RMS ENTERPRISE
RMS-ENT (V4.6 OR HIGHER)

RMS ENTERPRISE

AV FOR AN IT WORLD

Table of Contents

RMS Enterprise

Overview

RMS (Resource Management Suite®) *Enterprise* is an innovative meeting room management and equipment monitoring software package that provides centralized remote management of networked AV equipment and building systems. Use *RMS Enterprise* to:

- Simplify operation, support and security with enterprise scalable software
- Improve Help Desk performance to meet Service Level Agreements through proactive maintenance
- Reduce energy consumption and extend useful life of devices with enhanced reporting features

RMS Enterprise is a client/server application where the NetLinx system acts as the client and the RMS Enterprise application server listens for connections from NetLinx systems. NetLinx and the RMS Enterprise application server communicate using TCP/IP sockets. In order to establish communication, each NetLinx system must be able to resolve and connect to the RMS Enterprise application server. This can be accomplished with a variety of Network configurations including local area networks (LAN), wide area networks (WAN), and the Internet.

This document is intended primarily for the RMS System Administrator and describes Admin-level functions of the RMS Enterprise user interface (UI).

System Recommendations, Requirements and Installation Instructions

RMS Enterprise is a true enterprise-level application, and has specific minimum system requirements that must be met to ensure a successful deployment. The *RMS Enterprise Installation Manual* is provided to ensure that all the necessary prerequisites are met, and that the necessary configuration options are identified prior to the installation of the RMS Enterprise server and RMS Database server.

The *RMS Enterprise Installation Manual* is available to view/download from www.amx.com (see *Additional RMS Enterprise Documentation* on page 19).

Accessing the RMS Enterprise UI

The RMS Enterprise UI is accessed via web browser.

1. To open the main RMS Enterprise UI, enter the following URL in your browser's address bar:

    http://rmsServerURL/rms/#/

    or

    http://rmsServerURL:8080/rms/#/

    (depending on how Tomcat is configured - refer to the RMS Enterprise Installation Guide for details on Tomcat installation and configuration)

2. This opens the *Please Sign In* page (FIG. 1):

FIG. 1 Sign In

Enter a valid Username and Password, and click **Sign In** to access the main RMS Enterprise (HTML) UI (FIG. 2):

See page 20 for a description of the RMS Enterprise HTML interface.

FIG. 2 Example RMS Enterprise HTML Interface (Dashboard view)

Accessing RMS-ENT-CLOUD (RMS Enterprise Hosted Cloud Service) UI

RMS-ENT-CLOUD is accessed via web browser. To open the main RMS Enterprise Web UI, enter the following URL in your browser's address bar:

> http://rms-<servername>.amxservice.com/#/

NOTE: *As of RMS Enterprise v4.6, many of the menus and options that are familiar to administrators of previous versions of RMS Enterprise are now contained in the "Classic UI". Click the Classic UI button in the HTML UI menu bar to open the Classic UI workspace. See the The RMS Enterprise Work Area (v4.6 or higher) section on page 20 for details.*

Additional RMS Enterprise Documentation

Refer to the following supplemental RMS Enterprise documents (available to view/download from www.amx.com):

- **RMS Enterprise Installation Guide** - Provides installation instructions for RMS Enterprise. This document includes the RMS Installation Checklist to ensure all the necessary prerequisites are met and all the necessary configuration options are identified prior to the installation of the RMS server. It also provides information on installing and configuring prerequisite software as well as adding the Scheduling Interface and Scheduling Plug-In, and adding the RMS Transporter application.
- **RMS Enterprise NetLinx Programmers Guide** - Provides detailed NetLinx programming information for RMS systems.
- **RMS Update Manager Installation Guide** - Provides instructions for installing the RMS Transporter installation file (*RMSTransporter.exe*), in order to add RMS Update Manager functionality to RMS Enterprise. See the *Update Manager Configuration (Classic UI)* on page 265 for details.
- **RMS Scheduling Interface Installation Guides** - Provide instructions for installing and configuring the RMS Enterprise Scheduling Interfaces:

    Installation Guide - RMS Enterprise Interface for Exchange EWS

    Installation Guide - RMS Enterprise Interface for Lotus Notes Domino

    Installation Guide - RMS Enterprise Scheduling Interface for Google Calendar
- **RMS-ENT-QR RMS QRS Quick Response Scheduling Quick Start Guide** - Provides quick-start instructions for adding Mobile Scheduling to your RMS Enterprise system.
- **RMS Enterprise Transporter Installation Guide** - Provides instructions for installing and configuring the RMS Enterprise Transporter Firmware File Transfer Utility for RMS Enterprise.

The RMS Enterprise Work Area (v4.6 or higher)

Overview

While many of the concepts utilized by RMS Enterprise v4.6 (or higher) are similar to previous versions of RMS Enterprise, the UI has been updated substantially. In v4.6 (or higher), some functionality is contained in the new RMS Enterprise *HTML* interface (see *RMS HTML UI Features* below), while many of the core admin functions are contained in the "Classic UI" view (see the *RMS Classic UI Features* section on page 24).

This section describes both the HTML and the "Classic UI" interfaces, both of which are typically used by RMS system administrators.

HTML Interface

Classic UI Interface
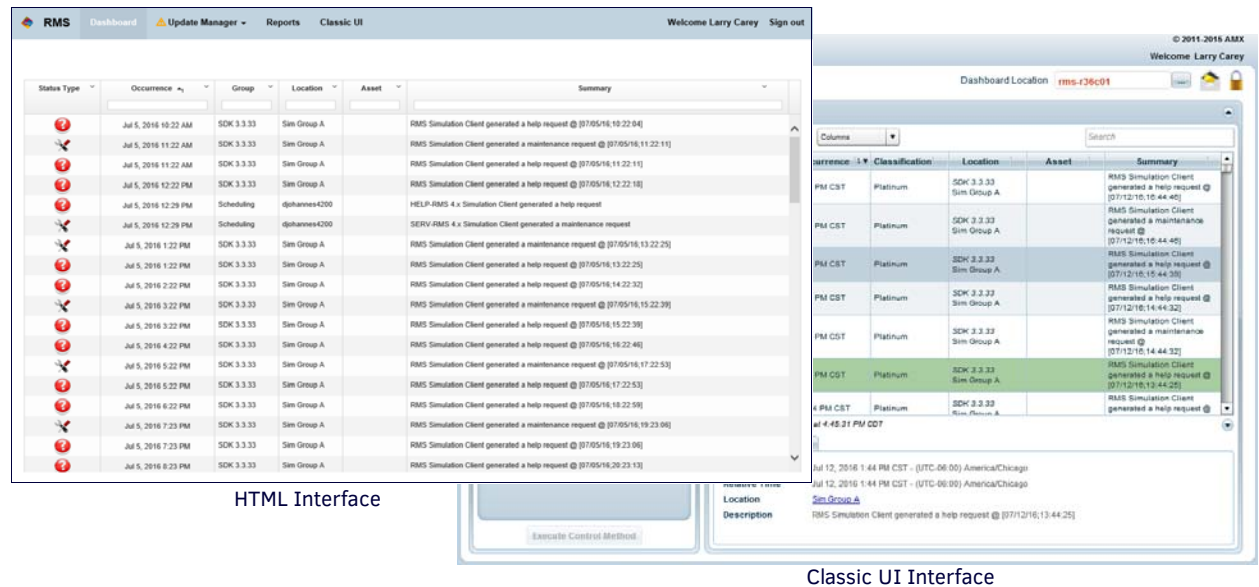
FIG. 3 Example RMS Enterprise HTML and Classic UI Interface

RMS Enterprise HTML UI

With RMS Enterprise v4.6 (or higher), users log into RMS via the HTML interface (FIG. 4). Once logged in, the HTML interface presents a simplified version of the RMS Hotlist, and provides options for using the Update Manager as well as options for generating Reports.

Click to sign out of RMS
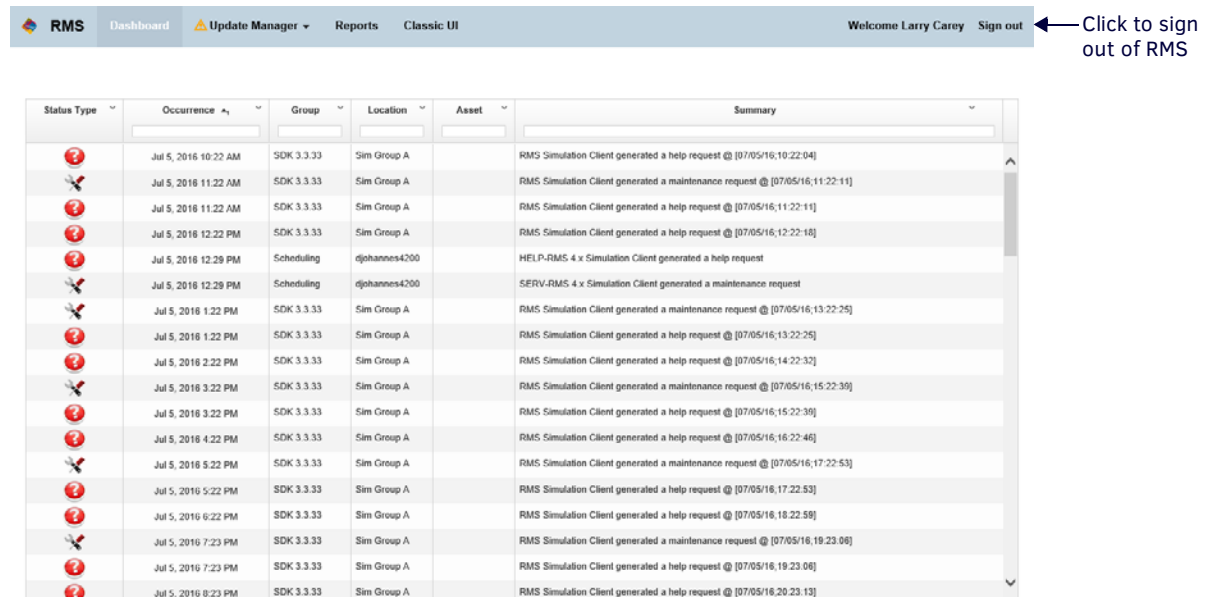
FIG. 4 Example RMS Enterprise HTML Interface (Dashboard view)

NOTE: *The HTML Interface provides the option to open the RMS Enterprise "Classic UI", which is similar to previous versions of RMS Enterprise (see below).*

RMS HTML UI Features

Use the new HTML UI to access the following functionality:

- Log in/out of RMS Enterprise (see *Sign In Page* on page 21)
- The simplified HTML Dashboard view (see *Dashboard* on page 22)
- Update Manager (see *Update Manager Menu* on page 22)
- Report Management (see *Reports Page* on page 23)

RMS HTML UI - Menu Bar

The four tabs along the top of the HTML UI Window (*Dashboard*, *Update Manager*, *Reports* and *Classic UI*) provide access to the functions contained in the HTML UI (FIG. 5).

FIG. 5 RMS HTML UI - Menu Bar

The menu bar in the HTML interface provides the following options:

RMS Enterprise HTML Menu Bar Options	
Dashboard	Click to open the Dashboard view. This is also the initial view of RMS Enterprise when a user logs in via the *Please Sign In* page (see *Accessing the RMS Enterprise UI* on page 18). In v4.6, the HTML Dashboard view consists of a simplified Hotlist - it is read-only and is intended to provide a quick indication of current system status. To manage Locations, Assets, Users and Notifications, use the "Classic UI" option (see below).
Update Manager	The *Update Manager* functionality in RMS Enterprise provides the ability to check for updated firmware files for AMX devices in the RMS System. RMS checks the device database to establish a listing of the devices in the system, and checks the online AMX InConcert Resource Center for firmware files that apply to those devices. When newer firmware is found, Update Manager downloads the firmware and provides the option of transferring the updated firmware files to the appropriate devices. The options in the **Update Manager** menu allow you to check for updates, use the File Manager utility, and view Transfer History. Refer to the *Update Manager (HTML UI)* section on page 28 for details.
Reports	RMS Enterprise provides a comprehensive set of reports that allow users to extrapolate various kinds of meaningful information from the RMS database. The options in the Reports page allow you to configure and run various system reports. Refer to the *Reports (HTML UI)* section on page 45 for details.
Classic UI	Click to switch to the RMS Enterprise Classic UI - this UI contains many of the core RMS admin functions including managing Locations, Assets, Users and Notifications. Refer to the *RMS Enterprise "Classic UI"* section on page 24 for details.

Sign In Page

The *Sign In* page represents the user authentication form and the associated error handling for invalid user credentials, disabled user accounts, and other login associated failures. Additionally, the *Sign In* window enforces user password expiry rules and user failed login attempt rules. More details on user authentication configuration options can be found in the *Management - Users (Classic UI)* section on page 177.

- If the *Enable Guest Account (Anonymous Access)* option is enabled (via the *Security Policy* page), the *Sign In As Guest* option is included in the Sign In window (FIG. 6):
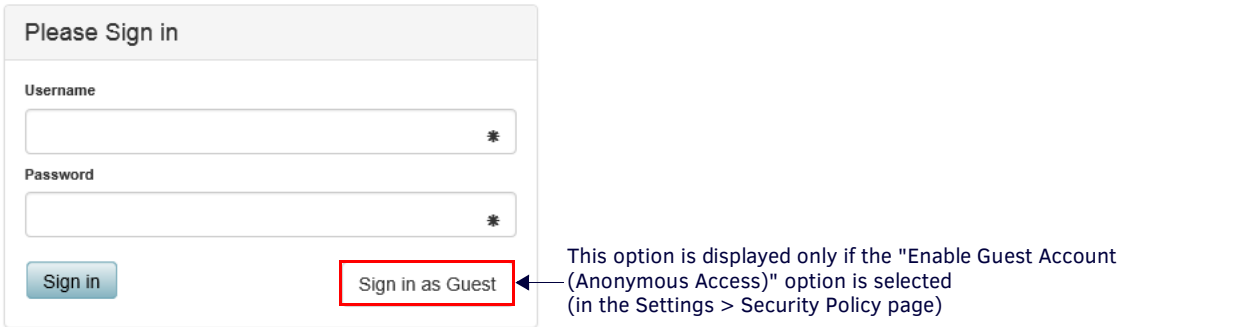
FIG. 6 User Sign-In Form

This option does not require entry of a Username Password to sign in. See the *Security Policy* section on page 212 for details.

NOTE: *The Guest account is only available for installed RMS Servers; it cannot be enabled for AMX Cloud hosted services.*

- The *Sign In* window will not be displayed if the user is authenticated via an external Single-Sign-On implementation such as Windows Integrated Authentication or SiteMinder. See *Appendix A: Using Directory Services* on page 277 for details.

The initial view in the RMS HTML UI is the *Dashboard*. In the HTML UI, the Dashboard represents a simplified read-only version of the Hotlist (see *Dashboard* on page 22).

Dashboard

Select **Dashboard** to access the Dashboard page view (FIG. 7): .

FIG. 7 HTML UI - example Dashboard page

NOTE: *The HTML Dashboard page presents the current RMS Hotlist as read-only information.*

Filtering the Dashboard List

Use the text fields provided in the *Occurrence*, *Group*, *Location*, *Asset* and *Summary* columns to filter the results listed in the HTML UI Dashboard. As characters are typed into any of these fields, the list is filtered to only show results that include the entered characters. For example, to list only Hotlist items that include the term "Projector" as an asset, enter "*Projector*" into the text field at the top of the Asset column (FIG. 8): .

"Asset" column filter set to "Projector"

"Asset" column only shows results that include the term "Projector"

FIG. 8 HTML UI - example Dashboard page filtered to show only "Projector" Assets

NOTE: *Click the "x" icon in the text field to clear the field and remove the filter.*

Update Manager Menu

Click **Update Manager** to access the Update Manager menu (FIG. 9): .

FIG. 9 HTML UI - Update Manager Menu

The *Update Manager* options allow RMS to check for device firmware updates, and upload firmware files to devices on your system's network. Update Manager is described in the *Update Manager (HTML UI)* section on page 28.

Reports Page

RMS Enterprise provides a comprehensive set of reports that allow users to extrapolate various kinds of meaningful information from the RMS database. The options in the (HTML UI) **Reports** page allow you to configure and run various system reports (FIG. 10):

FIG. 10 Reports Page

The options in the *Reports* page are described in the *Reports (HTML UI)* section on page 45.

Classic UI

In the HTML interface, click on Classic UI to open the RMS Enterprise Classic UI in a separate window. The Classic UI layout is similar to previous versions of RMS Enterprise. Note that several menus have been updated and some functions (including Update Manager and Reporting) are now accessed via the HTML interface. Many of the core admin functions are contained in the "Classic UI" view (see the *RMS Enterprise "Classic UI"* section on page 24).

Sign Out

Click the **Sign Out** link (upper-right corner of the window) to sign out of the RMS System (FIG. 11):

FIG. 11 Sign Out link

Once you sign out, you will have to provide a valid Username and Password to sign back into the system (see *Accessing the RMS Enterprise UI* on page 18).

RMS Enterprise "Classic UI"

In the RMS HTML interface, select **Classic UI** in the menu bar to open the RMS Enterprise interface shown in FIG. 12: .
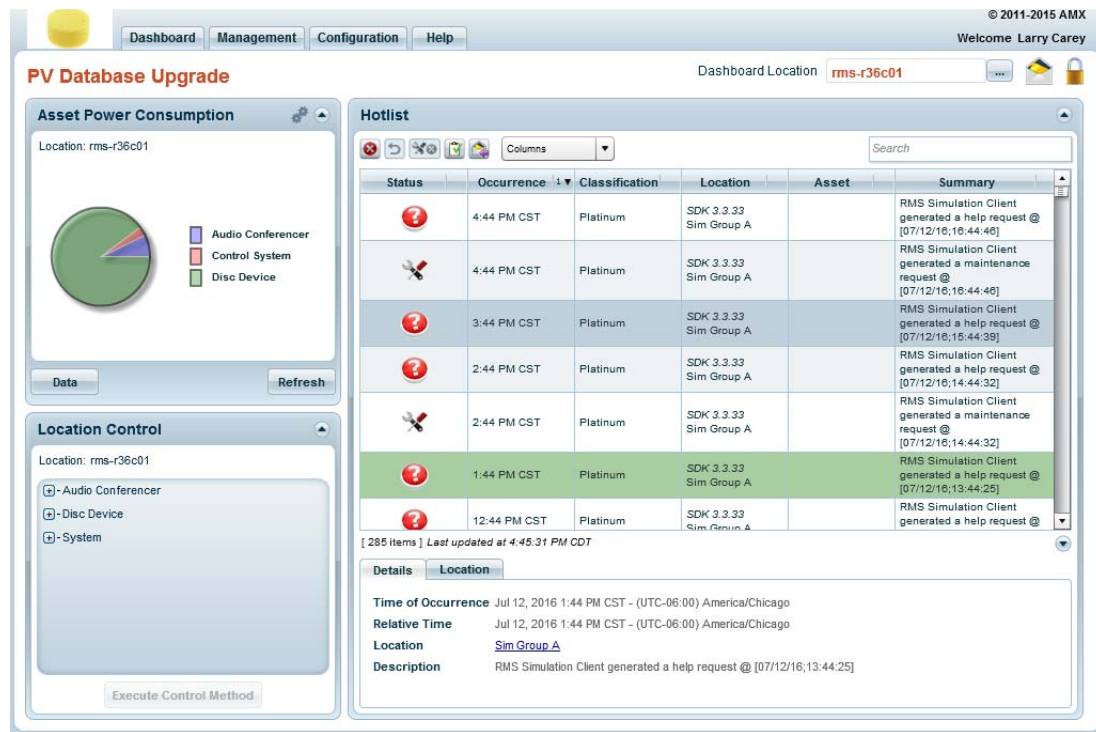
FIG. 12 Example RMS Enterprise Classic Interface (Dashboard view)

NOTE: *In RMS Enterprise v4.6 (or higher), several menu options as well as the Sign Out option are available via the HTML interface. See page 20 for details.*

The initial view in the RMS Classic UI is the *Dashboard*. The Dashboard provides access to many core features and commonly used functions of RMS. The Classic UI Dashboard is customizable via the use of *Widgets*. Widgets provide specific utilities or specialized information views that can be added to or removed from the Dashboard such as Lamp Life, Source Usage, Hotlist, and more. See the *Dashboard Widgets* section on page 59 for details.

RMS Classic UI Features

Use the Classic UI to access the following functionality:

- The "Classic" Dashboard view with Widget support (see page 59).
- The *My Profile* page (see page 84).
- Client Gateways/Locations Management (see page 93, page 103).
- Asset Management (see page 125).
- Control Macros Management (see page 165).
- User Management (see page 177).
- Notifications Management (see page 201).

Title Bar

The options in the Title Bar provide access to all aspects of the application, as described in the following sections (FIG. 13):
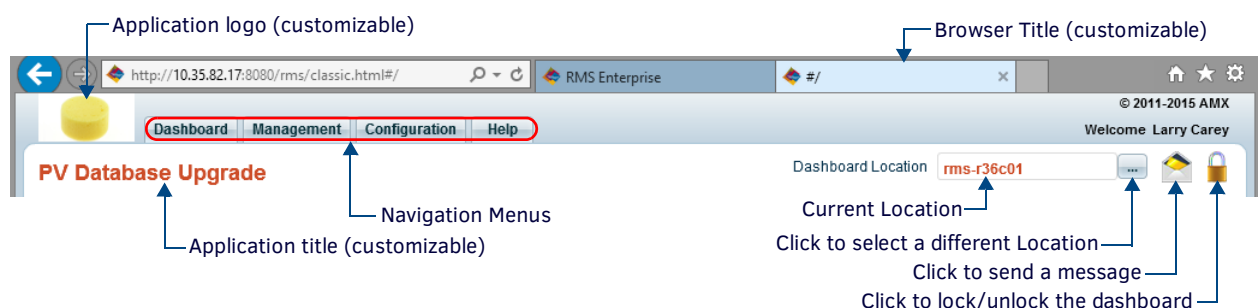
FIG. 13 RMS Work area - Title Bar UI elements

Several items in the Title Bar (Browser Title, Application Title and Logo image) can be customized via options in the *System Configuration > Web Application Settings* page. See the *Web Application Settings* section on page 209 for information.

Navigation Menus

The five tabs along the top of the Main Window (*Dashboard*, *Management*, *Reports, Configuration* and *Help)* provide access to the top-level menus representing the main categories of functionality in RMS (FIG. 14). The main window is populated with options and functions based on this top-level selection.

FIG. 14 Navigation Menus

Dashboard Menu

Click inside the **Dashboard** tab to access the Dashboard menu (FIG. 15): .
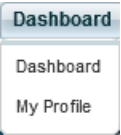
FIG. 15 Dashboard Menu

The options in the Dashboard menu are described in the *Dashboard (Classic UI)* section on page 56:

- **Dashboard** - page 56
- **My Profile** - page 84

NOTE: *In RMS Enterprise v4.6 (or higher), users sign in and out via the HTML interface (see Sign In Page on page 21).*

Management Menu

Click inside the **Management** tab to access the *Management* menu (FIG. 16):
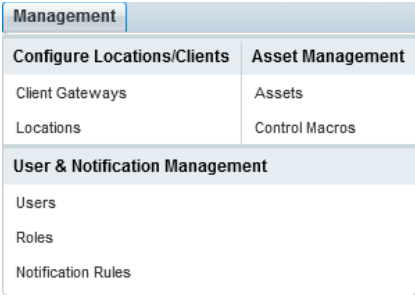
FIG. 16 Management Menu

The options in the Management menu are described in the following sections:

- **Configure Locations/Clients**
  see *Management - Client Gateways (Classic UI)* on page 93
  see *Management - Locations (Classic UI)* on page 103
- **Asset Management**
  see *Management - Assets (Classic UI)* on page 125
  see *Management - Control Macros (Classic UI)* on page 165
- **User & Notification Management**
  see *Management - Users (Classic UI)* on page 177
  see *Management - Roles (Classic UI)* on page 192
  see *Management - Notification Rules (Classic UI)* on page 201

Configuration Menu

Click inside the **Configuration** tab to access the *Configuration* menu (FIG. 17):

FIG. 17 Configuration Menu

The Configuration menu provides access to many system-level settings, including *System Configuration*, *Notification Configuration*, *Location Configuration*, *Asset Configuration* (including RFID Tracking options) and *Update Manager Configuration*.

The options in the Configuration menu are described in the following sections:

- **System Configuration -** page 209
- **Notification Configuration** - page 236
- **Location Configuration** - page 242
- **Asset Configuration** - page 246
- **Update Manager Configuration** - page 265

NOTE: *The Email Server (SMTP) option is not available for AMX cloud hosted services.*

Help Menu

Click inside the **Help** tab to access the *Help* menu (FIG. 18). The Help menu provides access to RMS help documentation, online resources, RMS system information.

FIG. 18 Help Menu

- The options in the Help menu are described in the *Help / Diagnostics (Classic UI)* section on page 270.
- The **Help > Diagnostics** sub-menu provides access to the Diagnostics pages described in the *Diagnostics* section on page 271. Also refer to the *Diagnostics Page - Log Settings Tab* section on page 273.

Navigation Back Button

RMS provides a top level *Back* button that allows users to quickly return to the previous page or view (FIG. 19).

Client Gateway Management　　　　　　　　**Back to Dashboard**

Click to jump to the page indicated in the arrow icon
(previous page based on current workflow)
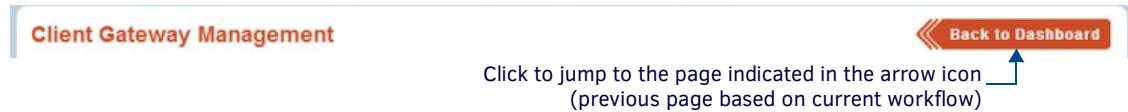
FIG. 19 Back Button

This button provides Back-Linking, based on the current workflow.

NOTE: *RMS Enterprise uses Workflows to manage user navigation throughout the RMS UI. When a user selects a menu item from the main menu, they begin a new workflow, closing out any previous workflows.*

Search Window

Many windows, pages and dialogs in the RMS Classic UI feature a **Search** window, to facilitate searching within a specific context of the RMS application. Search windows allow the user to perform a search that is relative to the area in which the Search option is presented. For example, the Search window provided in the *Groups* window of the *Locations* page allows the user to search for Location Groups or Location Names, as they are listed in the Groups window (FIG. 20).

Enter a string to search for, within the Groups window
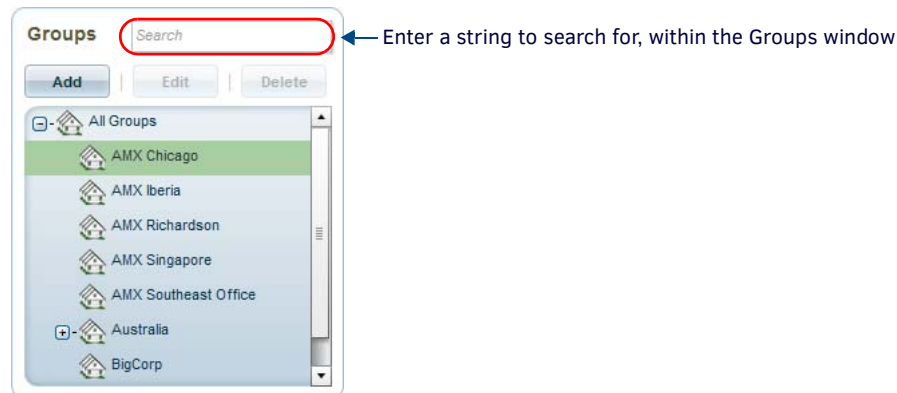
FIG. 20 Search Window - Locations window & Main Page

Likewise, the Search window presented in the *Client Gateway* page (for example) allows the user to search within the Client Gateways table (FIG. 21).

Enter a string to search for, within the Client Gateway table
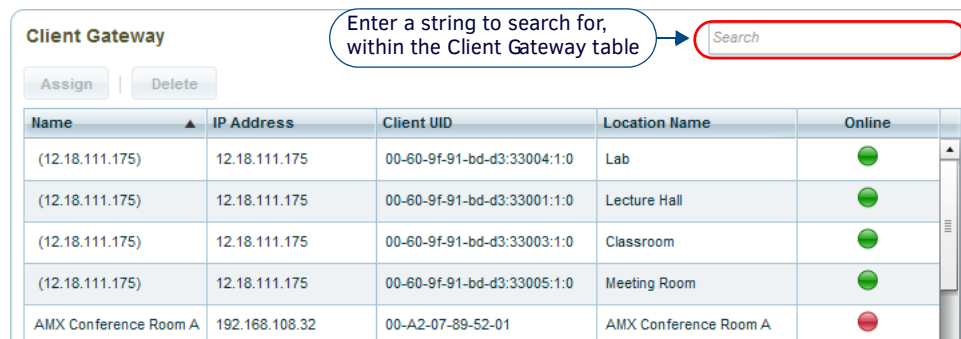
FIG. 21 Search Window - Client Gateway page

- The Search will be performed against data columns with alphanumeric text presented in the window or page.
- RMS supports wildcard (*) searching.

While each Search window performs a search that is limited to the specific area of the application in which it is presented, all searches in RMS work in basically the same way:

1. Enter a text string in the *Search* field
2. Press **Enter**.
3. The data view is filtered to show only the search results.

Clearing the Search Filter

To remove the search results filter, click the "**X**" button inside the *Search* window (FIG. 22).

FIG. 22 Search Window - Clearing the Search filter

Alternatively, manually delete the text (backspace or highlight text and hit the delete button).

Update Manager (HTML UI)

Overview

The *Update Manager* functionality in RMS Enterprise provides the ability to check for updated firmware files for AMX devices in the RMS System. RMS checks the device database to establish a listing of the devices in the system, and checks the online AMX InConcert Resource Center for firmware files that apply to those devices. When newer firmware is found, Update Manager downloads the firmware and provides the option of transferring the updated firmware files to the appropriate devices.

Update Manager is accessed via the RMS HTML interface menu bar (FIG. 23):

FIG. 23 RMS HTML UI - Update Manager menu option

There are two ways to approach using Update Manager:

1. To maintain the latest available firmware on managed devices, start in the **Check for Updates** page. Refer to the *Updating Devices With the Most Recent Firmware from AMX* (below) for details.
2. To reload or downgrade firmware on managed devices, start in the **File Manager** page. Options in this page also provide the ability to upload Firmware (ZIP) files to the RMS Server from a local directory. Refer to the *File Manager (Files) page* section on page 32 for details.

RMS Transporter Utility

The actual transfer of firmware files to devices is handled via the *RMS Transporter* utility (installed separately). *RMS Transporter* allows the simultaneous transfer of firmware to all devices on your system's network for a given firmware file. The RMS File Transporter utility is intended to be installed on a separate server than the RMS Enterprise Server.

RMS Transporter allows viewing of transfers to all devices in real time, so you can see at a glimpse the status of all file transfers, as well as the status of files that were transferred in previous sessions. Detailed log files are available for viewing of historical data for each system or installation, whether it be one small room, or a campus wide system.

RMS Transporter is installed separately from RMS Enterprise, and has it's own versioning (independent of RMS Enterprise). In order to use the Update Manager functionality in RMS, RMS Transporter must be installed and configured according to the instructions in the *RMS Enterprise Transporter Installation Guide*.

NOTE: *The Update Manager menu is present in the RMS Enterprise (v4.6 or higher) HTML UI interface, even if RMS File Transporter has not been installed.*

NOTE: *The installation file for the RMS Transporter utility (RMSTransporter.exe) is available to download from the RMS Enterprise page at www.amx.com. Refer to the RMS Enterprise File Transporter Installation Manual for instructions on installation and configuration.*

Used in conjunction with the RMS Transporter utility, Update Manager ensures that all AMX devices are updated to the latest firmware version with a minimum amount of physical effort.

FIG. 24 illustrates the basic layout of an RMS Enterprise System that uses two RMS Transporter servers to update firmware files on AMX devices in the RMS system:
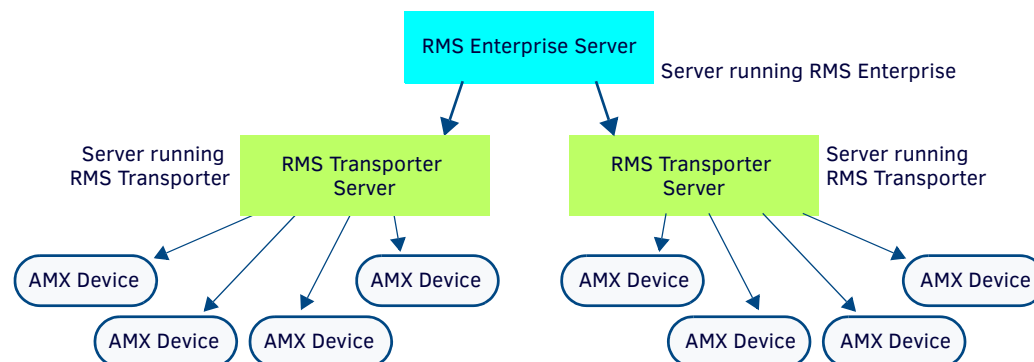
FIG. 24 RMS Transporter - basic system layout

As indicated, multiple RMS Transporter servers can communicate with the RMS Enterprise Server.
- Each RMS Transporter server communicates with the RMS Enterprise Server over Port **80**.
- Each RMS Transporter Server communicates with AMX devices over port **1319**.
- Each RMS Transporter Server communicates with AMX devices via HTTP over port **8081** (default). This port can be changed in the Transporter configuration tool. Refer to the RMS Enterprise File Transporter Installation Manual for instructions on installation and configuration.

Configuring RMS Transporter

RMS Transporter must be configured before the Update Manager function can be used. The options in the *Update Manager Configuration* category of the Configuration menu allow you to view and manage AMX Device Credentials, Transporter Assignments and Transporter Management. Refer to the *Update Manager Configuration (Classic UI)* section on page 265 for details.

KIT Firmware Files

RMS Transporter transfers ***.KIT** AMX device firmware files. KIT files are available to download from www.amx.com, bundled within ZIP files. Traditionally, the ZIP files provided by AMX contain the KIT (firmware) file itself as well as a readme.txt file (describing changes in the new firmware version), and any other support files required by the target device.

Descriptor File

In order for a downloaded AMX firmware file to be transfered via RMS Transporter, the ZIP file must contain an additional *Descriptor (XML) file*. This file is required by RMS Transporter.

If the Descriptor file is not present in the ZIP file, RMS Transporter will indicate the error and the file cannot be transfered (see *Firmware File Requirements for Update Manager* on page 42).

NOTE: *Firmware KIT files released after January 15, 2015 include a Descriptor file and are therefore supported by Transporter.*

Update Manager Work Area

Update Manager Menu

Update Manager options are accessed via the **Update Manager** menu, in the RMS Enterprise HTML interface (FIG. 25):
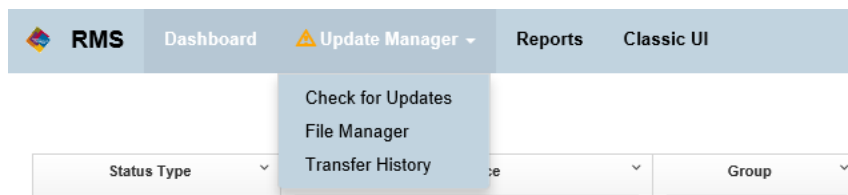
FIG. 25 Update Manager menu options

- Select **Check for Updates** to open the *Firmware Updates - Files* page (see FIG. 26).
- Select **File Manager** to open the *File Manager* page (see FIG. 28 on page 32).
- Select **Transfer History** to open the *Transfer History* page (see FIG. 29 on page 33).

