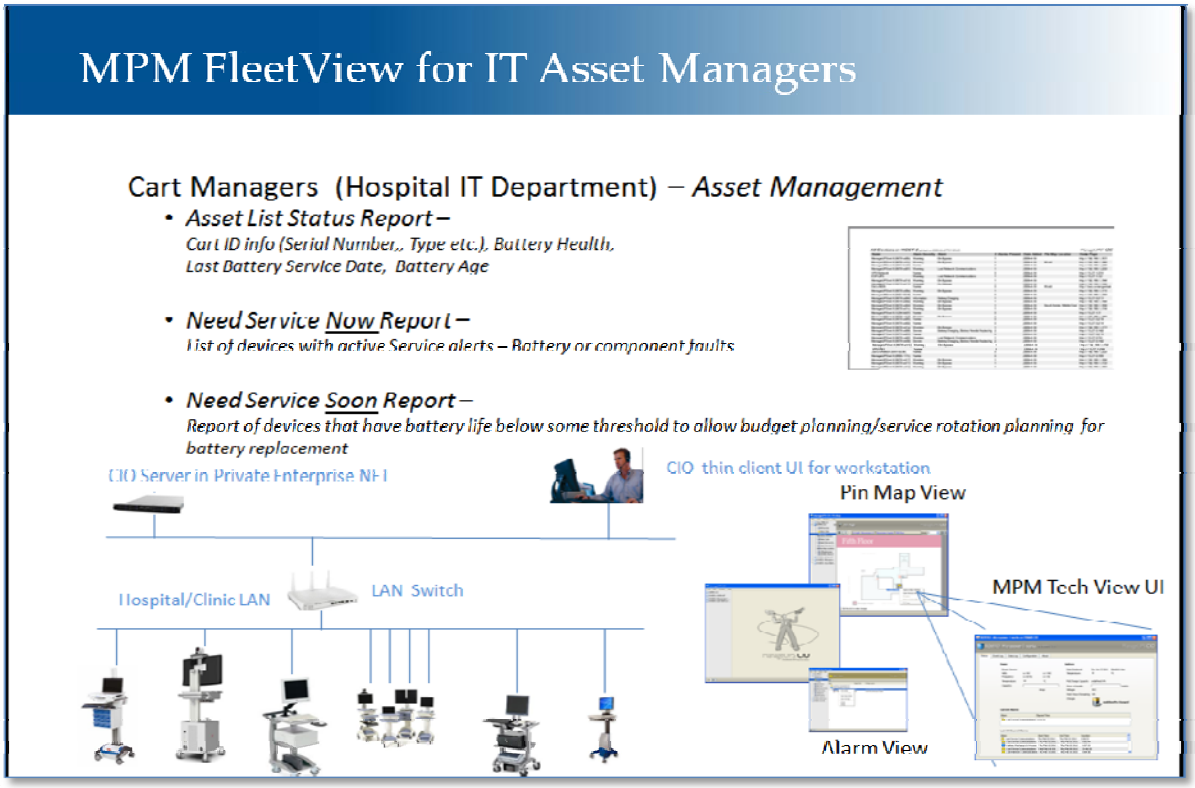
CIO makes it easy to keep track of battery health, battery charge levels and service alerts associated with the batteries or with POWERVAR charger/inverter systems.

WHAT IS MANAGEUPS CIO?

ManageUPS® CIO is server-based application software for managing network-attached, critical power infrastructure in large facilities, campus or enterprise network environments.

The MPM Fleetview Edition is preconfigured for powered carts.

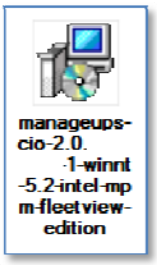
ManageUPS CIO can also be used to monitor fleets of stationary UPS devices, environment sensors, motion sensors, HVAC units, branch circuits, and other types of devices in critical facilities infrastructure.



QUICK START : EIGHT STEPS TO "UP AND RUNNING"

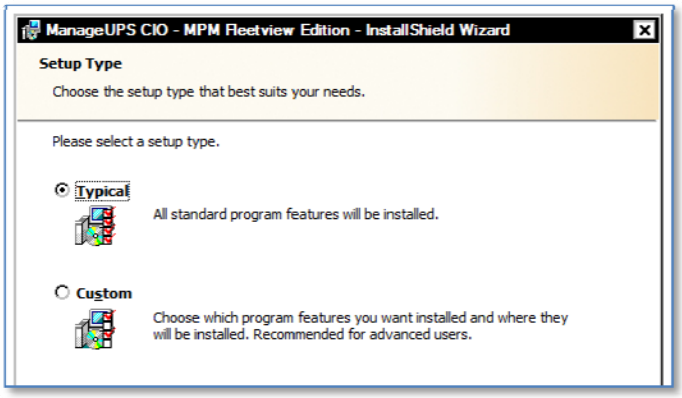
1. Provision a server-class computer on your enterprise LAN or WAN that you will use to host the CIO server application. The server can be *physical or virtual*. *(See Appendix A: System Requirements & Terminology)*

2. Download *CIO MPM FleetView Edition* install package, and save it to the server desktop *(or other convenient location):* http://connectivity.powervar.com/mpm/download.asp



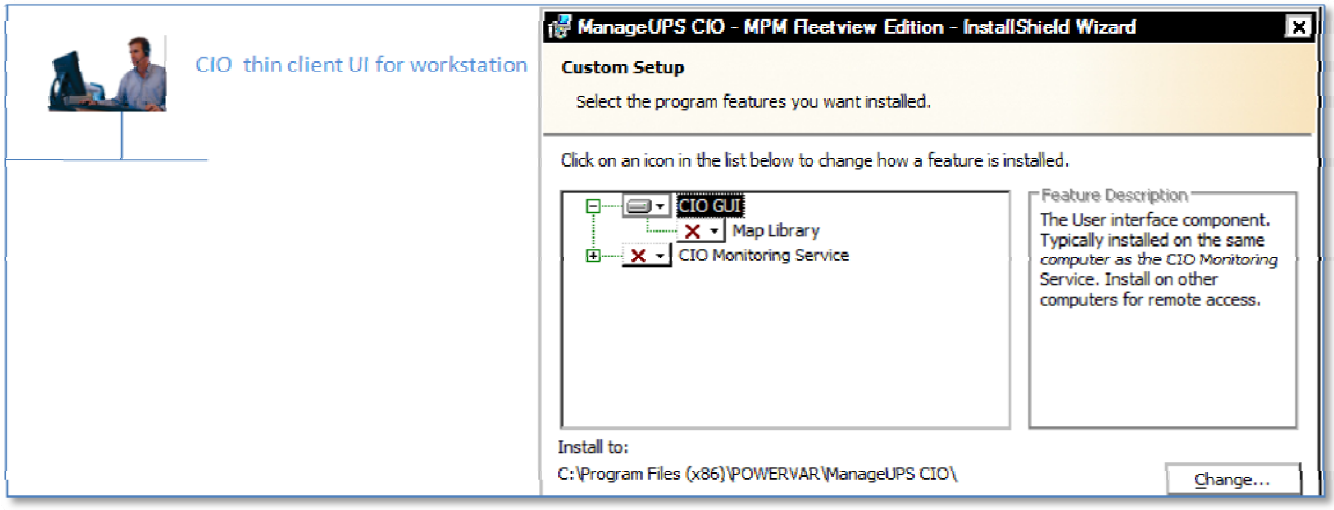
3. Install CIO:
Run the "Typical" install on the host server to install all components.

If you have a CIO license key, enter the key when prompted during install.



If no license key ... . you can add a key later. CIO will let you add up to 5 devices and will run for 2 days without a license key for easy trial)

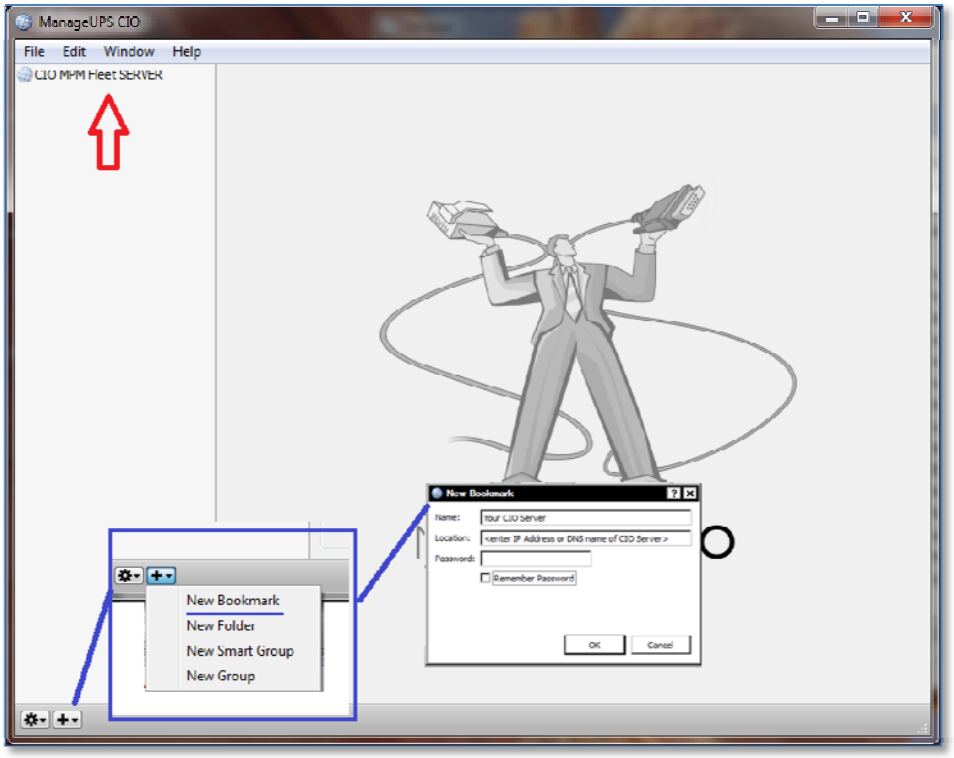
OPTIONAL Remote "Client" GUI-only Install …
To run the GUI client on any remote workstations that you will use to work with CIO, select "Custom" and configure as shown below to only install the thin-client components. (**X out** the *CIO Monitoring Service* and *Map Library* components)



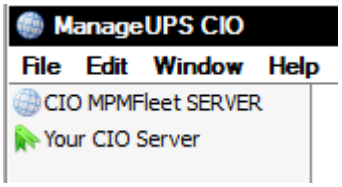
4. Find the CIO Client icon that the installer placed on your desktop ...

5. Start the Client -- *Double click the icon to open the CIO Client.*

   If you are working from the CIO server desktop, or are working from a workstation on the same LAN (subnet) as the CIO server, a blue globe CIO *Server link* should appear automatically as shown at the red "up" arrow below.



If you don't see a blue globe *CIO Server* link appear automatically , you may need to create a *bookmark* to the remote server location using the options marked above in blue.

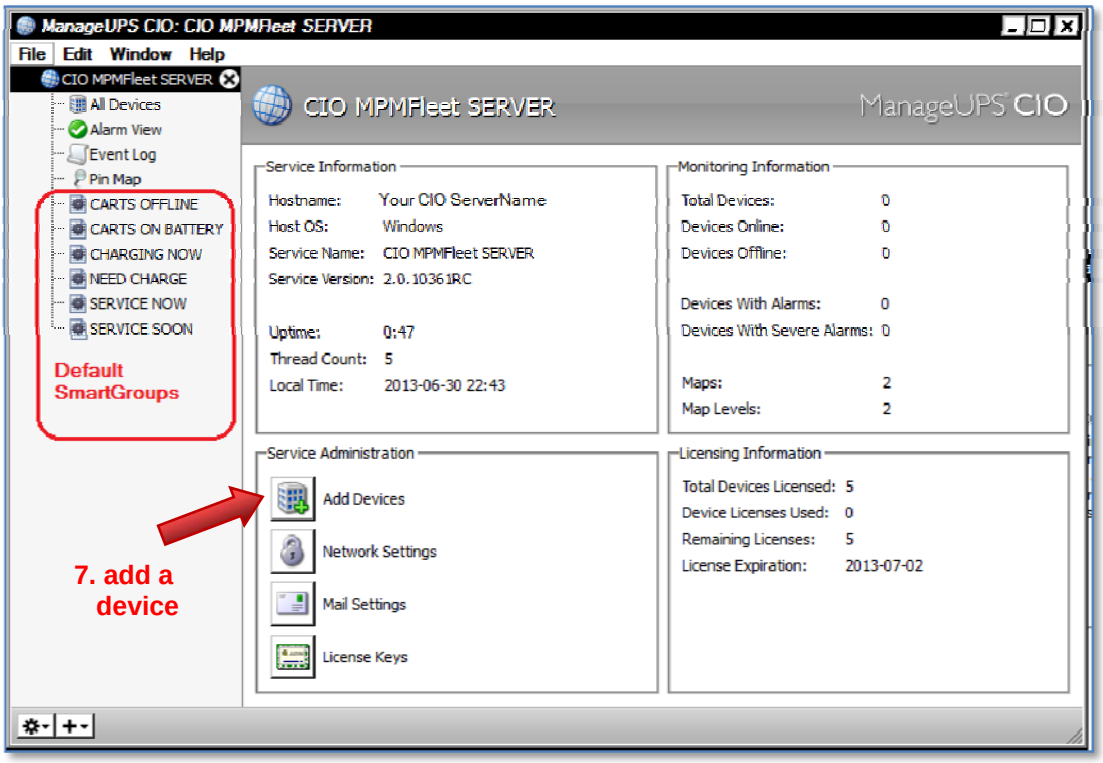


The bookmark will appear as green arrow pointer icon as shown at right..