Firmware Updates (Files) page

Select **Update Manager > Check for Updates** to open the **Firmware Updates (Files)** page (FIG. 26). This page displays all firmware updates found for the AMX devices in the RMS System, listed by file:
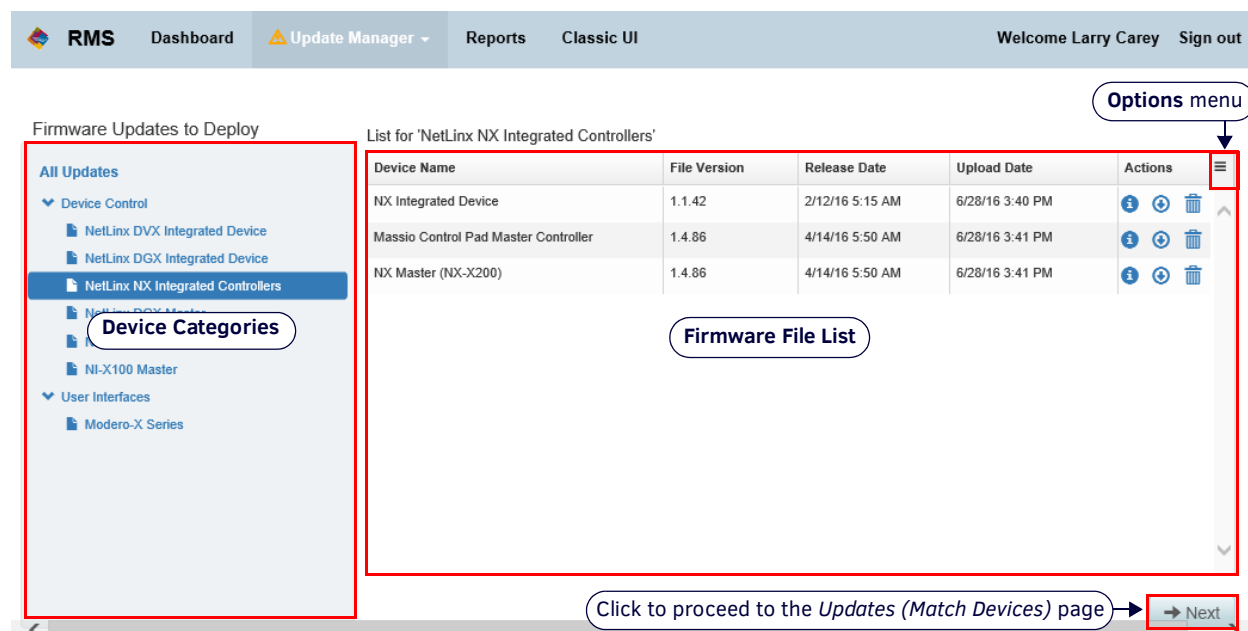
FIG. 26 Firmware Updates (Files) page

Firmware Updates (Files) page options	
Device Categories window	This window provides a listing of firmware updates that are available for the devices detected in the RMS system, categorized by device type. Use this window to filter the Firmware File list by device type as desired. • Click **All Updates** at the top of the list to show all uploaded firmware files in the File List View window, regardless of the device type. • Click on a device category (i.e. Device Control, User Interfaces etc.) to filter the File List View to show only firmware files for the selected device category. • Click on a device subcategory (i.e. NetLinx Integrated Control, etc.) to filter the File List View to show only firmware files for the selected device subcategory.
Firmware File List	This window lists the firmware updates that are ready to deploy (based on the filter selection made in the *Firmware Updates to Deploy* window). This window provides the following (read-only) information for each firmware update in the list: • Device Name: The name of the Device associated with each firmware update. • File Version: The version of each firmware update. • Release Date: The release date of each firmware update. • Upload Date: The date on which each firmware update was uploaded to the RMS Server. • Actions: The icons in this column provide access to file details and options to download a copy of each firmware update in the list as well as to delete any firmware update from the RMS Server. See the *File Actions* section on page 30 for details.
Options menu	Click the menu icon in the upper-right corner of the Firmware File List to open the *Options* menu. This menu contains data export and view options (see *Update Manager Options Menu* on page 34):
Next	Once one or more files have been selected for transfer, click the **Next** button to proceed to the *Devices* page (see page 31).

File Actions

The *Actions* column in the *Firmware Updates (Files)* page (FIG. 26 on page 29) and the *File Manager (Files)* page (FIG. 28 on page 32) contains three icons that provide the following file functions:

File Actions		
	File Info	Click the **File Info** icon to invoke a File Information window that provides basic (read-only) information on the selected file. This information represents the release notes for the selected firmware file. See the *Viewing File Information* section on page 43 for details.
	Download a Copy	Click the **Download a Copy** icon to download a copy of the selected firmware (KIT file only) to the local file system. See the *Copying a Firmware KIT File to a Local Directory* section on page 43 for details.
	Delete	Click the **Delete** icon to delete the selected file from the RMS Enterprise Server. See the *Deleting a Firmware File from the RMS Server* section on page 44 for details.

Firmware Updates (Devices) Page

Click the **Next** button in the **Firmware Updates - Files** page (see FIG. 26 on page 29) to access the **Devices** page (FIG. 27). This page lists potential target system devices for the selected firmware file, based on the device type associated with the firmware file:
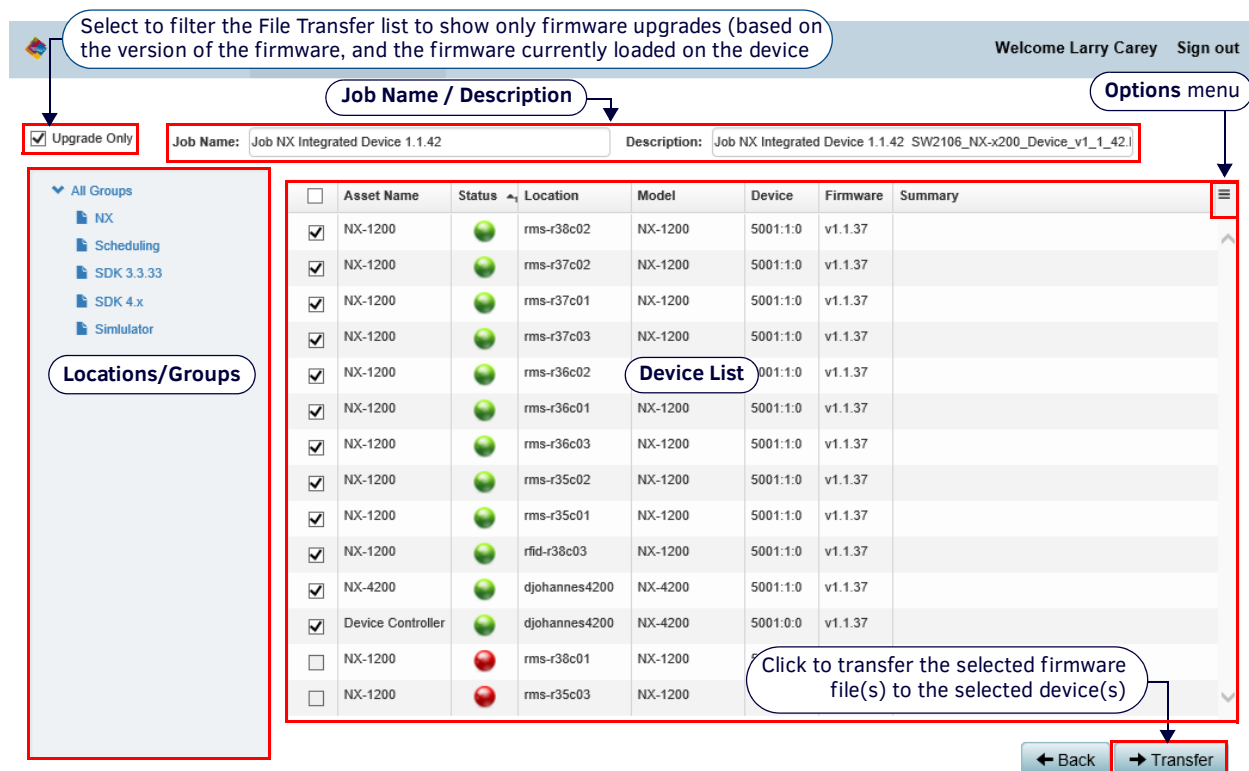
FIG. 27 Firmware Updates (Devices) page

Firmware Updates (Devices) page options	
Upgrade Only	With this option selected, this page only indicates firmware files that are newer than the firmware currently loaded on each listed device (default setting). De-select this option if you intend to reload same version or older firmware.
Job Name	Indicates the current Job name for the selected transfer. Click within this field to edit the Job Name if desired. By default, the Job Name indicates the device type and version number of each firmware file.
Description	Indicates the current Description for the selected transfer. By default, the Description indicates the device type and version number of each firmware file, plus the filename (*.KIT) of the firmware file. Click within this field to edit the Description text if desired.
Locations/Groups window	This window provides a listing of Locations and Location Groups in the RMS system. Use this window to filter the Device list by Location or Location Group as desired. Click **All Groups** to list all available updates.
Device List	This window lists the managed devices that have firmware updates available for deployment (based on the filter selection made in the *Locations/Groups* window). This window provides the following information for each device update in the list: • Device Checkboxes: Each device must be selected to be included in this Job. Use the top checkbox to select/de-select all files, or select each device individually. • Asset Name: Indicates the name of the asset associated with each file. • Status: The upgrade status of each firmware file, based on device type and the current firmware available for that device type. See the *Device Status Icons* section on page 32 for details. • Location: Indicates the target Location for this Job (read-only). • Model: Indicates the target device model for this Job (read-only). • Device: Indicates the target device for this Job (read-only). • Firmware: Indicates the current firmware version on the target device. • Summary: Provides a summary of each file in this Job (read-only).
Options menu	Click the menu icon in the upper-right corner of the Device List to open the *Options* menu. This menu contains data export and view options (see *Update Manager Options Menu* on page 34):
Back	Click to return to the Updates (Files) tab
Transfer	Once one or more devices have been selected for transfer, click the **Transfer** button to initiate the file transfer(s).
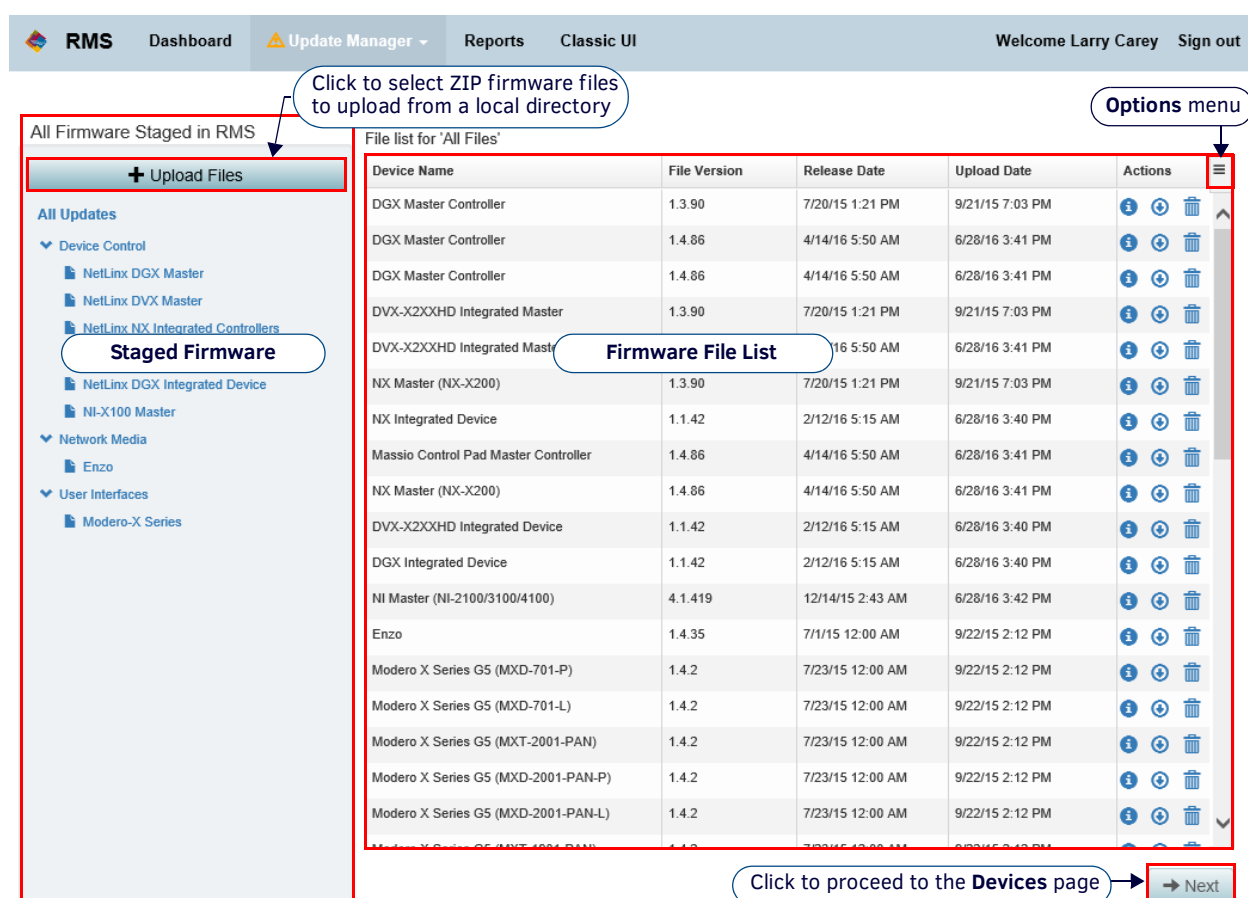
Device Status Icons

The *Status* column in the Device List in the Updates (Match Devices) page uses colored icons to indicate the current status of each device:

Device Status Icons	
🟢	**Green** indicates that the firmware is newer than the current firmware, and represents an upgrade.
🟠	**Orange** indicates that the firmware is the same or older than the current firmware and represents a "reload" or a "downgrade".
🔴	**Red** indicates an error - no file will be transferred. Possible reasons for transfer errors include: • The client (NetLinx Controller) is currently offline • No Transport has been assigned to the Location • The RMS Transporter Server is off-line • The target asset(s) are off-line

File Manager (Files) page

Select **Update Manager > File Manager** to open the *File Manager (Files)* page. The options in this page provide the ability to reload existing firmware, downgrade firmware, and upload firmware files from a local directory to the RMS Enterprise server. This page consists of two windows: the *Staged Firmware* window, and the *Firmware File List* window (FIG. 28):

FIG. 28 File Manager (Files) page

File Manager (Files) page options	
Staged Firmware window	This window contains the *Upload Files* button, and provides a listing of the device types that have had firmware ZIP files uploaded. Use this view to filter the actual firmware files that are listed in the File List window by device type as desired. • Click **All Updates a**t the top of the list to show all uploaded firmware files in the Firmware File List window, regardless of the device type. • Click on a device category to filter the Firmware File List to show only firmware files for the selected device category. • Click on a device subcategory to filter the Firmware File List to show only firmware files for the selected device subcategory.

File Manager (Files) page options (Cont.)	
Firmware File List window	This window lists the firmware files that are ready to deploy. This window provides the following (read-only) information for each firmware update in the list: • Device Name: The name of the Device associated with each firmware update. • File Version: The version of each firmware update. • Release Date: The release date of each firmware update. • Upload Date: The date on which each firmware update was uploaded to the RMS Server. • Actions: The icons in this column provide access to file details and options to download a copy of each firmware update in the list as well as to delete any firmware update from the RMS Server. See the *File Actions* section on page 30 for details.
Options menu	Click the menu icon in the upper-right corner of the Firmware File List to open the *Options* menu. This menu contains data export and view options (see *Update Manager Options Menu* on page 34):
Next	Once one or more files have been selected for transfer, click the **Next** button to proceed to the **Devices** page (see page 31).

Transfer History Page

Select **Update Manager > Transfer History** to open the *Transfer History* page (FIG. 29). This page provides a listing of the 25 most recent file transfer operations (Jobs) initiated via Update Manager, and indicates the status of each.

FIG. 29 Transfer History Page

The columns in the Transfer History table are described below:

Transfer History page options	
Date/Time	Indicates the date and time that each transfer operation was started.
Job	Each Job represents a transfer operation that may include several individual files. Job Names are automatically generated, based on the device category, device type and version number associated with each firmware file transfered. Each Job Name in the History table is a link that opens a *Transfer Details* window that provides details for each transfer operation.
Status	Indicates the current status of each Job: • STARTING: Indicates that the firmware file is currently being transfered from the RMS Server to the RMS Transporter server. As part of this process, RMS checks for potential resource conflicts. If a resource conflict is found, then the status changed to WAITING. • RUNNING: Indicates that the file(s) contained in the current Job are in process of transferring to the target devices. • FINISHED: Indicates that all file transfers contained within the current Job have successfully completed. • FAILED: Indicates that one or more of the file transfers contained within the current Job have failed.
File Transfer %	Indicates the aggregate percentage complete for each Job. *Note: To see the progress of the individual files within the Job, refer to the Active Transfer page.* *FINISHED* transfers are indicated to be 100%. If a transfer has FAILED, this column indicates how far the transfer operation had progressed at the point of failure.

Transfer Page

The *Transfer* page is invoked when a Transfer is selected from the *Updates (Match Devices)* page, or when one of the transfer jobs is selected in the *History* page. This page provides file information and current status for each file transfer (FIG. 30):

FIG. 30 Transfer page

The table in this page indicates the target *Model*, *Location* and *Group* for each file transfer. Further, this table provides *Status* and *File Transfer %* (percent complete) information to indicate the progress of each transfer:

Transfer page	
Model	Indicates the target device model for this Job (read-only).
Location	Indicates the target Location for this Job (read-only).
Group	Indicates the target Location Group for this Job (read-only).
Status	Indicates the current transfer status of each file:
File Transfer %	Indicates the current percentage complete for each file.
Summary	Provides a brief summary of the current Job. For failed transfers, it indicates the reason that a given file transfer has failed, and where in the reboot/wait process the transfer was when the failure occurred.

NOTE: *Once the transfer is complete, the target device(s) are automatically rebooted.*

Update Manager Options Menu

Click the menu icon in the upper-right corner of the Firmware File List (in any of the Update Manager pages) to open the *Options* menu (FIG. 31).
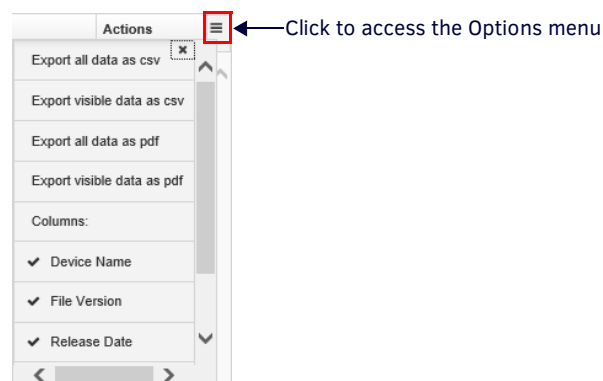
FIG. 31 Update Manager - Options menu

This menu contains the following data export and view options for Update Manager:

Options menu	
Export All Data as CSV	Select this option to export the contents of the current tab as a CSV file.
Export Visible Data as CSV	Select this option to export only the currently visible contents of the current tab as a CSV file.
Export All Data as PDF	Select this option to export the contents of the current tab as a PDF file.
Export Visible Data as PDF	Select this option to export only the currently visible contents of the current tab as a PDF file.
Columns	Select or de-select column names to show or hide specific columns in the current tab. By default, all columns are selected for display in all tabs.

Update Manager Badge

RMS automatically checks the online AMX InConcert Resource Center for device firmware updates, based on the AMX devices currently detected in the RMS system. This check occurs once a day. When device firmware updates are found, the Update Manager Badge (notification icon) is displayed on the *Update Manager* tab (FIG. 32):

Update Manager Badge (indicating that device firmware updates are available to deploy)
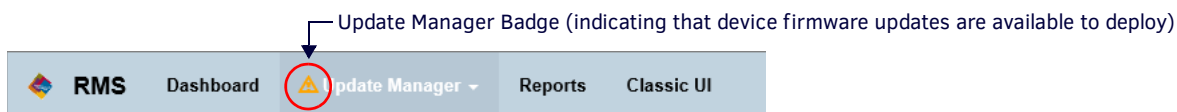
FIG. 32 Update Manager Badge

NOTE: *Update Manager checks the RMS server every 15 minutes for firmware updates that need to be deployed.*

The Update Manager Badge can be enabled/disabled via for each User via the **Show Update Manager Badge** option in the *User Profile* tab of the *User Management* page (FIG. 33):

FIG. 33 Management > User & Notification Management > Users Page (User Profile tab) - Show Update Manager Badge option

Note that while by default all Users will see the Update Manager Badge, only Users with the following permissions are allowed to transfer firmware files to system devices:

- **Global System Permissions**: *Manage Clients and Locations* (Manage)
- **Location Level Permissions for Assets**: *Assets* (View, Manage)

NOTE: *User permissions are managed via Role assignments. Refer to the Management - Roles (Classic UI) section on page 192 for details.*

Updating Devices With the Most Recent Firmware from AMX

1. In the RMS Enterprise HTML interface, check the **Update Manager** menu option. If the *Update Manager Badge* is displayed on this tab, it is an indication that there is updated device firmware available for one or more devices in the system (FIG. 34):

Update Manager Badge (indicating that device firmware updates are available to deploy)
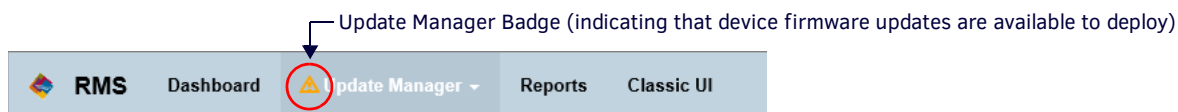
FIG. 34 Update Manager Badge

2. Open the Update Manager menu, and select **Check For Updates** (FIG. 35):
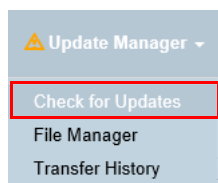
FIG. 35 Update Manager menu - Check For Updates

> **NOTE:** *RMS Enterprise (v4.5.3 or higher) features Auto-Staging functionality. Auto-Staging allows Update Manager to automatically check for updated firmware, and download the new firmware files to the RMS Transporter server (at which point the files are "staged" to be transfered to the appropriate system devices). The Auto-Staging feature is configured via options in the Auto-Staging Settings page - see page 268 for details.*

3. This opens the **Firmware Updates** (**Files)** page, indicating all device firmware files that are available to deploy (FIG. 36):

"*NX Master (NX-2200)*" firmware is selected

With a firmware file selected, click **Next** to proceed to the *Match Devices* page
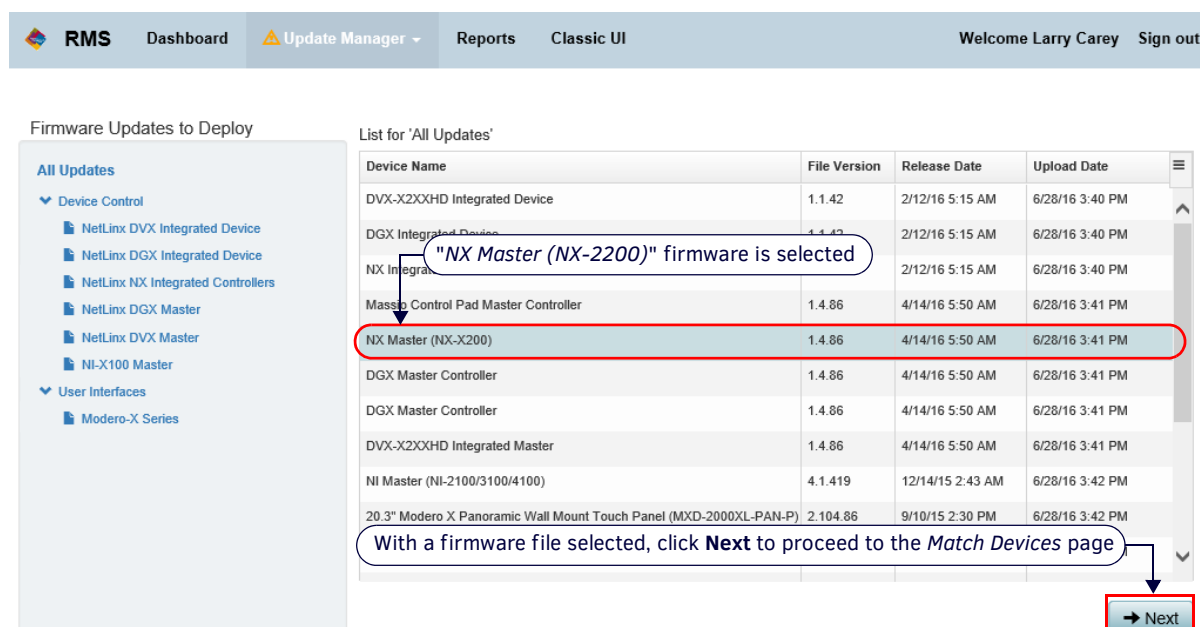
FIG. 36 Firmware Updates (Files) page

- This page lists only firmware files that are more recent than the firmware that is currently loaded on the system devices.
- The files are listed in this page according to *Device Type*. Note that the file list can be filtered by device type via the *Device Categories* window. By default, **All Devices** is selected (to show updates for all device types).
- In some cases, several different AMX devices may use the same firmware file. For example, all G5 touch panels use the same firmware, regardless of the specific model. Likewise, all of the Device Control devices indicated in FIG. 36 use the same Master firmware.

  In these cases, it does not matter which file is selected in the *Updates (Select Files)* tab because they are in fact representing the same firmware. Note that in FIG. 36, the *File Version*, *Release Date* and *Upload Date* are identical for all three devices listed. This is an indication that these devices are using the same firmware file.

4. Select a file to deploy (for example, "NX Master" is selected in FIG. 36), and click **Next** to proceed to the **Devices** page. Use the options in this page to select specific devices as targets for the selected firmware update (FIG. 37):

> **NOTE:** *the "Next" button is only enabled once a firmware file has been selected.*
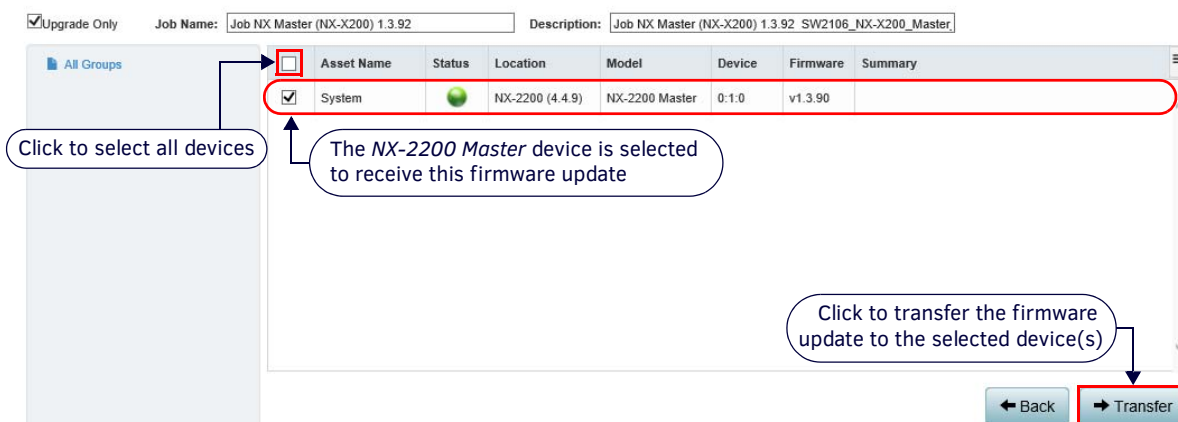
FIG. 37 Firmware Updates (Devices) page

This page lists all system devices that use the selected firmware file. In the example shown in FIG. 37, there is only one device (a NX-2200 Master) that can use the selected firmware file.

5. Select the device(s) that are to receive the selected firmware (select the checkbox next to the *Asset Name* column heading to select all listed devices).

6. Click **Transfer** to transfer the selected firmware update to the selected system device(s).

   NOTE: *The Transfer button is enabled only when at least one device has been selected as the target for the firmware transfer.*

7. The status of the transfer is indicated in the *Transfer*s page (FIG. 38):

FIG. 38 Transfer page

This page indicates the target *Model*, *Location* and *Group* for each file transfer, as well as *Status* and *File Transfer %* (percent complete) information to indicate the progress of each transfer.

NOTE: *Once the transfer is complete, the target device(s) are automatically rebooted.*

Reloading Existing Firmware

To reload the same version of firmware that is currently present on target system device(s):

1. In the RMS Enterprise HTML interface, open the *Update Manager* menu, and select **File Manager** (FIG. 39):
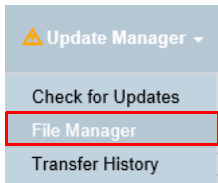
FIG. 39 Update Manager menu - File Manager

2. This opens the **File Manager** (**Files)** page, listing all firmware files that are present on the RMS server (FIG. 40):

FIG. 40 File Manager (Files) page

> **NOTE:** *The files are listed in this tab according to Device Type. Note that the file list can be filtered by device type via the Device Categories window (select All Files to show updates for all device types).*

3. Select a file to deploy (for example, "*NX Master, File Version 1.3.92*" is selected in FIG. 40), and click **Next** to proceed to the **Files** page. Use the options in this tab to select specific devices as targets for the selected firmware.

> **NOTE:** *The "Next" button is only enabled once a firmware file has been selected.*

4. In the **File Manager (Devices)** page, de-select the **Upgrade Only** option in the upper-left corner of this tab to display *all* firmware files, including those that do not represent an upgrade (FIG. 41):

FIG. 41 File Manager (Devices) page

NOTE: *When the Upgrade Only option is selected (the default setting), only firmware files that represent upgrades are displayed in the Files tab. In the case of reloading existing firmware, if a newer version has been downloaded from AMX, then this selection would prevent the display of any firmware versions other than the most recent release.*

NOTE: *Update Manager remembers the Upgrade Only setting. Be sure to check this option when opening the Files (Match Devices) page.*

The File Manager (Devices) page lists all system devices that use the selected firmware file. In the example shown in FIG. 42, there is only one device (a NX-2200 Master) that can use the selected firmware file:
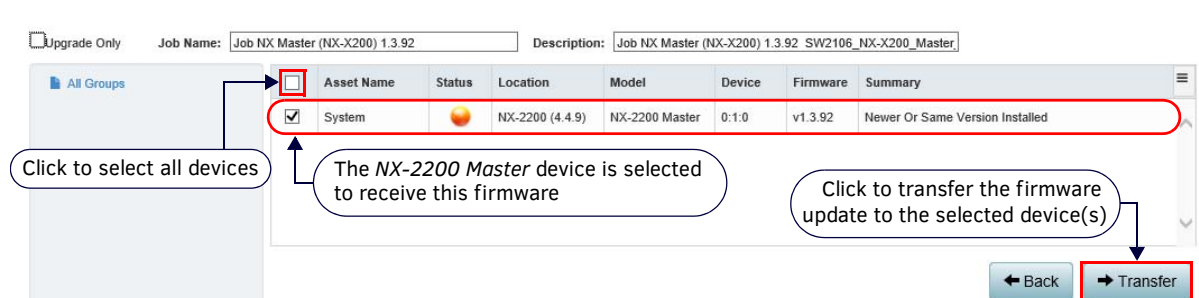
FIG. 42 File Manager (Devices) page

5. In the File Manager (Devices) page, select the device(s) that are to receive the selected firmware (select the checkbox next to the *Asset Name* column heading to select all listed devices).
   - Note that in this case, the orange icon in the *Status* column indicates that the firmware is the same or older than the current firmware and represents a "reload" or a "downgrade" (see *Device Status Icons* on page 32 for details).
   - Note that the *Summary* column indicates "Newer Or Same Version Installed" (in this case, the selected firmware is the same version as the firmware currently loaded on the selected target device).

6. Click **Transfer** to transfer the selected firmware file to the selected system device(s).

   NOTE: *The Transfer button is enabled only when at least one device has been selected as the target for the firmware transfer.*

7. The status of the transfer is indicated in the **Updates** (*File Transfer*) page (FIG. 43):

FIG. 43 Update Manager - Updates (File Transfer) tab

This page indicates the target Model, Location and Group for each file transfer. Further, this table provides *Status* and *File Transfer* % (percent complete) information to indicate the progress of each transfer:

Updates (File Transfer) tab - Active Transfer Table Columns	
Model	Indicates the target device model for this Job (read-only).
Location	Indicates the target Location for this Job (read-only).
Group	Indicates the target Location Group for this Job (read-only).
Status	Indicates the current transfer status of each file:
File Transfer %	Indicates the current percentage complete for each file.
Summary	Indicates the reason that a given file transfer has failed, and where in the reboot/wait process the transfer was when the failure occurred.

NOTE: *Once the transfer is complete, the target device(s) are automatically rebooted.*

Downgrading Firmware

The process of downgrading firmware (loading an older version) is essentially the same as for reloading existing firmware (see the *Reloading Existing Firmware* section on page 38). To downgrade the firmware on target system device(s):

1. In RMS Enterprise (HTML interface), select **Update Manager > File Manager**.

2. This opens the *File Manager (Files)* page, listing all device firmware files that are present on the RMS server.

   NOTE: *The files are listed in this page according to Device Type. Note that the file list can be filtered by device type via the Device Categories window (select All Files to show updates for all device types).*

3. Select a firmware file with the desired release version to deploy , and click **Next** to proceed to the *Firmware Manager (Devices)* page. Use the options in this page to select specific devices as targets for the selected firmware.

   NOTE: *The "Next" button is only enabled once a firmware file has been selected.*

4. In the **Files** (*Match Device*) page, de-select the **Upgrade Only** option in the upper-left corner to display *all* firmware files, including those that do not represent an upgrade.

   NOTE: *When the Upgrade Only option is selected (the default setting), only firmware files that represent upgrades are displayed in the Files tab. In the case of reloading existing firmware, if a newer version has been downloaded from AMX, then this selection would prevent the display of any firmware versions other than the most recent release.*

   NOTE: *Update Manager remembers the Upgrade Only setting. Be sure to check this option when opening the Files (Match Devices) tab.*

   The File Manager (Devices) page lists all system devices that use the selected firmware file.

5. In the File Manager (Devices) page, select the device(s) that are to receive the selected firmware (select the checkbox next to the *Asset Name* column heading to select all listed devices).

   - Note that when downgrading firmware, the orange icon in the *Status* column indicates that the firmware is the same or older than the current firmware and represents a "reload" or a "downgrade" (see *Device Status Icons* on page 32 for details).
   - Note that the *Summary* column indicates "Newer Or Same Version Installed" (in this case, the selected firmware is older than the firmware currently loaded on the selected target device).

6. Click **Transfer** to transfer the selected firmware file to the selected system device(s).

   NOTE: *The Transfer button is enabled only when at least one device has been selected as the target for the firmware transfer.*

7. The status of the transfer is indicated in the *File Transfer* page.

This page indicates the target Model, Location and Group for each file transfer. Further, this table provides *Status* and *File Transfer %* (percent complete) information to indicate the progress of each transfer.

NOTE: *Once the transfer is complete, the target device(s) are automatically rebooted.*

Uploading Firmware From a Local Directory

To upload firmware files from a local directory to the RMS Server, so that it can be transfered via Update Manager:

1. In RMS Enterprise (HTML interface), select on the **Update Manager** > **File Manager** (FIG. 44):
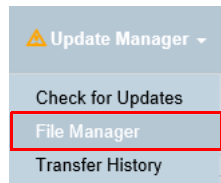
FIG. 44 Update Manager menu - File Manager

2. This opens the *File Manager (Files)* page (FIG. 45):

FIG. 45 Update Manager - File Manager (Files) page

3. Click **Upload Files** to locate and select a firmware (ZIP) file to upload, via the *Choose File to Upload* dialog (FIG. 46):
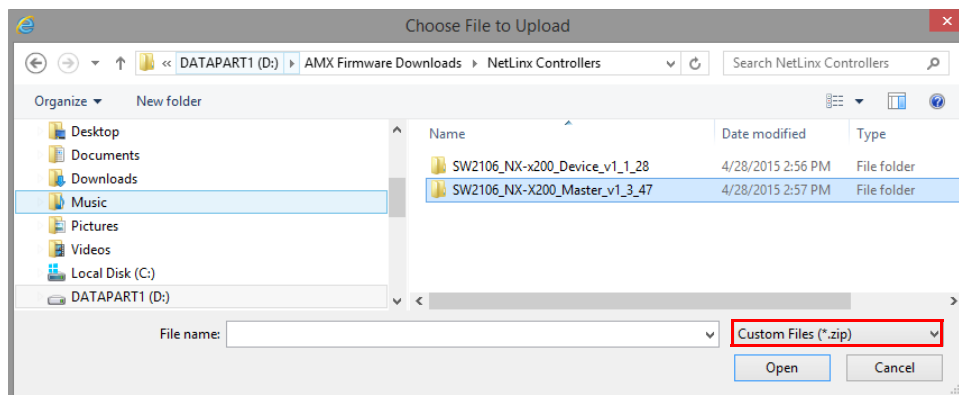
FIG. 46 Choose Files to Upload dialog

> **NOTE:** *Verify that the file types option is set to "Custom Files (*.zip)".*

4. Click **Open** to close this dialog and begin uploading the selected firmware (ZIP) file.

5. The upload transfer status is indicated in a status window similar to the one shown in FIG. 47:
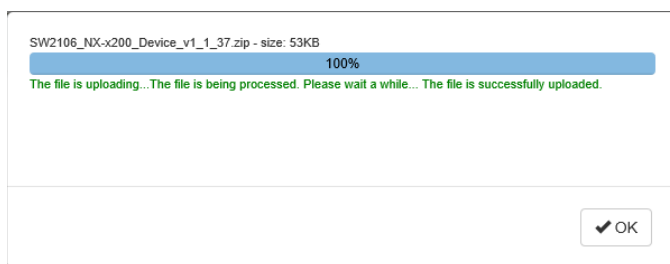
FIG. 47 Upload file transfer status window

6. Repeat this process to add as many firmware files as desired to the File list.
   - As files are uploaded, the *Uploaded Files by Device Type* window is updated to indicate the device category and subcategory to which each file belongs.
   - The actual firmware files contained in the uploaded ZIP file are added to the *File List View* window.

Firmware File Requirements for Update Manager

The selected Firmware ZIP file must contain the following in order to be used with Update Manager:
   - The **.KIT** file
   - a **Readme.txt** file
   - a **Descriptor.xml** file

If any of these are missing, the user will get an upload failure message indicating what is missing (FIG. 48):

Only Firmware ZIP files that include a "Descriptor" file can be deployed via RMS Transporter
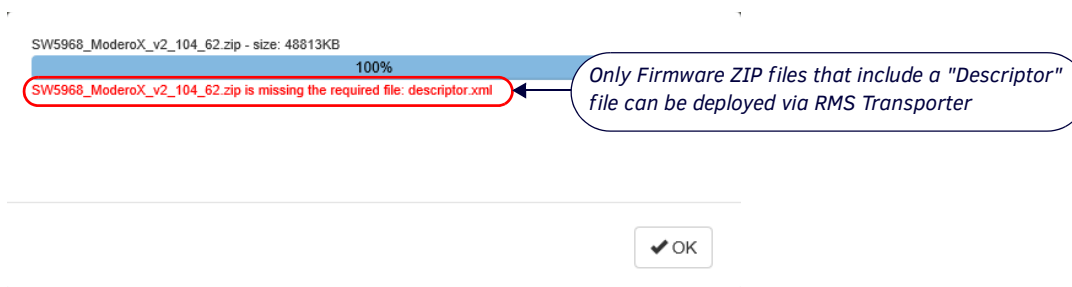
FIG. 48 Update Manager - Transfer Status window (Missing Descriptor File)

In this case, click **OK** to close the error dialog. The file will not be added to the Files list.

Viewing File Information

1. In the *File Manager (Files) page*, click on the **File Info** icon for any file in the list to view the file revision history associated with the selected firmware version (FIG. 49). .

Device Name	File Version ▲	Release Date	Upload Date	Actions
NX Integrated Device	1.1.42	2/12/16 5:15 AM	6/28/16 3:40 PM	ⓘ ⊕ 🗑
DVX-X2XXHD Integrated Device	1.1.42	2/12/16 5:15 AM	6/28/16 3:40 PM	ⓘ ⊕ 🗑
DGX Integrated Device	1.1.42	2/12/16 5:15 AM	6/28/16 3:40 PM	ⓘ ⊕ 🗑
DGX Master Controller	1.3.90	7/20/15 1:21 PM	9/21/15 7:03 PM	ⓘ ⊕ 🗑

FIG. 49 Update Manager - File Manager (Files) page - File Info

2. This opens the *File Information* window for the selected file (FIG. 50): .

> ***DVX-X2XXHD Integrated Master (202792 KB, 6/28/2016 3:41:06 PM)***
> *Product Name: NX-1200, NX-2200, NX-3200, NX-4200 Master Controllers*
> *Enova DVX-x2xx*
> *Enova DGX 8/16/32/64*
> *Massio Control Pads MCP-10x*
> *Enova DGX 800/1600/3200/6400*
>
> *FG #: FG2106-01, FG2106-02, FG2106-03, FG2106-04*
> *FG1906-07, FG1906-09, FG1906-11,*
> *FG1906-12, FG1906-13, FG1906-14, FG1906-15,*
> *FG1906-16, FG1906-17, FG1906-18, FG1906-22,*
> *FG1906-22*
> *FG1060-08, FG1060-16, FG1060-32, FG1060-64,*
> *FG2102-06L-B, FG2102-06L-W, FG2102-06P-B,*
> *FG2102-06P-W, FG2102-08-B, FG2102-08-W*
> *FG1061-08, FG1061-16, FG1061-32, FG1061-64*
>
> *Current Firmware Version: 1.4.86*
> *Release Date: 4/14/16*
>
> OK

FIG. 50 Update Manager - example File Info window

- Use the scroll bar to view the entire file.
- Click **OK** to close this window

Copying a Firmware KIT File to a Local Directory

To download a copy of a Firmware File from the RMS Server to a local directory:

1. Select **File Manager** from the Update Manager menu to open the *File Manager (Files)* page (see FIG. 40 on page 38).
2. Select a Firmware File in the *Firmware File List* window.
3. Click the **Download a Copy** icon in the *Actions* column (FIG. 53).

Device Name	File Version ▲	Release Date	Upload Date	Actions
NX Integrated Device	1.1.42	2/12/16 5:15 AM	6/28/16 3:40 PM	ⓘ ⊕ 🗑
DVX-X2XXHD Integrated Device	1.1.42	2/12/16 5:15 AM	6/28/16 3:40 PM	ⓘ ⊕ 🗑
DGX Integrated Device	1.1.42	2/12/16 5:15 AM	6/28/16 3:40 PM	ⓘ ⊕ 🗑
DGX Master Controller	1.3.90	7/20/15 1:21 PM	9/21/15 7:03 PM	ⓘ ⊕ 🗑

FIG. 51 Update Manager - File Manager (Files) page - Download a Copy

4. The browser will prompt you to Open or Save the file (FIG. 52):

> Do you want to open or save **SW2106_NX-X200_Master_v1_4_86.kit** from **10.35.82.17**?   Open   Save ▼   Cancel   ✕
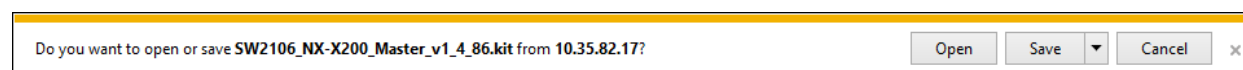
FIG. 52 Downloading a Copy of a selected Firmware File

5. Click **Save**.

NOTE: *See File Actions section on page 30 for details.*

Deleting a Firmware File from the RMS Server

To delete a firmware file from the RMS Enterprise Server

1. Select **File Manager** from the Update Manager menu to open the *File Manager* page (see FIG. 40 on page 38).
2. Select a Firmware File in the *Report Selection* window.
3. Click the **Delete** icon in the *Actions* column (FIG. 53).

Device Name	File Version ⌄	Release Date	Upload Date	Actions
NX Integrated Device	1.1.42	2/12/16 5:15 AM	6/28/16 3:40 PM	ⓘ ⊕ 🗑
DVX-X2XXHD Integrated Device	1.1.42	2/12/16 5:15 AM	6/28/16 3:40 PM	ⓘ ⊕ 🗑
DGX Integrated Device	1.1.42	2/12/16 5:15 AM	6/28/16 3:40 PM	ⓘ ⊕ 🗑
DGX Master Controller	1.3.90	7/20/15 1:21 PM	9/21/15 7:03 PM	ⓘ ⊕ 🗑

FIG. 53 Update Manager - Files (Select Files) page

4. The system will prompt you to verify this action (FIG. 54):

Warning

Are you sure you want to delete the selected file from RMS Server?

Yes   No

FIG. 54 Warning - Deleting a Firmware File

5. Click **Yes** to delete.

The selected firmware file is deleted from the RMS Enterprise Server.

NOTE: *See File Actions* section on page 30 for details.

Reports (HTML UI)

Overview

RMS Enterprise provides a comprehensive set of reports that allow users to extrapolate various kinds of meaningful information from the RMS database. The options in the (HTML UI) **Reports** page allow you to configure and run various system reports, as described in the following section.

To open the *Reports* page, select **Reports** in the RMS HTML interface menu bar (FIG. 55):

FIG. 55 RMS HTML UI - Reports menu option

NOTE: *The authenticated user must have the specific permissions to see the various report options in the Report Manager menu, as indicated in the Report Types table on page 47. See the Management - Roles (Classic UI) section on page 192 for additional details on creating User Roles.*

Report Security

RMS Enterprise provides secure user access to Reports, reporting data, and the report viewer. An authenticated user in the RMS web application must have VIEW reporting access defined in one or more permission Roles to access the Reporting Management UI. If a user does not possess any reporting *View* permissions then access to reporting will be restricted and no reporting option will be displayed in the users navigation menu.

- Each report in RMS may define supplemental permission requirements to access that report. For example, a *Source Usage* report may also require asset VIEW or MANAGE permissions to access the *Source Usage* report. If the authenticated user does not have asset VIEW or MANAGE permissions, the *Source Usage* report will not be displayed in the RMS UI.
- Location based reports also impose security on the data provided in the report to limit the report output data to only those Locations where the user has reporting permissions. For example, if a user has reporting permissions to Location A but not Location B, then the *Source Usage* report will only provide data on Location A and not any for Location B.
- As part of the RMS web application, the RMS Report viewer enforces user authenticated access to the RMS application before being able to access and view Reports.

Reports Page

All System Reports are configured and managed via options in the **Reports** page in the RMS HTML interface (FIG. 56):
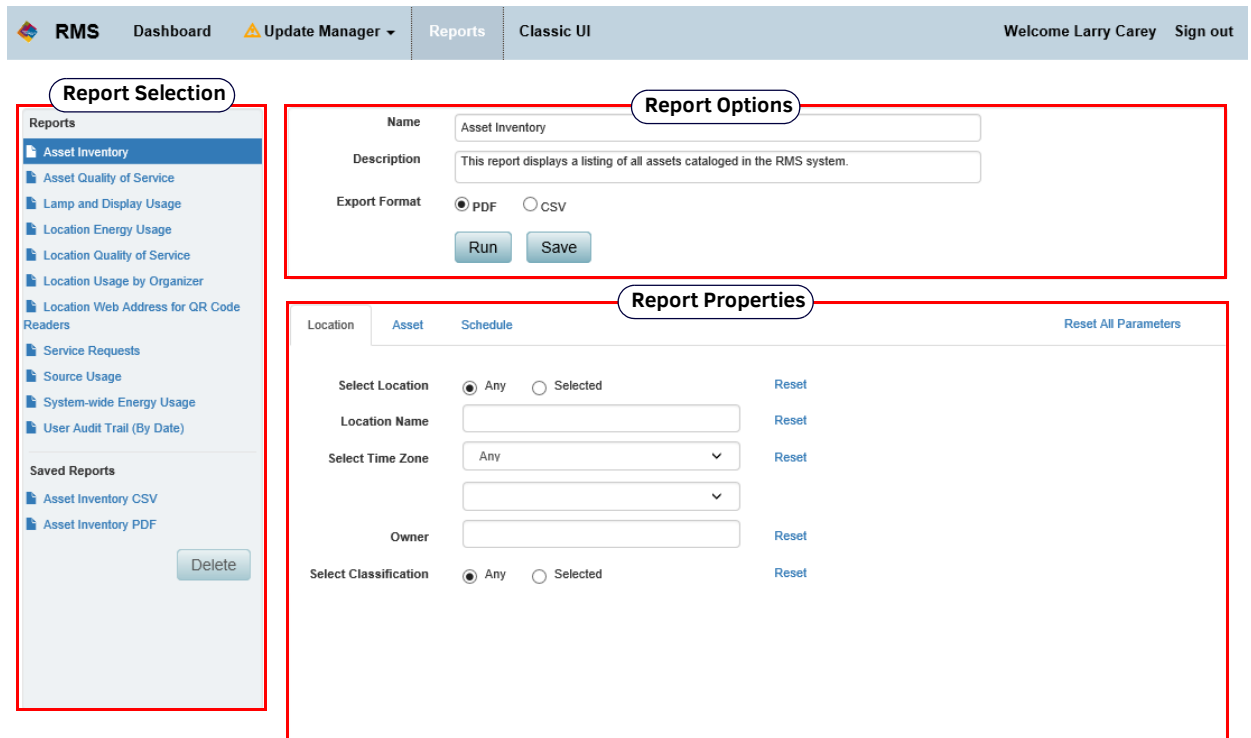
FIG. 56 HTML UI - Reports page

Report Selection Window

System Reports and user-defined Saved Reports are listed in the **Report Selection** window. Click to select a Report to run or to customize and save as a user-defined report (FIG. 57).

Selected Report (highlighted)

System Reports

Saved (user-defined) Reports
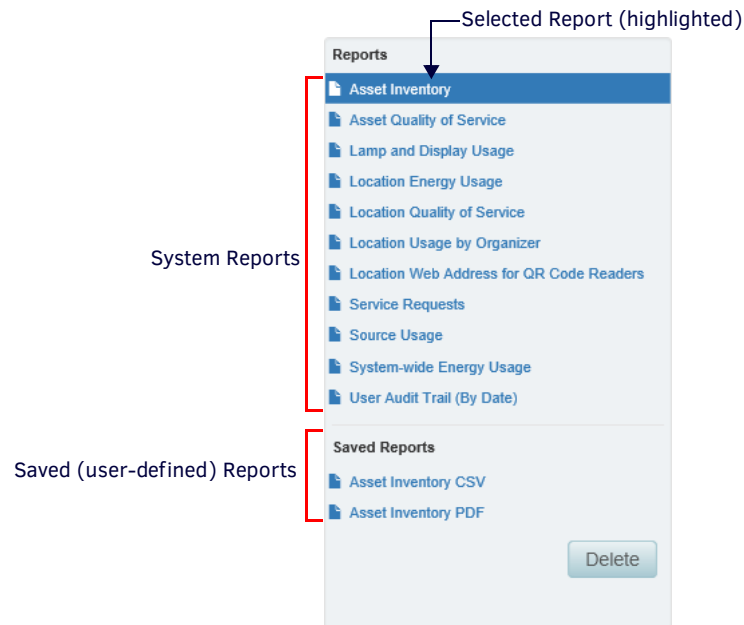
FIG. 57 Reports Page - Report Selection Window

- **Reports** - The *Reports* list indicates a set pre-configured system reports .These reports cannot be deleted. However, any system report can be edited, and saved as a "Saved Report"
- **Saved Reports** - When a system report is edited and saved, it is listed under *Saved Reports*. These reports can be edited and deleted as desired.

Report Options Window

When a Report is selected in the Report Selection window, the *Report Options* window is populated with the Report's *Name* and *Description* (FIG. 58):

FIG. 58 Reports Page - Report Options Window

Note that *Name* and *Description* are editable fields.

- The **Export Format** options are *PDF* (default selection) and *CSV*.
- Click **Run** to generate the selected export, in the selected file format.
- Click **Save** to save the selected report as a user-defined *Saved Report*. Note that user-defined reports are listed under *Saved Reports* in the Report Selection window.

Report Properties Window

The *Report Properties* window of the Reporting Menu page provides information and various report options specific to the selected System Report (FIG. 59):

FIG. 59 Report Properties Window (example General tab)

- The information and options presented in the *Report Properties* window is divided into tabs. Each tab represents a set of related filtering criteria that help refine the output of the report.
- The specific tabs (and the information and options they contain) are presented according to the type of Report selected.

System Reports

Each of the System Reports available for selection are described below:

NOTE: *Users must have certain permissions to access the various System Report types, as indicated in the table below. Only users with the permissions listed below will have access to the various report types. User Permissions are configured in the Role Management page. See the Management - Roles (Classic UI) section on page 192 for details on Roles and User Permissions*

Report Types		
Report Type	**Description**	**Required User Permissions**
Asset Inventory	Provides a listing of all Assets cataloged.	View Assets, Manage Assets
Asset Quality of Service	Provides uptime and quality of service data for each Asset.	View Assets, Manage Assets
Lamp and Display Usage	Provides usage data for each Lamp and Display Asset.	View Assets, Manage Assets
Location Energy Usage	Provides information on energy consumed for each Location.	Manage Clients and Locations
Location Quality of Service	Provides uptime and quality of service data for each control system, sorted by Location.	View Assets, Manage Assets
Location Usage by Organizer	Provides information on Location usage by each event organizer.	Manage Clients and Locations
Location Web Address for QR Code Readers	Provides a listing of schedulable locations and their URLs, using the required resolvable base address for RMS (for use with Mobile Scheduling via *QRS Quick Response Scheduling Door Signs*). See the *Mobile Scheduling* section on page 214 for details.	View Assets, Manage Assets
Service Requests	Provides a listing of records for each service request stored in the RMS system, organized by Location Group and Location.	View Assets, Manage Assets
Source Usage	Provides a listing of the current source usage for each source based Asset.	View Assets, Manage Assets
System-wide Energy Usage	Provides a summarized view of the energy consumed across all the locations and assets.	Manage Clients and Locations
User Audit Trail (By Date)	Provides a detailed listing of user audited activity, sorted by date.	Manage Users

Quality of Service Reports

Quality of Service (QoS) is determined by the number of times a particular threshold of a status type that contributes to QoS calculations is tripped. Status types that initially contribute to Quality of Service calculations include:

- Location Communication Error
- Control System Error
- Network
- Security
- System Communication Error

Working With System Reports

Running a Report

1. Select a Report (in the *Report Selection* window).
2. Select either **PDF** or **CSV** as the format for the exported Report file.
3. Click **Run** to generate the Report as specified.

The Report is automatically opened in a separate window. Examples of an exported Report (both formats) are shown in FIG. 60:
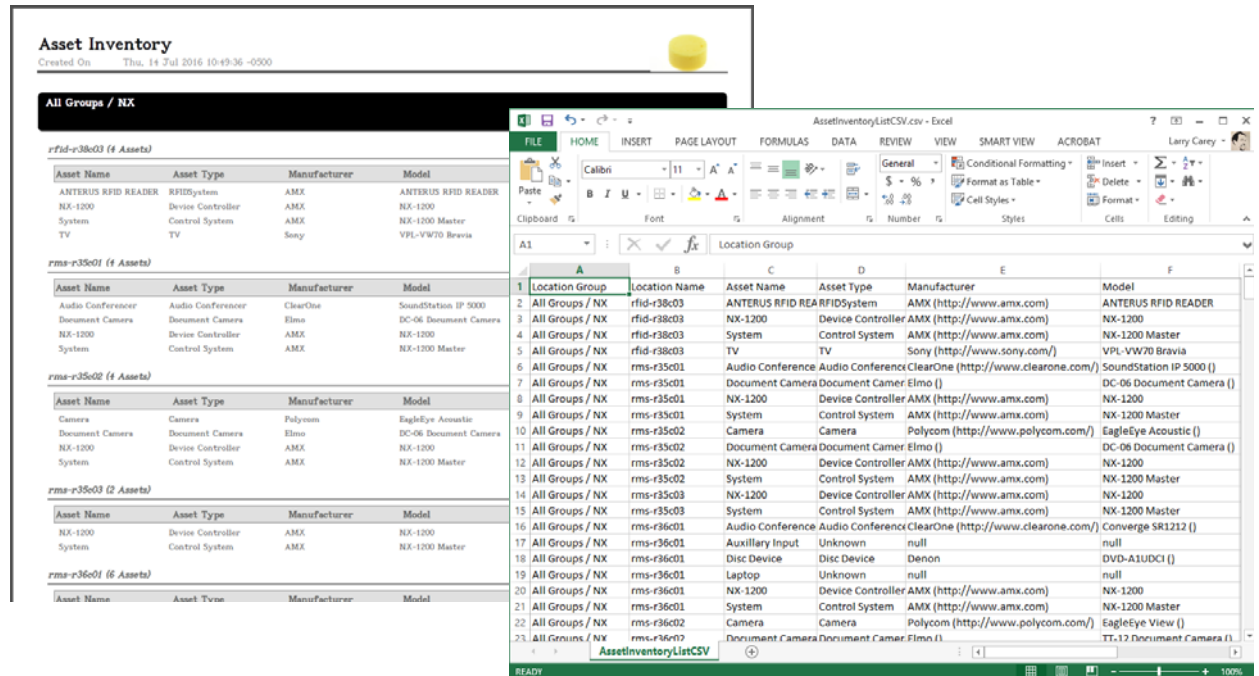
FIG. 60 Example Report Output (PDF and CSV formats)

Saved Reports

Any system report (listed under *Reports* in the Report Selection Window) can be edited and saved as a "Saved Report" and listed under *Saved Reports* in the Report Selection Window. Saved Reports can be edited and deleted as desired.

Creating a Saved Report

1. In the Reports page, select a System Report to edit (under *Reports* in the Report Selection Window - see FIG. 57 on page 46).
2. Edit the report *Name* and *Description* in the Report Options Window to describe the custom report you are creating (FIG. 61):

FIG. 61 Report Options Window

> **NOTE:** *Editing the Description is optional, but editing the Name is necessary. The report Name must be unique in order for it to be stored in the Saved Report section.*

3. Edit the settings in the *Report Properties Window* tabs to customize the report to your needs (FIG. 62).

FIG. 62 Report Properties Window

Note that the tabs and options presented in the Report Properties window depend on the type of Report Type selected. Refer to the *Report Properties* section on page 50 for descriptions of the fields and options presented in each tab of the Report Properties Window.

4. Click **Save** (in the *Report Options Window*) to save this report as a Saved Report.

Saved Reports are listed under *Saved Reports* in the Report Selection Window (FIG. 63)*:*

example Saved Report

FIG. 63 Report Properties Window indicating an example Saved Report

NOTE: *System Reports can also be edited and run (without saving) if necessary. If changes are not saved, they are lost when the report is closed.*

Deleting a Saved Report

Saved Reports can be deleted, but System Reports cannot. To delete a Saved Report:

1. Select a saved Report in the Report Selection window.
2. Click **Delete**.
3. The system will prompt you to verify this action (FIG. 64):

FIG. 64 Warning - Deleting a Saved Report

4. Click **Yes** to delete.

The selected report is removed from the *Saved Reports* list.

Report Properties

The options presented in the tabs of the *Report Properties* window depend on the type of Report Type selected. Some Report Types only require a few options in a single tab, while others present multiple tabs with additional options.

- Note that for any reporting option that requires text input, an asterisk (*****) can be used as a wildcard character.
- Required fields are indicated, and a message is displayed if a required field has not been filled in.
- Use the **Reset** option to reset the parameters for an individual report item.
- Use the **Reset All Parameters** option to reset all parameters in all tabs.

General Tab

The options presented in the *General* tab allow you to add or remove specific information on the selected report type. Note that the options presented in this tab depend on the type of report selected. An example General tab (for the Asset Inventory report) is shown in FIG. 65:
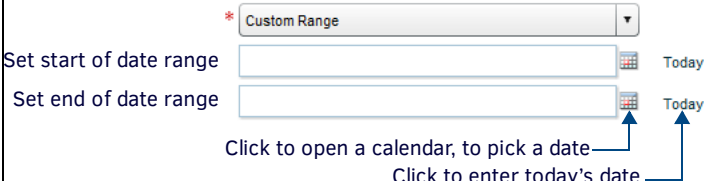
FIG. 65 Report Properties - General tab (Asset Quality of Service report options shown as an example)

Report Properties - General tab options		
Report Property	**Description**	**Used in Report(s)**
Summary Type	Select *Yearly*, *Monthly* or *Daily* from the drop-down menu. The default selection is *Yearly*.	Asset Quality of Service Location Energy Usage Location Quality of Service System-wide Energy Usage
Event Organizer Name	Enter the name of the event organizer to be used in this report.	Location Usage by Organizer
Select Date Range	Select a date range from the options presented in the drop-down menu. Select Custom Range to specify a custom date range. The default selection is *Today*. See *Date Range Options* on page 51 for details.	Asset Quality of Service Location Energy Usage Location Quality of Service Location Usage by Organizer Service Requests System-wide Energy Usage User Audit Trail (By Date)
Detail	Select this option to include detailed energy usage records the Report. By default, the *Include Detailed Records in Report* option is de-selected.	Location Energy Usage System-wide Energy Usage
Hours of Usage	Select *Any*, <=, >=, *Equal To*, *Not Equal To* or *Between* from the drop-down menu. The default selection is *Any*. See *Range Options* on page 52 for details.	Lamp and Display Usage Location Usage by Organizer Source Usage
Charts & Graphs	By default, the *Include Charts & Graphs in Report* option is selected. De-select to exclude charts and graphs from the Report. Note that when this option is selected, 50 days of data is displayed.	Asset Quality of Service Lamp and Display Usage Location Quality of Service Location Usage by Organizer Service Requests Source Usage System-wide Energy Usage User Audit Trail (By Date)
Service Requests	By default, the *Include Service Records in Report* option is de-selected. Select this option to include service records the Report.	Service Requests
Location Summary	By default, the *Include Summary for Each Location* option is selected. De-select to exclude Location summary information from this Report.	Location Energy Usage

Report Properties - General tab options (Cont.)		
Report Property	**Description**	**Used in Report(s)**
Energy Cost per kWh	Enter the energy cost per kilowatt hour (in dollars). This is a required field for *Location Energy Usage* reports.	Location Energy Usage System-wide Energy Usage
Environmental Impact (lbs CO2/kWh)	Enter the environmental impact per kilowatt hour (in lbs of CO2). This is a required field for *Location Energy Usage* reports.	Location Energy Usage System-wide Energy Usage
Quality of Service (Percentage) for Summary Period	Select *Any*, *<=*, *>=*, *Equal To*, *Not Equal To* or *Between* from the drop-down menu. The default selection is *Any*. See *Range Options* on page 52 for details.	Asset Quality of Service Location Quality of Service
Downtime (in Hours) per Summary Period	Select *Any*, *<=*, *>=*, *Equal To*, *Not Equal To* or *Between* from the drop-down menu. The default selection is *Any*. See *Range Options* on page 52 for details.	Asset Quality of Service Location Quality of Service
Uptime (in Hours) per Summary Period	Select *Any*, *<=*, *>=*, *Equal To*, *Not Equal To* or *Between* from the drop-down menu. The default selection is *Any*. See *Range Options* on page 52 for details.	Asset Quality of Service Location Quality of Service
URL	Enter the base URL for the location(s) that will use mobile scheduling. This base URL can be either internal or external and must be determined by the System Administrator. This is a required field for *Location Web Address for QR Code Readers* reports. See the *Mobile Scheduling* section on page 214 for details.	Location Web Address for QR Code Readers
User Name	Enter the login ID used to log into the RMS UI; it also includes the "*not authenticated*" account.	User Audit Trail (By Date)
Target	Enter the name of the target string to be used in this report.	User Audit Trail (By Date)
Action	Enter the name of the action string to be used in this report. Examples of an action string include *execute scheduled control macro*, *add*, *location*, *modify location*, *etc.*)	User Audit Trail (By Date)
Location	Enter a name to be used in this report for the selected Locations.	User Audit Trail (By Date)

Date Range Options

The following table provides descriptions of the Date Range options available via the **Select Date Range** drop-down menu (presented in the *General* tab of the Report Properties window for many reports).

Date Range Options	
Today	The report(s) will include data from today's date only.
Week To Date	The report(s) will include data from the beginning of the current week (Monday) through today's date only.
Month To Date	The report(s) will include data from the beginning of the current month through today's date only.
Quarter To Date	The report(s) will include data from the beginning of the current quarter (Q1-Q4) through today's date only.
Year To Date	The report(s) will include data from the beginning of the current year through today's date only.
Yesterday	The report(s) will include data from yesterday's date only.
Last Week	The report(s) will include data from last week only.
Last Month	The report(s) will include data from last month only.
Last Quarter	The report(s) will include data from last quarter (Q1-Q4) only.
Last Year	The report(s) will include data from last year only.
Quarter	The *Quarter* sub-menu provides Q1-Q4 date range options.
Month	The *Month* sub-menu provides monthly date range options.
Custom Range	This selection invokes the following additional fields, which allow you to define a custom date range: * Custom Range ▼ Set start of date range [____] 🗓 Today Set end of date range [____] 🗓 Today Click to open a calendar, to pick a date Click to enter today's date

NOTE: *When the Include Charts & Graphs in Report option is selected in the Report Properties page - General tab (default setting), only 50 days of data will be displayed.*

Range Options

The following table provides descriptions of the Range options available via drop-down menu for many reports (examples include, *Battery Level, Hours of Usage*, *Temperature Range*, etc).

Note that when any option other than *Any* is selected, a text field is provided to the right of the drop-down menu, to allow entry of the range value (FIG. 66).

FIG. 66 Range Options - Text Field for entry of Range value

Range Options	
Any	Report any result, with no range limits.
<=	Report only results that are less than or equal to the value entered.
>=	Report only results that are greater than or equal to the value entered.
Equal To	Report only results that are equal to the value entered.
Not Equal To	Report any results that are not equal to the value entered.
Between	Report only results that are equal to or between the two values entered. Note that when this option is selected, two text fields are provided.

Location Tab

This tab is available for all reports that include location-based data. The options presented in the *Location* tab allow you to specify which locations to include in the report based on Location Name, Owner, Classification, and Time Zone. An example Location tab (for the Asset Inventory report) is shown in FIG. 67:

FIG. 67 Report Properties - Location tab (Asset Quality of Service report options shown as an example)

Report Properties - Location tab options		
Report Property	**Description**	**Used in Report(s)**
Select Location	By default, *Any* is selected. To specify one or more Locations to be included n this report, click *Selected*. This option presents a Location selection window that allows you to select one or more Locations to include.	Asset Inventory Asset Quality of Service Lamp and Display Usage Location Energy Usage Location Quality of Service Location Usage by Organizer Location Web Address for QR Code Readers Service Requests Source Usage
Location Name	Enter a name to be used in this report for the selected Locations.	Asset Inventory Asset Quality of Service Lamp and Display Usage Location Energy Usage Location Quality of Service Location Usage by Organizer Location Web Address for QR Code Readers Service Requests Source Usage

Report Properties - Location tab options (Cont.)		
Report Property	**Description**	**Used in Report(s)**
Select Time Zone	By default, *Any* is selected. To specify a Time Zone, select from the drop-down menu. Note that when a time zone is selected, a second drop-down menu is provided to select a local time zone as well.	Asset Inventory Asset Quality of Service Lamp and Display Usage Location Energy Usage Location Quality of Service Location Usage by Organizer Location Web Address for QR Code Readers Service Requests Source Usage
Owner	Enter a name to be used in this report as the "owner" for the selected Locations.	Asset Inventory Asset Quality of Service Lamp and Display Usage Location Energy Usage Location Quality of Service Location Usage by Organizer Location Web Address for QR Code Readers Service Requests Source Usage
Select Classification	By default, *Any* is selected. To specify one or more RMS account Classifications (*Platinum*, *Gold*, *Silver*, *Bronze*, etc.) to be included in this report, click *Selected*. This option presents a Classification selection window that allows you to select one or more classification levels to include.	Asset Inventory Asset Quality of Service Lamp and Display Usage Location Energy Usage Location Quality of Service Location Usage by Organizer Location Web Address for QR Code Readers Service Requests Source Usage

Asset Tab

This tab is available for all reports that include asset-based data The options presented in the *Asset* tab allow you to specify which assets to include in the report based on Asset Name, Firmware version, Maintenance Status, Manufacturer Name, Metadata Property, Model Name, Type and Serial Number. An example Asset tab is shown in FIG. 68:

FIG. 68 Report Properties - Asset tab (Asset Quality of Service report options shown as an example)

Report Properties - Asset tab options		
Report Property	**Description**	**Used in Report(s)**
Asset Name	Enter a name for the Asset in this report.	Asset Quality of Service Source Usage
Manufacturer Name	Enter a name for the manufacturer of the Asset in this report.	Asset Quality of Service Source Usage
Model Name	Enter a Model Name for the Asset in this report.	Asset Quality of Service Source Usage
Select Asset Types	By default, *Any* is selected. To specify one or more Asset Types to be included in this report, click *Selected*. This option presents a Asset Types selection window that allows you to select one or more asset types to include.	Asset Quality of Service Source Usage
Serial Number	Enter the serial number for the Asset in this report.	Asset Inventory
Firmware	Enter the firmware version number for the Asset in this report.	Asset Inventory

Report Properties - Asset tab options (Cont.)		
Report Property	**Description**	**Used in Report(s)**
Maintenance Status	Enter a maintenance status for the Asset in this report.	Asset Inventory
Metadata Property	Enter a metadata property for the Asset in this report.	Asset Inventory

Schedule Tab

This tab is available for all reports. The options presented in the *Schedule* tab allow you to schedule and e-mail a single tailored report or recurring reports. An example Schedule tab is shown in FIG. 69:

FIG. 69 Report Properties - Schedule tab

NOTE: *The options in the Scheduling tab are only enabled if an Email Server (SMTP) has been configured and enabled. If the Schedule tab options are unavailable, you must configure and enable an Email Server (SMTP) before creating a report schedule (see the Email Server (SMTP) section on page 220 for details.*

Report Properties - Schedule tab options		
Report Property	**Description**	**Used in Report(s)**
Enable Schedule	By default scheduling is turned off - select this option to enable the scheduling options.	All
Description	Enter a description of the report (maximum of 250 characters).	All
Start Date	Required field: enter the start date and time for the scheduled report.	All
Recipients	Required field: enter the e-mail address of the recipient(s) of the schedule report.	All
Recurring	Select this option to enable and configure recurring reports. Reports can be configured to run daily, weekly, monthly, quarterly, bi-annually or yearly. The user can also configure the when to end the automated reports (never, after a set number of occurrence or by a specific calendar date. By default the Recurring Reports option is disabled	All

Service Provider Tab

This tab is available only for Service Request reports. The options presented in the *Service Provider* tab allow you to specify which service requests to include in the report based on Service Request Status, Service Request Type, and/or specific Service Request Message. An example Service Provider tab is shown in FIG. 70:

| General | Service Provider | Location | Schedule | | Reset All Parameters |

Service Request Type	Any	Reset
Service Request Status	All	Reset
Service Request Message		Reset

FIG. 70 Report Properties - Service Provider tab

Report Properties - Service Provider tab options		
Report Property	**Description**	**Used in Report(s)**
Service Request Type	Select *Any*, *Help Request* or *Maintenance Request* from the drop-down menu. The default selection is *Any*.	Service Requests
Service Request Status	Select *Any*, *Open* or *Fulfilled* from the drop-down menu. The default selection is *Any*.	Service Requests
Service Request Message	Use this text field to search the message field sent by the end-user (text that is visible in the Summary column of the Hotlist).	Service Requests

Dashboard (Classic UI)

Overview

The initial view of the RMS Enterprise Classic UI is the *Dashboard*.