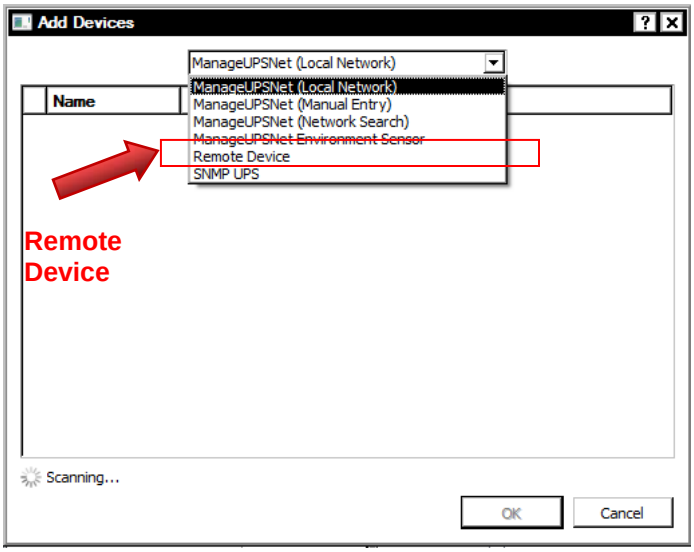
*(**Note:** Firewalls need to allow TCP port 5055 to be open between the CIO server and remote workstations running the CIO Client.)*

6. Click the blue globe *CIO Server link* or green arrow *Bookmark* to connect to the CIO server.

   The *CIO/ MPM FleetView Edition* starts with six pre-configured *SmartGroups* as shown below. You can add or delete *SmartGroups* and *Groups* or edit the rules of *SmartGroups* any time using the "+" or "Gear > add new" buttons at the bottom left of the screen.



7. The next step is to add at least one device (powered mobile cart) to the monitoring inventory that will be managed via CIO. Click the **Add Devices** button (above) to open the Add Devices dialog (below).
   Select **Remote Device** from the dropdown menu.



The ***Remote Devices*** option allows devices with Dynamic IP address configuration to initiate connections to the CIO Server.

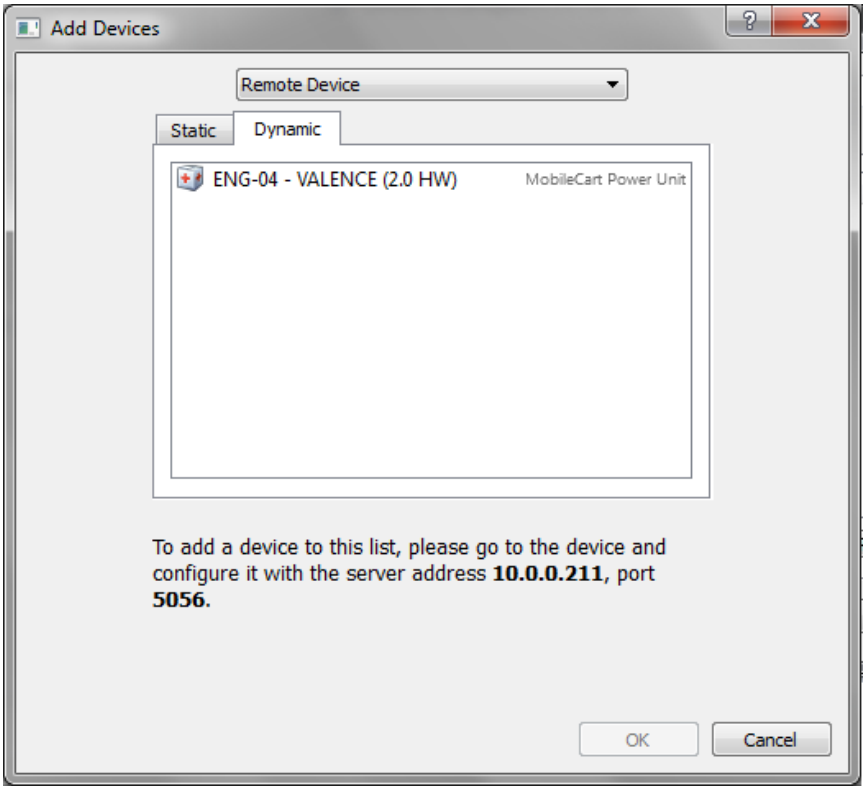
Click ***Dynamic*** to open the tab to display devices trying to connect to CIO server that are not yet added to the monitoring inventory.

Select the devices listed in the dialog and click OK to add these devices to CIO monitoring inventory.

Devices in the monitoring inventory appear in the ***All Devices*** list.

The list will be empty when:

- No devices are configured yet to connect to CIO. (See step 8 below)
- All devices pre-configured to connect to CIO have been accepted (OK).



8. Configure a mobile cart to connect to CIO:

- Note the CIO Server IP and TCP port listed in the dialog above.
- Go to the TechView UI of a cart PC running MPMView to configure that cart to connect to the CIO server, See Appendix C, MPMView Agent Configuration.

See Section III: Using CIO, for an overview of each of the features of the product: Alarm View, Pin Map, Event Log, Network settings, Folders, Groups , SmartGroups, Mail Settings and License Key dialogs.

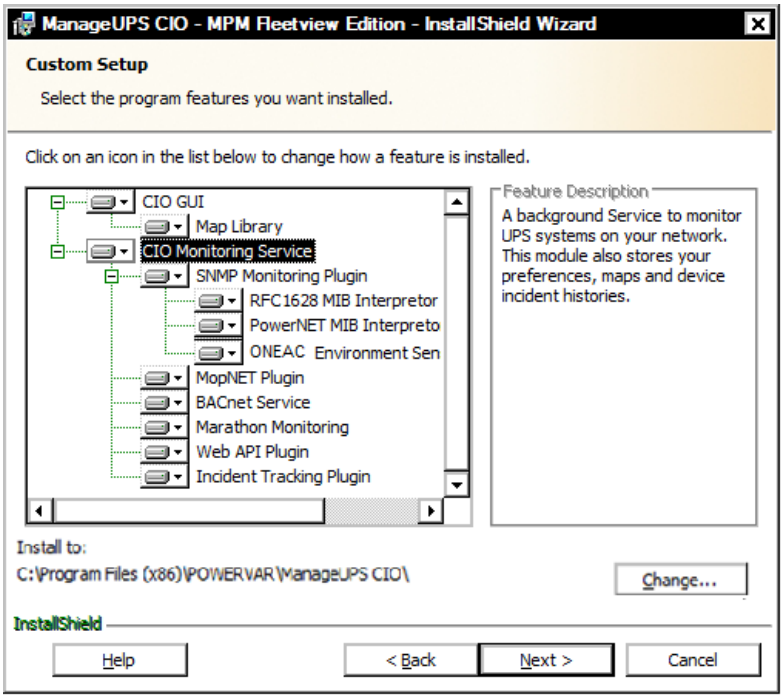
SECTION II: INSTALLATION DETAILS

INSTALLATION – MS WINDOWS

ManageUPS CIO is packaged for installation on Windows.
Server class OS (Win2k, 2k3, 2k8) are preferred as host for *CIO Monitoring Service*. Workstation class OS (XP Professional / Windows7) are suitable for the *CIO GUI* running on remote workstation.

Download and Run the MSI installer::

When you reach the *Setup Type* dialog – select *Custom* to reach the *Custom Setup dialog.* Point to each of the program elements in the tree diagram and review the *Feature Description* entry to familiarize yourself with the various components of the product.



Typical installations will install both the *GUI* and the *Monitoring Service* on the primary server computer that will host the *CIO Monitoring Service*.

When you only want the *CIO GUI* installed (for use on remote workstations), block the *CIO Monitoring Service* elements from being installed as shown above.

INSTALLATION - LINUX

ManageUPS-CIO for Linux is packaged as an RPM file. Install ManageUPS-CIO by opening a console with root permissions and enter the following command:

```
$> rpm –ivh /path/to/manageups-cio-install-package.rpm
```

Be sure to enter the proper path, and the proper installation package file name when entering this command. Once the RPM has finished installing the program will be running with a default 2 day, 5 device license key. The section *CIO License Manager* (Section II Page 22) will show how to install the license key.

NOTE: If you are running a local firewall on this computer, you must allow communication on ports 5055 and 161 for ManageUPS CIO to function properly.

NOTE: To run ManageUPS CIO as a "GUI Only" install, create (touch) an empty file called "noautostart." This will disable the daemon's automatic start on boot up. You can then run the GUI and navigate to ManageUPS-CIO services on running on other servers.

```
$> touch /opt/powervar/etc/noautostart
```

INSTALLATION NOTES – WINDOWS OR LINUX

REMOTE GUI INSTALLATION

When installing the *GUI* on a separate workstation computer that will be on a different subnet than the *CIO Monitoring Service* server, you should note the DNS name or IP address of the CIO server host. You may need this to be able to connect to the CIO Monitoring Server.

SECURE CIO SERVER FOR REMOTE ACCESS

By default, the GUI uses TCP port 5055 to connect to the Monitoring Service on a remote computer. The Monitoring Service uses port 5055 to monitor mopnet agents and port 161 to monitor SNMP agents. You may need to make sure these ports are open on all routers or firewalls between the CIO GUI, CIO server and the individual UPS agents.

You can change the default port settings between CIO Service and GUI using the Service Security dialog available from the main screen:

See *CIO Service Security Settings* for more information.

SECTION III: USING CIO

USING CIO: FEATURES EXPLAINED

STARTING THE CIO GUI - WINDOWS

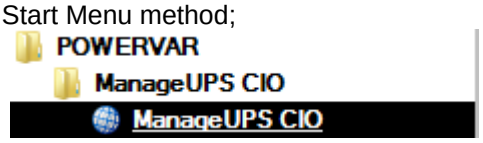
The installer will leave a *blue globe* icon on your desktop as a shortcut the *GUI*.

You can leave this on the Desktop.

Or, drag it to the Quick Launch *Toolbar* located on the *Taskbar*.

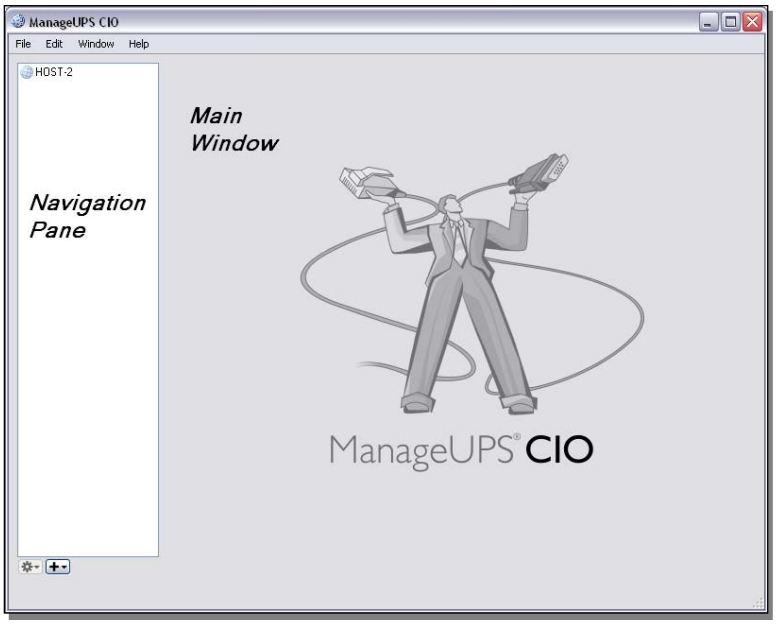
Or, delete it and use the Start Menu method;

Start >>All Programs >>



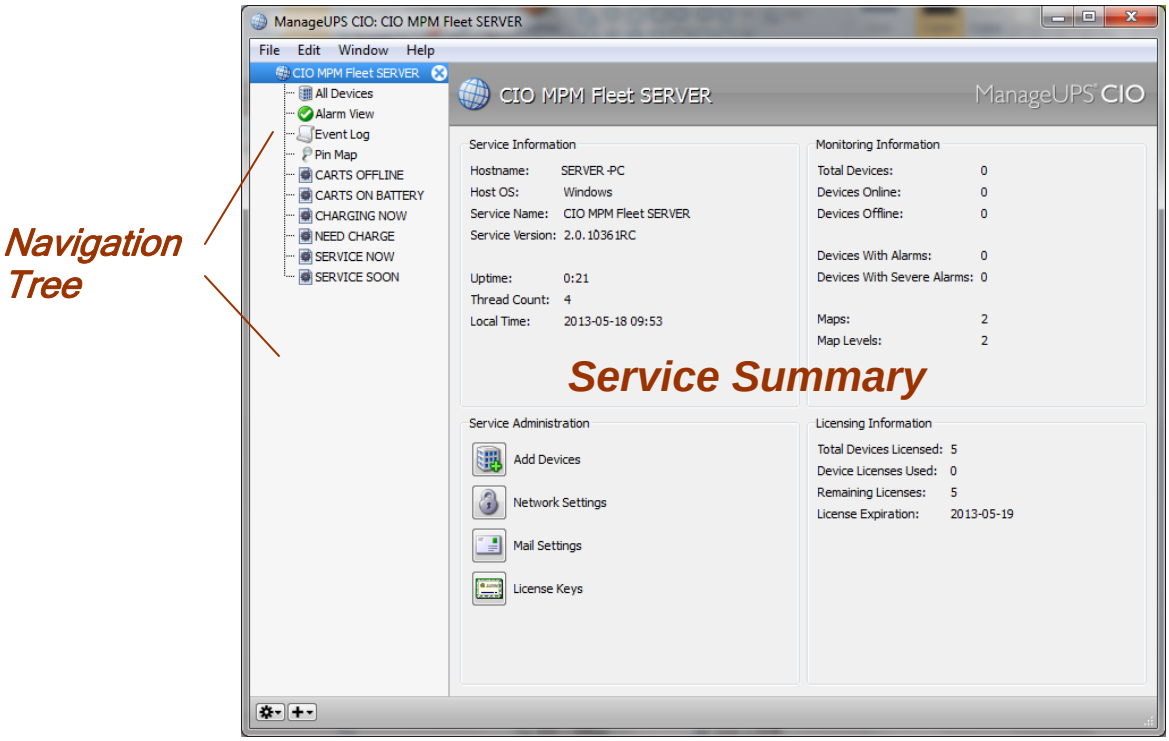
When the *GUI* first starts, the screen will appear as the image below.

A “Computer name” should appear in the *Navigation Pane*. This is the name of the computer on the Local network that is running a copy of the *CIO Monitoring Service*.



Select the entry in the *Navigation Pane* with the mouse cursor and click to open the connection between *GUI* and *Service*.

When the *GUI* connects to the *CIO Monitoring Service*, the *Service* summary information will be displayed in the *Main* window, and the *Navigation Tree* will open under the *Computer Name* entry in the *Navigation Pane*.



You will use the *Navigation Tree* to open various windows when you use CIO.