NOTE: *To access the RMS Classic UI described in the following sections, select "Classic UI" from the RMS Enterprise HTML interface menu bar.*

The Dashboard presents user-selectable *Widgets* including the Hotlist, Lamp Life, Source Usage, etc (see the *Dashboard Widgets* section on page 59 for details), as well as access to the *Dashboard*, *Management*, *Reports, Configuration* and *Help* menus. The data presented on the Dashboard is specific to the currently selected Location. The *Select Location* option allows you to switch views to a different Location (see *Selecting a Location via the Dashboard* on page 57 for details). FIG. 71 shows the Dashboard in a typical configuration:
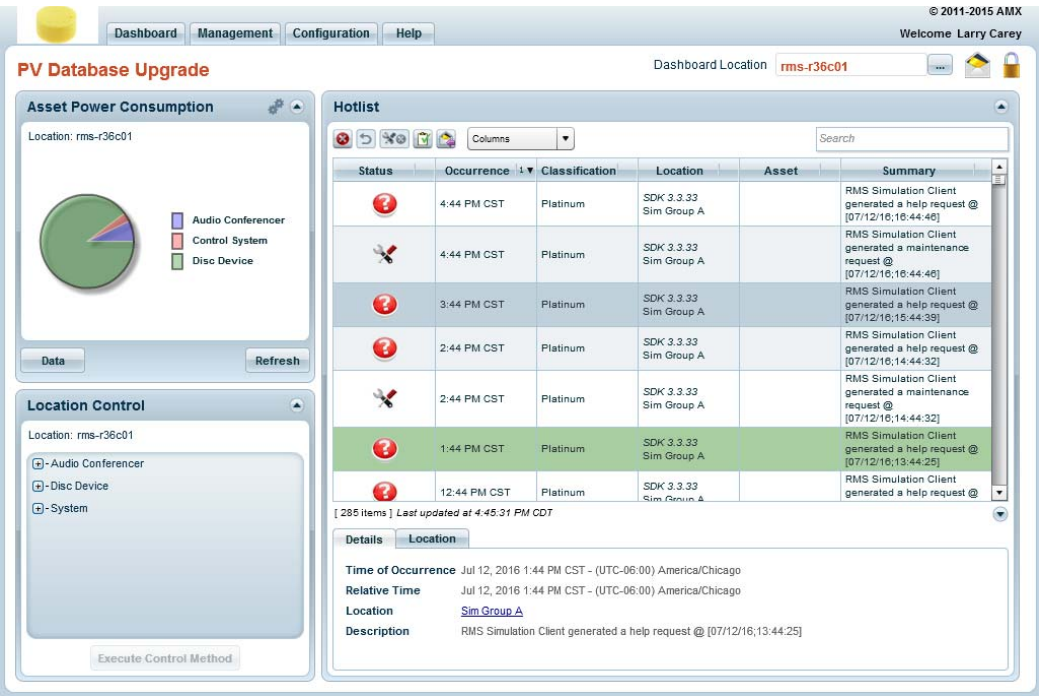
FIG. 71 RMS Work area - example Dashboard view

NOTE: *The Dashboard is customizable - add and remove Widgets, and arrange the placement of the Widgets and various work area elements to optimize the UI for your purposes. See the Dashboard Widgets section on page 59 for details.*

Dashboard Menu

Click inside the **Dashboard** tab to access the *Dashboard* menu (FIG. 72).
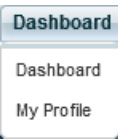
FIG. 72 Dashboard Menu

The options in the Dashboard menu allow you to access the Dashboard, view and edit your User Profile, view and manage your User Notifications, and log out of the RMS system, as described in the following sections.

Dashboard Menu Options	
Dashboard	Select **Dashboard** to open the *Dashboard* page (see FIG. 71 on page 56).
My Profile	Select **My Profile** to open the *My Profile* page. This page contains several tabs - *General Setting*, *My Contacts*, *Notification Schedule* and *My Notifications*. By default, this page opens to the **General Setting** tab. See the *Dashboard - My Profile (Classic UI)* section on page 84 for details.

Using the Dashboard

The *Dashboard* is the primary area of the RMS UI; it is where most users will access RMS functionality. In fact, once the system is configured, most non-admin users will have little reason to access any other part of the RMS UI.

The functionality available on the Dashboard page will vary depending on which Widgets are present. See the *Dashboard Widgets* section on page 59 for details on each Widget, and on adding/removing/arranging Widgets. However, there is a default Dashboard layout configuration that presents basic RMS functions (see *Default Dashboard Layout* on page 63). This default layout includes the *Hotlist*, *Lamp Life* and *Source Usage* widgets.

Selecting a Location via the Dashboard

Use the **Select Location** drop-down menu in the upper-right corner of the Dashboard to change the Location being monitored:

1. Click on the down-arrow next to the **Select Location** field (FIG. 73): .

Click to open the Select Location dialog

Currently selected Location
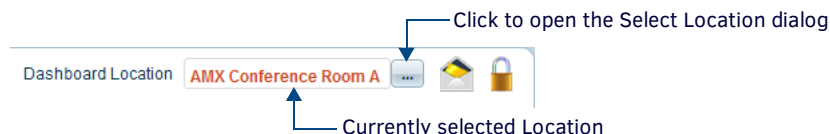
FIG. 73 Dashboard - Select Location

2. This opens the *Select Location* dialog (FIG. 74):
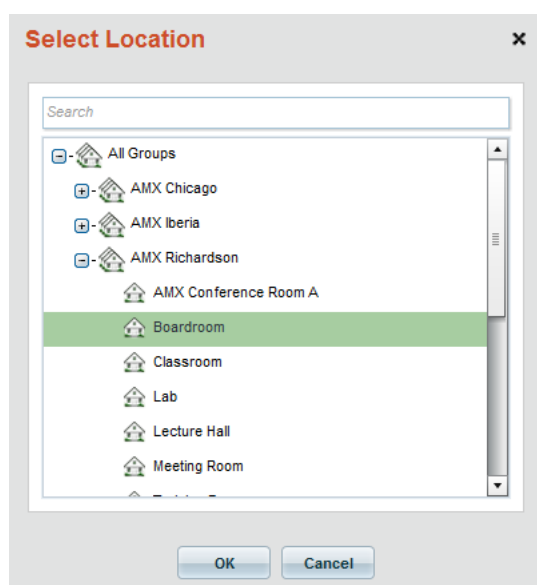
FIG. 74 Select Location dialog

3. Select a Location and click **OK** to change the monitored Location and close this dialog.

The RMS Dashboard now indicates data on the newly selected Location.

See the *Management - Locations (Classic UI)* section on page 103 for details.

Sending a Message to a Location via the Dashboard

Use the **Send Message** icon in the upper-right corner of the Dashboard to send a message to the touch panel(s) in the current Location:

1. Click on the **Send Message** icon (FIG. 75): .

Click to open the Send Message dialog

Currently selected Location
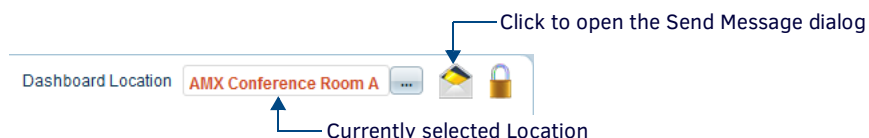
FIG. 75 Dashboard - Send Message

2. This opens the first of two *Send Message* dialogs (FIG. 76). In this dialog, select the Location to which you want to send this Message.

3. Click **Next** to proceed to the second *Send Message* dialog (FIG. 76): .
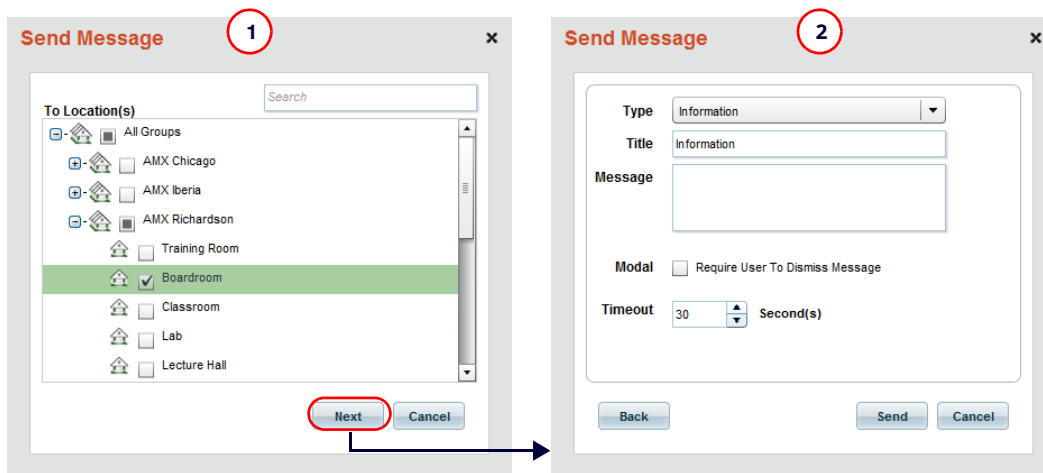
FIG. 76 Dashboard - Send Message

4. Select a message type from the **Type** down-down.

    Message types are arbitrary, designed to provide distinction between the various types of messages that might be sent to a Location. Therefore there are no inherit characteristics for each Message Type, assign them in any way that helps you to differentiate between types of messages.

    NOTE: *By default, new Messages are set to the Information message type.*

5. Enter a title for this message in the **Title** text field. The text is displayed as it will appear in the message in the *Message Preview* window.

6. Enter the message text in the **Message** text field.

7. Click the *Require User To Acknowledge Message* option next to **Modal** to require that the user must acknowledge the message dialog before it is removed from the screen (on the Touch Panel).

8. Set the **Timeout** value, in seconds (optional). If the message contains a timeout, the popup page will automatically be closed (on the Touch Panel) after the elapsed number of seconds.

9. Click **Send** to send the message to the selected Location.

Locking and Unlocking the Dashboard Layout

Click on the **Lock / Unlock** icon to unlock the Dashboard Layout and enable access to the Available Widgets window (FIG. 75):   .

Click to unlock/lock the Dashboard Layout

FIG. 77 Dashboard - Lock/Unlock the Dashboard Layout

See the *Adding, Removing and Arranging Widgets* section on page 60 for details.

Dashboard Widgets

The RMS Enterprise Classic UI Dashboard is highly customizable, via the use of *Widgets*. Widgets provide specific utilities or specialized information views that can be added to or removed from the Dashboard. Widgets allow you to customize the Dashboard page so that only the features and functions you need are displayed.

Widgets can be added and removed from the Dashboard (via the *Available Widgets* window), and arranged to suit your preferences (FIG. 78).
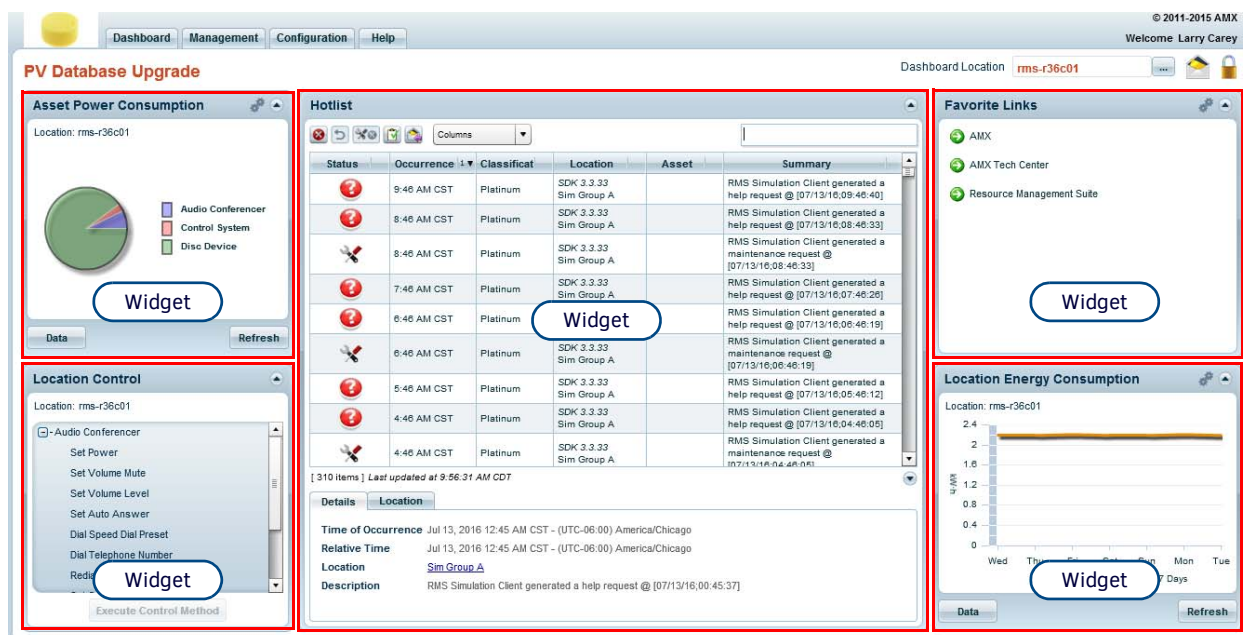
FIG. 78 Example Dashboard with Widgets

The Dashboard Widgets available are:

Dashboard Widgets	
Asset Power Consumption	See the *Asset Power Consumption Widget* section on page 72.
Control Macro Schedule	See the *Control Macro Schedule Widget* section on page 73.
Favorite Links	See the *Favorite Links Widget* section on page 74.
Hotlist	See the *Hotlist Widget* section on page 64.
Lamp Life	See the *Lamp Life Widget* section on page 77.
Location Control	See the *Location Control Widget* section on page 77.
Location Energy Consumption	See the *Location Energy Consumption Widget* section on page 79.
Source Usage	See the *Source Usage Widget* section on page 81.
System Status	See the *System Status Widget* section on page 82.

Widget Placement

Widgets can be placed in one of the three main columns that comprise the Classic UI Dashboard layout. When the Dashboard is unlocked, a set of Widget Placement guidelines are displayed on the work area. These guidelines indicate the location of the three main regions for Widget placement (FIG. 79):

FIG. 79 Dashboard - Widget Placement Guidelines

- The center column is the Main Content Region - intended for primary content widgets such as the *Hotlist* and *System Status* widgets.
- The left and right columns are intended for smaller utility or specialized informational widgets.
- Multiple widgets can be "stacked" vertically within any of the main regions.

NOTE: *Certain widgets may be restricted as to the column in which they can be placed. For example, since the Hotlist Widget is intended as primary content and the widget itself requires larger screen space, it is restricted from being placed into the left or right columns and is only eligible to be placed in the center column.*

Adding, Removing and Arranging Widgets

Locking / Unlocking the Dashboard Layout

By default, the Dashboard is Locked, which prevents any changes being made to the Dashboard Layout. A locked Dashboard also precludes access to the Available Widgets window.

In order to access the Available Widgets window, the Dashboard must be Unlocked, via the **Lock / Unlock** icon in the upper-right corner of the Dashboard (FIG. 80):
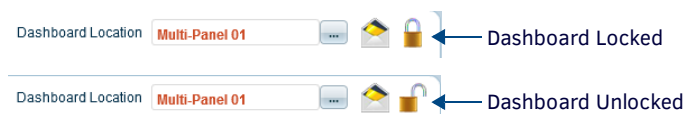
FIG. 80 Dashboard Lock / Unlock Icon

Click on the Lock / Unlock icon to unlock the Dashboard Layout and enable access to the Available Widgets window. Once configuring their dashboard for their preferences, a user should lock their dashboard to prevent inadvertent, unintended changes.

Accessing the Available Widgets Window

Widgets are available for selection via the *Available Widgets* window - an expandable panel that "flies out" from the right side of the screen. Hover over this panel with the mouse cursor to expand and display the listing of available dashboard widgets (FIG. 81).
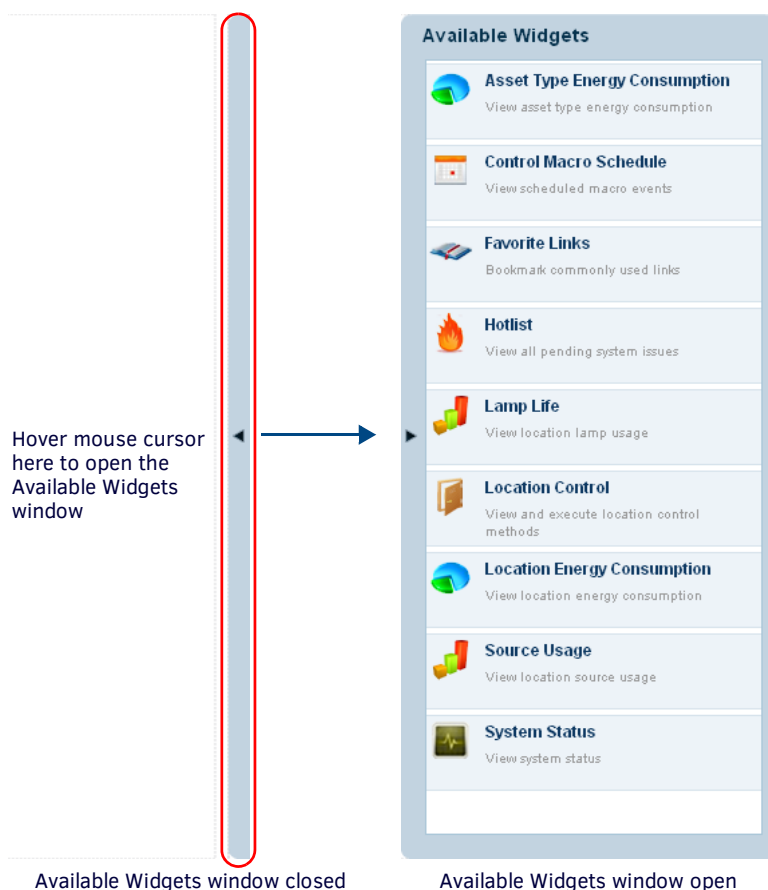
FIG. 81 Accessing the Available Widgets Window

Note that the Widgets listed in the Available Widgets window only include widgets that are not already on the Dashboard.

Adding a Widget to the Dashboard

1. Unlock the Dashboard Layout (see *Locking / Unlocking the Dashboard Layout* on page 60).
2. Open the Available Widgets window (see *Accessing the Available Widgets Window* on page 60).

3.   Left-click and drag the widget from the Available Widgets window to the desired column and widget position on the Dashboard.

4.   Release the left mouse button to "drop" the widget in place. The Dashboard will automatically rearrange and re-size any existing widgets to accommodate the new widget.

Note that while dragging a widget, if the mouse cursor displays a small red "X" icon, then that widget is not eligible to be dropped into that target dashboard column. For example, the Hotlist widget is intended to be placed in the center column, since the side columns are too small to accommodate the data displayed in the Hotlist. If you attempt to place the Hotlist widget in a side column, the red "X" icon indicates that this placement is not allowed (FIG. 82):
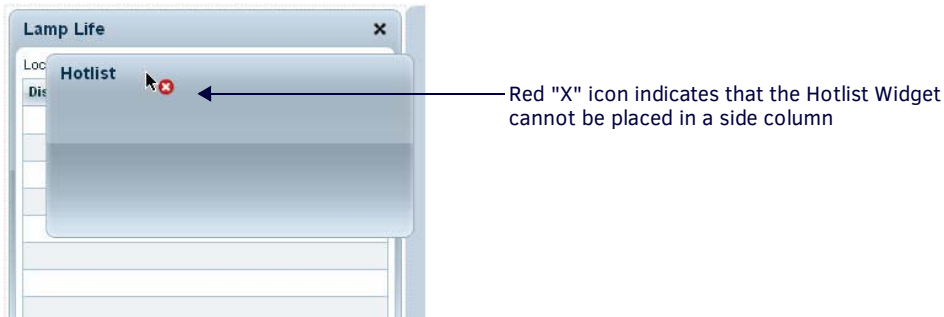
FIG. 82 Widget Placement not Allowed

Removing a Widget From the Dashboard

1.   Unlock the Dashboard Layout (see *Locking / Unlocking the Dashboard Layout* on page 60).

2.   When the Dashboard is unlocked, each Widget features a "Close" (x) icon the upper-right corner (FIG. 83):
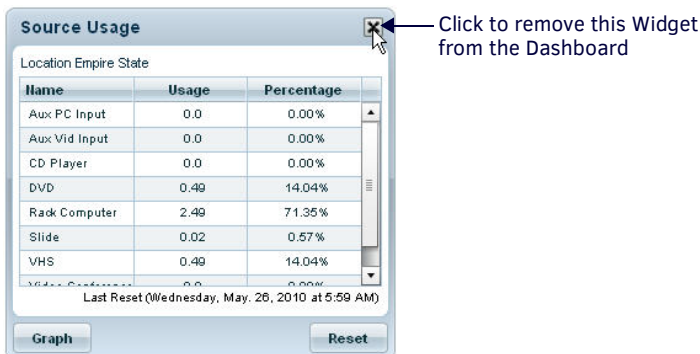
FIG. 83 Removing a Widget from the Dashboard

3.   Click the Close icon to remove the Widget from the Dashboard.

Re-Arranging Widgets on the Dashboard

1.   Unlock the Dashboard Layout (see *Locking / Unlocking the Dashboard Layout* on page 60).

2.   Left-click inside the title bar of the widget that you want to move, and drag it to the desired position in the Dashboard (FIG. 84):
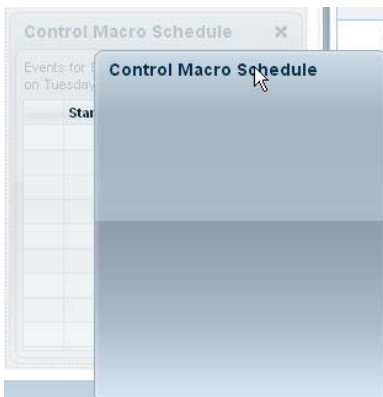
FIG. 84 Moving a Widget

3.   Release the left mouse button to "drop" the widget in place.
   ● The Dashboard will automatically rearrange and resize any existing widgets to accommodate the new widget.
   ● Note that while dragging a widget, if the mouse cursor displays a small red "X" icon, then that widget is not eligible to be dropped to that target dashboard column (see FIG. 82 on page 61).

Re-sizing the Columns of the Dashboard

In some cases you may need to provide more room than is currently available on the Dashboard, in order to add widgets. For example, in the default Dashboard layout (see FIG. 86 on page 63), the right column is unused. In this case, it can be difficult to add a widget to the right column because the target space into which a widget may be dropped is compressed. In this case, you may need to increase the size of the right column, to allow placement of a widget.

The three main columns can be resized via the separator lines between the columns (FIG. 85):

FIG. 85 Resizing the Three Main Columns

Dashboard Layout - User Persistence

The Dashboard widget selection, widget layout, widget sizing and column sizing are persisted with each user account, to allow a unique customized user dashboard for each user. Unlike the behavior for regular users, if the *Guest* account is used, these settings are persisted only to the local computer's Internet cache, thus these settings are not propagated or synchronized to other computers using the Guest account. See the *Default Anonymous / Guest User Account* section on page 179 for details.

NOTE: *The Guest account is only available for installed RMS Servers; it cannot be enabled for AMX Cloud hosted services.*

The following user personalizations are persisted:

Dashboard Layout - User Persistence	
Dashboard	• Selected widgets • Widget layout • Widget height • Column widths • Selected location
Hotlist	• Details preview pane collapsed/expanded • Optional display columns • Multiple column sorting order or sorting direction
Favorite Links	User preferred URL listing
All horizontal and vertical resizing splitter containers	Splitter position
All data grids	• Column widths • Column position (order) • Column(s) sorted by • Sort direction

NOTE: *When making a change to the UI that causes the user personalization to be updated, it may take up to 10 seconds for the changes to be persisted on the RMS server.*

Default Dashboard Layout

The default Dashboard layout is shown in FIG. 86:
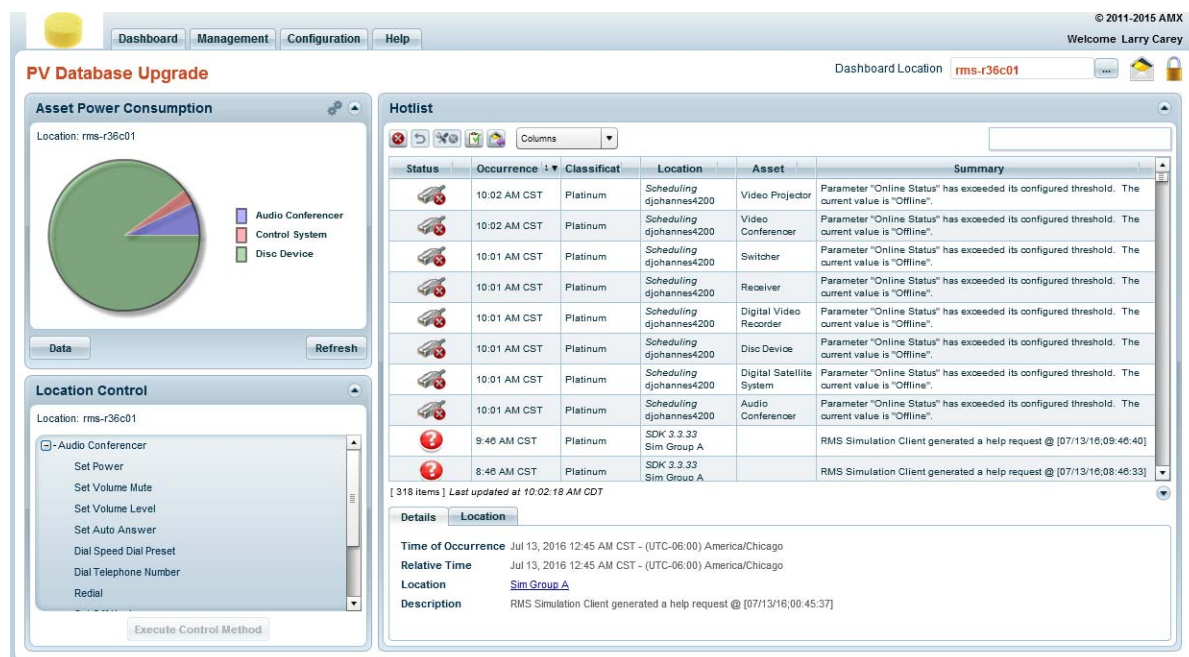
FIG. 86 Default Dashboard Layout

The default Dashboard layout includes:

- In the left column - *Asset Power Consumption* and *Location Control* widgets
- In the center column - *Hotlist* widget
- In the right column - no widgets are in the right column in the default layout.

Returning the Dashboard to the Default Layout

Use the **Reset User Preference** option in either the *My Profile* page (see *My Profile - General Setting Tab* on page 85), or the *User Management* page (see *User Properties Window - User Profile Tab* on page 182) to return the Dashboard to it's default layout:

1. Select **My Profile** in the *Dashboard* menu to open the *My Profile* page (**General Setting** tab).

    Alternatively, select **Users** under *User & User Notification Management* in the *Management* menu to open the *User Management* page, and select a user in the *Users* window. This opens the **User Profile** tab of the *User Properties* window.

    Note that the options in the *My Profile* page are the same as those presented in the **User Profile** tab of the User Properties window.

2. Click the **Reset User's Preferences** button at the bottom of the page (FIG. 87).
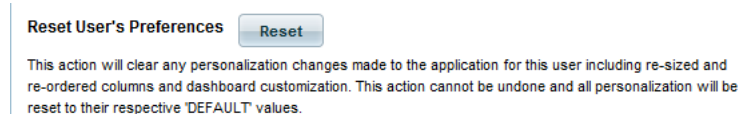
FIG. 87 My Profile page - Reset User's Preferences button

> **NOTE:** *This action will clear any personalization changes made to the application for this user including re-sized and re-ordered columns and dashboard customization. This action cannot be undone and all personalization will be reset to their respective 'DEFAULT' values.*

3. The system will indicate that the User's Preferences have been reset (FIG. 88):
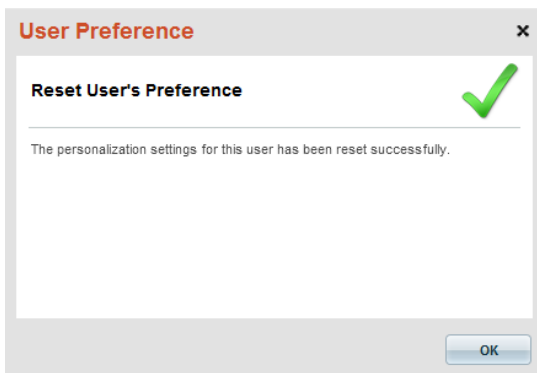
FIG. 88 Reset User's Preferences dialog

4.   Click **OK** to close the Reset User Preferences dialog and return to the My Profile page.

Hotlist Widget
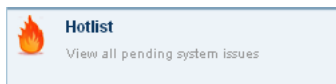
FIG. 89 Hotlist Widget Icon (Available Widgets window)

The *Hotlist* Widget is provided as the primary content widget and is only allowed to be placed in the center   column of the Dashboard. The Hotlist widget is included in the default Dashboard Layout (see *Default Dashboard Layout* on page 63), and it can be added / removed from the Dashboard, like any other Widget. The Hotlist widget displays all current system exceptions and issues that need to be addressed in the RMS system (FIG. 90) for the locations the currently authenticated user has permissions to view.

FIG. 90 Hotlist Widget

NOTE: *RMS Enterprise v4.6 (or higher) provides a simplified, read-only version of the Hotlist as the primary view in the HTML interface. See the RMS Enterprise HTML UI section on page 20 for details.*

Hotlist Widget - Security

Only items that are relevant to the currently authenticated user are displayed in the Hotlist: When a user signs into RMS, the data shown in the Hotlist Data Grid is limited to only Hotlist records that the user has permissions to view. For example, if a Location is in maintenance mode, only users with location management permissions may see this record. Similarly, if an asset parameter is tripped or if a help request has been received, only users with asset view permissions to that location will see those Hotlist records.

See the *Management - Roles (Classic UI)* section on page 192 for details on Roles and Permissions.

Hotlist Widget - Data Synchronization

When a user signs into RMS, a full listing of Hotlist records that the current user has permissions to view are displayed in the Hotlist Data Grid. Subsequently, only *changed* Hotlist records are retrieved from the server, based on a timestamp from the last receipt.

The timestamp is displayed below the Hotlist Data Grid (FIG. 91):

	4:30 AM CDT May 18, 2011	Platinum	*Sample University* Classroom E01-123	Projector 1	Parameter "Lamp Hours" has exceeded its configured threshold. The current value is "1456 Hours".
[6 items] *Last updated at 12:40:33 PM CDT*					
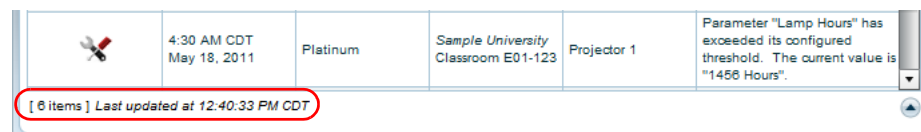
FIG. 91 Hotlist Widget - Data Synchronization Timestamp

Hotlist Widget Toolbar

The toolbar at the top of the Hotlist widget provides access to the following functions:

Dismiss selected Hotlist items
Reset Asset Parameters on selected Hotlist records
Disable maintenance mode on selected Hotlist records
Fulfill the Service Requests on selected Hotlist records
Send message to locations on selected Hotlist records

Columns ▼ ← Select the columns to be displayed in the Hotlist data grid
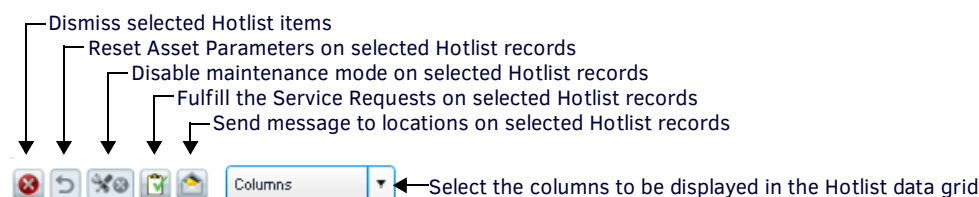
FIG. 92 Hotlist Widget Toolbar

Hotlist Widget Toolbar	
Dismiss selected Hotlist items	Click to dismiss the selected Hotlist item(s). When a Hotlist item is dismissed, it is permanently removed from the Hotlist data grid. See *Dismissing Hotlist Items* on page 68 for details. *Note: The Dismiss button is only enabled when one or more Hotlist records that support dismissal are selected in the Hotlist Data Grid. Not all Hotlist records can be dismissed.*
Reset asset parameters on selected Hotlist items	Click to reset the Asset parameters for the selected Hotlist item(s). This option is only enabled for Hotlist items that contain an Asset, and where the current user has Manage permission for the asset location. See *Resetting Asset Parameters for a Hotlist Item* on page 68 for details.
Disable maintenance mode on selected Hotlist items	Click to disable Maintenance Mode for the Asset or Location in the selected Hotlist Item. This option is only available for Hotlist Items that include an Asset or Location that is currently in Maintenance Mode, and only if the current user has the proper management permissions to disable the maintenance mode. • See the *Maintenance Mode for Locations* section on page 122 for details. • See the *Maintenance Mode for Assets* section on page 154 for details. • See the *System Maintenance Mode* section on page 210 for details.
Fulfill the Service Requests for the selected Hotlist items	Click this option once a pending Service Request has been fulfilled. When this option is clicked, the selected Hotlist items are removed from the data grid, since they are no longer considered to be pending.
Send Message to locations on selected Hotlist records	Click to send a message to the selected Hotlist records. This action invokes the *Send Message* dialog. This option is only enabled for Hotlist items that contain a location. See *Sending a Message to a Location* on page 68 for details.
Columns	Click inside this field to select which columns to display in the Hotlist Data Grid, from the drop-down menu. See *Specifying Columns in the Hotlist Data Grid* on page 68 for details.

Hotlist Widget Search Window

The *Search* window in the upper-right corner of the Hotlist widget allows you to search the Hotlist Data Grid to find a specific entry or set of entries (FIG. 93).

DVD| ✖ ← Click to clear the Search window

FIG. 93 Hotlist Widget Search Field

Performing a Hotlist Search

1. Enter a text string in the Hotlist Widget *Search* window.
2. Press **Enter** to perform the search. The search query will be applied against all visible columns of data.

> **NOTE:** *Since searches are performed against the data displayed in the Hotlist Data Grid, you might need to select additional columns for display. See the Specifying Columns in the Hotlist Data Grid section on page 68 for details.*

Hotlist Widget Data Grid

The main display area of the Hotlist widget is the Hotlist Data Grid. All Hotlist items are displayed in the Data Grid (FIG. 94).

Status	Occurrence 1 ▼	Classification	Location	Asset	Summary
🔧	7:26 PM CDT May 23, 2011	Platinum	*Sample University* Classroom E01-123	PDU	Parameter "Rack Temperature" has exceeded its configured threshold. The current value is "110 C".
🖥	9:33 PM CDT May 22, 2011	Platinum	*Swinburne University* Building 1	System	Parameter "System Online" has exceeded its configured threshold. The current value is "Offline".
🔧	10:41 AM CDT May 20, 2011	Platinum	*AMX Singapore* Singapore Training Room	Projector	Parameter "Lamp Hours" has exceeded its configured threshold. The current value is "402 Hours".
🔧	4:30 AM CDT May 18, 2011	Platinum	*Sample University* Classroom E01-123	Projector 2	Parameter "Lamp Hours" has exceeded its configured threshold. The current value is "2140 Hours".
🔧	4:30 AM CDT May 18, 2011	Platinum	*Sample University* Classroom E01-123	Projector 1	Parameter "Lamp Hours" has exceeded its configured threshold. The current value is "1456 Hours".
🖥	12:33 AM CDT May 18, 2011	Platinum	*AMX Singapore* Singapore Training Room	Training Room Main Panel	Parameter "Online Status" has exceeded its configured threshold. The current value is "Offline".