- All Devices is a sort-able list view of all UPS Agents in the management inventory.
- Alarm View is a specialized list of devices that are reporting an alert of some type.
- Pin Map includes a starter set of country and continent maps. You will want to add your own maps or floor plans or digital photos to help you visualize the location of managed UPS. Any JPG, PNG or GIF image file can be used as a background image in the *Pin Map* hierarchy.
- icons represent pre-defined *Smart Groups* that contain lists of devices meeting specific selection or filter rules. You can change the rules of these *Smart Groups* – or add your own *Smart Groups*.
- Groups, Bookmarks and Folders (not shown) can also be added to the *Navigation Tree*. These will be explained later.

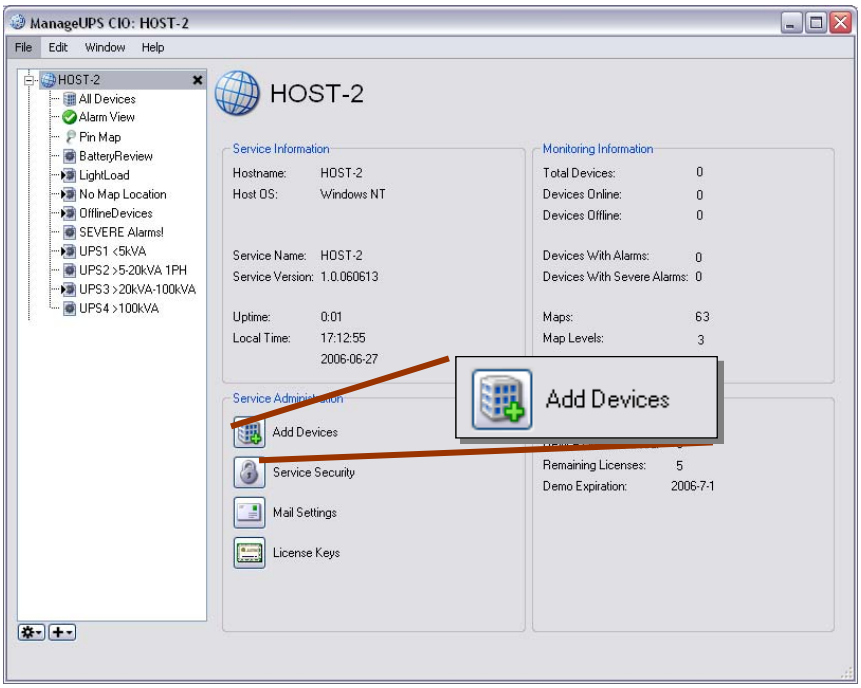
The next step is to add *Agent* connections to the *All Devices* inventory.

STARTING THE CIO GUI - LINUX

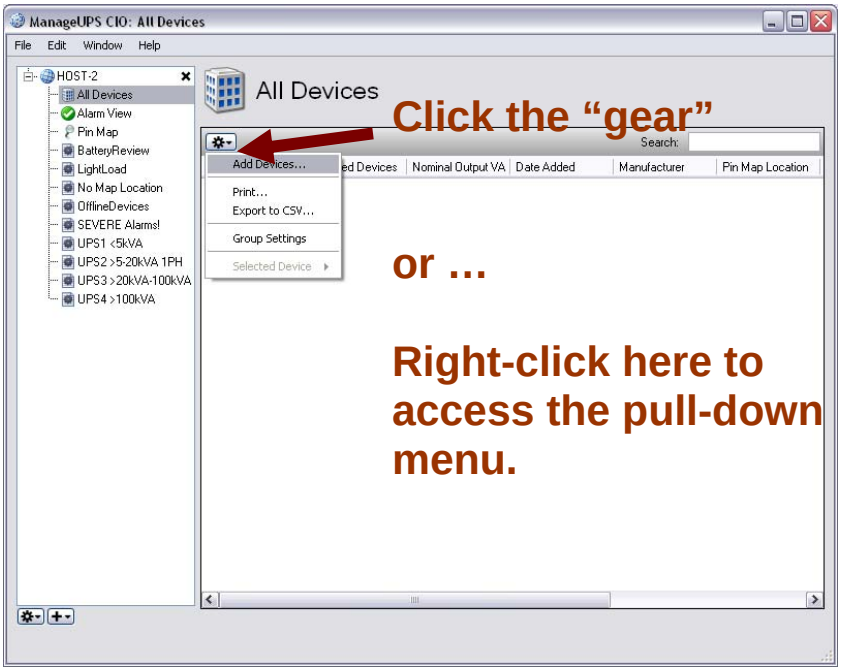
The ManageUPS-CIO GUI is located at `/opt/powervar/bin/cio`. You may enter this path in a console prompt, or create a shortcut on your desktop.

ADDING DEVICES TO THE "ALL DEVICES" INVENTORY

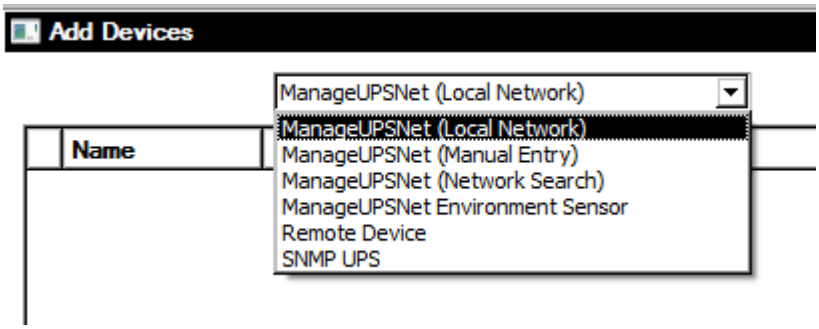
You can access the *Add Devices* dialog from the button on the *main screen.*



Or, from the *Options* dialog at the top of the *All Devices* window.



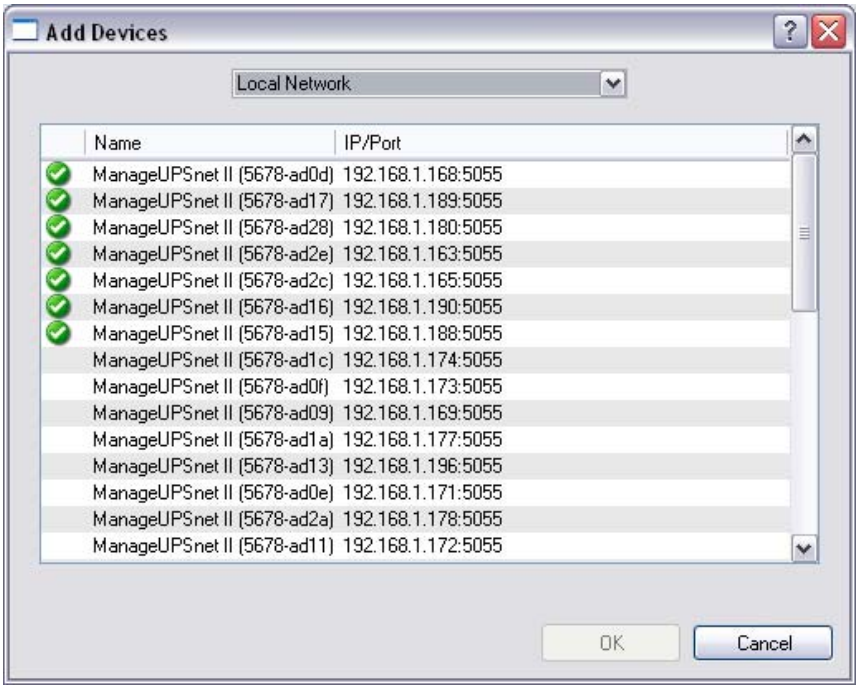
There are several methods for adding UPS devices to the managed inventory. There is a method for adding Environment Sensors and a method for adding Remote Devices (MPMView Agents)



Local Network

All ManageUPS II and III NET ADAPTERS use MDNS technology to publish their presence on the LAN to any application that is designed to recognize this information.

The *Add Devices - Local Network* option in ManageUPS CIO is designed to recognize this information. This enables automatic listing of any ManageUPS NET agents on the same LAN (subnet) as the computer hosting the *CIO Monitoring Service*



Devices on the local net that are already in the *All Devices* inventory are marked with green check mark as shown above.

IP Network Search

Initiates search of a specific subnet range for any ManageUPS NET or MopUPS agents.

A server computer running MopUPS software may be a *Secondary* agent or a *Primary* agent.

Agent Level

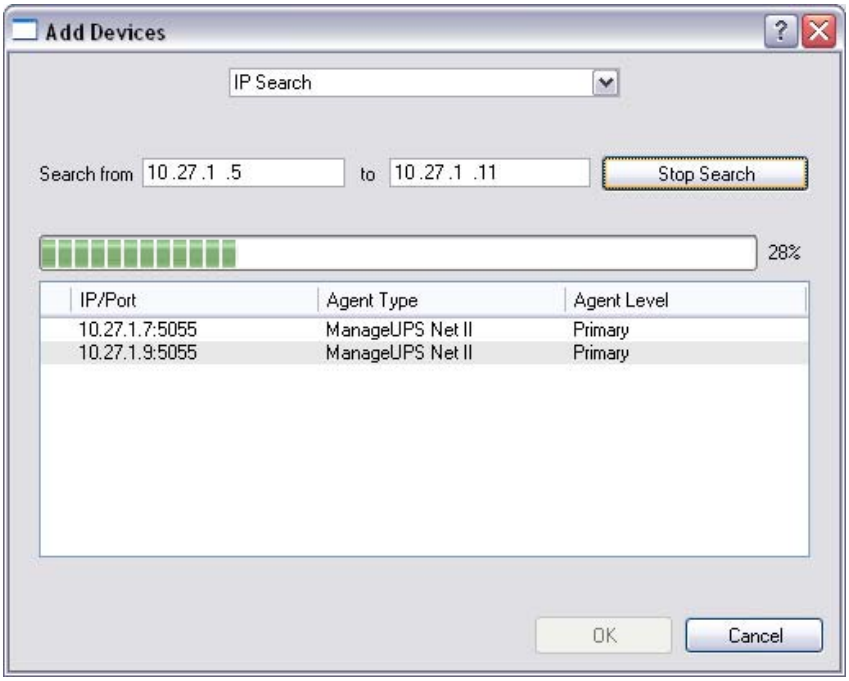
Primary: The Agent is communicating directly with the UPS.

Secondary: A proxy Agent has 2nd hand information retrieved from a UPS status server hosted in the primary Agent.

(See Section I, page 5 for more information on Agent type and level).

You will most likely want to exclude *Secondary* agents from your UPS inventory as unnecessary and potentially confusing duplicates of the UPS they represent.

The search result will show the "*Agent Level*" of discovered agents so you can easily exclude them from being added to the *All Devices* inventory.



ManageUPSNet Manual Entry – MOPNET

Use this option to add MopUPS or ManageUPS net agents using a known IP address or DNS host name.

Test Connection

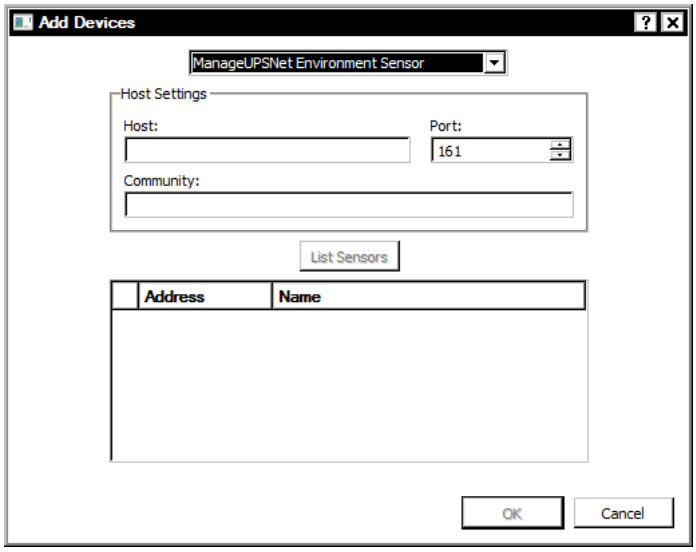
This option will be active when an entry is made in the *Host* entry box. Use this feature to verify that the DNS name or IP address entered manually is active and reachable on the network by ManageUPS CIO

SNMP (UPS)

Use this option to add SNMP agents using a known IP address or DNS host name. Select *RFC1628 Compliant UPS* for *Agent*s that conform to the standard UPS SNMP MIB (RFC1628). You will need to know the snmp "community" name – default is typically "public".

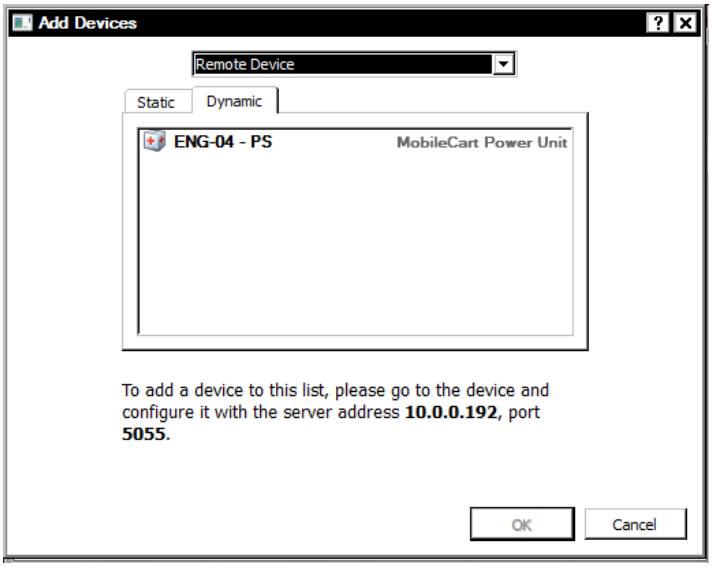
ManageUPSNet Environment Sensor – SNMP

Use this option to add Environment Sensors using a known IP or DNS host name. You will need to know the snmp "community" name – factory default is typically "public".



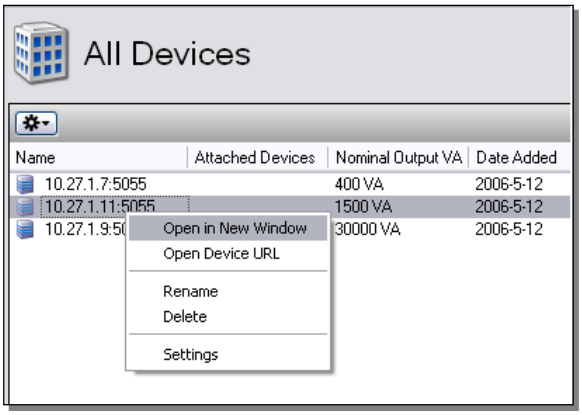
Remote Device (TCP – Dynamic IP address)

Use this option to add Devices represented by MPMView (Appendix C) and other Agent software from Powervar. Newer agents for on hosts with dynamic IP address settings can be configured to initiate a TCP connection to the CIO server.