FIG. 94 Hotlist Widget Data Grid

The default columns in the Hotlist Data Grid are described below:

Hotlist Widget Data Grid - Columns	
Default Columns	
Status Type (Icon)	These icons indicate the status of each Notification and Location. See the *Status Types* section on page 251 for details.
Occurrence	These timestamps display an occurrence timestamp in the current user's time zone.
Classification	This column provides the Classification levels assigned to each Location. Classification Levels allow you to classify Locations based on your own criteria. Classification Levels are arbitrary, and provide distinction between Locations in searches. See the *Location Classification* section on page 242 for details.
Location & Group Name	This column lists the names assigned to the Location associated with each Hotlist item. See the *Location Configuration (Classic UI)* section on page 242 for details.
Asset	This column lists the name of the Asset associated with each Hotlist item. See the *Management - Assets (Classic UI)* section on page 125 for details.
Summary	This text represents the verbiage entered by the originator of each Hotlist item.
Other Columns (selectable via the *Columns* drop-down menu)	
Use the *Columns* drop-down menu in the Hotlist toolbar to select specific columns to display in the Data Grid:	
Status Type (Name)	These names indicate the status of each Notification and Location. See the *Status Types* section on page 251 for details.
Date Occurrence	This column displays an occurrence timestamp in the current user's time zone.
Time Occurrence	This column displays an occurrence timestamp in the current user's time zone.
Location Name	This column lists the names assigned to the Location associated with each Hotlist item. See the *Management - Locations (Classic UI)* section on page 103 for details.
Location Group Name	This column lists the names assigned to the Location Group associated with each Hotlist item. See the *Management - Locations (Classic UI)* section on page 103 for details.
Asset Parameter Name	This column lists the Asset Parameter associated with each Hotlist item. See the *Management - Assets (Classic UI)* section on page 125 for details.

Hotlist Widget Data Grid Tooltips

Hovering over each cell on a Hotlist record displays supplemental information, relative to the selected Hotlist Item. (FIG. 95).

🖥	9:33 PM CDT May 22, 2011	Platinum	*Swinburne University* Building 1	System	Parameter "System Online" has exceeded its configured threshold. The current value is "Offline".
🔧	Location Communication Error (Priority Level: 75)	Platinum	*AMX Singapore* Singapore Training Room	Projector	Parameter "Lamp Hours" has exceeded its configured threshold. The current value is "402 Hours".

FIG. 95 Hotlist Widget Data Grid - Hotlist Item Tooltip

Hotlist Widget Context Menu

Right-click on a list item in the Hotlist Data Grid to access the Hotlist Context Menu. Note that options presented in this context menu vary depending on the selected item

Hotlist Widget Context Menu	
Assign Client Gateway:	Click to assign the selected new client system (Client Gateway) to a location, via the *Assign Client Gateway* dialog. This option is only visible for Hotlist Items that contain an unassigned Client Gateway. See the *Assigning a Client Gateway To a Location* section on page 98 for details.
Dismiss:	Click to dismiss the selected Hotlist item. When a Hotlist item is dismissed, it is permanently removed from the Data Grid. This option is only visible for Hotlist Items that support dismissal. See *Dismissing Hotlist Items* on page 68 for details.
Select As Dashboard Location:	Click to set the Location of the selected Hotlist Item as the Dashboard Location. This option is only visible for Hotlist Items that contain a Location
Disable Maintenance Mode:	Click to disable Maintenance Mode for the Asset or Location in the selected Hotlist Item. This option is only available for Hotlist Items that include an Asset or Location that is currently in Maintenance Mode, and only if the current user has the proper management permissions to disable the maintenance mode. • See the *Maintenance Mode for Locations* section on page 122 for details. • See the *Maintenance Mode for Assets* section on page 154 for details. • See the *System Maintenance Mode* section on page 210 for details.
Fulfill:	Click this option once a pending Service Request has been fulfilled. When this option is clicked, the selected Hotlist items are removed from the data grid, since they are no longer pending.
Send Message To Location:	Click to invoke the Asset Management page, to send a message to the Location associated with the selected Hotlist item. This action invokes the *Send Message* dialog. This option is only visible for Hotlist items that contain a Location. See *Sending a Message to a Location* on page 68 for details.
View Location:	Click to invoke the *Location page*, in which you can view/edit a selected Location's properties. This option is only visible for Hotlist items that contain a Location and where the authenticated user account has global Manage Clients and Location permission. See *Management - Locations (Classic UI)* on page 103 for details.
Refresh:	Refresh the data in this widget from the RMS Server.

Hotlist Data Grid Multi-Column Sorting

The Hotlist Data Grid supports multi-column sorting. Each column header displays a small number to represent the sorting order (FIG. 96).
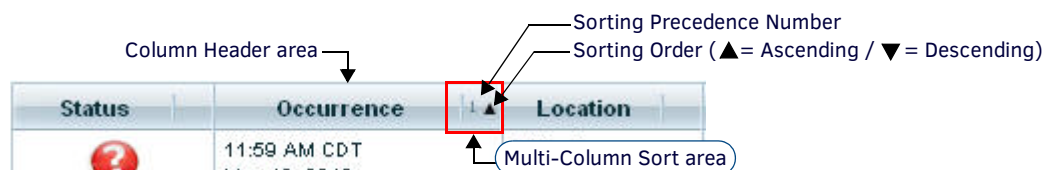
FIG. 96 Hotlist Data Grid - Column Header and Multi-Column Sort Areas

- Click in the Column Header area to sort the rows of Data Grid by that column.
- Click in the Multi-Column Sort area of the header to sort by additional columns.

The following example illustrates sorting three columns in the Data Grid:

1. Click the *Occurrence* Column Header area to start sorting:
   a. Click within the Multi-Column Sort area of the *Occurrence* column to arrange it in ascending order (indicated by an "up" arrow in the Multi-Column Sort area)
   b. Click the arrow again to toggle the sort to descending order (indicated by a "down" arrow in the Multi-Column Sort area).
2. Click in the Multi-Column Sort area of the *Location* column to arrange it in ascending order, while keeping the *Occurrence* column sorted in descending order.
3. Click in the Multi-Column Sort area for any other column header to include other columns in the sort.

To start over, click the Column Header area, and repeat steps 1 to 3.

NOTE: *Column sorting is stored and recalled with each user's personalization profile.*

Hotlist Status Type / Priority Sorting

A discrete *Hotlist Priority* value is assigned to each Status Type via options in the *Status Types* page of the *System Configuration* UI (*System Configuration > Asset Configuration > Status Types*). See the *Status Types* section on page 251 for details. When applying a sort on the *Status* column, Hotlist items are sorted based on the Hotlist priority values associated with each Status Type.

NOTE: *A Hotlist item may contain more than one status type, in which case the highest priority level is used for sorting.*

Hover the mouse cursor over the Status icon to display the Status Type name and Priority Level (FIG. 97):

FIG. 97 Hotlist Widget Data Grid - Status Details

Repositioning Columns in the Hotlist Data Grid

The columns in the Hotlist Data Grid can be repositioned by dragging the column header to a new position.

NOTE: *Column order is stored and recalled with each user's personalization profile.*

Specifying Columns in the Hotlist Data Grid

Use the *Columns* drop-down menu in the Hotlist Widget toolbar (see FIG. 92 on page 65) to specify the columns to display in the Hotlist Data Grid.

- Checkmarks in the drop-down menu indicate the columns that are currently displayed.
- See the Hotlist Widget Data Grid - Columns table on page 66.

NOTE: *Column selection is stored and recalled with each user's personalization profile.*

Dismissing Hotlist Items

Certain Hotlist Items can be dismissed. These typically include Hotlist items that require human interaction to resolve, such as Help and Maintenance requests received from clients. The dismissal of a Hotlist item permanently removes it from the Hotlist data grid. Selected Hotlist Items can be dismissed via the *Dismiss* button in the Hotlist Widget Toolbar (see FIG. 92 on page 65), or via the Hotlist Widget Context Menu (see page 67).

- The *Dismiss* option is enabled only when you have selected one or more Hotlist items that support dismissal.
- If multiple Hotlist items are selected, and one or more of the selected items are not eligible for dismissal, the Dismiss option is disabled.

NOTE: *Dismissing a Hotlist item is not the same as fulfilling a Service Request. Dismissal does not indicate that the request was fulfilled or resolved. See Removing Fulfilled Service Requests below.*

Resetting Asset Parameters for a Hotlist Item

Select one or more Hotlist Items that contain an asset and click the **Reset Asset Parameters** button in the Hotlist Widget Toolbar (see FIG. 92 on page 65).

This button is only enabled for Hotlist Items that contain an asset, and only if the authenticated user has the Manage permission to the selected asset location.

Removing Fulfilled Service Requests

Once a service request has been fulfilled, it can be removed from the data grid.

To remove a fulfilled (resolved) service request, select one or more service request items in the Hotlist data grid that are considered to be fulfilled, and select the **Fulfill** option from the Hotlist Widget Toolbar (see FIG. 92 on page 65) or the Hotlist Widget Context menu (see page 67).

Disabling Maintenance For Hotlist Items

Hotlist items that represent Locations or Assets that are currently in *Maintenance Mode* can be taken out of Maintenance Mode via options in the Hotlist Widget:

Select a Hotlist item that indicates "In Maintenance" (in the *Status* column), and select the **Disable Maintenance Mode** option from the Hotlist Widget Toolbar (see FIG. 92 on page 65) or the Hotlist Widget Context menu (see page 67).

This option is only enabled for Hotlist items that are currently in Maintenance Mode, and only if the currently authenticated user has the proper management permissions to disable Maintenance Mode.

- See the *Maintenance Mode for Locations* section on page 122
- See the *Maintenance Mode for Assets* section on page 154
- See the *System Maintenance Mode* section on page 210.

Sending a Message to a Location

You can send a message to a Location via options in the Hotlist Widget:

Select a Hotlist item that contains a Location, and select the **Send Message to Location** option from the Hotlist Widget Toolbar (see FIG. 92 on page 65) or the Hotlist Widget Context menu (see page 67).

This option is only enabled for Hotlist items that contain a Location.

Hotlist Item Properties Window

When a Hotlist item is selected in the Data Grid, additional details are displayed in the *Hotlist Item Properties* window (below the Data Grid). The *Hotlist Item Properties* window reveal additional information about the selected Hotlist item.

- Only tabs that contain relevant hotlist item related information are displayed.
- The tabs contains cross-links to provide shortcuts to relevant areas of the application.

Hotlist Item Properties Window - Details tab

FIG. 98 shows an example of the **Details** tab.
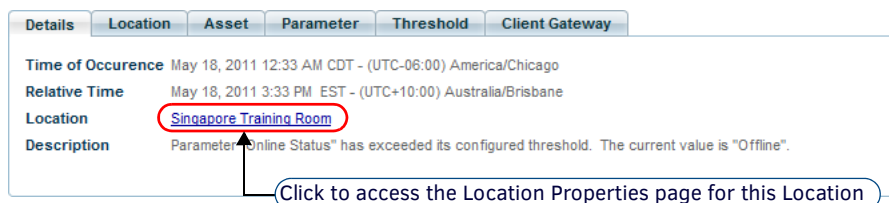
FIG. 98 Hotlist Widget Properties Window - Details tab

Hotlist Item Properties Window - Details tab Options	
Time of Occurrence	This field displays the time of occurrence for the selected Hotlist record in the current user's preferred time zone. • If the user has not configured a preferred time zone, then the time will be rendered in the default system time zone. • Absolute time is represented in the Hotlist Data Grid in the *Occurrence* column.
Relative Time	This field displays the time value relative to the Hotlist item. In other words, the time in the context of the source of the event that caused the Hotlist item. For example, in the case of System events (i.e. if a new client system is detected, or if an outbound communication error occurs), the Relative Time would be in the time zone of the server/system. In the case of Location sourced events (i.e. if a device parameter exceeded its threshold value), then the relative context time would be in the time zone of the Location.
Location	This field displays the Location of the selected Hotlist record in the form of a hyper link. Click this link to access the *Location Properties* page for the indicated Location. See the *Location Properties Page* section on page 108.
Description	This field provides a summary description of the selected Hotlist record.

Hotlist Item Properties Window - Location tab

FIG. 99 shows an example of the **Location** tab.
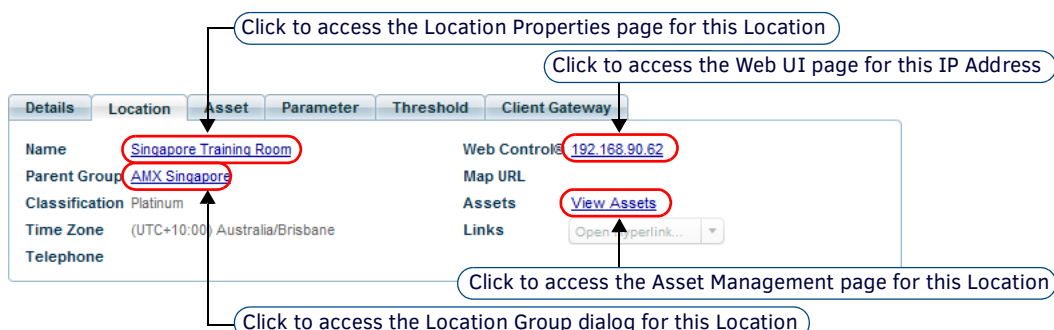
FIG. 99 Hotlist Widget Properties Window - Location tab

Hotlist Item Properties Window - Location tab Options	
Name	This hyperlink displays the name of the Location of the selected Hotlist record. Click the link to access the *Location Properties* page for the indicated Location. See the *Location Properties Page* section on page 108.
Parent Group	This hyperlink displays the Parent Group of the Location of the selected Hotlist record. Click the link to access the *Location Group* dialog for the indicated Location. The options in this dialog allow to select a different Parent Group or Location. See the *Management - Locations (Classic UI)* section on page 103 for details.
Classification	This field displays the Classification level assigned to the Location of the selected Hotlist record. Classification Levels allow you to classify Locations based on your own criteria. Classification Levels can provide distinction between Locations in searches. See the *Location Classification* section on page 242 for details.
Time Zone	This field displays the time zone associated with the Location of the selected Hotlist record.
Telephone	This field displays the telephone number associated with the Location of the selected Hotlist record, if one has been specified in the *Location Properties Page - Settings Tab* (see page 108).
Web Control®	This hyperlink displays the IP address of the AMX Web Control page associated with the Location of the selected Hotlist record. AMX Web Control provides quick access to any HTML based control panels that may have been programmed into the NetLinx system (or non-NetLinx system, such as CP-3000 keypads, which also send a web page URL). Click the link to open the Web Control page in a new browser window. See the *Using Web Control for a Location* section on page 124 for details.
Map URL	This hyperlink displays the Map URL associated with the Location of the selected Hotlist record, if one has been specified in the *Location Properties Page - Settings Tab* (see page 108). Click the link to open the Map URL in a new browser window.

Hotlist Item Properties Window - Location tab Options (Cont.)	
Assets	Click the *View Assets* hyperlink to access the Asset Management page for the Location of the selected Hotlist record. See the *Management - Assets (Classic UI)* section on page 125 for details.
Links	Click to open a drop-down menu of user-defined links in the Location metadata.

Hotlist Item Properties Window - Asset tab

FIG. 100 shows an example of the **Asset** tab.
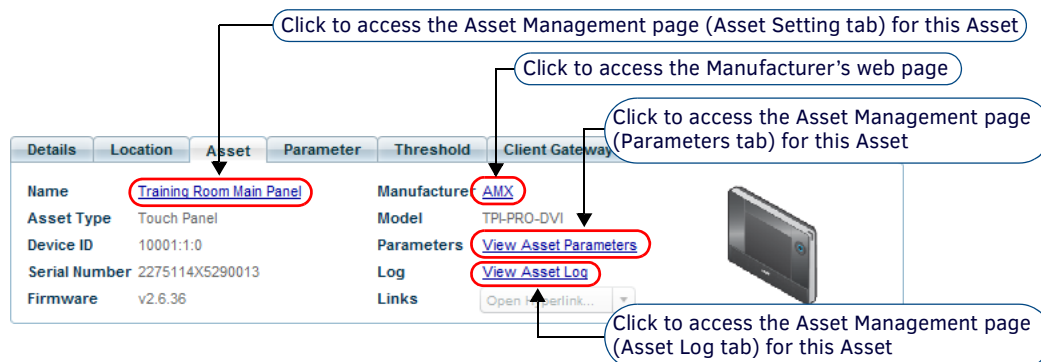
FIG. 100 Hotlist Widget Properties Window - Asset tab

Hotlist Item Properties Window - Asset tab Options	
Name	This hyperlink displays the name of the Asset in the selected Hotlist record. Click the link to access the *Asset Management* page for the indicated Asset. See the *Management - Assets (Classic UI)* section on page 125 for details.
Asset Type	This field displays the asset type associated with the Asset in the selected Hotlist record.
Device ID	This field displays the Device ID (D:P:S) assignment of the Asset in the selected Hotlist record.
Serial Number	This field displays the Serial Number associated with the Asset in the selected Hotlist record.
Firmware	This field displays the Firmware version Number associated with the Asset in the selected Hotlist record.
Manufacturer	This hyperlink displays the name of the Manufacturer associated with the Asset in the selected Hotlist record. Click the link to access the web page for the indicated Manufacturer in a new browser window.
Model	This field displays the Model (name) associated with the Asset in the selected Hotlist record.
Parameters	Click *View Asset Parameters* to open the Asset Management page - *Parameters* tab for the Asset in the selected Hotlist record. See the *Asset Properties page - Parameters Tab* section on page 134 for details.
Log	Click View Asset Log to open the Asset Management page - *Asset Log* tab for the Asset in the selected Hotlist record. See the *Asset Properties page - Asset Log Tab* section on page 136 for details.
Links	Click to open a drop-down menu of user-defined links in the Asset metadata.

Hotlist Item Properties Window - Parameter tab

FIG. 101 shows an example of the **Parameter** tab.
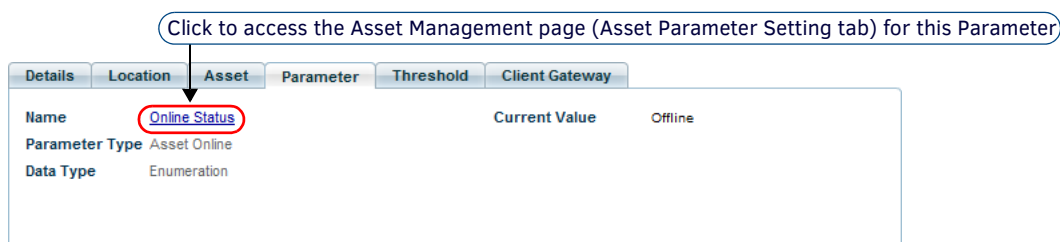
FIG. 101 Hotlist Widget Properties Window - Parameter tab

Hotlist Item Properties Window - Parameter tab Options	
Name	This hyperlink displays the name of the parameter in the selected Hotlist record. Click the link to access the *Asset Parameter Properties* page (*Asset Parameter Settings* tab) for the indicated parameter. See the *Asset Parameter Properties Page - Asset Parameter Setting Tab* section on page 139 for details.
Parameter Type	This field displays the type associated with the parameter in the selected Hotlist record.
Data Type	This field displays the data type of the parameter in the selected Hotlist record. See the *Metadata Data Types* section on page 227 for details.
Current Value	This field displays the current value of the parameter in the selected Hotlist record.

Hotlist Item Properties Window - Threshold tab

FIG. 102 shows an example of the **Threshold** tab.

Double-click to access the Parameter Threshold Editor dialog for this Parameter
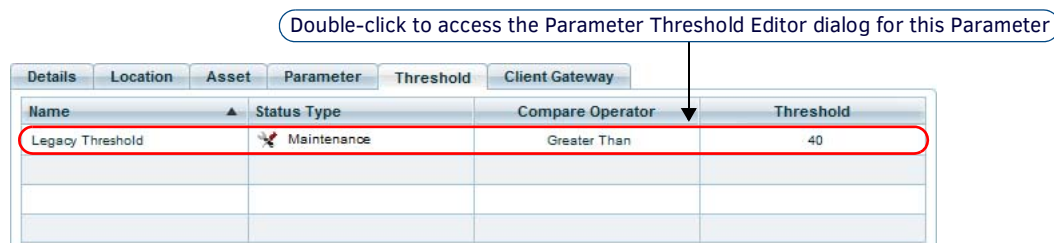
FIG. 102 Hotlist Widget Properties Window - Threshold tab

This tab presents the following threshold information for the parameter in the selected Hotlist record in a four-column table.

Hotlist Item Properties Window - Threshold tab Options	
Name	This column displays the name of each parameter threshold.
Status Type	This column displays the status type of each parameter threshold. See the *Status Types* section on page 251 for details.
Compare Operator	This column displays the compare operator of each parameter threshold.
Threshold	This column displays the threshold for of each parameter (as specified in the *Asset Parameter Properties* Page). See the *Asset Parameter Properties Page* section on page 139 for details.

Double-click any threshold in this tab to access the *Parameter Threshold Editor* dialog for the selected threshold. See the *Parameter Threshold Editor Dialog* section on page 143 for details.

Hotlist Item Properties Window - Client Gateway tab

FIG. 103 shows an example of the **Client Gateway** tab.

FIG. 103 Hotlist Widget Properties Window - Client Gateway tab

Hotlist Item Properties Window - Client Gateway tab Options	
Client Name	This field displays the name of the Location associated with the Client Gateway in the selected Hotlist record.
Client UID	This field displays the UID (Unique Identifier) associated with the Client Gateway in the selected Hotlist record.
IP Address	This field displays the IP Address of the Client Gateway in the selected Hotlist record.
IP Port	This field displays the IP Port used by the Client Gateway in the selected Hotlist record.
MAC Address	This field displays the MAC Address of the Client Gateway in the selected Hotlist record.
RMS SDK Version	This field displays the version number of the RMS SDK used by the Client Gateway in the selected Hotlist record.
RMS SDK Protocol	This field displays the RMS SDK protocol used by the Client Gateway in the selected Hotlist record.
RMS SDK Protocol Version	This field displays the version number of the RMS SDK protocol used by the Client Gateway in the selected Hotlist record.
Communication Active	This field indicates the current state of communication for the Client Gateway in the selected Hotlist record (*true* = connected, *false* = disconnected).

Closing the Hotlist Item Properties Window

The Hotlist Item Properties window can be closed by clicking on the arrow icon on the right side above the detail panel (FIG. 104):
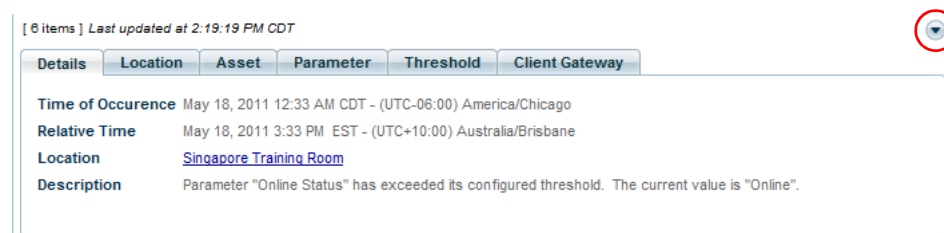
FIG. 104 Hotlist Widget Properties Window - Close button

When closed, Hotlist Item Properties information is not obtained from the RMS server.

NOTE: *The open / close state of the Hotlist Item Properties window is stored and recalled with each user's personalization profile.*

Asset Power Consumption Widget
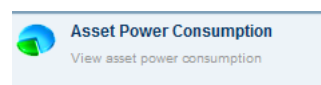
FIG. 105 Asset Power Consumption Widget Icon (Available Widgets window)

The *Asset Power Consumption* widget is a location-based widget that displays a summary of energy consumption for the currently selected Location, by Asset Type. This widget provides a *Data* view as well as a *Graph* view of the energy consumption data (FIG. 110).
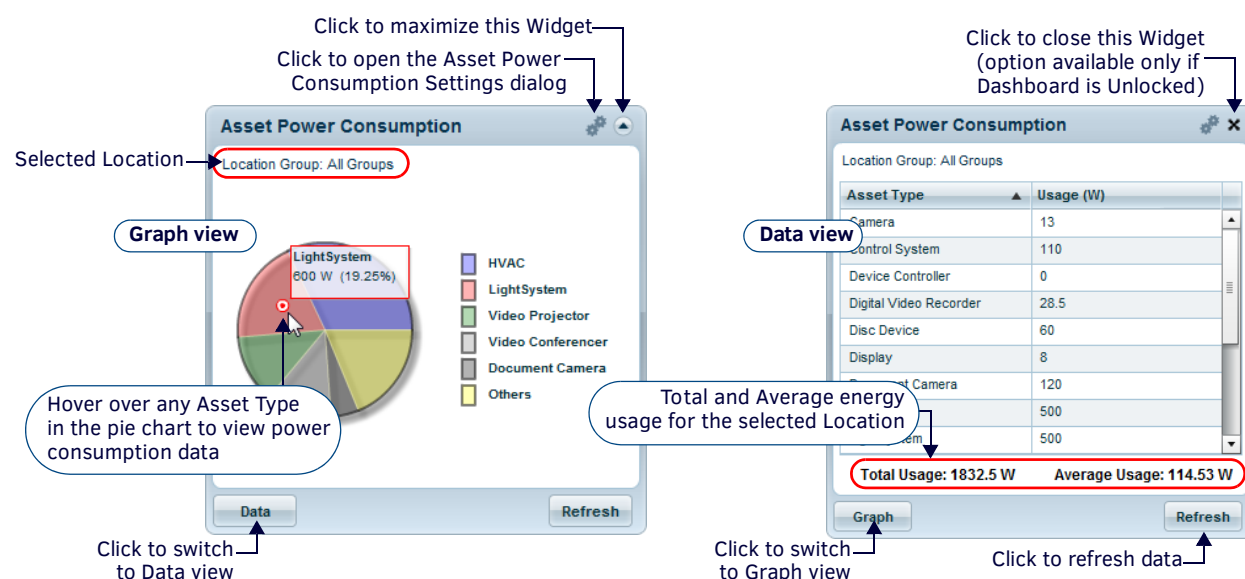
FIG. 106 Asset Power Consumption Widget

Click the **Data**/**Graph** button to toggle the view between the data grid and a pie-chart view:

- **Data** view displays the Usage (in Watts) for each Asset Type, as well as *Total Usage* and *Average Usage* statistics for the selected Location.
- **Graph** view displays energy consumption data for the selected Location in the form of a pie chart, showing the percentage of overall consumption for each Asset Type in the Location.

   NOTE: *Hover over any area in the pie chart to view power consumption data for that Asset Type.*

Click **Refresh** to refresh the data.

- This widget automatically updates its data when a new Location is selected.
- This widget polls the RMS Server for updated listings every 60 seconds for power status.
- By default, it displays energy consumption data for the past 7 days.

Configuring the Asset Power Consumption Widget

By default, the *Asset Power Consumption* widget displays data on the Location currently selected on the Dashboard. The options in *Asset Power Consumption Settings* dialog allow you to specify a Location Group or Location to display instead:

1. Click the *Configuration* button in the upper-right corner of the widget's title bar (see FIG. 106 on page 72) to access the *Asset Power Consumption Settings* dialog (FIG. 107). Note that by default, **Show Dashboard selected location** is selected.
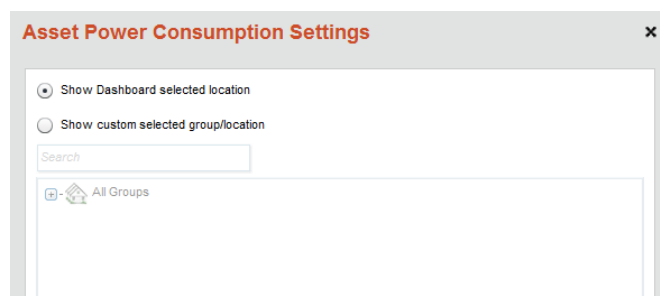
FIG. 107 Asset Power Consumption Settings dialog

2. Click **Show custom selected group/location** to enable the Location Groups selection window shown in FIG. 108:
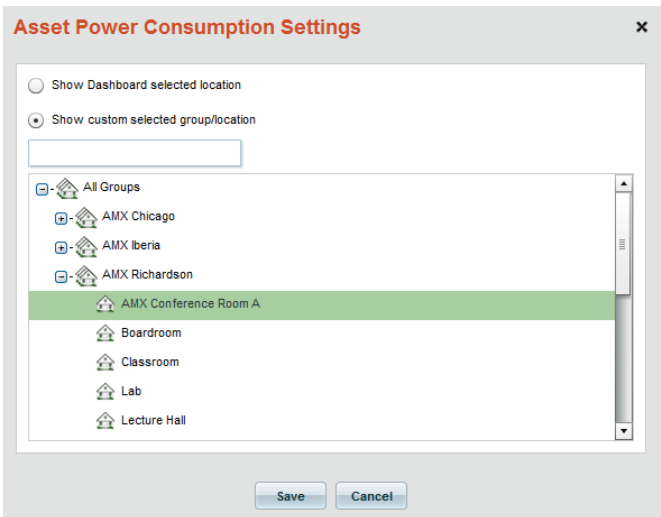
FIG. 108 Asset Power Consumption Settings dialog

> Use the *Search* window to search for a Location Group or Location name.

3.   Select a Location Group or Location.

4.   Click **Save** to save your changes and close this dialog.

Note that the selected Location is indicated in the Widget (see FIG. 106 on page 72).

Control Macro Schedule Widget

FIG. 109 Control Macro Schedule Widget Icon (Available Widgets window)

The *Control Macro Schedule* widget is a location-based widget that displays a listing of Control Macro Schedules specific to the currently selected Location (FIG. 110).
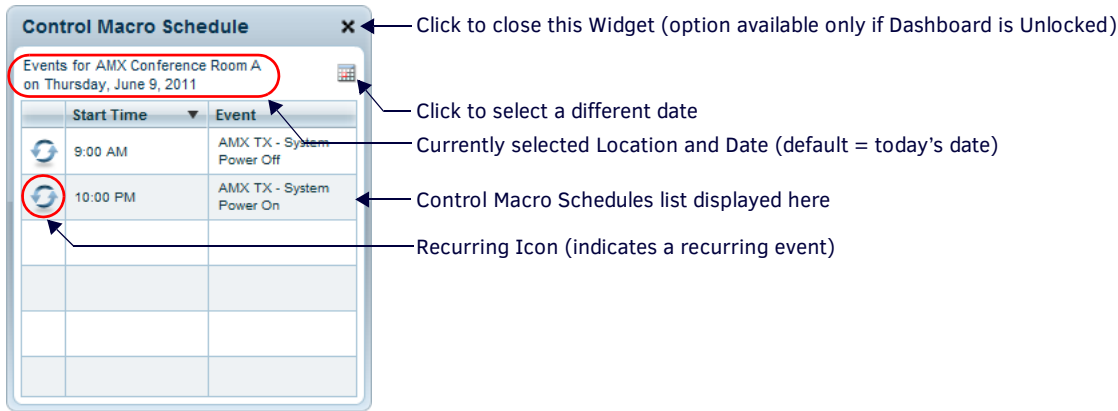
FIG. 110 Control Macro Schedule Widget

The *Control Macro Schedule* widget provides a listing of scheduled control macro events for the selected Location.

- This widget automatically updates data when a new Location is selected.
- Recurring Control Macro Schedules are indicated by the *Recurring* icon.

Changing the Selected Date

By default the data shown in the widget is for today's date. The user can change the Date and the content will update accordingly:

1.   Click the calendar icon in the upper-right corner of the widget. This opens a pop-up calendar (FIG. 111):
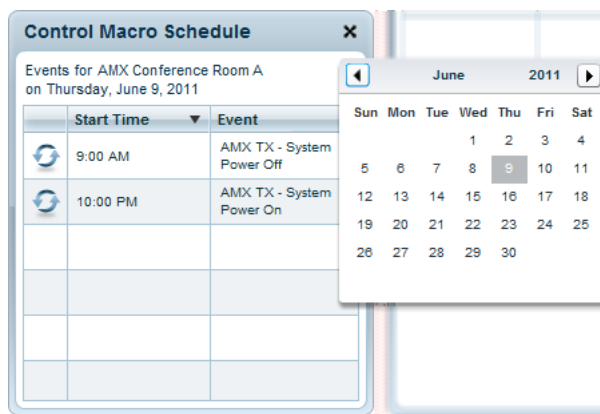
Click on a date to close the calendar

FIG. 111 Control Macro Schedule Widget with Pop-Up Calendar

2. Click on the desired date to close the calendar and update the *Control Macro Schedule* widget.

Editing a Control Macro Schedule

Double-click on a Control Macro Schedule in this widget to open the control macro management pages to the editor view for the selected macro (only if the user has control macro global permissions).

See the *Management - Control Macros (Classic UI)* section on page 165 for details.

Control Macro Schedule Context Menu

Right-click on a Control Macro Schedule listing to display a context menu with the following options:

Control Macro Schedule Context Menu	
View Control Macro	Open the control macro management pages to the editor view for the selected macro (only if the user has control macro global permissions). See the *Management - Control Macros (Classic UI)* section on page 165 for details.
Refresh	Refresh the data in this widget from the RMS Server.

Favorite Links Widget

FIG. 112 Favorite Links Widget Icon (Available Widgets window)

The *Favorite Links* widget allows users to save custom URL bookmarks for quick and convenient access (FIG. 113).

Configuration - click to open the *Favorite Link Settings* dialog

Click to close this Widget (option available only if Dashboard is Unlocked)

Clink Links to open bookmarks in a new browser window

Hover over a link to view the URL information
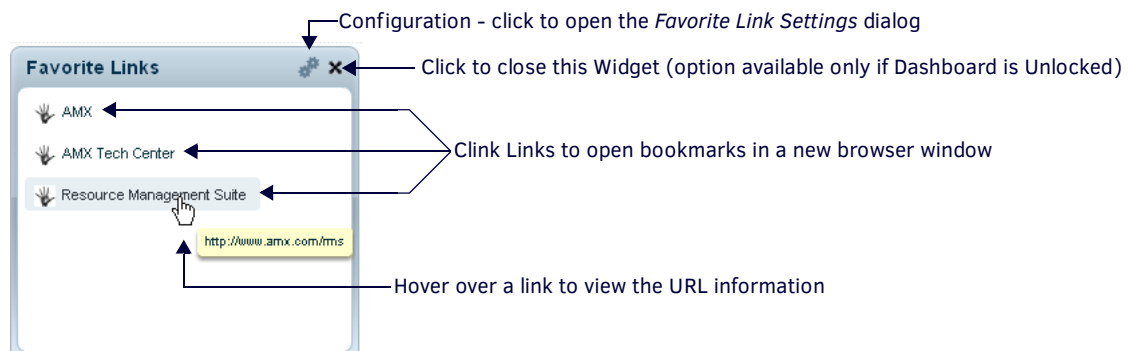
FIG. 113 Favorite Links Widget

Click a bookmark link to open a new web browser window and navigate to the desired page URL. Hover over the link to display the raw URL as a tool-tip.
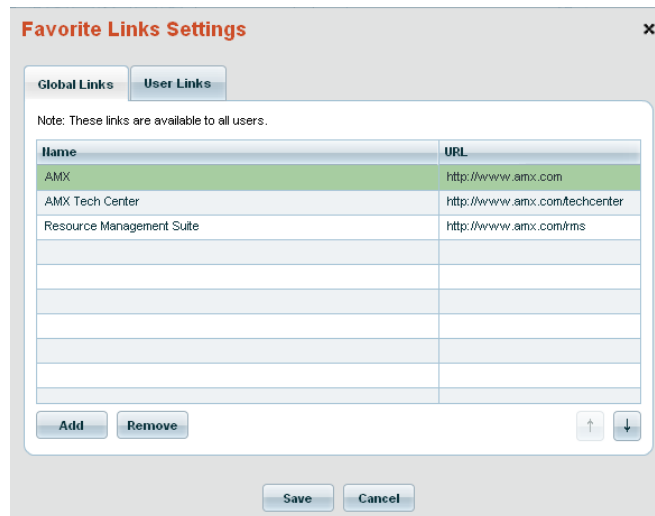
Global Links vs User Links

There are two types of Favorites links:

- *Global* links are available to all users. Global links can only be edited by users that have global system configuration permissions assigned. See the *Management - Roles (Classic UI)* section on page 192 for details on configuring Global System Permissions for users.
- *User* links are available only to the individual authenticated user.

Adding a Favorite Link

1. Click the *Configuration* button in the upper-right corner of the widget's title bar (see FIG. 113 on page 74) to access the *Favorite Links Settings* dialog.