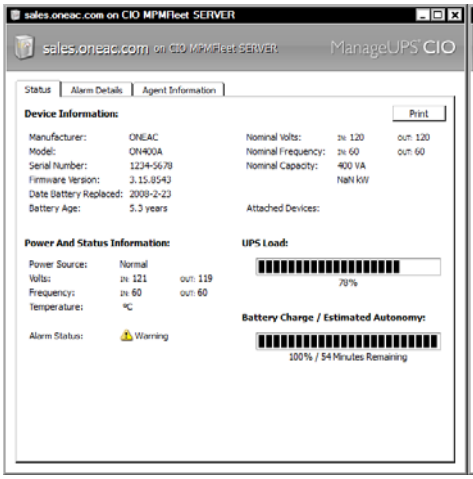


NAVIGATE TO DEVICE LEVEL VIEW

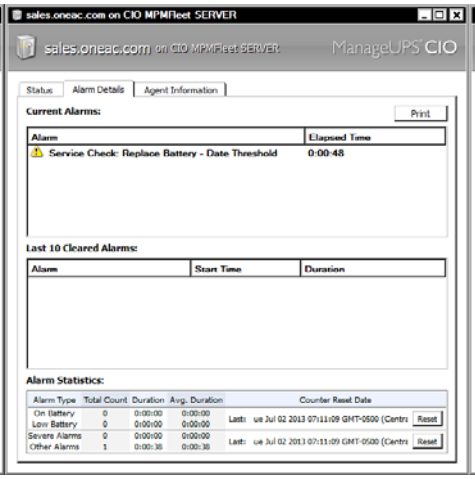
Once you have added a device or devices to the *All Devices* list, you can navigate to the *Device Level* view by double-clicking the device entry in the list or by right clicking the device entry to access the options menu.



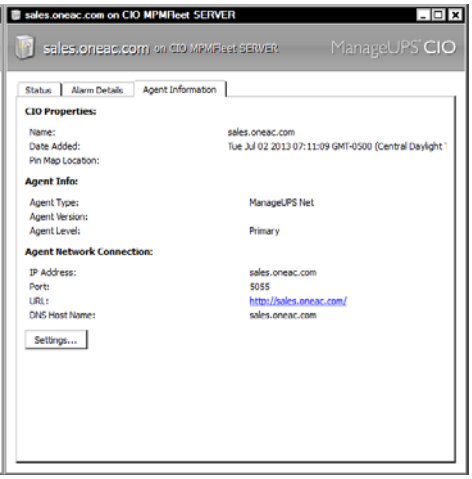
In the *Device Level* view there are three tabs; *Status*, *Alarm History* and *Agent Information*



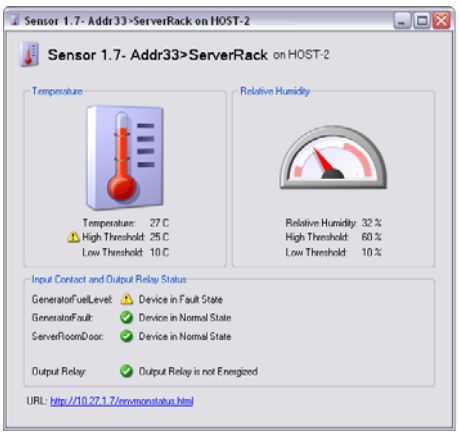
UPS Device Status Tab



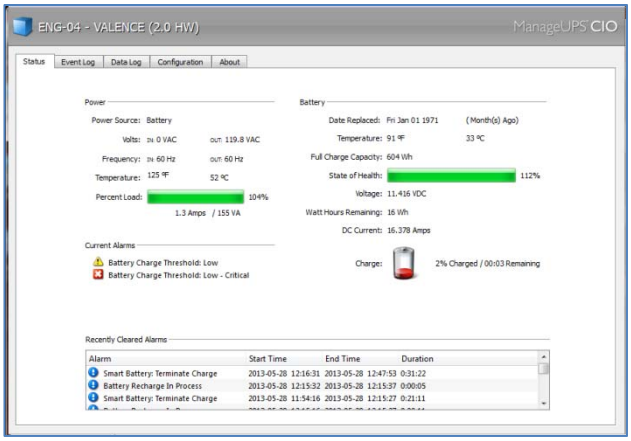
UPS Alarm Details



UPS Agent Info

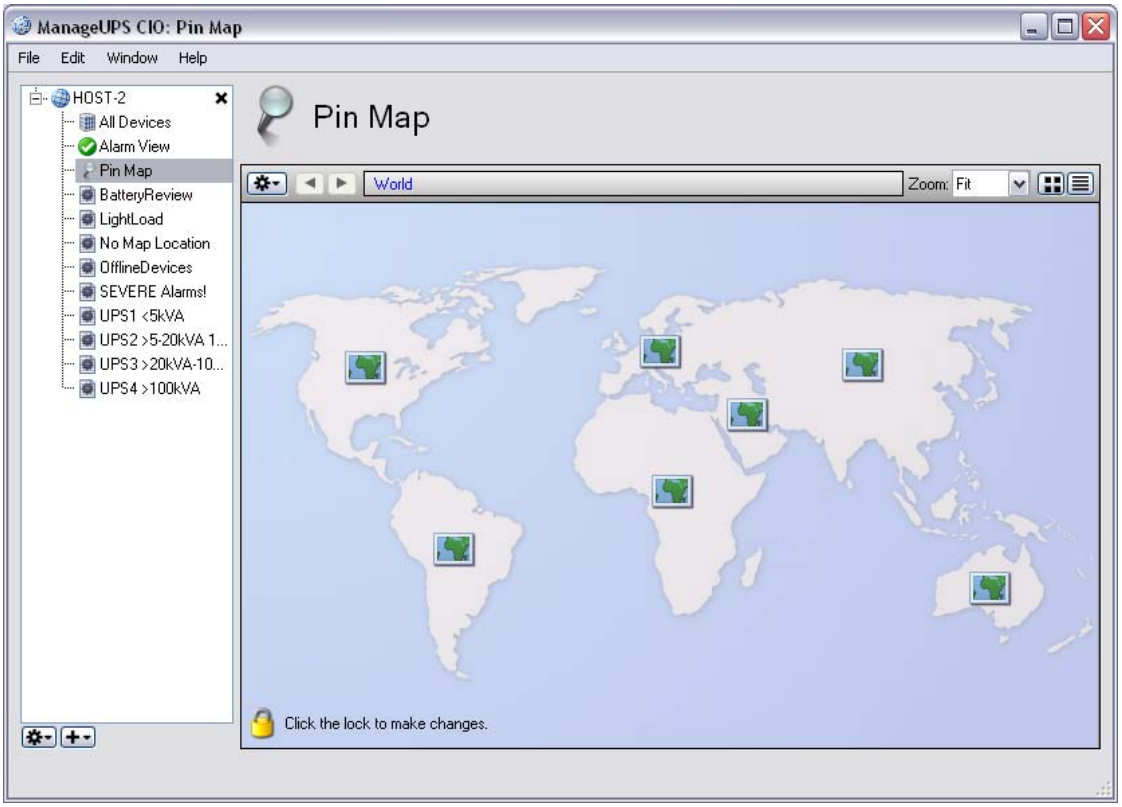


Environment Sensor Device status



MPM Device presents *MPM TechView UI* via CIO

SETTING UP YOUR PIN MAP



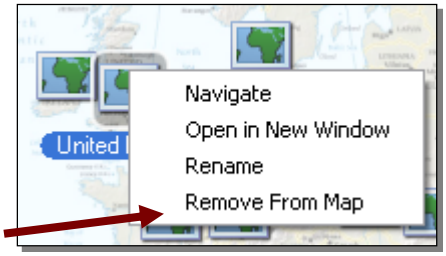
Pin Map includes a starter set of country and continent maps.

You may prefer to add your own maps, floor plans or digital photos to the map hierarchy to help you visualize the location of managed UPS.

Any JPG, PNG or GIF type image file can be used as background image in the *Pin Map* hierarchy

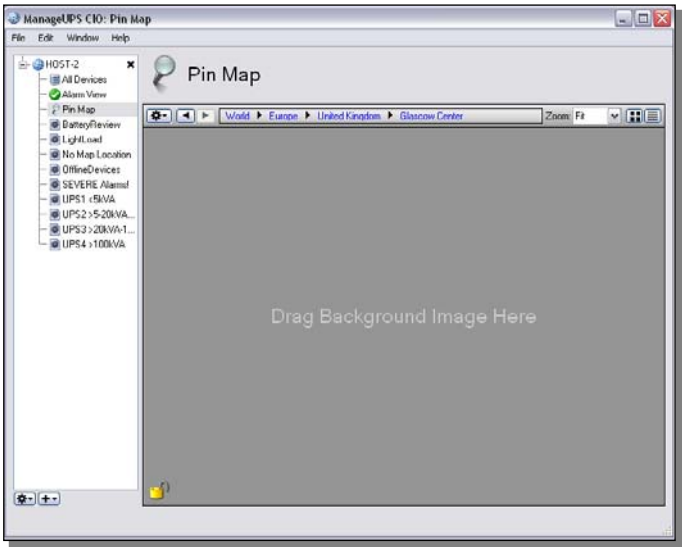
Removing default sub-maps

The small map icon on each of the continents in the image above represents a sub-map that exists at a layer below the current view. Right-click on any unneeded sub-map icon to open a dialog that lets you *Remove* that sub-map from the Map hierarchy.



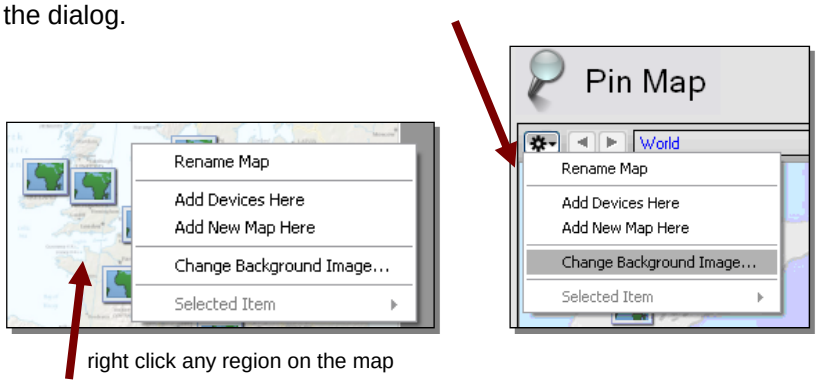
Changing a Background Map Image

The easiest way to add or change a background image may be to drag-and-drop the image file from its folder location onto the map window using the mouse.



To browse your computer for image files that may be located in various directories, use the *Change Background Image* dialog option.

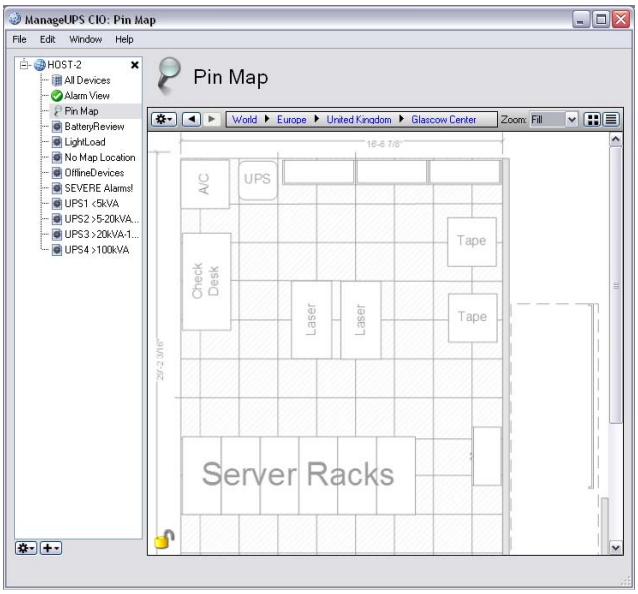
To change the background image at any level of the *Pin Map* – right click any region on the map, or use the *Options* button (gear symbol) to open the dialog.



The *Change Background Image* option will open a dialog to browse the file directory to locate the graphic image you want to use.

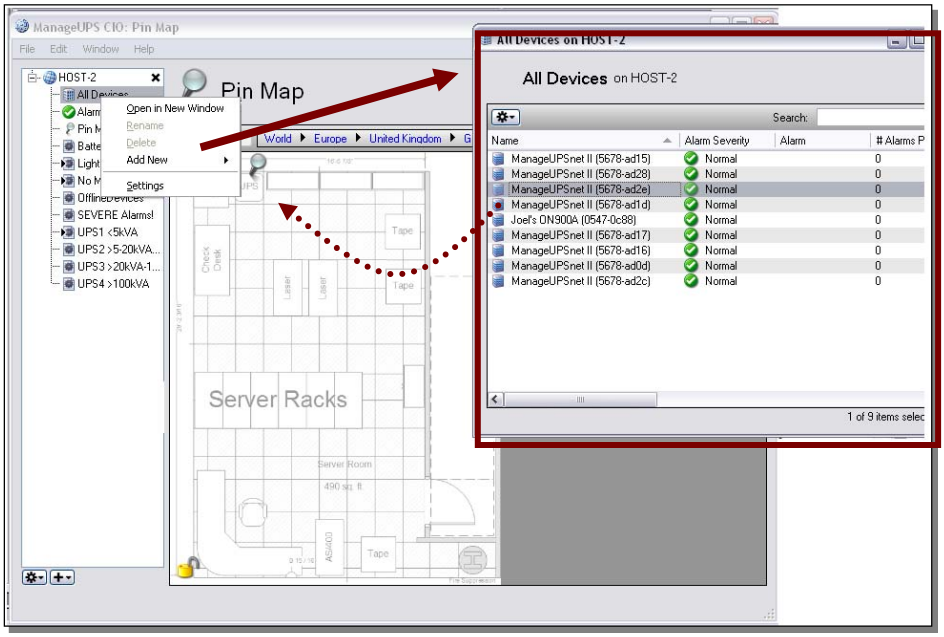
Any JPG, PNG or GIF image file can be used as background image in the *Pin Map* hierarchy.

The example following uses an image of a facility floor plan.



Placing devices on the Pin Maps

To add a device to a specific location on a map, right click any *list view* in the *Navigation Tree* and choose *pen in new window,* locate the device in the list, and drag it to the location on the map.



The lock icon at the bottom left of the map window will lock the positions of the pins on the map to prevent accidental moves or deletes. Click the lock icon to toggle between lock and unlock state.

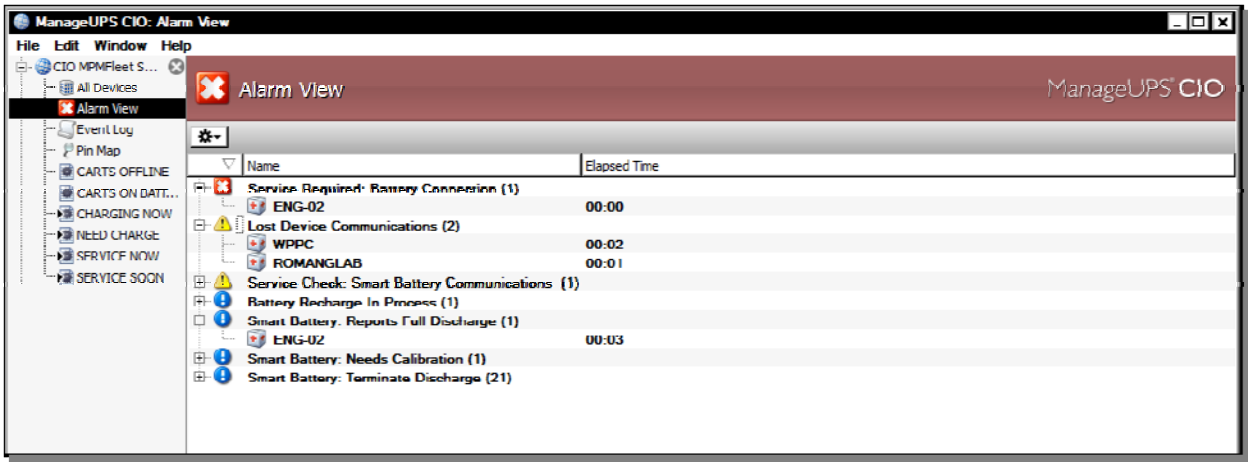
Alarm Indication on Pin Maps

Sub-map icons will display the color of the most severe alarm condition present on devices that are in that branch of the map tree.

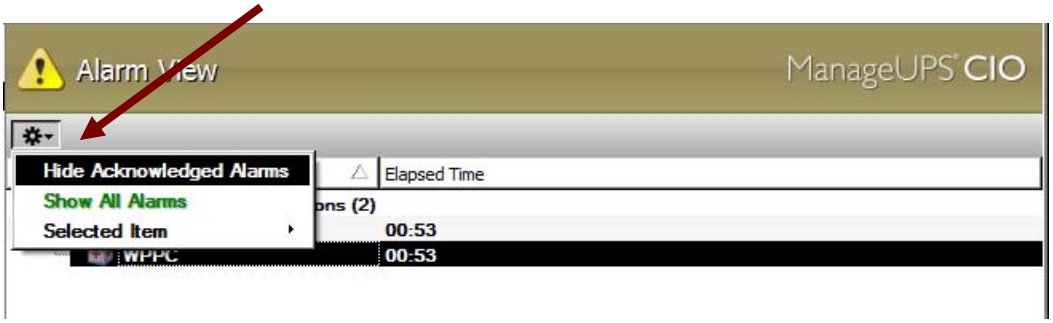
Pins will display the color code of any alarm condition when an alarm is present on the device it represents on the map.

TOUR THE ALARM VIEW

Alarm View is a specialized list of devices that are reporting an alert of some type.



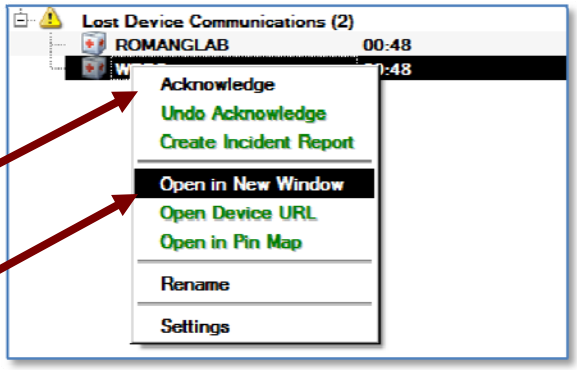
In the options dialog (Gear button) for the *Alarm View* – there is an option to *Hide Acknowledged Alarms* or *Show All Alarms.*



Acknowledged alarms will not be visible in the *AlarmView* list if the "*Hide*" option is selected. The red/yellow indicator of the corresponding *Pin and sub-map* icons will also be turned off.

Right click any device line in the *AlarmView* List to open the *device navigation dialog*.

If an alarm condition has been escallated to your incident tracking system, you can acknowledge the alarm in CIO using the *Acknowledge* option.

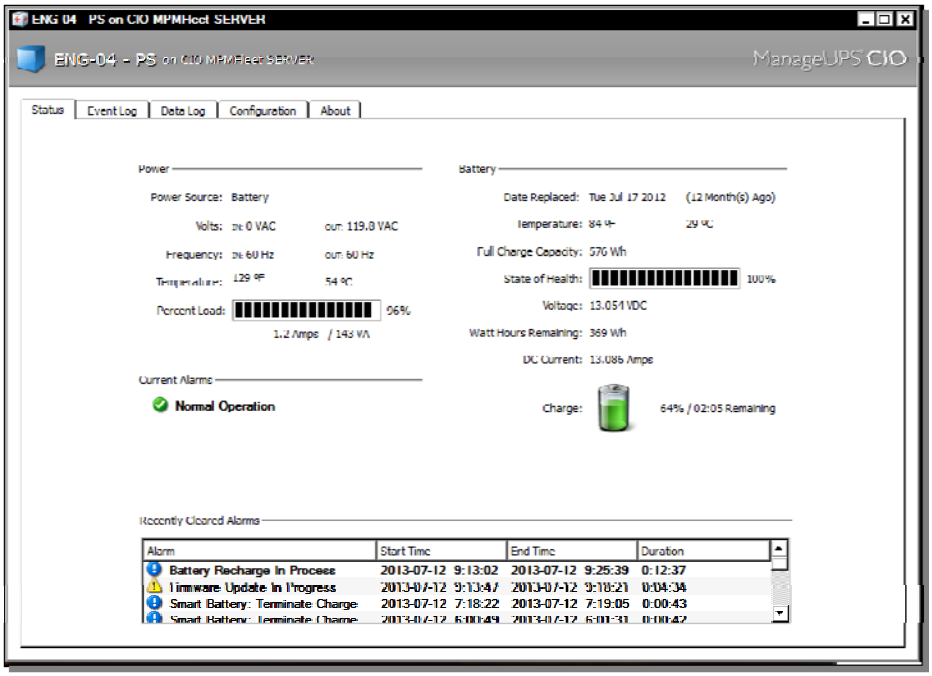


Select *Open in New Window* or double click any device line entry in the list view to open the CIO *Device Detail* screen.

NOTE: the *Create Incident Report* option is enabled only when an *Incident Tracking Plugin* license is installed in the CIO server.

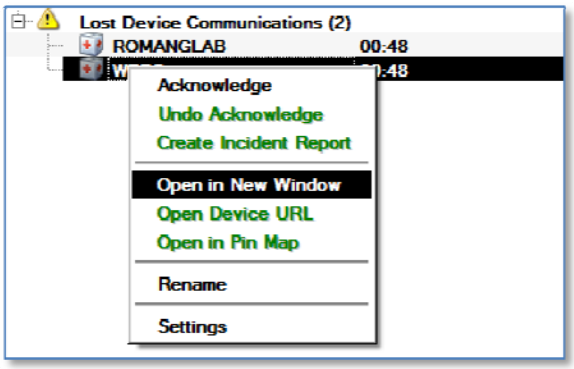
For MPM Devices monitored by CIO, the device UI in CIO is a remote connection to *MPMViev, TechView UI* on the remote workstation.

When you work with the *TechView UI* via CIO it is the same as working directly with *MPMView* locally on the remote workstation. All of the Configuration options in *TechView* are also available via the CIO remote interface to *MPMView*.



When you work with the event and data logs through this view – you are viewing the data and event logs stored on the remote workstation's *MPMView* directory.

The navigation options for *Open Device URL* are for other types of UPS or Temperature Sensor devices that are represented by dedicated management cards that have embedded WEB servers.

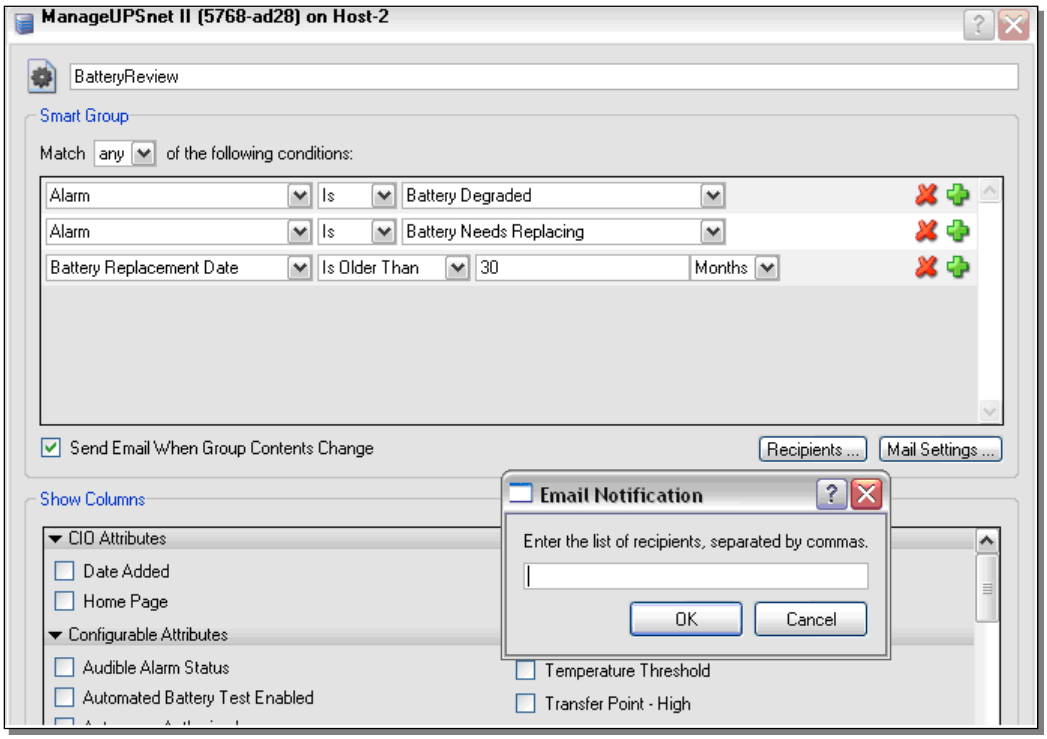


USING SMART GROUPS

Smart Groups contain lists of devices with properties from the *All Devices* inventory that meet specific *conditions* or rules. (See comment box: WHEN WILL SMARTGROUP CONTENTS CHANGE? A WORD ABOUT PROPERTIES)

Select a *Smart Group* from the *Navigation Tree* and *right-click* in the list area, or use the options button to open the *Group Settings* dialog.

You can change the rules of any default *Smart Group* – or add your own *Smart Groups*

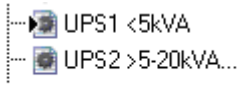


Show Columns dialog defines which columns will be displayed in the *List View* for that *Smart Group*.

Change of State Notification:

MnageUPS CIO offers two ways to let you know when the contents of a SmartGroup have changed, *On Screen* and via *Email*.

On Screen Notification
When the contents of a *Smart Group* changes, the *Smart Group* icon will display a small "open me" triangle to let you know that the contents have changed since the last time the Smart Group was opened.

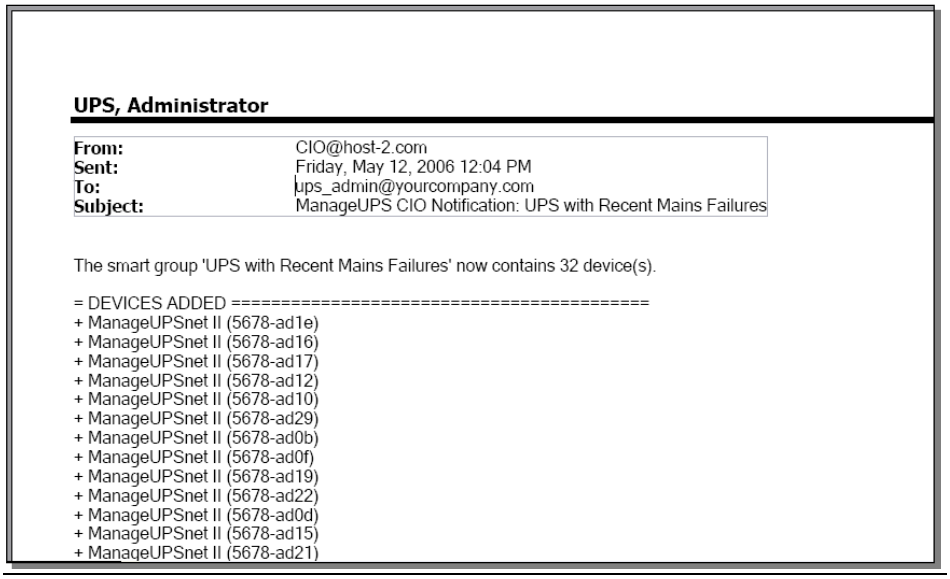


Email Notification - *Send Email when Group Contents Change:*
You can set CIO to send an email whenever the contents of a Smart-Group change. Use the *Recipients* dialog to define the destination of the email. Use *Mail Settings* to verify that CIO can route email thru your network mail server. (See page 21 for Mail Settings)

Alarm Storm Management

In the event of an alarm storm – (such as a wide spread mains failure that causes all UPS to switch to battery, or a network failure that breaks monitoring communications paths), CIO waits for the change activity to settle down before sending a single email summarizing the changes

Below is an example of an email summarizing the results of a mains failure that affected 32 UPS at about the same time.