2. If the currently authenticated user has global system configuration permissions assigned, the initial view is the **Global Links** tab (FIG. 114):
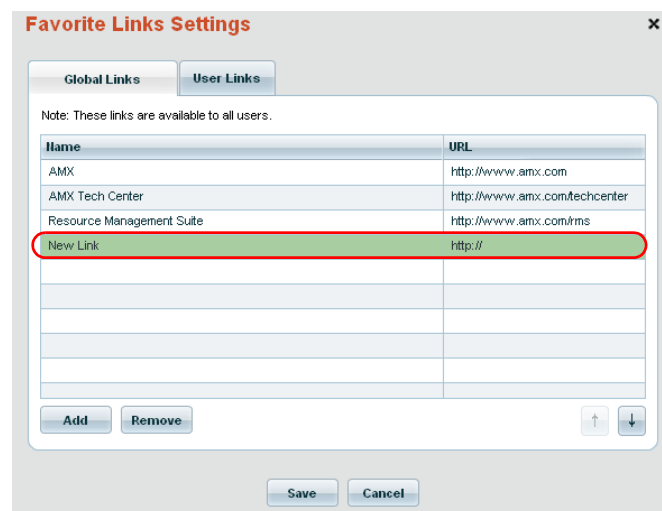
FIG. 114 Favorite Links Settings dialog - Global Links tab

If the current user does not have global system configuration permissions assigned, then only the **User Links** tab (FIG. 115) is displayed.

3. In either the **Global Links** or the **User Links** tab, click the **Add** button. This action adds a new highlighted entry to the Favorites list, initially named "*New Link*" (FIG. 115).

FIG. 115 Favorite Links Settings dialog - new Global Link entry

4. Click the new entry in the *Name* column and enter the name of this link, as it will be displayed in the *Favorite Links* widget.

5. Click in the *URL* column and enter the URL information for the new link (FIG. 116).
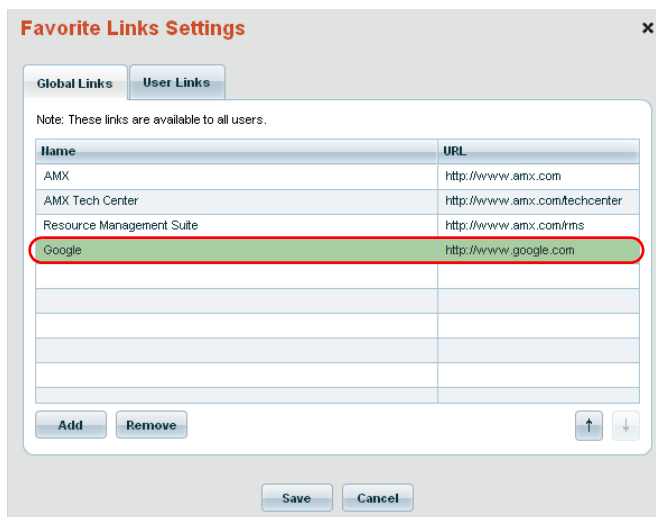
FIG. 116 Favorite Links Settings dialog – Entering new Link information

6.   Click **Save** to save the new Link.

At this point the new Link is displayed in the *Favorite Links* widget (FIG. 117):

FIG. 117 Favorite Links widget – showing new link

Removing a Favorite Link

1.   Click the Configuration button in the title bar of the Favorite Links widget (see FIG. 113 on page 74) to open the *Favorite Links Settings* dialog.

2.   Select a link.

3.   Click **Remove**.

4.   Click **Save**.

The link is now removed from the *Favorite Links* widget.

Lamp Life Widget

FIG. 118 Lamp Life Widget Icon (Available Widgets window)

The *Lamp Life* widget is a location-based widget that displays a listing of all assets and lamp-based asset parameters specific to the currently selected Location (FIG. 119).
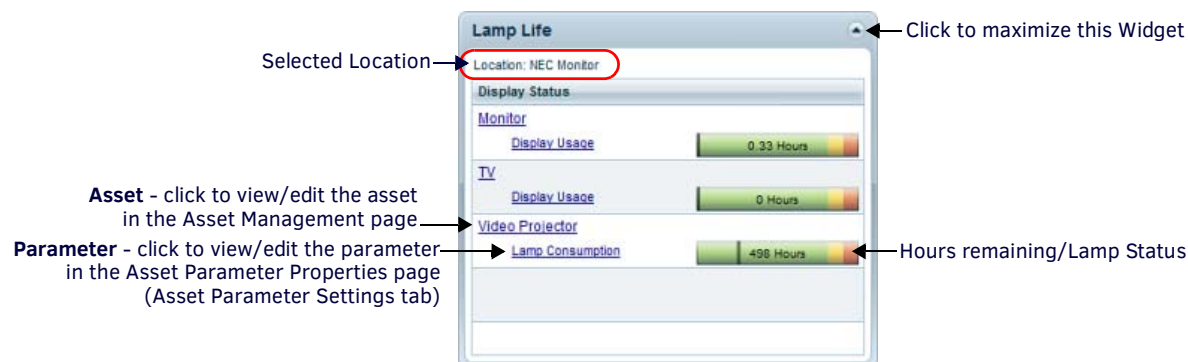
FIG. 119 Lamp Life Widget

The Lamp Life widget displays a listing of assets that have parameters of **PARAMETER_TYPE == LAMP_USAGE**. This includes *Video Projectors* (showing Lamp Consumption), *Monitors* (showing Display Usage, and *TVs* (also showing Display Usage).

- This widget automatically updates its data when a new Location is selected.
- This widget polls the RMS Server for updated listings every 60 seconds.

The data grid on the Lamp Life widget displays the following information, specific to the selected Location:

Lamp Life Widget	
Asset (hyperlink)	The name of each Asset contained in the selected Location (default = *Display*). Click on this link to view/edit the asset in the *Asset Management* page (see the *Management - Assets (Classic UI)* section on page 125 for details).
Parameter (hyperlink)	The name of the Parameter associated with each Asset (default = *Lamp Hours*). Click on this link to view/edit the parameter in the *Asset Properties* page - **Asset Parameter Settings** tab (see the *Working With Asset Parameters* section on page 158 for details).
Hours Remaining	Estimated time remaining on the lamp based on the expected lamp life.
Lamp Status	The estimated time remaining is indicated with color-coded bargraphs: If the lamp is past the established threshold, it displays the message "*Replace Lamp*" in red.

Location Control Widget

FIG. 120 Location Control Icon (Available Widgets window)

The *Location Control* widget is a location-based widget that displays a tree listing of assets and asset control functions specific to the currently selected Location (FIG. 121).
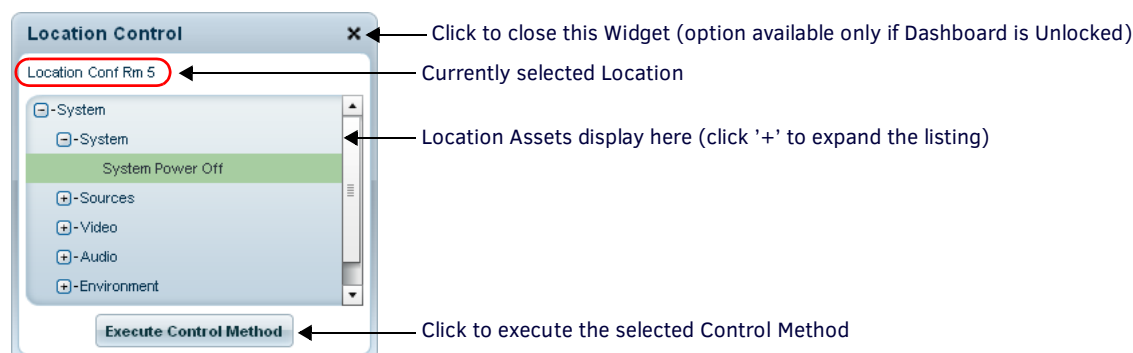
FIG. 121 Location Control Widget

NOTE: *This widget automatically updates data when a new Location is selected.*

Use this widget to execute control functions on the Assets that belong to the selected Location.

Executing a Control Method for an Asset

1.   Click the + sign next to *System* to show all Asset Types that have been assigned to this Location (FIG. 122).
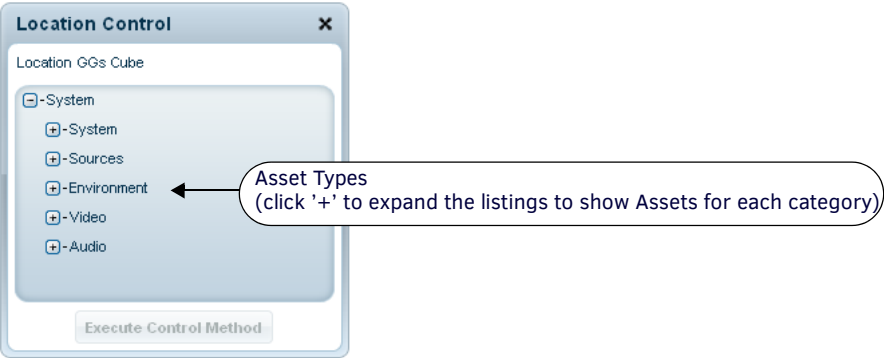
FIG. 122 Location Control Widget showing Asset Types for the selected Location

2.   Click the + sign next to any of the *Asset Types* to list the Assets in that category.

3.   Click the + sign next to any of the *Assets* to list the Control Methods assigned to that device, if necessary.

4.   Select a Control Method and click the **Execute Control Method** button (FIG. 123):
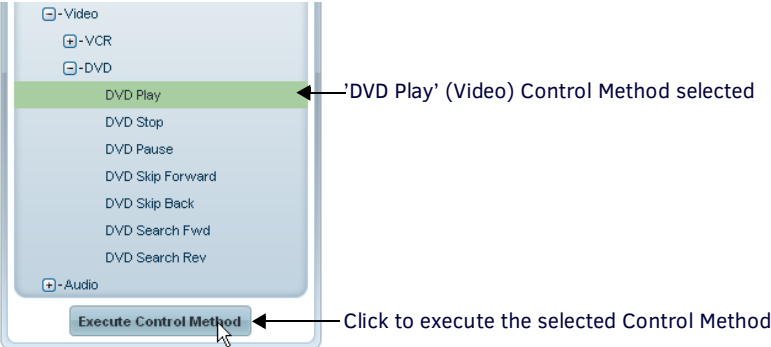
FIG. 123 Location Control Widget executing the 'DVD Play' Control for 'DVD'

NOTE: *The system will prompt for any required function arguments (parameters) if necessary.*

Control Method Context Menu

Right-click on a Control Method listing to display a context menu with the following options:

Location Control Widget Context Menu	
Execute Control Method	Executes the selected Control Method.
Refresh	Refresh the data in this widget from the RMS Server.

Location Energy Consumption Widget

FIG. 124 Location Energy Consumption Widget Icon (Available Widgets window)

The *Location Energy Consumption* widget displays a cumulative listing of the energy usage in the selected Location, according to the selected time interval. There are two views available for this widget: *Graph* and *Data*. Click the **Graph/Data** button to toggle the view (FIG. 125).
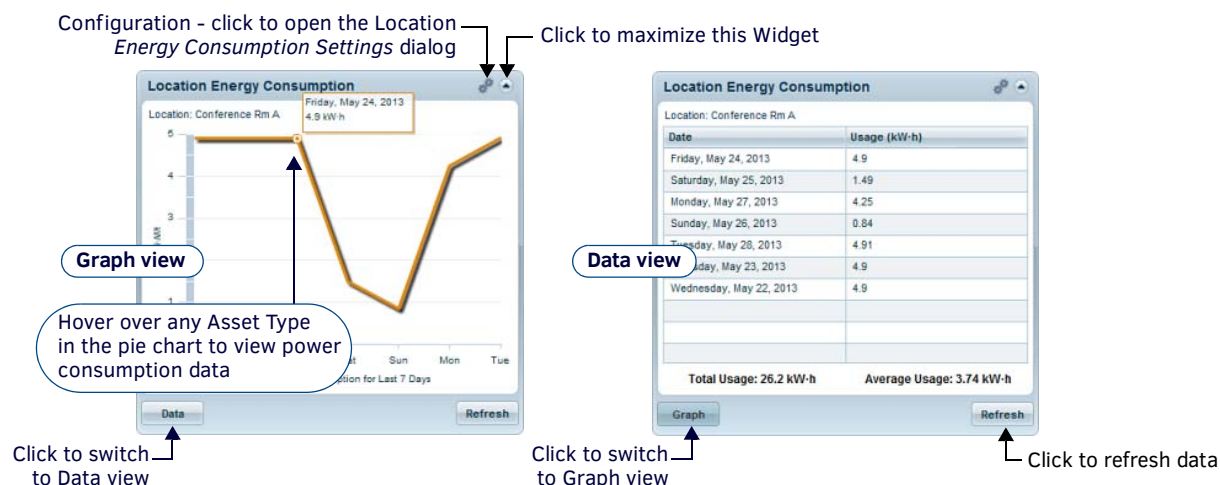
FIG. 125 Location Energy Consumption Widget

Click the **Data/Graph** button to toggle the view between the data grid and a line-chart view:

- **Data** view displays energy consumption data for the selected Location in the form of a data grid. The data grid provides energy usage data (kW/h by date) as well as *Total Usage* and *Average Usage* statistics for the selected Location.
- **Graph** view displays energy consumption data for the selected Location in the form of a line graph.

  The line graph shows energy consumption over the Time Interval specified in the *Location Energy Consumption Settings* dialog (see *Configuring the Location Energy Consumption Widget* below).

  NOTE: *Hover the mouse cursor over a peak or low-point on the graph to view a time stamp for that point in the graph.*

Click **Refresh** to refresh the data. This option is only available to users with manage asset permissions to this location.

- This widget automatically updates its data when a new Location is selected.
- This widget polls the RMS Server for updated listings every 60 seconds for power status.
- By default, it displays energy consumption data for the past 7 days.

Configuring the Location Energy Consumption Widget

The *Location Energy Consumption Settings* widget displays data on the Location currently selected on the Dashboard, in specific time intervals. The options in *Asset Power Consumption Settings* dialog allow you to specify a Location Group or Location to display instead, as well as specify a different time interval for the line graph:

1. Click the *Configuration* button in the upper-right corner of the widget's title bar (see FIG. 125 on page 79) to access the *Location Energy Consumption Settings* dialog. Note that by default, **Show Dashboard selected location** is selected.
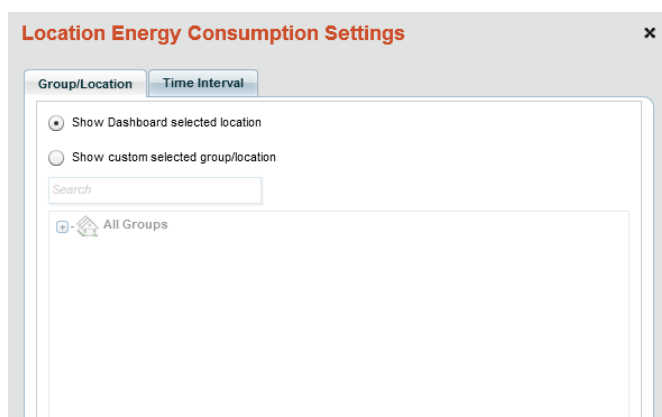
FIG. 126 Location Energy Power Consumption Settings dialog

2. Click **Show custom selected group/location** to enable the Location Groups selection window shown in FIG. 127:
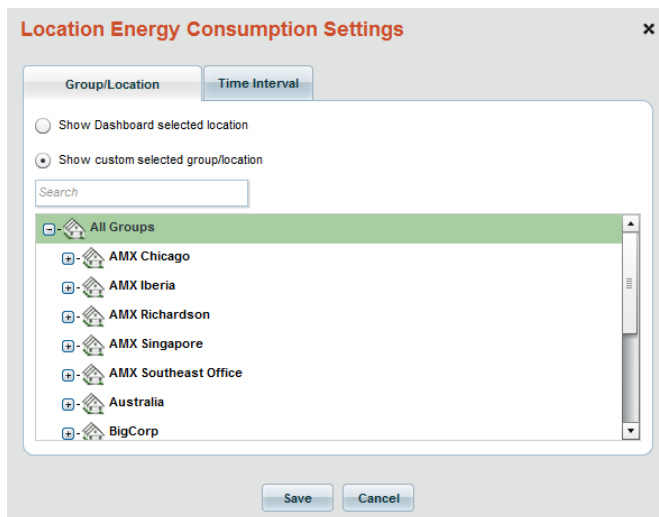
FIG. 127 Location Energy Consumption Settings dialog - Group/Location tab

3.   In the **Time Interval** tab (FIG. 128), the default setting is **Last 30 Days**. This setting displays location energy usage data for the past 30-day period only. The other options on this tab are *Last 7 Days*, *Last 12 Months*, and *Last 7 Years*.
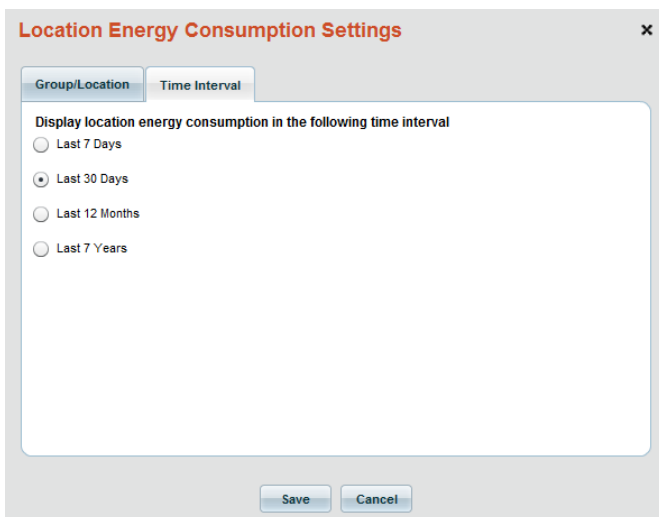
FIG. 128 Location Energy Consumption Settings dialog - Time Interval tab

Select the desired time interval for the location energy consumption data displayed in this widget.

4.   Click **Save** to save your changes and close this dialog.

Source Usage Widget

FIG. 129 Source Usage Widget Icon (Available Widgets window)

The *Source Usage* widget is a location-based widget that displays a listing of all source usage devices, their usage time in hours, and a relative percentage of consumption related to all other sources. There are two views available for this widget: *Graph* and *Data*. Click the **Graph**/**Data** button to toggle the view (FIG. 130).
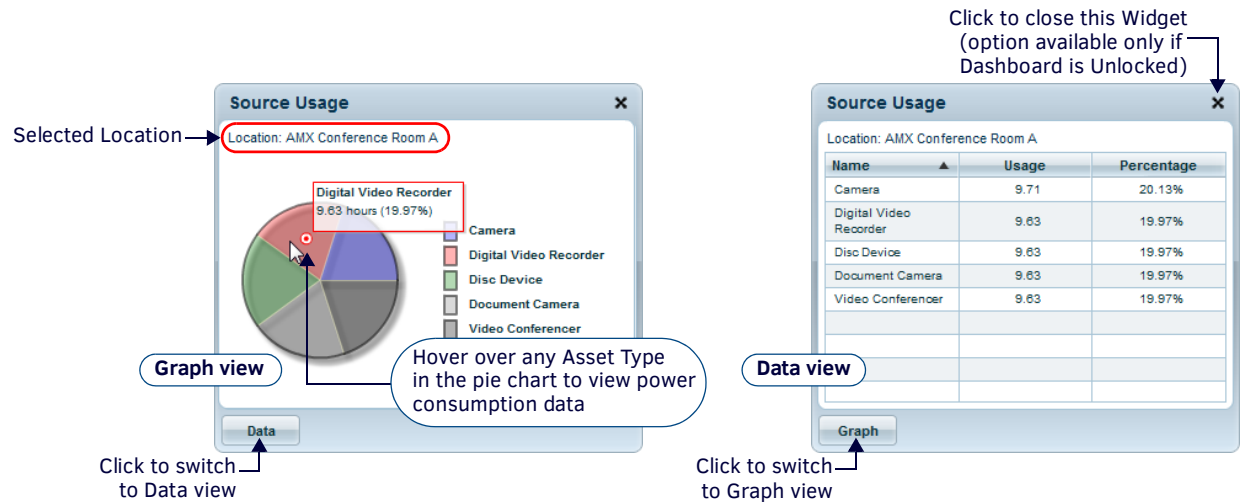
FIG. 130 Source Usage Widget

Click the **Data**/**Graph** button to toggle the view between the data grid and a pie-chart view:

- **Data** view displays Source Usage data for the selected Location in the form of a data grid. The data grid provides source usage data in hours and percentage of overall usage for the selected Location.
- **Graph** view displays energy consumption data for the selected Location in the form of a pie chart, showing the percentage of overall consumption for each Asset Type in the Location.

NOTE: *Hover over any area in the pie chart to view power consumption data for that Asset Type.*

Click **Refresh** to refresh the data.

- This widget automatically updates its data when a new Location is selected.
- This widget polls the RMS Server for updated listings every 60 seconds for power status.

System Status Widget
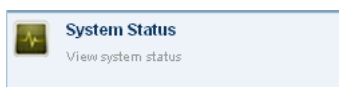
FIG. 131 System Status Widget Icon (Available Widgets window)

The *System Status* widget displays location-level information across multiple Locations, to provide a comparison view at a glance. All System Status items are displayed in this widget (FIG. 132).
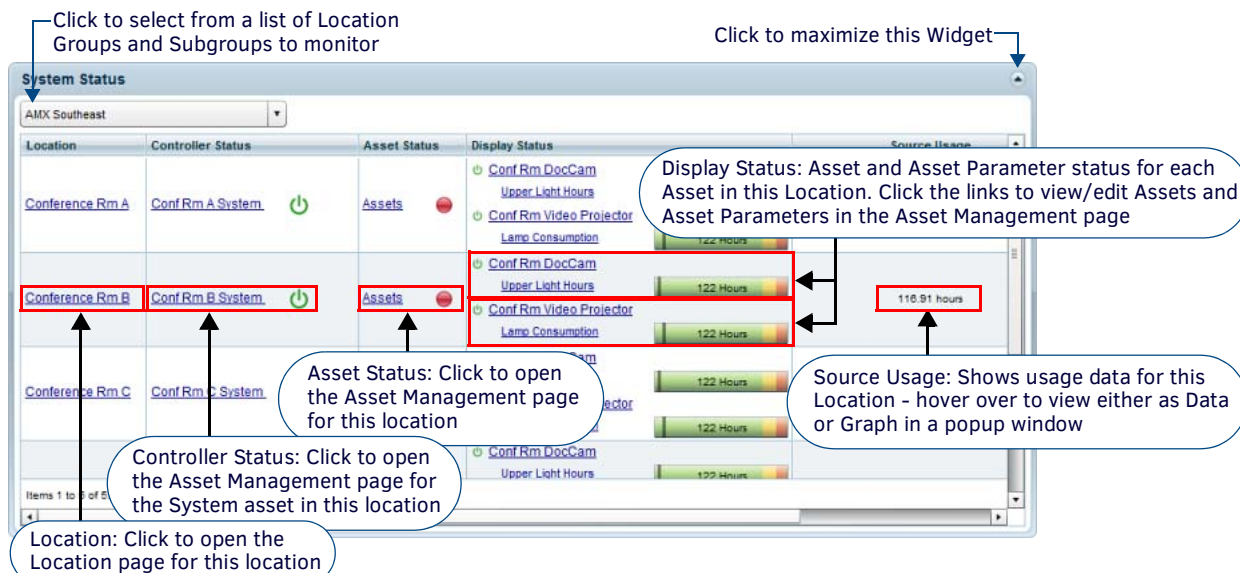
FIG. 132 System Status Widget

NOTE: *When a user logs into RMS, System Status data is limited to Location Groups and Locations that are relevant to the authenticated user, based on the user's permissions settings. See the Management - Roles (Classic UI) section on page 192 for information on setting user Permissions.*

The System Status data grid provides system information in the following columns:

System Status Widget Data Grid	
Location:	Click to open the *Location* page with this Location pre-selected to view/edit (see the *Management - Locations (Classic UI)* on page 103 for details).
Controller Status:	Click to open the *Asset Management* page with this system asset pre-selected to view/edit (see the *Management - Assets (Classic UI)* section on page 125 for details). The Power status indicates the asset's current power status (green = on, red = off).
Asset Status:	Click to open the *Asset Management* page to view/edit a listing of all Assets for this Location (see the *Management - Assets (Classic UI)* section on page 125 for details). The Communication status icon indicates the asset's current communication status (*Online* or *Offline*).
Display Status:	Click the *Asset* link to open the *Asset Management* page to view/edit this asset in the *Asset Management* page (see the *Management - Assets (Classic UI)* section on page 125 for details). Click the *Asset Parameter* link to view/edit the selected asset parameter, in the *Asset Parameter Properties* page - **Asset Parameter Settings** tab).See the *Working With Asset Parameters* section on page 158 for details. The bargraphs indicate the current usage value for each asset parameter. Hover over the bargraph to view the *Current Value* and the *Max Value* for each parameter in a text popup window.
Display Status (Cont.):	
Source Usage:	This columns a summary of usage in hours for each Asset.

NOTE: *This widget is a center content widget - it can only be placed in the center area of the Dashboard.*

Source Usage Popup Window

Hover the mouse cursor over any cell in the **Source Usage** column to display detailed Source Usage information for that Location in a popup window. This popup is essentially the same as the *Source Usage* widget (see page 81), but it is specific to the Location in the selected System Status item. There are two views available for this popup window: *Data* (default) and *Graph.* Click the **Data** button to toggle to Graph view, and vice-versa. Click the close icon in the upper-right corner of the window to close the Source Usage popup.

System Status Widget Context Menu

Right-click on an item in the System Status data grid to access the System Status Widget Context Menu:

System Status Widget Context Menu	
Select As Dashboard Location	This option selects the current Location for location-oriented widgets.
Send Message To Location	This option sends a message to the selected Location. See the *Sending a Message to a Location* section on page 116 for details.
View Location	This option opens the *Location Properties* page for the selected Location. See the *Location Properties Page* section on page 108 for details.
View Location Assets	This option opens the *Edit Assets* page for the selected Location. See the *Management - Assets (Classic UI)* section on page 125 for details.
Refresh	Click to refresh the data in this widget.

Dashboard - My Profile (Classic UI)

Overview

Select **My Profile** in the (Classic UI) *Dashboard* menu to open the *My Profile* page (FIG. 133):
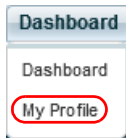
FIG. 133 Dashboard Menu - My Profile

NOTE: *To access the RMS Classic UI described in this section, select "Classic UI" from the RMS Enterprise HTML interface menu bar.*

The My Profile page contains several tabs - *General Setting*, *My Contacts*, *Notification Schedule* and *My Notifications* (FIG. 134).

FIG. 134 My Profile page

User Profiles - Personalization

Each user account defined in the RMS system maintains its own discrete set of user preferences.

NOTE: *The RMS HTML interface (see page 20) is not customizable.*

The following aspects of the RMS Classic UI can be personalized for each user:

User Personalization (Classic UI)	
Dashboard	• Selected widgets • Widget layout • Widget height • Column widths • Selected location
Hotlist	• Details preview pane collapsed/expanded • Optional display columns • Multiple column sorting order or sorting direction
Favorite Links	User preferred URL listing
All horizontal and vertical resizing splitter containers	Splitter position

User Personalization (Classic UI - Cont.)	
All data grids	• Column widths • Column position (order) • Column(s) sorted by • Sort direction

When making a change to the Classic UI that causes the user personalization to be updated, it may take up to 10 seconds for the changes to be persisted on the RMS server. Thus, if a user makes a change to the UI and then immediately closes the web browser, the user preference may not have time to be properly persisted before the application is unloaded from memory.

All changes are immediately propagated to the RMS server when the user logs out.

User Profiles - Persistence

Each user account defined in the RMS system maintains its own discrete set of user preferences.

The exception is the *Guest* account. Since the "Guest" account is not a distinct user account, it instead persists its settings to a local computer cache rather than the RMS database. This allows unique "Guest" personalization on a computer basis, and prevents multiple "Guest" users from affecting the UI experience of other "Guest" users.

NOTE: *The Guest account is only available for installed RMS Servers; it cannot be enabled for AMX Cloud hosted services.*

A user's personalization settings can be reset to default in the User Management pages (via the *Reset User Preferences* option) while editing a user's profile. This same option is also available to each user under their 'My Profile' management pages.

My Profile - General Setting Tab

Use the **General Setting** tab of the *My Profile* page to manage and view general user settings for this user (FIG. 135):

FIG. 135 My Profile page - General Setting tab

The options in the *My Profile* page - **General Setting** tab (FIG. 135) are described below:

My Profile - General Setting Tab Options	
Account Enabled	This checkbox determines whether this account is enabled or not. • By default, all user accounts are enabled. • De-select this checkbox to disable this user account. *Note: This option is not available in the System Administrator user account.*
First Name	Enter the user's first name in this text field (*required*).
Last Name	Enter the user's last name in this text field (*required*).
Username	Enter the username (for this user's login credentials) in this text field (*required*).
Password	Enter the Password (for this user's login credentials) in this text field (*required*).
Re-Type Password	Re-enter the Password (for verification) in this text field (*required*).

My Profile - General Setting Tab Options (Cont.)	
Show Update Manager Badge:	With this option selected, the RMS UI will show an alert icon on the Update Manager tab when new firmware updates are available to download via *Update Manager* (default = *enabled*). Refer to the *Update Manager (HTML UI)* section on page 28 for details.
Time Zone	Use these two drop-down menus (*Location* and *Time Zones*) to set the Country and Time Zone for this user account (*optional*). By default, this time zone is set to the System Time Zone (see the *Setting the Default Application Time Zone and Locale (Language)* section on page 212 for details).
Reset User's Preferences	This action will clear any personalization changes made to the application for this user including re-sized and re-ordered columns and dashboard customization. This action cannot be undone and all personalization settings will be reset to their respective default values. Click **Reset** to reset this user's configured preferences to their default values.

Entering General User Profile Information

1. Open the *My Profile* page - **General Setting** tab (see FIG. 135 on page 85).
2. Fill in the fields as desired.
3. Click **Save** to save your changes.

Editing General User Profile Information

1. Open the *My Profile* page - **General Setting** tab (see FIG. 135 on page 85).
2. Edit the fields as desired.
3. Click **Save** to save your changes.

Setting a Custom Time Zone for a User

1. Open the *My Profile* page - **General Setting** tab (see FIG. 135 on page 85).
2. Use the *Location* and *Time Zone* drop-down menus to select a time zone for this account.
3. Click **Save** to save your changes.

Resetting User Preferences

1. Open the *My Profile* page - **General Setting** tab (see FIG. 135 on page 85).
2. Click the **Reset User's Preferences** button to reset this user's configured preferences to their default values.

This action will clear any personalization changes made to the application for this user including re-sized and re-ordered columns and dashboard customization (see *User Profiles - Personalization* on page 84).

This action cannot be undone and all personalization will be reset to their respective 'DEFAULT' values.

My Profile - My Contacts Tab

Use the **My Contacts** tab of the *My Profile* page to manage and view contact information for this user (FIG. 136).

FIG. 136 My Profile page - My Contacts tab

The options in this tab are described below:

My Profile - My Contacts Tab Options	
E-Mail	
Enable	This checkbox determines whether or not this E-Mail contact is enabled. • By default, all Contacts are enabled. • De-select this checkbox to disable this E-Mail Contact.
E-Mail Address	Enter the contact's E-Mail address in this text field.
Location	Select *Home* or *Work* from the Location drop-down menu. Defaults: • 1st email row or if new rows are added - Home • 2nd email row - Work.
E-Mail Type	Select *HTML*, *Text* or *Short Text* as the Email type for this contact (default = *HTML*).
Add E-Mail	Click to add an (empty) E-Mail contact entry to the list.
Phone	
Phone Number	Enter the contact's Phone Number in this text field.
Location	Select *Home*, *Work* or *Mobile* from the Location drop-down menu. Defaults: • 1st phone row or if new rows are added - *Home* • 2nd phone row - *Work* • 3rd phone row - *Mobile*
Add Phone	Click to add an (empty) Phone contact entry to the list.

Adding an E-Mail Contact

1. Open the *My Profile* page - **My Contacts** tab.
2. Under *E-Mail*, enter the new Email Contact information in the fields provided. If there are no empty E-Mail Contact fields to fill in, click the **Add E-Mail** button to add a new (empty) E-Mail contact entry to the list.
3. Click the **Save** button at the bottom of the page to save your changes.

Adding a Phone Contact

1. Open the *My Profile* page - **My Contacts** tab.
2. Under *Phone*, enter the new Phone Contact information in the fields provided. If there are no empty Phone Contact fields to fill in, click the **Add Phone** button to add a new (empty) Phone contact entry to the list.
3. Click the **Save** button at the bottom of the page to save your changes.

Editing a Contact

1. Open the *My Profile* page - **My Contacts** tab.
2. Click inside the text fields to edit E-Mail and Phone contact information as desired.
3. Click the **Save** button at the bottom of the page to save your changes.

Removing a Contact

1. Open the *My Profile* page - **My Contacts** tab.
2. Click the "X" button to delete a contact (FIG. 137). Note that this action also removes the row from the display, so that it is no longer visible.
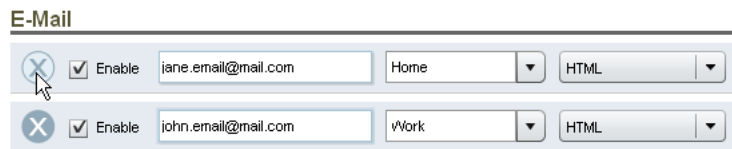
FIG. 137 Deleting an Email Contact

3. Click the **Save** button at the bottom of the page to save your changes.

My Profile - Notification Schedule Tab

Use the **Notification Schedule** tab of the *My Profile* page to define a Notification Schedule (a daily time schedule for delivery notifications) for the current user account (FIG. 138).

FIG. 138 My Profile page - Notification Schedule tab

NOTE: *Email notifications can only be sent if an SMTP Email server has been setup/configured (Settings > System Configuration > Email Server (SMTP)). See the Email Server (SMTP)* section on page 220 *for details.*

- The Notification Schedule applies to all contacts associated with that user.
- This notification schedule can be ignored by the override flag on a rule definition - see the *Adding a User Notification* section on page 90 for details.

The options in this tab are described below:

My Profile - Notification Schedule Tab Options	
Schedule options	
Never Send Notifications	Select this option to never send notifications to this user. Note that when this option is selected, all fields on this page are disabled.
Always Send Notifications	Select this option to always send notifications to this user. Note that when this option is selected, all fields on this page are disabled. This is the default selection.
Only Send Notifications According to Schedule	Select this option to only send notifications to this user according to the Notification Schedule defined on this page (via the *Schedule Date and Time* options described below).
Schedule Date and Time options *Note: The schedule options are enabled only if the Only Send Notifications According to Schedule option is selected.*	
Day	Click inside the checkboxes to specify which day(s) notifications will be sent. When a day is selected to be included in the Notification Schedule, the *Start Time* and *End Time* fields are activated.
Start Time	Use the up and down arrows, and select AM or PM to specify the time of day at which notifications will start being delivered to this user. Default = 7:00 AM
End Time	Use the up and down arrows, and select AM or PM to specify the time of day at which notifications will stop being delivered to this user. Default = 7:00 PM

Specifying User Notification Options

1. Open the *My Profile* page - **Notification Schedule** tab.
2. Under **Schedule**, select a scheduling option.
   - If you select *Never Send Notifications*, notifications will never be sent to this user.
   - If you select *Always Send Notifications*, notifications will always be sent to this user. This is the default setting for all user accounts.

- If you select *Only Send Notifications According to Schedule*, use the weekday calendar to specify the day(s) of the week on which you will receive notifications, as well as a Start Time and End Time for receiving Notifications on each selected day. See *Specifying a Notification Schedule* below for details.

3. Click **Save** to save your changes.

Specifying a User Notification Schedule

Refer to *Scheduling User Notifications*

My Profile - My Notifications Tab

Use the **My Notifications** tab of the *My Profile* page to view and manage user-defined notification rules for the current user (FIG. 138).

FIG. 139 My Profile page - My Notifications tab

The Notification list represents all Notifications to all contacts associated with the current user.

Adding a User Notification

1. Open the *My Profile* page - **My Notifications** tab.
2. Click the **Add** button to open the *Edit Notification Rule* dialog (**Rule** tab - FIG. 140).