UPS, Administrator

From: CIO@host-2.com
Sent: Friday, May 12, 2006 12:04 PM
To: ups_admin@yourcompany.com
Subject: ManageUPS CIO Notification: UPS with Recent Mains Failures

The smart group 'UPS with Recent Mains Failures' now contains 32 device(s).

= DEVICES ADDED ==========
+ ManageUPSnet II (5678-ad1e)
+ ManageUPSnet II (5678-ad16)
+ ManageUPSnet II (5678-ad17)
+ ManageUPSnet II (5678-ad12)
+ ManageUPSnet II (5678-ad10)
+ ManageUPSnet II (5678-ad29)
+ ManageUPSnet II (5678-ad0b)
+ ManageUPSnet II (5678-ad0f)
+ ManageUPSnet II (5678-ad19)
+ ManageUPSnet II (5678-ad22)
+ ManageUPSnet II (5678-ad0d)
+ ManageUPSnet II (5678-ad15)
+ ManageUPSnet II (5678-ad21)

WHEN WILL SMARTGROUP CONTENTS CHANGE?
A WORD ABOUT PROPERTIES

SmartGroups are very potent mechanisms that can be used to accomplish a variety of tasks.

SmartGroup rules remain active even when the *SmartGroup* window is closed. In other words, the *SmartGroup* continues to watch the *All Devices* inventory for devices with *properties* that satisfy the rules established in the *SmartGroup Settings* dialog..

It is likely clear that the content of a *SmartGroup* will change if the rules establish *thresholds* for *properties* that you expect to change – such as input volts, %load, battery age, or specific alarm conditions.

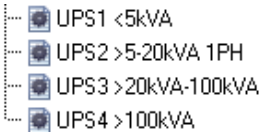
It might be less obvious that the content of a *SmartGroup* could change if the watched *properties* are things that normally do not change…such as UPS manufacturer – or UPS power rating.

When new devices are added to the *All Devices* list and have *properties* that meet the conditions of a *SmartGroup,* the contents of that *SmartGroup* will change to include the new devices.

For example, a default *SmartGroup* watches for devices that do not have a *Pin Map* association. If the entire existing inventory has been assigned a *PinMap* location, new devices will automatically appear in the "No Map Location" *SmartGroup* until you place them on an appropriate map.

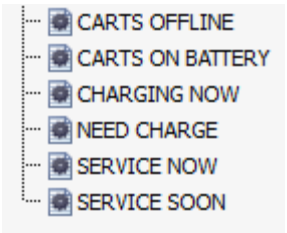
Default SmartGroups

A number of pre-defined *SmartGroup*s are created for you when you install ManageUPS CIO.



Some partition the *All Devices* inventory based on the power rating of a UPS (standard edition)

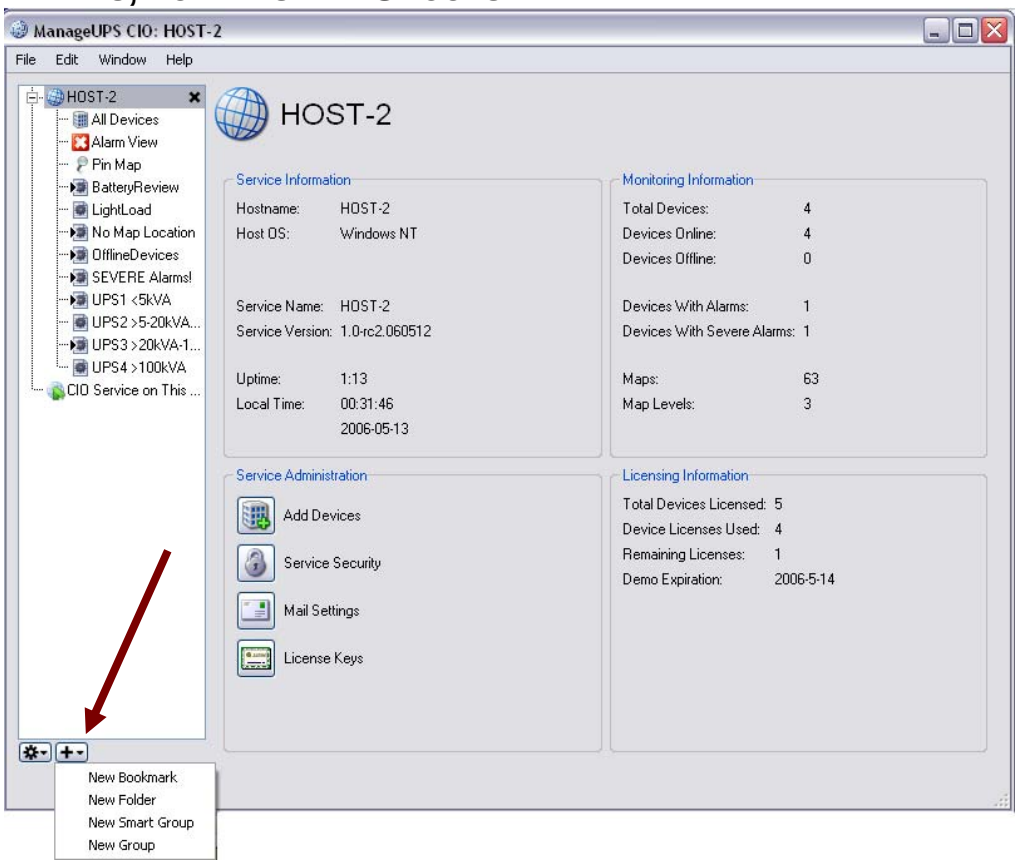
In the *MPM Fleetview Edition,* predefined SmartGroups watch for specific service indications, charging indications and devices off the network.



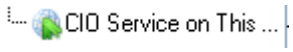
You can delete the default *SmartGroups*, modify the rules or add more *SmartGroups*.

If you end up with a long list of *SmartGroups* that begin to clutter the navigation pane, use the *Folders* feature to contain Groups that you use to create monthly reports or inventory analyses that you don't need to see on a daily basis..

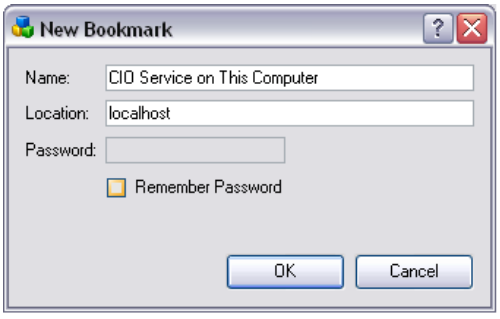
ABOUT BOOKMARKS, FOLDERS AND GROUPS



Bookmarks



Bookmarks are useful when the *CIO GUI* and *CIO Monitoring Service* are installed on different computers that are on different networks. *CIO Services* on remote subnets will not be visible to the *GUI* automatically. Setting a *Bookmark* to the IP address or *computer name* will let the *CIO GUI* navigate to the remote *CIO Service*.



If there is a network failure, the *CIO Service* will not be able to request or receive information from the monitored *Agents* and the *CIO GUI* will not be able to connect to the *CIO Service*.

Setting a bookmark for the *CIO Monitoring Service* on the *localhost* (same computer as the *GUI*) will allow the *GUI* to connect to the *Service* even if there is a network failure.

Folders

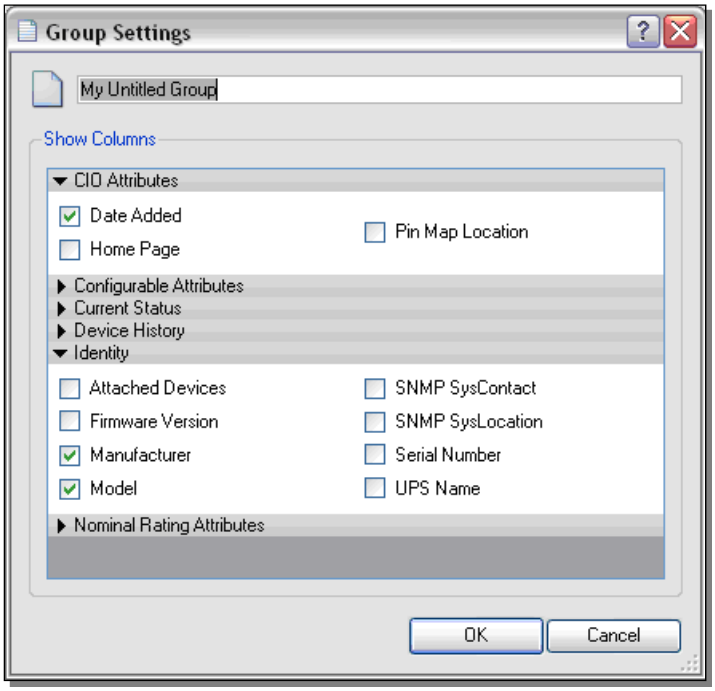
Folders are containers for collecting *Groups* or *Smart Groups* to reduce clutter on the *Navigation Tree*. Drag-and-drop items into Folders.

Groups

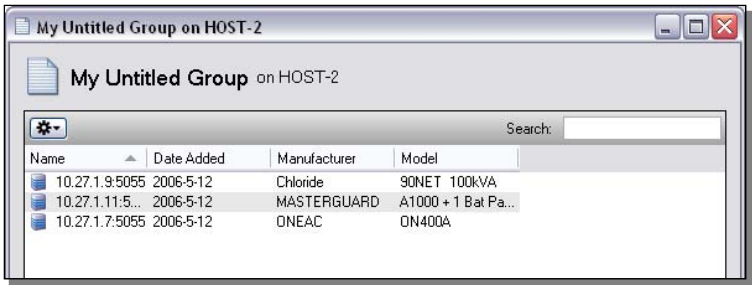
Place devices into your *Group* by dragging them from another *list view* opened in a separate window (such as *All Devices* or a *Smart Group*).

Groups are useful for setting up specific *list views* that display specific sets of information for reporting, export or analysis.

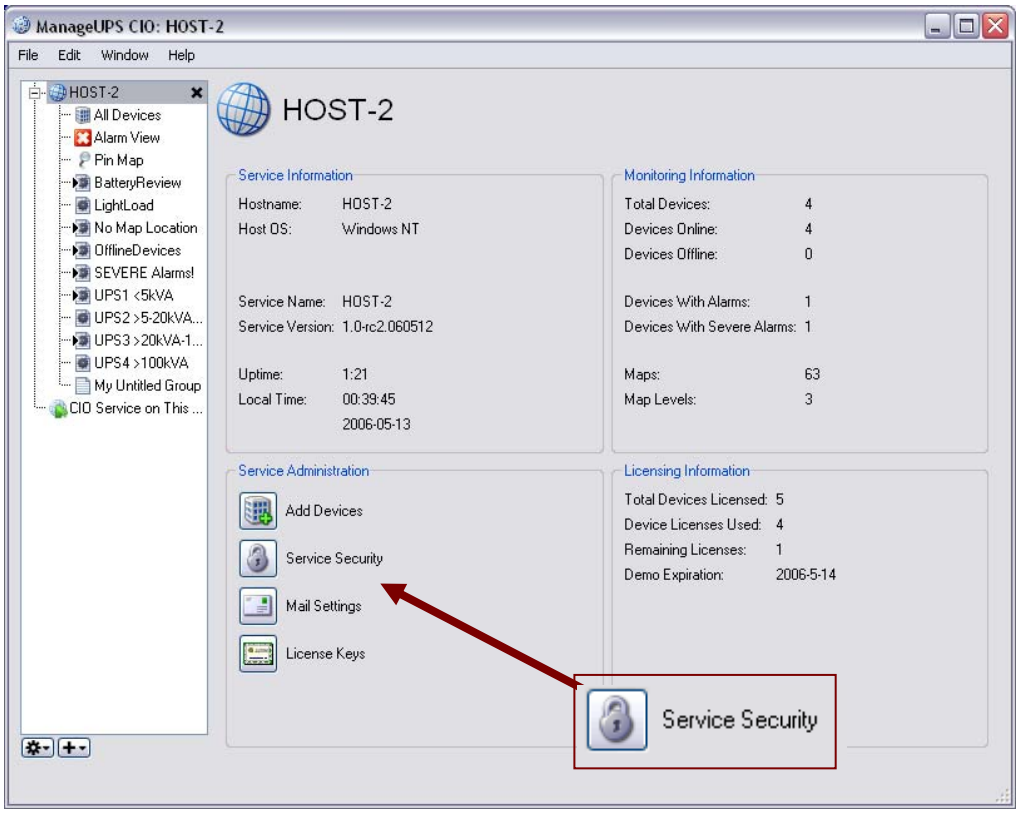
For example, you may want to create a report of all devices in the monitored inventory and show specific asset identify information such as manufacturer, model, serial number, etc. Use the *Group Settings* dialog to select the columns you want to display.



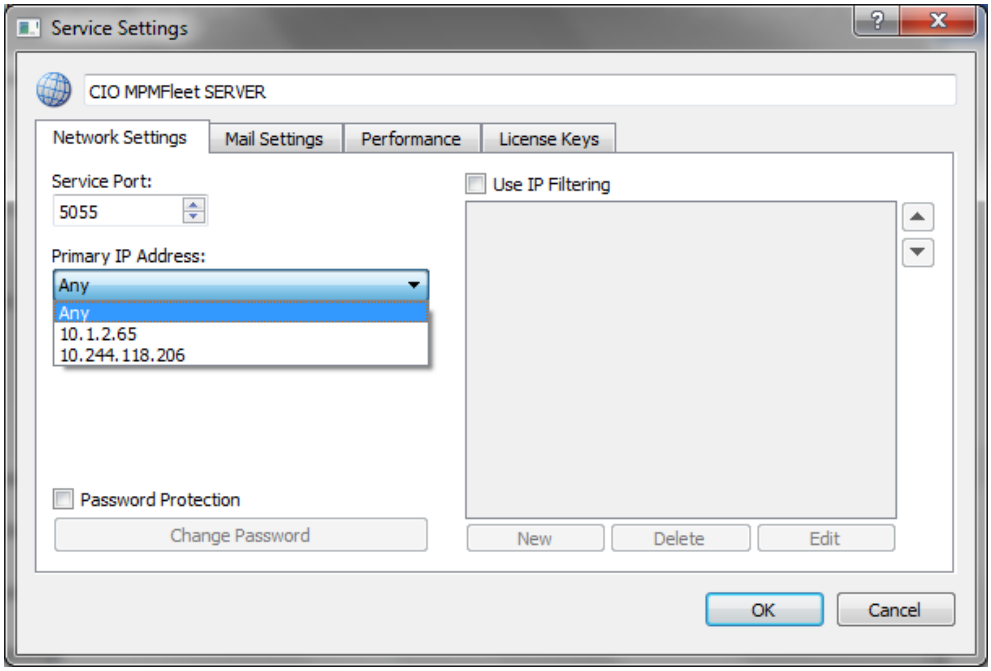
The *Group Settings* above result in the *List View* below.



CIO SERVICE SECURITY SETTINGS



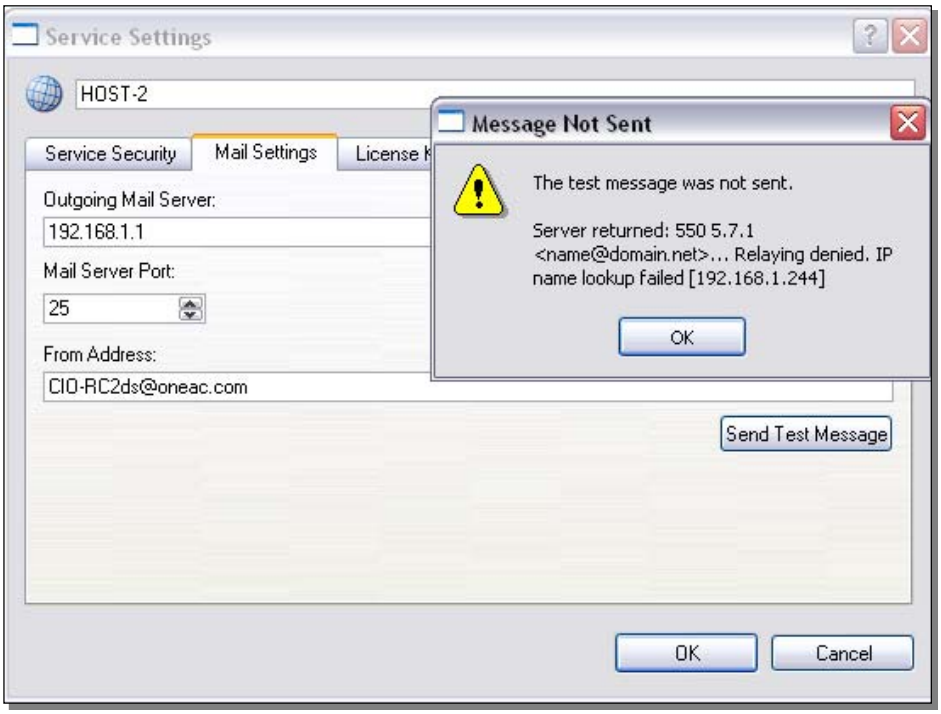
The *CIO Service* can be accessed from any workstation on your network running the *CIO GUI* application. To control access to the *Service* use the *Security Settings* dialog to set password, port or IP filtering options



On computers with more than one Ethernet interface, the Primary IP Address dialog lets you to select any or all CIO Server IP address(s) as the inbound connection address(s) for MPMView loaded on cart computers ..

CIO MAIL SETTINGS

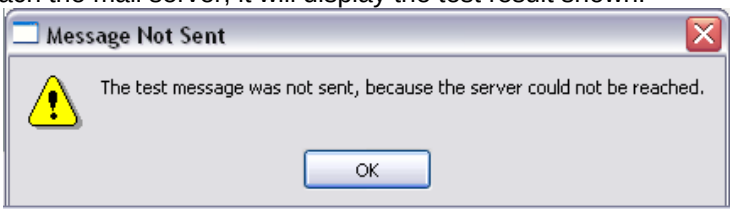
Configure the address or DNS name of the SMTP server that CIO should use to forward email



Use the *Test* feature to verify the settings.

If CIO can reach the server, but the mail server refuses the message, CIO will display the error message it receives from the mail server.

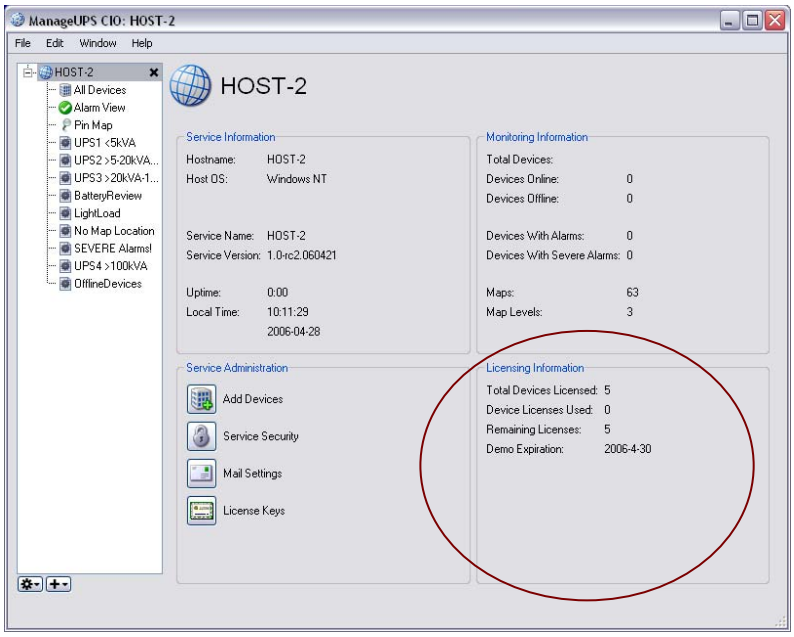
If CIO cannot reach the mail server, it will display the test result shown.



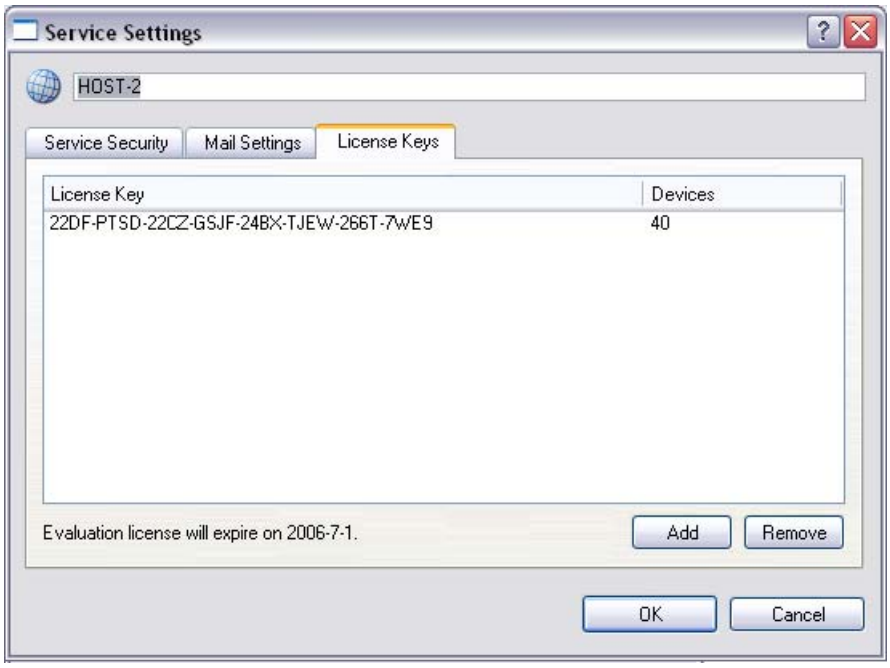
A successful message will return

CIO LICENSE MANAGER

Current License information is presented on the main screen.



Use the *License Manager Dialog* if you did not enter a License Key during installation, or need to add an additional key.



License Manager will translate and display the attributes of the key

A temporary or evaluation key will show the expiration date of the key.

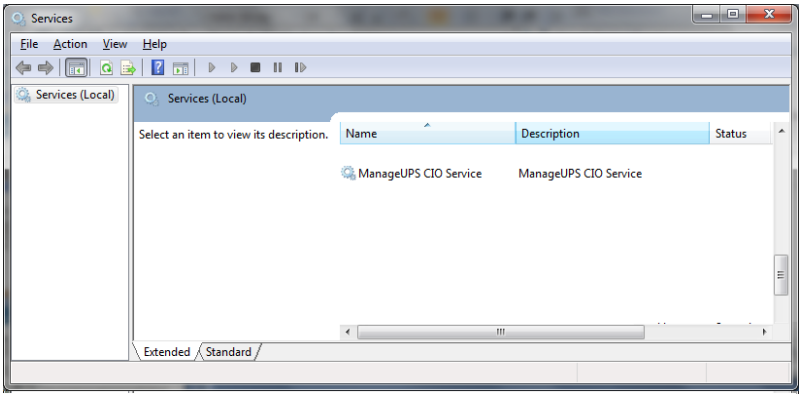
CONTROLLING THE CIO MONITORING SERVICE

MS WINDOWS

The *CIO Monitoring Service* installs and registers as a "*service*" under MS Windows. The ManageUPS *CIO Service* is configured to start automatically by the installer.

Windows *Services* are controlled through the *Services* module in the *Microsoft Management Console.*

To restart the *Service*, or to stop the *Service*, use the Windows Service Control Manager.



LINUX

You may use a graphical daemon manager if you choose. Otherwise, the console command options for starting, stopping and restarting the CIO service are :

```
$> /opt/powervar/bin/ciod start
$> /opt/powervar/bin/ciod stop
$> /opt/powervar/bin/ciod restart
```

NOTE: To run ManageUPS CIO as a "GUI Only" install, create (touch) an empty file called "noautostart." This will disable the daemon's automatic start on boot up. You can then run the GUI and navigate to ManageUPS-CIO services on running on other servers.

```
$> touch /opt/powervar/etc/noautostart
```

APPENDICES

APPENDICES

APPENDIX A : SYSTEM REQUIREMENTS & TERMINOLOGY

APPENDIX B: LIST OF MPM DEVICE PROPERTIES

APPENDIX C: MPMVIEW AGENT CONFIGURATION

APPENDIX A : SYSTEM REQUIREMENTS & TERMINOLOGY

SYSTEM REQUIREMENTS

Host for ManageUPS CIO Monitoring Service

- Server-class Intel computer (VM or physical)
- 1GHz CPU
- 1G RAM
- Ethernet network adapter

Host OS for ManageUPS CIO Monitoring Service

- Microsoft Windows 2000, 2003, 2008 Server products.
- Linux (Redhat 9, ES & SuSE 9.3)

Host OS for ManageUPS CIO GUI

- Any of the above listed OS
- Windows7 & XP Professional are suitable OS for remote ManageUPS *CIO GUI* installations.

Windows XP as Host OS for ManageUPS Monitoring CIO Service:

Security provisions in XP Service Pack 2 and Windows7 will slow the network search utility. Further, if there is a network failure that affects the ability of CIO to connect to more than 10 IP-address destinations, Windows security provisions will halt further network traffic from the host computer.

Security provisions added to Windows XP by Service Pack 2 and Windows7 will add significant and noticeable delays to all network traffic from the host computer if there are simultaneous attempts to connect to more than 10 unreachable IP destinations.

ManageUPS CIO monitoring service initiates IP connections 6 times per minute with each UPS being monitored. If 10 or more UPS IP addresses become unreachable destinations to CIO due to a network problem, XP SP2 or Windows7 will activate these security provisions. This will cause significant and noticeable delays in the host computer's network functions that impact all applications.

Windows XP or Windows7 may be an acceptable platform for your installation if;

A.) the total number of UPS devices to be monitored by ManageUPS CIO is less than 10,

and if;

B.) no other programs that initiate network connections (such as viruses, VoIP, or network utilities) are attempting to connect to unreachable network addresses from the XP /Windows7 computer.

Network Infrastructure and Security

CIO monitors UPS Management Agents on TCPIP networks using specific ports. You may need to verify that the default ports below are not blocked by network security policy.

- SNMP uses port 161
- MOPNET uses 5055
- Network Search uses port 5055
- Open agent URL function uses port 80

If the default ports are not allowed – you will need to know which ports are allowed for this use – and you will need to configure your UPS Agents to use the assigned alternate port for MOPNET or SNMP services.

UPS Network Management Agents

CIO will monitor devices that are represented on a TCPIP network by

- ManageUPS NET ADAPTER (MUN)
- ManageUPS NET ADAPTER II (MUN-II)
- ManageUPS NET ADAPTER III (MUN-III)
-
- MPMView Software
- MopUPS PROFESSIONAL software, Version 2.x
- MopUPS EXPRESS Version 1.x

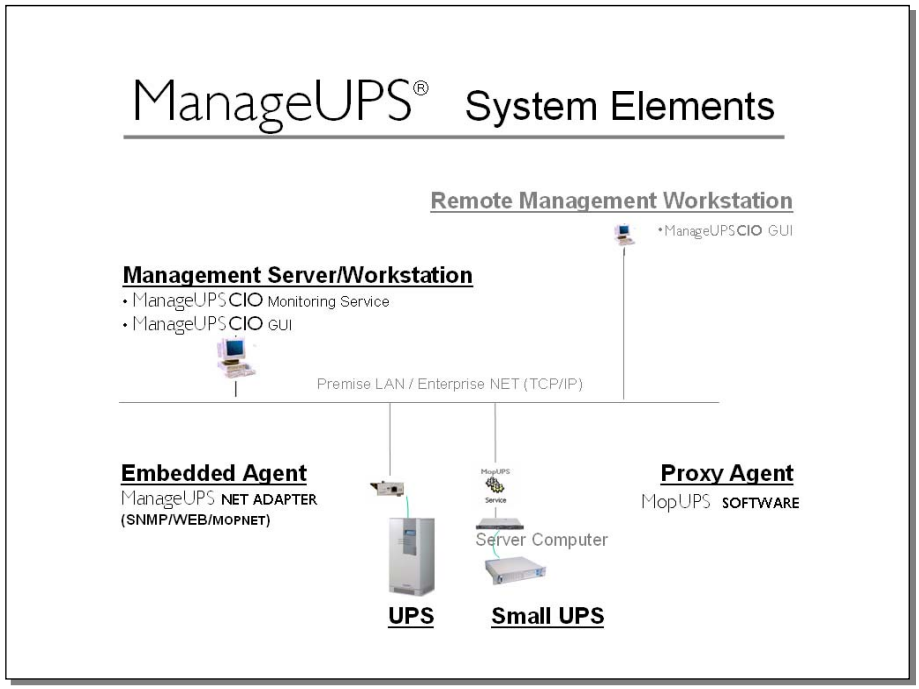
CIO will monitor Environment Sensors that are represented on a TCPIP network by

- ManageUPS NET ADAPTER II (MUN-II)
- ManageUPS NET ADAPTER III (MUN-III)

CIO will also monitor 3rd party UPS that are represented on a TCPIP network by an SNMP agent that is compliant with the standard UPS MIB (RFC1628) or the Powernet MIB.