FIG. 140 Edit Notification Rule dialog - Rule tab

3. In the **Rule** tab:
   a. Enter a name for this Notification Rule in the **Name** text field (50 characters max).
   b. Select **Enable** to enable this Notification Rule. When a Notification Rule is enabled, and an asset parameter is tripped that matches the Rule's criteria, a notification will be generated.
   c. Select **Override User Notification Schedule** to override user's existing Notification Schedule settings, when this Notification Rule is generated. If this option is selected, when an asset parameter is tripped that matches this Rule's criteria, the generated notification will be sent to all users despite their individual configured notification schedules.
4. In the **Status Types** tab (FIG. 141), select the status types that apply to this Notification Rule.

FIG. 141 Edit Notification Rule dialog - Status Types tab

- Select **Apply Notifications to All Status Types** to select all Status Types in the list.
- Click to select individual Status Types to apply to this Notification Rule.
- See *Status Types* on page 251 for details.

5. In the **Locations** tab (FIG. 142), select the Location Groups / Locations that apply to this Notification Rule.
   - Click **All Group**s to select all Locations Groups/Locations in the list.
   - Click the + sign next to each Location Group folder to expand the view to show Sub-Groups and Locations contained within each Group folder.
   - Click to select individual Location Groups to apply to this Notification Rule.

FIG. 142 Edit Notification Rule dialog - Locations tab

6. Click **Save** to save your changes and close the *Edit Notification Rule* dialog.

The new Notification Rule is represented in the **My Notifications** tab of the *My Profile* page (see FIG. 139 on page 90).

Editing a User Notification

1. Open the *My Profile* page - **My Notifications** tab.
2. Select a Notification Rule and click **Edit** to open the *Edit Notification Rule* dialog.
3. Edit the properties of the selected Notification Rule.
4. Click **Save** to save your changes and close the *Edit Notification Rule* dialog.

Deleting a User Notification

1. In the *My Profile* page - **My Notifications** tab, select a Notification Rule and click **Delete**.
2. The system will prompt you to verify this action before the selected Notification Rules is deleted (FIG. 143):
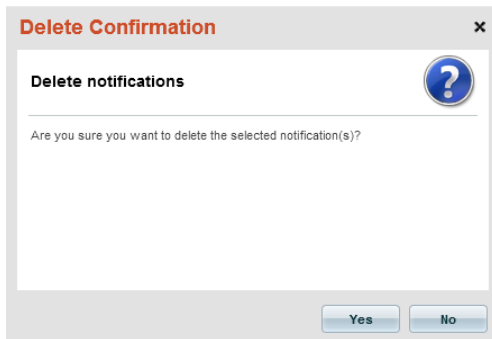
FIG. 143 Delete Confirmation dialog

3. Click **Yes** to proceed.

Management - Client Gateways (Classic UI)

Overview

Click inside the **Management** tab (Classic UI) to access the *Management* menu. The options in this menu allow you to configure Locations/Systems, manage Assets, and manage Users & Notifications, as described in the following sections.

The options in the **Configure Locations/Clients** category of the (Classic UI) *Management* menu allow you to configure and manage *Locations* and *Location Groups* as well as *Client Gateways* (FIG. 144):
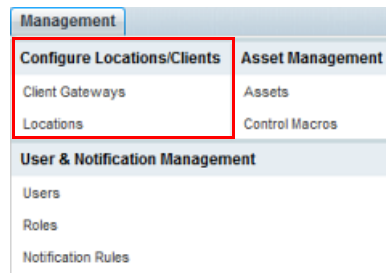
FIG. 144 Management menu - Configure Locations /Clients

NOTE: *To access the RMS Classic UI described in this section, select "Classic UI" from the RMS Enterprise HTML interface menu bar.*

Client Gateways

A *Client Gateway* is an electronic device capable of implementing the RMS Client API participating with the RMS Enterprise server. The Client Gateway is the bridge between the RMS system and the individual devices (or *Assets*) that are managed in the RMS system. In order for individual devices to be managed by the RMS system, they must be connected to a Client Gateway.

Each remote RMS (client) system or device that wishes to communicate with the RMS server is considered a Client Gateway. Each Client Gateway must implement the Client Gateway API to register and communicate with the RMS server. All Client Gateways must be approved and assigned to a Location by an RMS Administrator before it can participate in the RMS application.

NOTE: *Refer to the Management - Locations (Classic UI) section on page 103 for information on Location Groups and Locations.*

Client Gateway Management Page

Client Gateway management is provided via options in the **Client Gateway Management** page. To open the *Client Gateway Management* page, select **Client Gateways** under *Configure Locations/Clients* in the *Management* menu (FIG. 145).
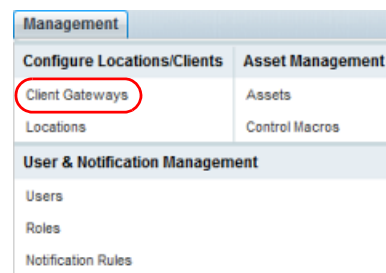
FIG. 145 Management > Configure Locations/Systems > Client Gateways

The features on this page are organized into several windows (FIG. 146):

- Use the **Group** window to view select Location Groups - see page 94.
- Use the **Client Gateway** window to view and manage Client Gateways - see page 95.
- Use the **Client Gateway Details** window to view detailed information in the selected Client Gateway - see page 96.
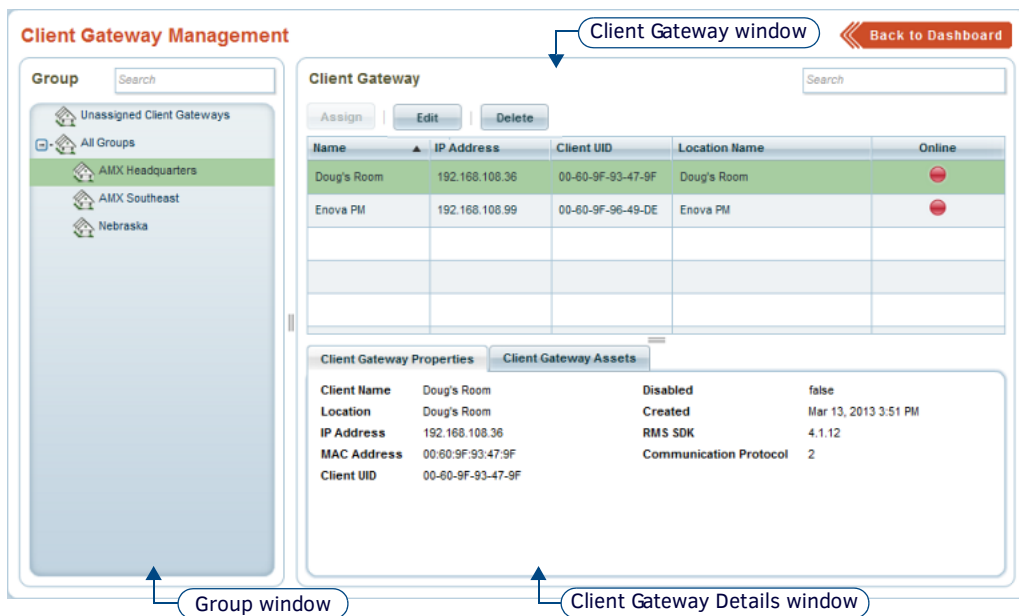
FIG. 146 Client Gateway Management page

NOTE: *Many options on this page are permission-dependant (see the Management - Roles (Classic UI) section on page 192 for details).*

Client Gateway Management Page - Group Window

To view the Client Gateway systems assigned to a specific Location, select a Location Group in the **Group** window (FIG. 147). Refer to the *Locations and Location Groups* section on page 103 for details on Location Groups.
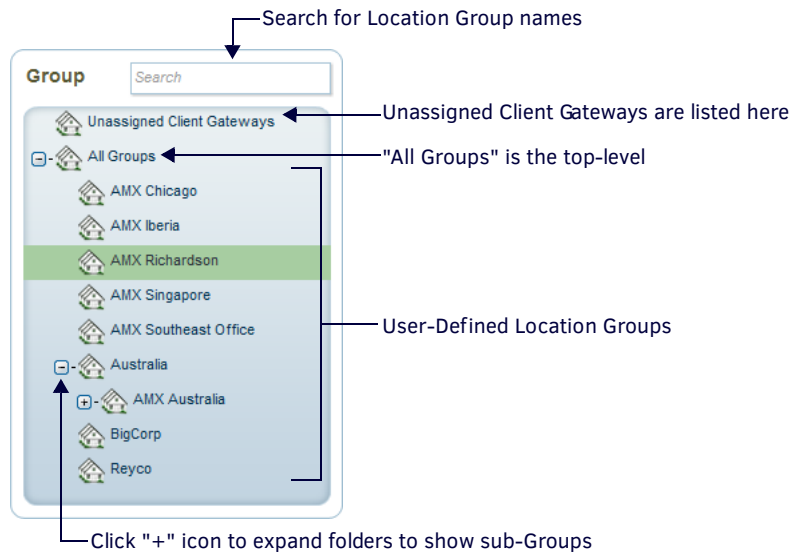
FIG. 147 Client Gateway Management page - Group window

When a Location Group is selected in the Group window, the Client Gateway window displays all associated Client Gateway records (see FIG. 148 on page 95). The options on the *Group* window are described below:

Group Window Options	
Search	Use this search field to perform a search for Location Group names. See *Searching for a Location Group* on page 98 for details.
Groups View	The Group view shows all current Groups and Parent Groups in a hierarchical tree structure. • Click the *Unassigned Client Gateways* entry to list all Client Gateways in the system that are not currently assigned to a Location. See the *Unassigned Client Gateways* section on page 97 for details. • The top-level entry is *All Groups*. • Click the plus sign (+) next to the *All Groups* entry to expand the list to show all Groups in the system. Click the minus sign (-) next to each entry to collapse each Group.

Client Management Group Window Context Menu

Right-click inside the *Group* window to access the Group window context menu, containing the following options:

Group Window Context Menu Options	
Expand All	Click to expand all Location Groups to show all contained Sub-Groups and Locations in the Group window.
Collapse All	Click to collapse all Location Groups in the Group window.
Refresh	This option refreshes the listing in the Group window.

Client Gateway Management Page - Client Gateway Window

Use the **Client Gateway** window to view and manage Client Gateways for each Location. The table in this window lists the Client Gateways assigned to the selected Location Group (FIG. 148).
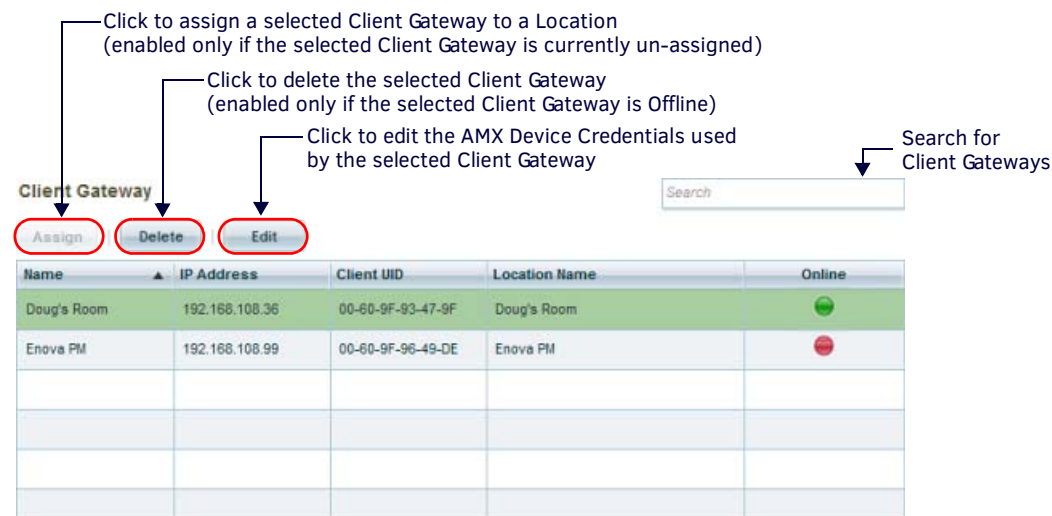
FIG. 148 Client Gateway Management page - Client Gateway window

Initially, this window is empty, until one or more Client Gateways connect to the RMS Server.

NOTE: *By default, the Unassigned Client Gateways entry is selected in the Groups window, so initially this window indicates all Client Gateways in the system that have not been assigned to Locations.*

The options in the *Client Gateway* window are described below:

Client Gateway Window Options	
Search	Use this search field to perform a search for Client Gateway names.
Assign	With an unassigned Client Gateway selected in the Gateways table, click **Assign** to assign the selected Gateway to a specific Location, via the *Assign Client Gateway* dialog. See *Assigning a Client Gateway To a Location* on page 98 for details.
Edit	Click to enter/edit the login credentials for this Client Gateway, via the *Client Gateway - AMX Device Credentials* dialog. See *Entering/Editing AMX Device Credentials* on page 101 for details.
Delete	Click to delete the selected Client Gateway. Note that the Delete button is only enabled for Client Gateways that are not currently Online. See *Deleting a Client Gateway* on page 101 for details.
Gateways Table	The Gateways table lists each Client that is included in the selected Location Group, providing basic Client Gateway properties (*Name*, *IP Address*, *Client UID*, *Location Name* and *Online*). Click any column heading to sort the table by that column. *Note: These read-only properties are provided by the Client Gateways.*

Client Gateway Window Context Menu

Right-click inside the Client Gateway window to access the Client Gateway window context menu, containing the following options:

Client Gateway Window Context Menu	
Assign	This option provides the same functionality as the **Assign** button. *Note: This option is only accessible for Unassigned / Online Client Gateways.* See the *Assigning a Client Gateway To a Location* section on page 98.
Reassign Client Gateway	This option allows you to reassign a client gateway record to another location. *Note: This option is only accessible for Assigned Client Gateways.* See the *Re-Assigning a Client Gateway To a Different Location* section on page 99
Edit	Click to enter/edit the login credentials for this Client Gateway, via the *Client Gateway - AMX Device Credentials* dialog. See *Entering/Editing AMX Device Credentials* on page 101 for details.

Client Gateway Window Context Menu (Cont.)	
Delete	This option provides the same functionality as the **Delete** button. *Note: This option is only accessible for Offline Client Gateways.* See the *Deleting a Client Gateway* section on page 101.
Refresh	This option refreshes the listing in the Client Gateway window.
Disconnect	This option forcefully disconnects a selected legacy socket connection. *Note: This option is only accessible for legacy (pre-RMS Enterprise) clients.* See the *Taking a Client Gateway Offline* section on page 99 for details.
Re-Initialize	This option forces the selected Client Gateway to re-initialize all device and parameter registrations.

Client Gateway Management Page - Client Gateway Details Window

When a Client Gateway is selected in the Gateways table, the *Client Gateway Details window* is updated to display extended information about the selected client without having to open the Client Gateway editor.

NOTE: *The Client Gateway Details window can be hidden by dragging the vertical divider all the way to the bottom of the screen.*

The information presented in the Client Gateway Details window is separated into two tabs (*Client Gateway Properties* and *Client Gateway Assets*):

Client Gateway Details Window - Client Gateway Properties Tab

When a Client Gateway is selected in the Gateways table, this tab displays detailed Gateway Properties information for the selected Client Gateway (FIG. 149):

FIG. 149 Client Gateway Management page - Client Gateway Details window (Client Gateway Properties tab)

Client Gateway Properties Tab Options	
Client Name	Displays the name of the selected Client Gateway.
Location	Displays the name of the Location associated with the selected Client Gateway.
IP Address	Displays the IP Address of the selected Client Gateway.
MAC Address	Displays the MAC Address of the selected Client Gateway.
Client UID	Displays the UID (Unique Identifier) associated with the selected Client Gateway.
Disabled	Indicates whether the selected Client Gateway is currently disabled (*false* = enabled, *true* = disabled). See the *Taking a Client Gateway Offline* section on page 99
Created	Displays the date on which the selected Client Gateway was created in the system.
RMS SDK	Displays the version number of the RMS SDK used by the selected Client Gateway.
Communication Protocol	Displays the version number of the RMS SDK protocol used by the selected Client Gateway.

These read-only properties are provided by the Client Gateways.

Client Gateway Details Window - Client Gateway Assets Tab

When an assigned Client Gateway is selected in the Gateways table, this tab displays a listing of all Assets contained in the Client Gateway's assigned Location (FIG. 150).

FIG. 150 Client Gateway Management page - Client Gateway Details window (Client Gateway Assets tab)

Client Gateway Assets Tab	
Asset	The *Asset Name*, as displayed in the *Asset Management page* (**Asset Setting** tab - *Information* section). This information is provided when the Asset is registered.
Device:Port:System	The D:P:S assignment as displayed in the *Asset Management page* (**Asset Setting** tab - *NetLinx Device Information* section). This information is provided when the Asset is registered.
Location	The Location to which this Asset's Client Gateway is associated.

Double-click any entry in the **Client Gateway Assets** tab to view/edit that Asset's properties in the *Asset Properties* page (see *Asset Properties Page* on page 131). See the *Management - Assets (Classic UI)* section on page 125 for details.

Working With Client Gateways

Unassigned Client Gateways

By default, when the *Client Gateway Management* page is opened, a special group called *Unassigned Client Gateways* is preselected in the Group window, and the unassigned Client Gateway systems are listed in the Client Gateway window (FIG. 151).
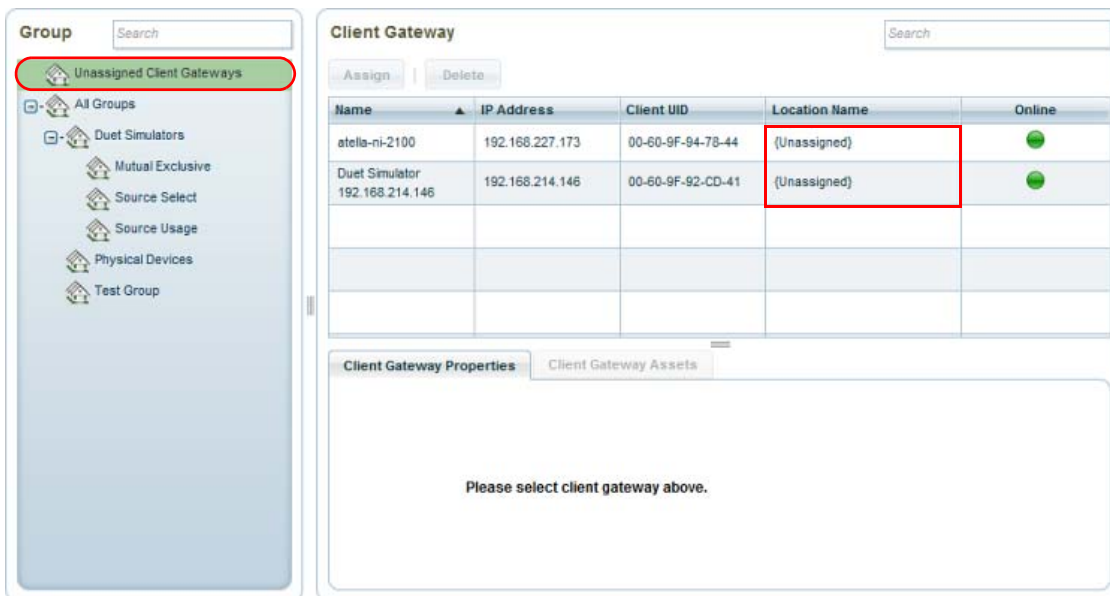
FIG. 151 Client Gateway Management page - Unassigned Client Gateways

Note that all unassigned Client Gateways are listed as "*Unassigned*" in the **Location Name** column (in the Client Gateway window). These records represent new Client Gateways that have connected to the RMS server, but have not yet been approved and assigned to a Location in RMS.

Unassigned Client Gateways - Hotlist Display

Every new unassigned Client Gateway will generate a Hotlist item (FIG. 152).
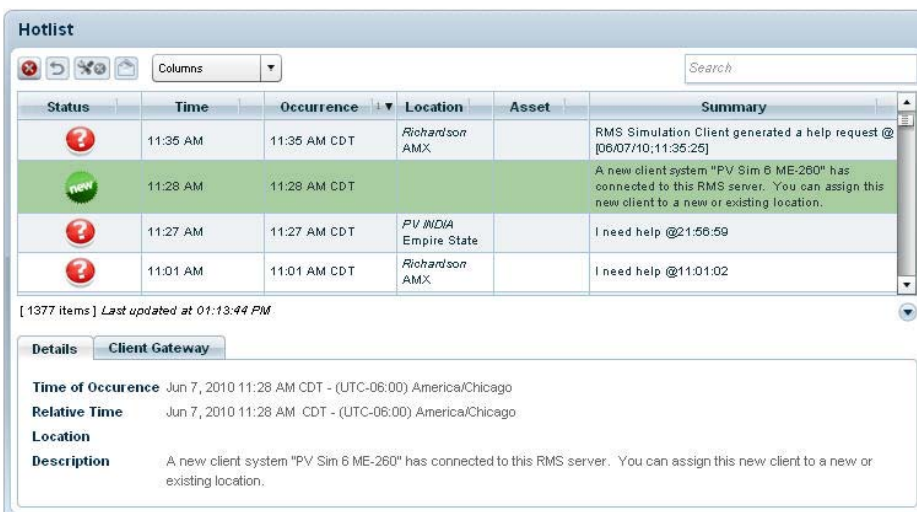
FIG. 152 Hotlist - New Unassigned Client Gateway Item

These Hotlist items can be dismissed to ignore these alerts if desired (see *Dismissing Hotlist Items* on page 68). Once dismissed, the unassigned Client Gateway will not generate a new Hotlist item, but will remain visible in the *Unassigned Client Gateways* listing in the *Client Gateway Management* page (see FIG. 151 on page 97). The dismissed Client Gateway will generate a new Hotlist item only if it is deleted from the RMS system and then re-establishes a connection to the RMS server. These Hotlist items are only visible to authenticated users that have the global permissions of Manage Clients & Locations (see the *Management - Roles (Classic UI)* section on page 192 for details).

NOTE: *The Client Gateway will only generate a new hotlist record if it is deleted from the RMS system, and later re-establishes a connection to the RMS Server.*

Searching for a Location Group

Use the *Search* tool in the *Group* window to search for a specific Location Group (FIG. 153).

Location Groups Search window

Groups list is filtered to show only search results
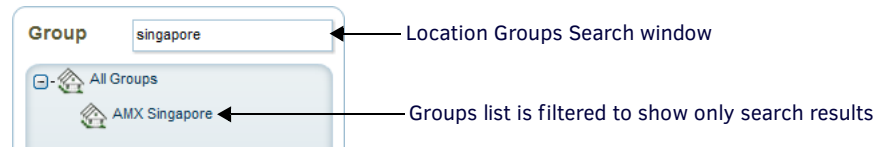
FIG. 153 Group window - Search window

Assigning a Client Gateway To a Location

Any online unassigned Client Gateway can be approved to participate in the RMS application by assigning it to a Location.

- If the client gateway is not connected (online), it cannot be assigned.
- Multiple client gateways can be assigned to a single location.

1. Select **Unassigned Client Gateways** in the *Groups* window to populate the Client Gateways Table with all Client Gateways detected by the RMS Server that have not been assigned to Locations.

2. Select an unassigned Client Gateway. Note that when a Client Gateway is selected, the *Client Gateway Properties* window is populated with detailed information for that Client Gateway.

3. Click the **Assign** button. This action invokes the first of two *Assign Client Gateway* dialogs (FIG. 154):
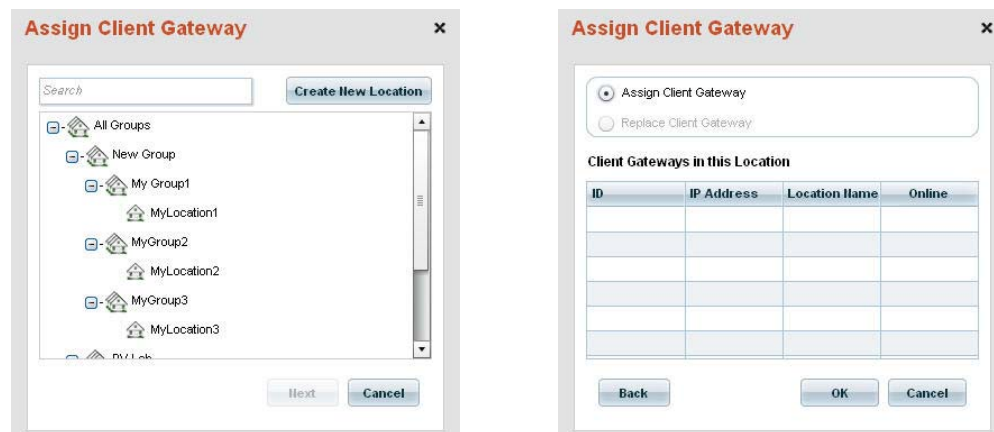
FIG. 154 Assign Client Gateway dialogs

4. Select a target Location for this Client Gateway assignment.

NOTE: *Optionally, click the Create New Location button to create a new Location for this Client Gateway. This option opens the Location page (see Adding a New Location on page 114). The Location you create is automatically assigned to this Client Gateway.*

5. Click **Next** to proceed to the second *Assign Client Gateway* dialog. This dialog presents the option to either simply assign this Client Gateway to the selected Location, or to replace an existing Client Gateway:

- If no Client Gateways have already been assigned to this Location, the *Client Gateways in this Location* table is empty. In this case, the default setting *Assign Client Gateway* is pre-selected.
- If one or more Client Gateways have already assigned to this Location, they are listed in the *Client Gateways in this Location* table. In this case you can select an entry in the table, and select the Replace Client Gateway option.

6. Click **OK** to save your changes and close this dialog.

Note that once the Client Gateway is assigned to a Location, it is automatically removed from the *Unassigned Client Gateways* listing.

Re-Assigning a Client Gateway To a Different Location

Any *assigned* Client Gateway (Online or Offline) can be re-assigned to a different Location.

NOTE: *The Re-Assign Client Gateway option is only available for Assigned Client Gateways.*

1. In the Client Gateways window, right-click on any assigned Client Gateway to access the context menu (FIG. 155).
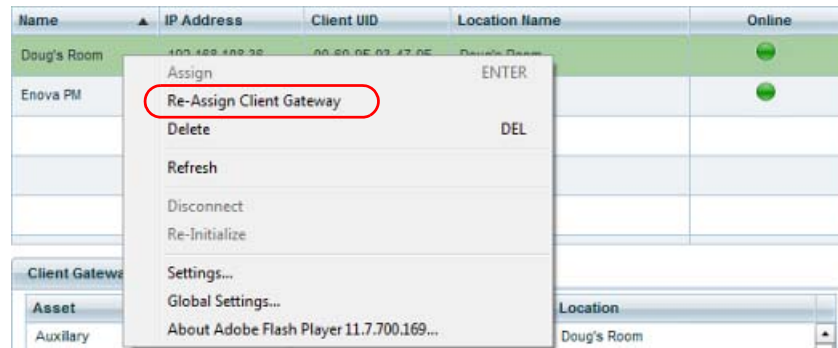
FIG. 155 Client Gateways Table - context menu (Re-Assign Client Gateway)

2. Select **Re-Assign Client Gateway**. This action invokes the *Assign Client Gateway* dialog (see FIG. 154 on page 98).

3. See the *Assigning a Client Gateway To a Location* section on page 98 for details on assigning a Client Gateway to a Location.

Taking a Client Gateway Offline

The process of taking a Client Gateway offline depends on whether the Client Gateway is running RMS Enterprise code or Legacy RMS (v3.x or earlier) code:

RMS Enterprise Systems

In RMS Enterprise, to take a Client Gateway (NetLinx Master) offline, you must disable the RMS Client option in the Master's Configuration Pages. To access the NetLinx Master's WebConsole from any PC that has access to the LAN that the target Master resides on:

1. Open a web browser and type the IP Address of the target Master in the Address Bar.

2. Press Enter to access WebConsole for that Master. The initial view is the *Web Control* page.

Accessing the RMS Web Configuration page - RMS SDK v4.3 (or higher)

On Masters running RMS SDK v4.3 (or higher), a link to the *RMS Web Configuration* page is provided on the initial page *Web Control* (FIG. 156):
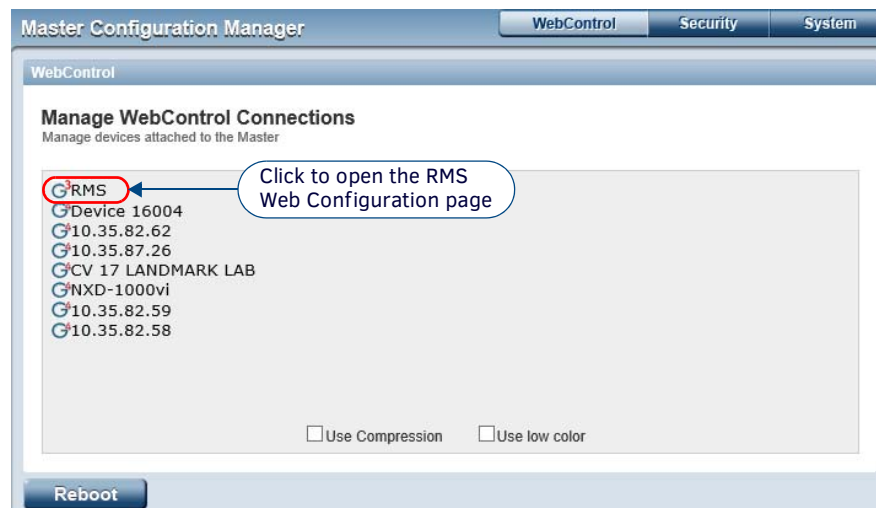
FIG. 156 NetLinx Master Configuration Manager - WebControl page (SDK v4.3 or higher)

Accessing the RMS Web Configuration page - RMS SDK v4.0 (or older)

On Masters running RMS SDK v4.0 (or older):

1. Click **System** to open the *Manage System* page.

2. Click the **Manage Devices** tab to view the *Device Options* (FIG. 157):

PAGE

FIG. 157 NetLinx Master Configuration Manager - Manage Devices tab (Device Options)

3. Under *Device Configuration Pages*, click on **+ Resource Management Suite**. This displays the **Configuration** option.

4. Click on *Configuration* (FIG. 158):
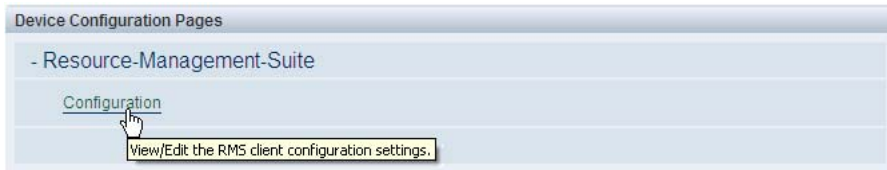
FIG. 158 Device Configuration Options - Resource Management Suite > Configuration

5. This opens the *RMS Web Configuration* page (FIG. 159):
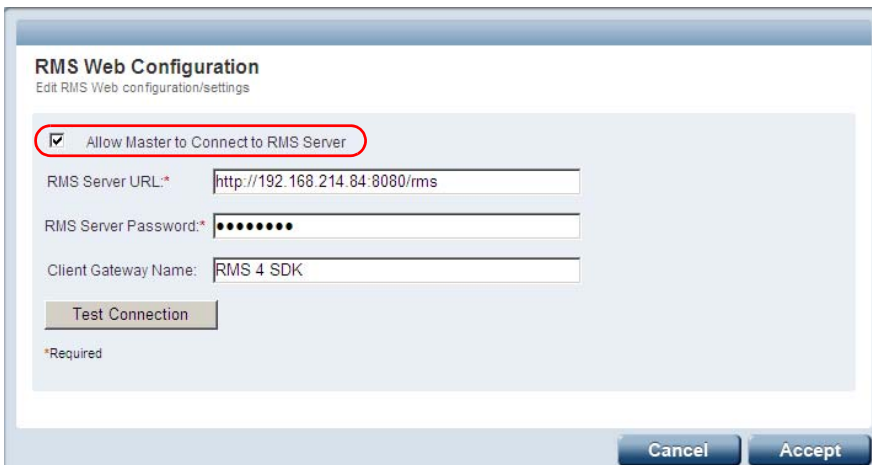
FIG. 159 Configuration > RMS Web Configuration page

6. De-select the **Allow Master to Connect to RMS Server** option.

Legacy (v3.x or Earlier) RMS Systems

1. In the Client Gateways window, right-click on any online Client Gateway (indicated with a green dot in the *Online* column) to access the context menu.

2. Select **Disconnect**. This forcefully disconnects a selected legacy socket connection.

3. The Client Gateway's Online status icon changes from green to red to indicate that it is now offline.

NOTE: *Once a Client Gateway is taken offline, it remains offline only until the next polling cycle at which time it will automatically go back online.*

Deleting a Client Gateway

Any disconnected (Offline) Client Gateway can be deleted from the RMS system. Only Offline Client Gateways can be deleted. Therefore, the physical device should be taken offline or removed before attempting to delete the entity from the RMS system.

NOTE: *Deleting a Client Gateway must be done with caution. Deleting a Client Gateway will also remove all assets, parameters and associated history from the RMS system.*

Online/Offline status is indicated for each Client Gateway in the *Status* column of the Client Gateway page (FIG. 160):

FIG. 160 Online / Offline Status icons

In some cases, you may need to take a Client Gateway offline, in order to delete it. See *Taking a Client Gateway Offline* on page 99.

1. Select one or more *offline* Client Gateways in the Client Gateways Table (Ctrl + click to multi-select).

2. Click the **Delete** button.

3. The system will prompt you to verify this action before the selected Client Gateway is deleted, via the *Delete Confirmation* dialog (FIG. 161):

FIG. 161 Delete Confirmation dialog - Client Gateways

4. Press **Yes** to proceed.

Entering/Editing AMX Device Credentials

Use the *Edit* option in the *Client Gateway Management* page to enter or edit the AMX Device Credentials for a selected Client Gateway. This feature allows you to override system-wide credentials for an individual device.

NOTE: System-wide *AMX Device Credentials* are configured via the *Update Manager Configuration* option in the *Configuration* menu (see *AMX Device Credentials* on page 265).

1. Select a Client Gateway in the Client Gateways Table.

2. Click the **Edit** button to open the *Client Gateway - AMX Device Credentials* dialog (FIG. 162):
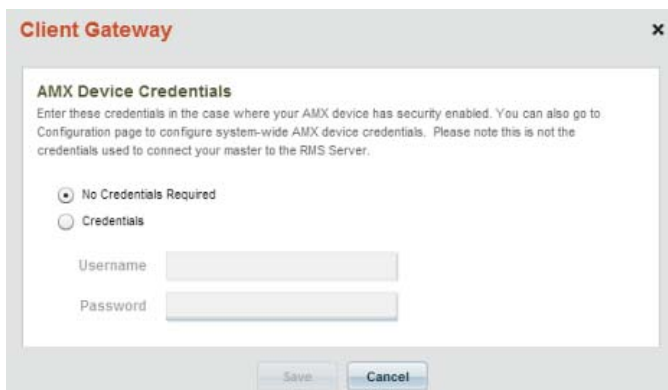
FIG. 162 Client Gateway - AMX Device Credentials dialog

NOTE: *The credentials entered in the Client Gateway - AMX Device Credentials dialog are only used by Update Manager.*

3. Note that by default, *No Credentials Required* is selected. To enter device credentials for this device, select **Credentials** to enable the *Username* and *Password* fields.

4. Enter the *Username* and *Password* required by this device.

5. Click **Save** to save changes and close this dialog.

Re-Initializing a Client Gateway

Re-Initializing forces a client gateway to re-initialize all device and parameter registration.

1. Select a Client Gateway in the Client Gateways Table.

2. Right-click to access the context menu, and select **Re-initialize** (FIG. 163). This forces the Client Gateway to re-initialize all device and parameter registration.
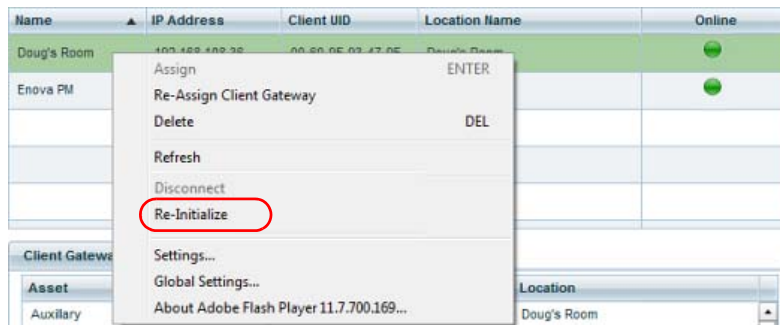
FIG. 163 Client Gateways Table - context menu

Searching for a Client Gateway

Use the Search tool in the Client Gateway window to search for a specific Client Gateway (FIG. 164).