SYSTEM ELEMENTS: DEVICE, AGENT AND MANAGER

The diagram below illustrates the main elements of the ManageUPS system.



UPS operate at the *device* layer – objects to be monitored and managed by the system.

Devices are represented by Agents. Agents monitor the devices locally and make Device information available on the network. Alarm conditions are detected or interpreted by the Agent and made available to the Manager layer.

Embedded Agents and Proxy Agents

Embedded Agent

Generally, embedded agents are preferred as more dependable. The host environment is a closed system, dedicated to specific device management functions.

The agent is hosted in an embedded system – software loaded as firmware in a special purpose computing platform.

The ManageUPS NET ADAPTER is a special purpose computing platform designed to host a variety of software services related to UPS management – Data and Event Logging, Network Shutdown Controller, UPS WEB server, FTP server for log download, configuration and firmware update, SNMP agent, Event Message service (email), Telnet Server etc., etc.

Proxy Agent

The Agent is hosted in a general purpose computing platform that may host other applications and services.

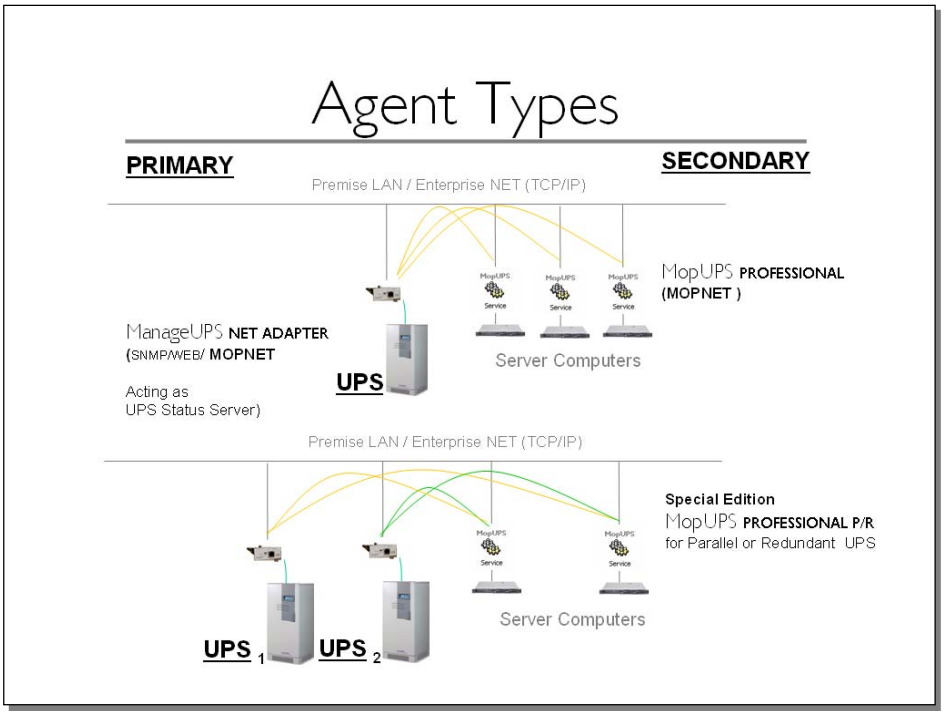
MopUPS PROFESSIONAL is software designed to monitor a specific UPS primarily for the purpose of calling automated shutdown of the server (MopUPS host) in the event of extended mains failures.

In some low power UPS applications, MopUPS may be a cost-effective agent to represent the UPS to ManageUPS CIO. (See Appendix B for more information on configuring MopUPS to serve as a Proxy Agent). However, it should be recognized that when MopUPS calls for shutdown of the server OS, MopUPS monitoring service will no longer be running and the UPS will become invisible to ManageUPS CIO until power is restored and the server is restarted.

Agent Level

Primary: An Agent communicating directly with a UPS.

Secondary: An Agent that retrieves information indirectly, from a UPS status server hosted in a primary Agent.



TERMINOLOGY BASES

If you are already familiar with BMS, BIS or NMS type management systems, you likely have an understanding of the methods, key concepts and specific terminology associated with these systems.

While the various management systems referenced use structural elements that are functionally similar across systems, specific terminology may differ.

The ManageUPS system and related documentation (including this *User Guide*) make use of concepts and terminology from internationally accepted sources that provide standardized frameworks for the topic of infrastructure management:

ISO/IEC 7498-4 – OSI (Open Systems Interconnection) Basic Reference Model, Part 4, Management framework.

ITIL (IT Infrastructure Library) developed and published by the UK OGC (Office of Government Commerce):

- *Service Support (2000) ISBN 0113300158*
- *ICT Infrastructure Management (2002) ISBN 0113308655*

IETF Standards 16 (SNMPv1) and 62(SNMPv3) covering the Network Management Framework.

ISO 16484-5 /ANSI/ASHRAE 135-2004 & CEN TC 247 -- BACnet – A data communication protocol for Building Automation and Control Networks.

Generally, the ISO/IEC 7498 and ITIL references provide concepts and terminology for the activity, focus and “best practice” of ICT systems infrastructure management

The IETF/SNMP references provide terminology and concepts for the *Agent* / *Manager* elements of the ManageUPS system

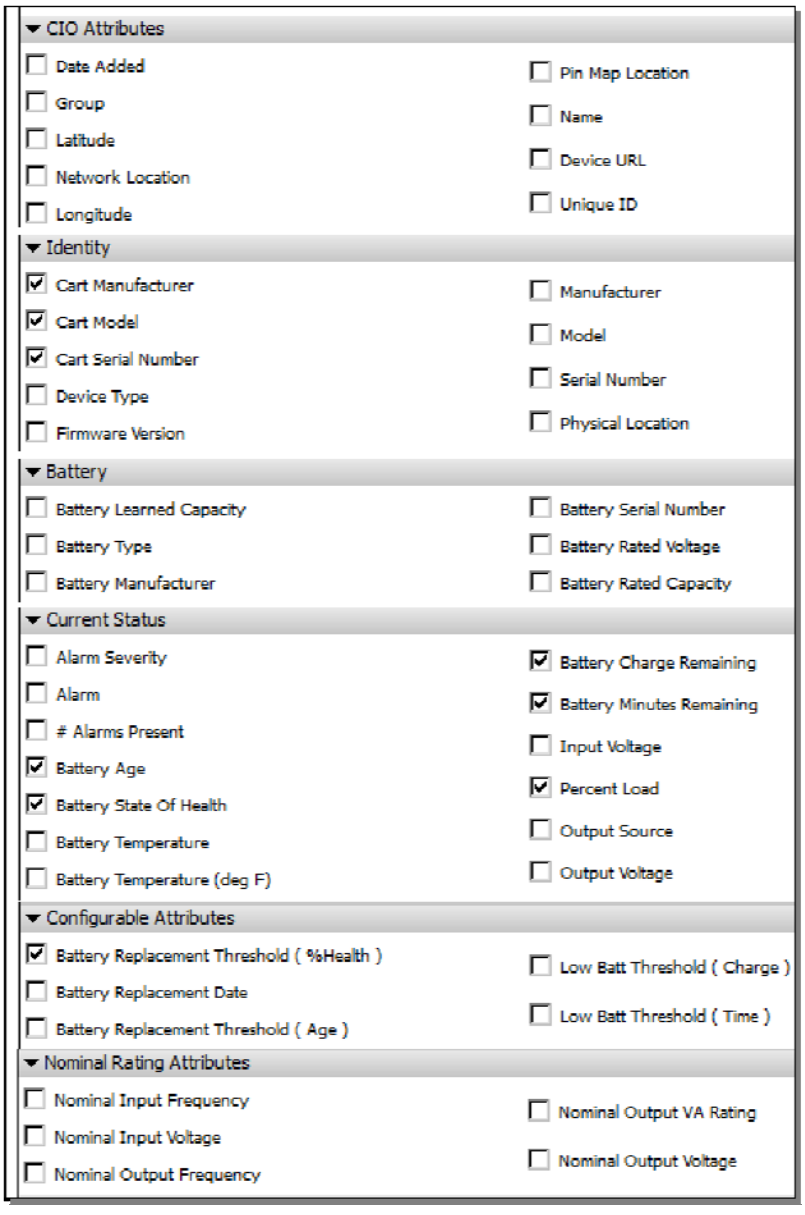
The ISO 16484 reference helps illustrate the similarities and differences between the more established management framework of the ICT community and the emerging standard management framework of the building automation and control community.

Acronyms and Vocabulary used in this topic

BMS	Building Management Systems
BIS	Building Information System
NMS	Network Management System
IEC	International Electro-technical Commission
ISO	International Organization for Standardization
OSI	Open Systems Interconnection
OGC	Office of Government Commerce (UK)
ITIL	Information Technology Infrastructure Library
ICT	The convergence of Information Technology,(IT) Telecommunications and Data Networking Technologies into a single technology (ITIL, ICTIM Glossary)
ICTIM	Information and Communications Technology Infrastructure Management
IETF	Internet Engineering Task Force
SNMP	Simple Network Management Protocol
ANSI	American National Standards Institute
ASHRAE	American Society of Heating, Refrigeration and Air-Conditioning Engineers
CEN	Committee for European Standardization

APPENDIX B : LIST OF PROPERTIES - MPM

LIST OF MPM PROPERTIES IN CIO



At left is a list of MPM Device properties that CIO may monitor or display.

These properties can be used in *SmartGroup* rules.

These properties can also be selected for display in any List View using the *Group Settings* dialog

In properties list at left,

Properties under the heading “CIO Properties” are properties of a device that are assigned by the CIO server and populated from within the CIO server..

All other properties in the list are specific MPM Device Properties that are “pushed” to the CIO server from the MPMView Agent.

APPENDIX C : MPMVIEW AS PROXY AGENT

MPMVIEW: AGENT CONFIGURATION

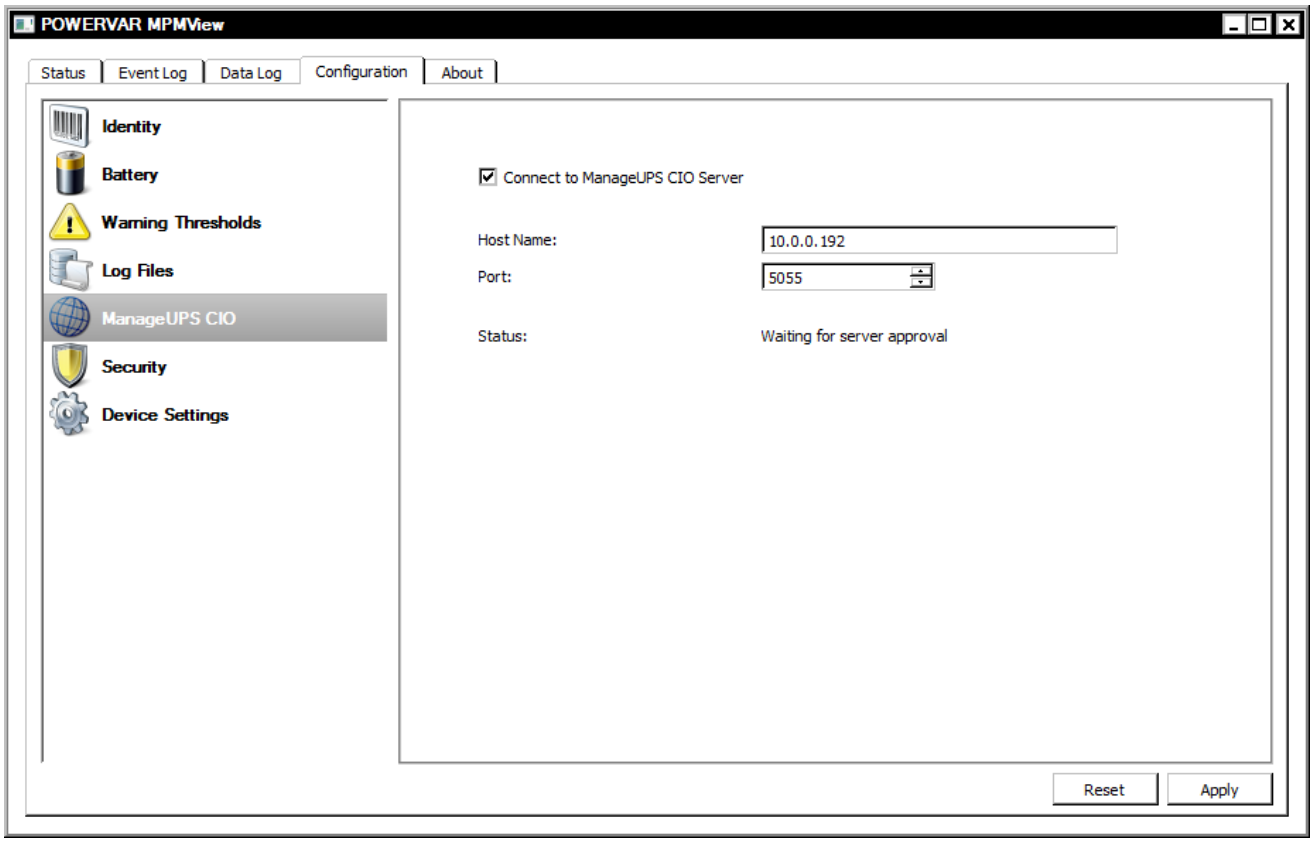
MPMView is POWERVAR's software for monitoring MPM charger/inverter system and associated battery in powered carts.

To use MPMView as an *Agent* for monitoring by ManageUPS CIO, open the TechView UI, then navigate to the Configuration tab>> ManageUPS CIO

Check the box and enter the IP address or DNS name of the CIO Server host.

Once the Agent has connected to the CIO server, it wil present the message as shown below, "waiting for server approval".

See Section I, page 4 of this manual to learn how to "approve" a device connection and add the device to the monitoring inventory.



***NOTE**: the default port for network communications between MPMView and the CIO Server is TCP port 5055. Make sure the port is open on all firewalls between the MPMView hosts and the CIO host.*