FIG. 164 Client Gateways Table - Search window

This tool searches the data columns displayed in the Client Gateway window (*ID*, *IP Address* and *Location Name*).

NOTE: *Note that since this search is performed against the data currently displayed in the Client Gateway window, the search is limited to the Client Gateways contained with the Group or sub-Group currently selected in the Groups window.*

Management - Locations (Classic UI)

Overview

Click inside the **Management** tab (Classic UI) to access the *Management* menu. The options in this menu allow you to configure Locations/Systems, manage Assets, and manage Users & Notifications, as described in the following sections.

The options in the **Configure Locations/Clients** category of the (Classic UI) *Management* menu allow you to configure and manage *Locations* and *Location Groups* as well as *Client Gateways* (FIG. 165):
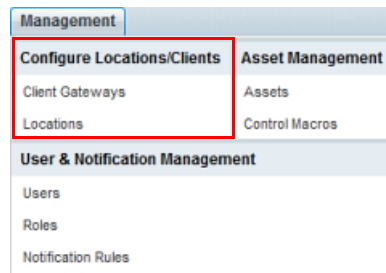
FIG. 165 Management menu - Configure Locations /Clients

NOTE: *To access the RMS Classic UI described in this section, select "Classic UI" from the RMS Enterprise HTML interface menu bar.*

Locations and Location Groups

All activities, assets, and service requests in the RMS system are Location-based.

- A **Location** is any physical or virtual space that is configured to be monitored or serviced by RMS (such as a classroom, conference room, lecture hall, foyer, network closet, basement, etc).

  Each Control System in the RMS application must be associated with one or more Locations to enable equipment monitoring and notifications.

- A **Location Group** represents a grouped set of Locations. Location Groups allow you to manage a defined set of Locations as a single entity for configuration, reporting and notification purposes.

Location Page

All Locations and Location Groups are configured and managed via options in the *Location* page (see FIG. 167 on page 104). To open the Location page, select **Locations** under *Configure Locations/Clients* in the Management menu (FIG. 166).
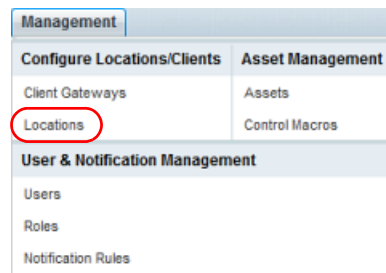
FIG. 166 Management > Configure Locations/Clients > Locations

The features on this page are organized into several windows (FIG. 167):

- Use the **Groups** window to view and manage Location Groups - see *Location Page - Groups Window* on page 104.
- Use the **Locations** window to view and manage Locations - see *Location Page - Locations Window* on page 105.
- Use the **Location Details** window to view detailed information in the selected Location - see *Location Page - Location Details Window* on page 107.
- Use the **Actions** window to execute various Locations-based actions - see *Location Page - Actions Window* on page 108.
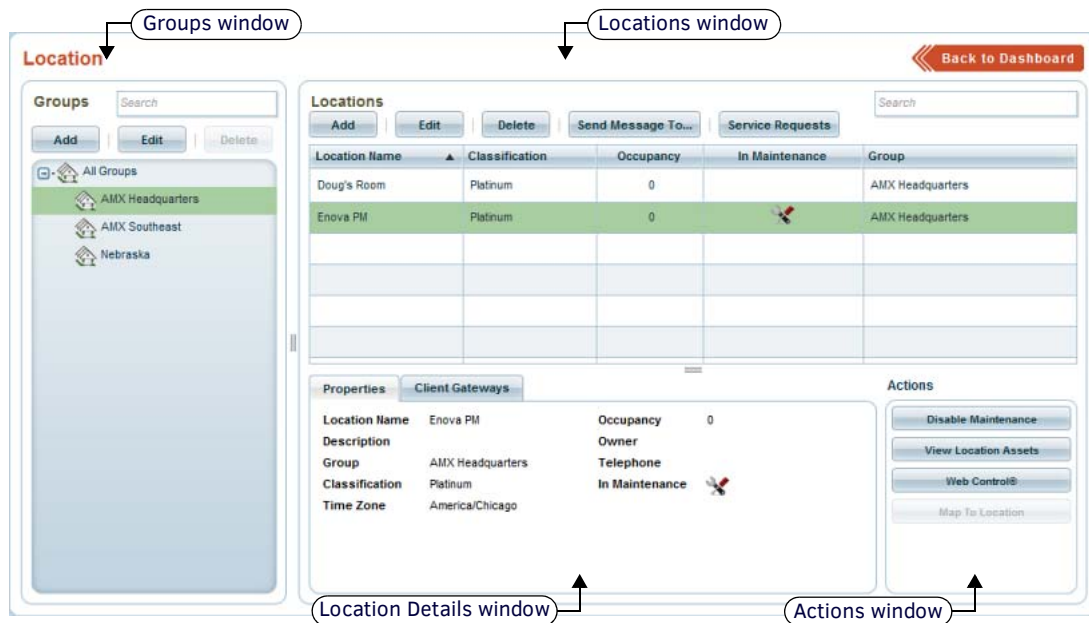
FIG. 167 Location page

NOTE: *Many options on this page are permission-dependant (see the Management - Roles (Classic UI) section on page 192 for details).*

Location Page - Groups Window

Location grouping is displayed in a hierarchal tree view in the **Groups** window (FIG. 168).
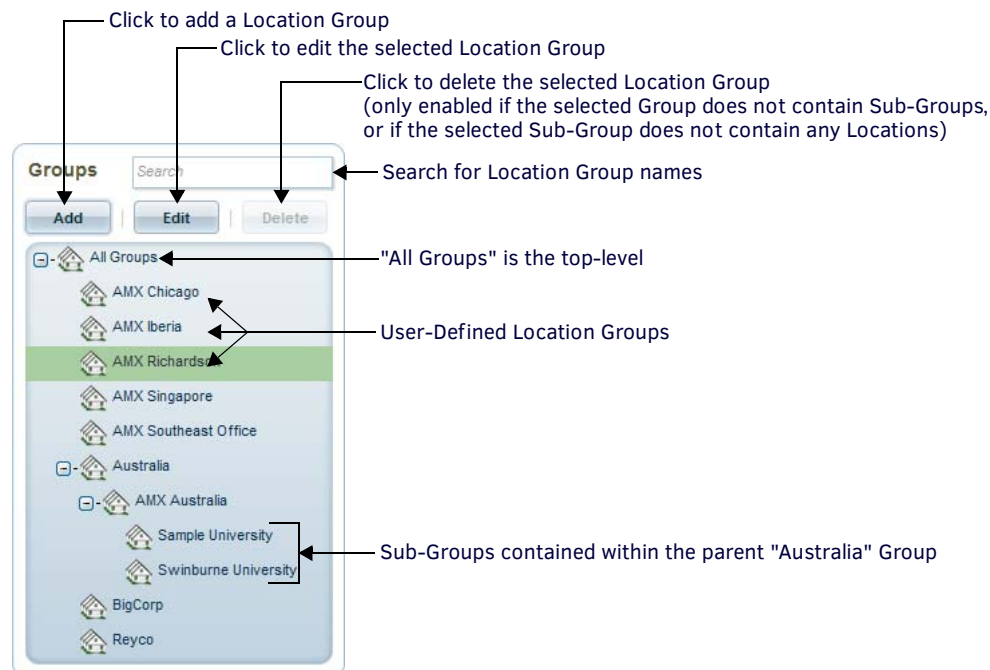
FIG. 168 Location page - Groups window

The Groups view shows all current Groups and Parent Groups in a hierarchical tree structure. The top-level entry is *All Groups*. Click the plus sign (+) next to the *All Groups* entry to expand the list to show all Groups in the system. Click the minus sign (-) next to each entry to collapse each Group.

● Initially, the only entry in the *Groups* window is **All Groups**, until one or more Location Groups are defined. See the *Adding (Creating) a New Location Group* section on page 111 for details.
● Location Groups can contain Locations or sub-Groups. See the *Adding a New Location* section on page 114 for details.

NOTE: *While there are no programmatic limits to the number of Locations, Location Groups or sub-Groups allowed, for application loading performance it is recommended that locations are divided into a logical grouping strategy.*

The options on the *Groups* window are described below.

Groups Window Options	
Search	Use this search field to perform a search for Location Group names. See *Searching For Location Groups* on page 111 for details.
Add	Click to invoke the *Location Group* dialog, in which you can define a new Location Group. See *Adding (Creating) a New Location Group* on page 111 for details.
Edit	Click to invoke the *Location Group* dialog, in which you can edit a selected Location Group. Alternatively, double-click on a Location Group to access the *Location Group* dialog. See *Editing a Location Group* on page 112 for details.
Delete	Click to delete the selected Location Group. *Note: This option is only available if the selected Location Group does not contain any Sub-Groups, or if the selected Sub-Group does not contain any Locations (see Editing a Location Group on page 112 for instructions on removing Locations from Groups).* See *Deleting a Location Group* on page 113 for details.

Groups Window Context Menu

Right-click inside the *Groups* window to access the following context menu:

Groups Window Context Menu Options	
Expand All	Click to expand all Location Groups to show all contained Sub-Groups.
Collapse All	Click to collapse all Location Groups in the Group window.
Add Group	Click to invoke the *Location Group* dialog (FIG. 177). Use the options in this dialog to create (add) a new Location Group. See *Adding (Creating) a New Location Group* on page 111 for details.
Edit Group	Click to invoke the *Location Group* dialog, in which you can edit a selected Location Group. Alternatively, double-click on a Location Group to access the *Location Group* dialog. See *Editing a Location Group* on page 112 for details.
Delete Group	Click to delete the selected Location Group. *Note: This option is only available if the selected Location Group does not contain any Sub-Groups, or if the selected Sub-Group does not contain any Locations (see Editing a Location Group on page 112 for instructions on removing Locations from Groups).* See the *Deleting a Location Group* on page 113 for details.
Refresh	This option refreshes the listing in the Group window.
Send Message To	Click to send a message to the selected Groups. Note that when a Group containing sub-Groups and or Locations is selected, this option will send a message to all sub-Groups and Locations contained therein. See *Sending a Message to a Location* on page 116 for details.

Location Page - Locations Window

The listing of Locations displayed in the **Locations** window (FIG. 169) represent either the Locations that are included in the Group selected in the *Location Groups* window, or the Locations returned as a result of a Location search (see *Searching for a Location* on page 114).
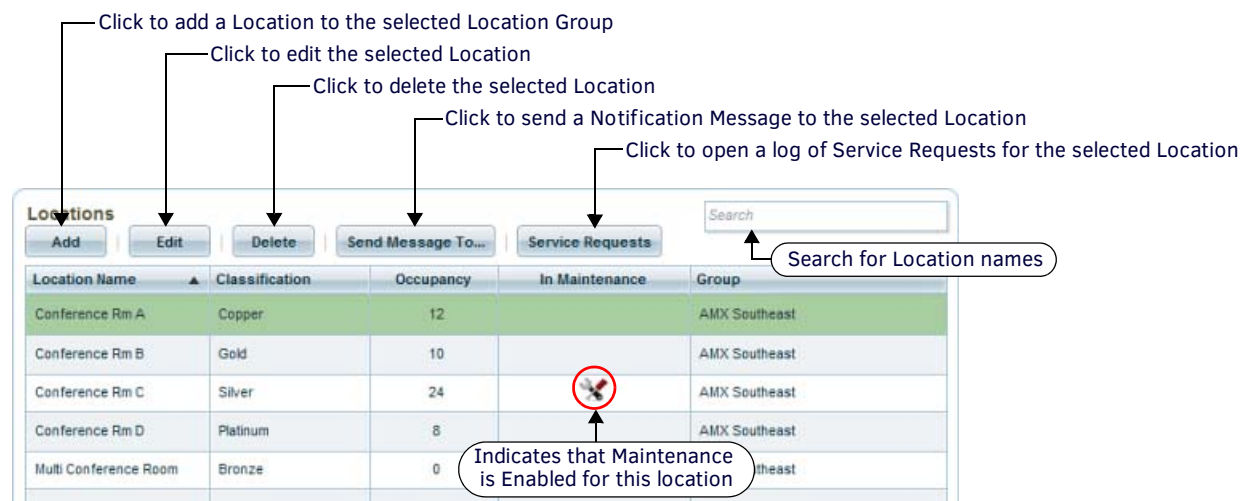
FIG. 169 Location page - Locations window

The Locations table lists each location that is included in the selected Location Group, providing basic Location Settings information (*Location Name*, *Group*, *Classification*, *Occupancy*, *Licensed*, *In Maintenance*). Click any column heading (other than *Licensed*) to sort the table by that column.

NOTE: *These properties are defined in the Locations page, when the page is created or edited.*

- See *Adding a New Location* on page 114.
- See *Editing a Location* on page 115.
- For information on Classification Levels, refer to the *Location Classification* section on page 242.

Initially, the Locations window is empty, until one or more Locations are defined. The Locations listed here can be sorted by clicking on the desired column header to sort by. Clicking the same column header will reverse the direction of the sort. Double-clicking a location in the listing will open the location editor page for the selected location.

The options in the *Locations* window are described below:

Locations Window Options	
Search	Use this search field to perform a search for Location names.
Add	Click to invoke the *Location page*, in which you can define a new Location. See *Adding a New Location* on page 114 for details.
Edit	Click to edit the selected Location in the **Settings** tab of the *Location* page. *Note: Alternatively, double-click on a Location to edit.* See *Editing a Location* on page 115 for details.
Delete	Click to delete the selected Location. See *Deleting a Location* on page 115 for details.
Send Message To	Click to invoke the *Send Message* dialog, which allows you to send a text message to the Touch Panel(s) in the Location or Location Group selected in the *Groups* window. See *Sending a Message to a Location* on page 116 for details.
Service Requests	Click to view a log of all service requests sent from the selected Location, in the *Service Requests* tab of the Location Properties page (see FIG. 175 on page 110).

Locations Window Context Menu

Right-click inside the *Locations* window to access the Locations window context menu:

Locations Window Context Menu Options	
Add	Click to create (add) a new Location. This action invokes the **Location Settings** tab of the *Location* page. See *Adding a New Location* on page 114 for details.
Edit	Click to edit the selected Location in the **Settings** tab of the *Location* page. *Note: Alternatively, double-click on a Location to edit.* See *Editing a Location* on page 115 for details.
Delete	Click to delete the selected Location. *Note: Any Client Gateways assigned to the Location will be unassigned after deletion.* See *Deleting a Location* on page 115 for details.
Refresh	Click to refresh the listing in the Locations window.
Select All Locations	Click to select all Locations in the Locations window.
Select None	Click to de-select all Locations in the Locations window.
Enable/Disable Maintenance Mode	Click to enable Maintenance Mode on the selected Location. When Maintenance is enabled for a Location, this button changes to "*Disable Maintenance*" (click to disable Maintenance), and the Maintenance icon is displayed in the *In Maintenance* column of the Locations window. • See *Maintenance Mode for Locations* on page 122 for details. • See *Enabling Maintenance Mode for a Location* on page 122.
View Location Assets	This action invokes the *Asset Management* page (FIG. 214 on page 126), listing all Assets contained in the selected Location. Refer to the *Management - Assets (Classic UI)* section on page 125 for details.
Send Message To	Click to invoke the *Send Message* dialog, which allows you to send a short text message to the Location Group selected in the Group window. See *Sending a Message to a Location* on page 116 for details.
Service Requests	Click to view a log of all service requests sent from the selected Location, in the *Service Requests* tab of the Location Properties page (see FIG. 175 on page 110).
Web Control®	If the selected Location has a Web Control URL configured, this option will open the Web Control application in a new browser window.
Open Location Map	If the selected location has a URL configured to link to map of the room (set via the *URL to Map of Location* field in the *Location Properties* page - **Settings** tab - see FIG. 173 on page 108), this option will open the link in a new browser window. *Note: The RMS Enterprise application does not provide any facility to generate and manage maps of your facility. This link is provided to allow users to access maps if such files are available.*

Location Page - Location Details Window

When a Location is selected in the location listing, the *Location Details window* is updated to display extended information about the selected location without having to open the location editor. The information presented in the Location Details window is separated into three tabs (*Properties*, *Assets* and *Client Gateways*):

Location Details Window - Properties Tab

This tab displays basic Properties for the selected Location (FIG. 170):
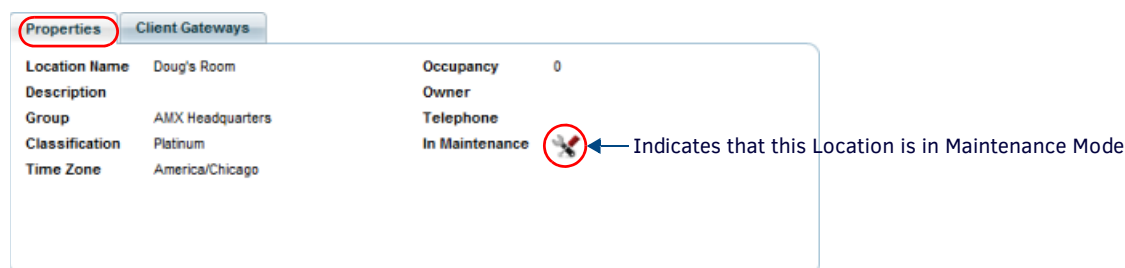
FIG. 170 Location page - Locations Details window (Properties tab)

Properties Tab	
Location Name	Displays the name of the selected Location.
Description	Displays a summary description of the selected Location.
Group	Displays the name of the selected Location's Parent Group.
Classification	Displays the Classification Level applied to this Location. See the *Location Classification* section on page 242 for details.
Time Zone	Displays the time zone associated with the selected Location. *Note: If a Time Zone is not specified for a Location, then the default System Time Zone will be used. The System Time Zone is set in the Localization page. See the Application Time Zone section on page 211 for details.*
Occupancy	Displays the occupancy value assigned to the selected Location.
Owner	Displays the name of the selected Location's Owner.
Telephone	Displays the telephone number associated with the selected Location.
In Maintenance	The presence of the *In Maintenance* icon indicates that the selected Location is currently in Maintenance Mode. See the *Maintenance Mode for Locations* section on page 122.

- This information is entered and can be edited in the *Location Properties* page - **Settings** tab (see page 108).
- See *Editing a Location* on page 115 for details.

Location Details Window - Client Gateways Tab

This tab displays information relating to the Client Gateways assigned to the selected Location in the form of a table (FIG. 171):

FIG. 171 Location page - Locations Details window (Client Gateways tab)

Client Gateways Tab Columns	
ID	Displays the device ID of each Client Gateway in the selected Location.
IP Address	Displays the IP Address of each Client Gateway in the selected Location.
RMS SDK	Displays the version number of the RMS SDK used by each Client Gateway in the selected Location.
Online	Indicated the current state (online/offline) of each Client Gateway in the selected Location (*green* = online, *red* = offline)

See *Management - Client Gateways (Classic UI)* on page 93 for details.

Location Page - Actions Window

The options in the *Actions* window allow you to perform several actions on a selected Location without having to leave the Locations page (FIG. 172).

FIG. 172 Location page – Actions window

Actions Window Options	
Enable/Disable Maintenance	Click to enable maintenance mode on the selected Location (see the *Maintenance Mode for Locations* section on page 122). When Maintenance is enabled for a Location, this button changes to "*Disable Maintenance*" (click to disable Maintenance), and the Maintenance icon is displayed in the *In Maintenance* column of the Locations window. • See *Enabling Maintenance Mode for a Location* on page 122 for details.
View Location Assets	Click to open the *Asset Management* page for the selected location. See the *Management - Assets (Classic UI)* section on page 125 for details.
Web Control	If the selected Location has a Web Control URL configured, this option will open the specified Web Control page in a new browser window. See the *Using Web Control for a Location* section on page 124 for details.
Map To Location	If the selected location has a map URL configured (via the *Web Control URL* field in the *Location Properties* page - **Settings** tab - see FIG. 173 on page 108), this option will open the link in a new browser window. See the *Viewing a Location Map* section on page 124 for details.

Location Properties Page

In the Location page, click **Add** or **Edit** to open the *Location Properties* page. This page contains three tabs: *Settings*, *Metadata* and *Service Requests*. Use the options in these tabs to define a new Location or to edit the properties of an existing Location, as described in the following sections.

Location Properties Page - Settings Tab

The initial view of the *Location Properties* page is the **Settings** tab (FIG. 173). This tab is opened when you select to create a new Location or to edit an existing Location.

FIG. 173 Location Properties page – Settings tab

The options on the *Location Properties* page - **Settings** tab are described below:

Settings Tab Options	
Name	Enter a descriptive name for this Location.
Description	Enter a brief text description for this Location (optional).

Settings Tab Options (Cont.)	
Group	By default, the newly created Location will be located inside the Location Group selected in the Group window. This can be changed via the *Group* drop-down menu. This menu operates just like the Groups window, showing all current Groups and Sub- Groups in a hierarchical tree structure (see the *Location Page - Groups Window* section on page 104). When this Location is created (via the *Apply* button), it will be added to the selected Group.
Owner	Enter the name of the Location's Owner in this text field (optional).
Classification Level	Select a Classification Level to apply to this Location. Click the down arrow to open the Classification Level menu. See the *Location Classification* section on page 242.
Locale	Use this drop-down menu to select a localization (language) option for this Location. • Default = *English (United States)*
Time Zone	Use these two drop-down menus to set the Country and Time Zone for this Location. Location time is calculated from UTC to the location or room's configured time zone. This calculated time includes daylight savings time shifts for the Location's configured time zone. • Default = *Current system time zone* • If a Time Zone is not specified for a Location, then the default System Time Zone will be used. The System Time Zone is set in the *Localization* page. See the *Application Time Zone* section on page 211 for details.
Occupancy	Occupancy represents the number of people that will utilize this Location. Use the up / down arrows to set an Occupancy number for this Location. Alternatively, manually type a numeric value into this field. This value is optional but helps users find a room that meets their needs through the RMS application's room search. • Range = 0-100,000 • Default = 0
Phone Number	Enter the phone number of this Location in this text field (optional).
URL To Map of Location	This is a URL link to a map of the room (optional). While the RMS application does not provide any facility to generate and manage maps of your facility, this link is provided so users can access a map of the facility with the room shown if you have access to such maps. • Enter the URL of the desired map file in this text field. • Click **Open** to open the file indicated in the URL. • Once this field is populated, the **Map To Location** button (in the *Actions* window) is enabled for this Location. See the *Viewing a Location Map* section on page 124 for details.
Web Control URL	This is the Web Control URL of the room (optional). This link is provided to allow quick access to any HTML based control panels that may have been programmed into the NetLinx system. • Enter the URL of the Web Control page in this text field. • Click **Open** to open the indicated URL. • Once this field is populated, the **Web Control URL button** (in the *Actions* window) is enabled for this Location. See the *Using Web Control for a Location* section on page 124 for details.
Scheduling Configuration	Before an RMS Location can synchronize with Exchange, each Location must be associated with a Resource Profile. Under *Scheduling Configuration*, open the Resource Profile drop-down list to select a Resource Profile to map to this Location. Refer to the Installation Guide for the RMS Enterprise Scheduling Interface (in the "Location to Resource Profile Mapping" section) for details.
Apply	Click to save changes.

Refer to the following sections for instructions on using the options in the *Location Properties* page - **Settings** tab:

- *Adding a New Location* section on page 114
- *Editing a Location* section on page 115
- *Deleting a Location* section on page 115

Location Properties Page - Metadata Tab

The **Metadata** tab of the *Location Properties* page (FIG. 174) provides the ability to enter Location-specific metadata:

FIG. 174 Location Properties page - Metadata tab

Location Metadata Properties

Each Location in the RMS system hosts a listing of metadata (user-defined) properties. Location metadata properties are derived either from the global metadata definitions or defined as discrete instance properties for the individual location record.

NOTE: *Global metadata definitions are managed via options in the System Configuration > Metadata page. See the Metadata section on page 225 for details.*

- Metadata definitions assigned to the *All Locations* category are automatically inherited on the location metadata listing page. The defined metadata property will be listed with its default value.   This metadata value can be edited to override the default value and assign a location specific instance value to the metadata property.
- Metadata definitions assigned to the *Location Groups* category are automatically inherited by all Locations contained in that Group. The defined metadata property will be listed with its default value.   This metadata value can be edited to override the default value and assign a location specific instance value to the metadata property.
- Metadata properties inherited by global definition cannot be deleted from the location instance. If an overriding value has been applied for the location instance, that value can be reverted back to the definitions default value.
- Location instance metadata properties can be created in an ad-hoc manner to capture unique properties for an individual location. These location instance metadata properties are not shared to any other location. Location instance metadata properties can be deleted from the location metadata listing page.
- The authenticated user must have the global permission of Manage Clients and Locations to access and manage location based metadata values.

The options on the *Location Properties* page - **Metadata** tab are described below:

Metadata Tab Options	
Add	Click to add a new Location Metadata item for the selected Location. See the *Adding Location Metadata* section on page 119 for details.
Edit	Click to edit an existing Location Metadata item for the selected Location. See the *Adding Location Metadata* section on page 119 for details.
Delete	Click to delete the selected Location Metadata item. See the *Deleting Location Metadata* section on page 120 for details.
Search	Use this search field to perform a search for Location Metadata names.
Location Metadata Table	Each Metadata entry associated with the selected Location is listed in this table. The columns in this table indicate each metadata entry's properties (*Category*, *Name*, *Value*, *Editable* and *Description*). These properties represent the properties defined in the *Metadata Editor* dialog (see the *Adding Location Metadata* section on page 119). • For descriptions of the *Metadata Categories*, see page 226. • For descriptions of the *Metadata Data Types*, see page 227.

Refer to the *Adding Location Metadata* section on page 119 for instructions on using the options in the *Location Properties* page - **Metadata** tab.

Location Properties Page - Service Requests Tab

Service Requests are messages sent to the RMS Server from a Touch Panel in the System. All service requests in the RMS system are Location-based. The **Service Requests** tab of the *Location Properties* page (FIG. 175) provides the ability to view and manage Service Requests:
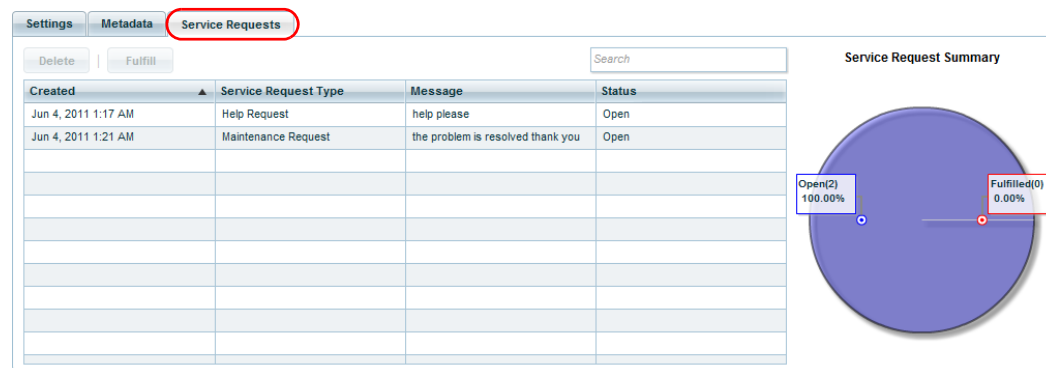
FIG. 175 Location Properties page - Service Requests tab

The options on the *Location Properties* page - **Service Requests** tab are described below:

Service Requests Tab Options	
Delete	Click to delete the selected Service Request(s). See *Deleting a Service Request For a Location* on page 121 for details.
Fulfill	Click to mark the selected Service Request(s) as *Fulfilled*. Note that this option is enabled only if the request is in the open state.See *Fulfilling a Service Request for a Location* on page 122 for details.
Search	Click to search for a specific Service Request. See *Searching for a Service Request* on page 121 for details.

Service Requests Tab Options (Cont.)	
Location Service Requests Table	Each Service Request associated with the selected Location is listed in this table. The columns in this table indicate each Service Request entry's properties (*Created*, *Message* and *Status*).
Service Request Summary window	The chart in this window provides a graphical summary of the status of the requests listed in the Location Service Requests Table (*Open* vs *Fulfilled*).

Refer to the following sections for instructions on using the options in the *Location Properties* page - **Service Requests** tab:

- *Deleting a Service Request For a Location* section on page 121
- *Fulfilling a Service Request for a Location* section on page 122

Working With Location Groups

Searching For Location Groups

Use the *Search* tool in the Groups window to search for a specific Location Group by name (FIG. 176).
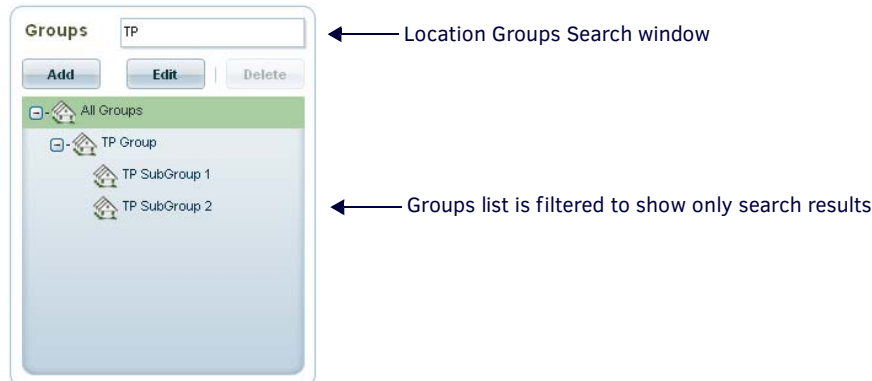
FIG. 176 Groups window - Search window

Adding (Creating) a New Location Group

Use the options in the *Location Group* dialog to add (create) a new Location Group:

1. Click the **Add** button in the *Location Groups* window (see FIG. 168 on page 104), or select **Add** in the Location Groups window context menu (see page 105) to invoke the *Location Group* dialog (FIG. 177).

FIG. 177 Location Group dialog (initial view)

2. In the **Group Name** text field, enter a name for the new Group.

3. By default, the parent Group for the new Location is the one selected in the Groups window at the point that the Add button is clicked, but it can be changed via the Parent Group drop-down menu. Select a Parent Group from the **Parent Group** menu.
   - Select *All Groups* to add the new Group as a top-level entry in the Groups list (displayed in the Groups window). If no other Groups have been defined, then the only option here is to select *All Groups*.
   - Once one or more Groups have been defined and added, they can be selected as Parent Groups for subsequent new Groups. To select a Parent Group for a new Group that you are creating, click the "plus" icon next to **All Groups** to expand the list to show all Groups, and select a Parent Group.

     When a Group is added to *All Groups*, it is represented in the Groups window as a Sub-Group, nested beneath the top-level All Groups entry.

When a Group is added to a *Parent Group*, it is represented in the Groups window as nested beneath the selected Parent Group (FIG. 178):

All Groups represents the top-level Parent Group

Location Group ("TP Group")
Sub-Groups to the "TP Group"
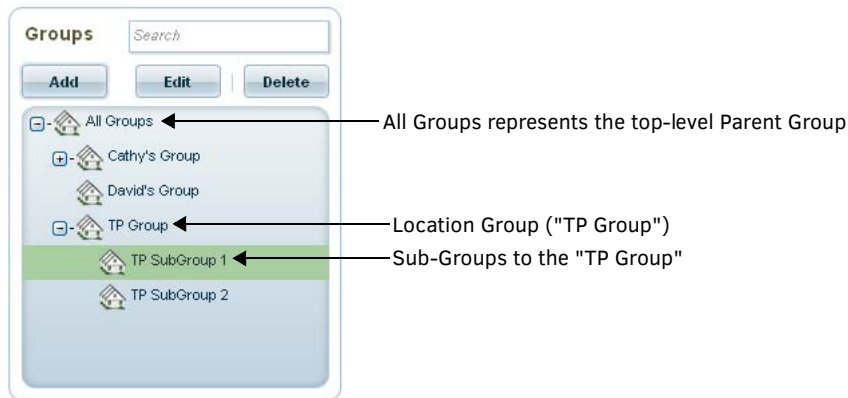
FIG. 178 Location Group window

4. In the **Description** field, enter a brief text description of this Group (optional).

5. Add Locations to this Group (optional):

NOTE: *RMS will allow you to create a new Location Group without adding any Locations. You can always add Locations later by editing the Group (see Editing a Location Group on page 112).*

   a. In the **Available Location** field, click the down arrow to open a drop-down menu of unassigned Locations available to add to this Location Group.

   The Locations listed in this menu represent Locations that have been defined, and are currently assigned to the top-level default "*All Groups*" (as opposed to a custom defined Location Group).

     • Each Location can only be included in one Location Group at a time.

     • See the *Adding a New Location* section on page 114 for details.

   b. Select a Location and click **Add**. This adds the selected Location to the list at the bottom of this dialog.

   c. Add other available Locations as desired, then click **Save** to save all changes and close the *Location Group* dialog (FIG. 179).

Click to select from a drop-down list of un-assigned Locations

Click to add the selected Location to this Group

Click to save changes and close this dialog
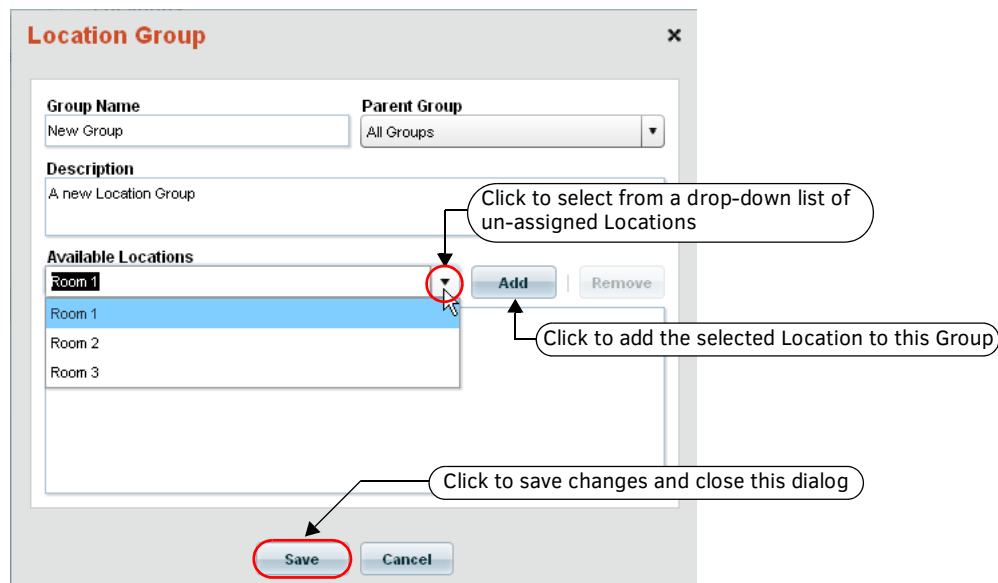
FIG. 179 Location Group dialog

The Location(s) added are represented in the *Locations* window when the Group is selected in the *Groups* window. See the *Location Page - Locations Window* section on page 105 for details.

Editing a Location Group

1. Select the Location Group that you want to edit in the *Location Groups* window.

2. Click the **Edit** button (in the *Groups* window) to invoke the *Location Group* dialog (see FIG. 177 on page 111). Alternatively, double-click on a Location Group to access this dialog.

3. Edit the Location Group's properties and its Locations list as desired.

   • To add a Location to this Group, select a Location, and click the **Add** button.

- To remove a Location from this Group, select the unwanted Location and click the **Remove** button.

4. Click **Save** to save all changes and close the *Location Group* dialog.

Deleting a Location Group

Location Groups can be deleted from the system only if they do not contain any Sub-Groups or Locations.

1. In the Location page, select a Location Group in the *Location Groups* window.

2. Click the **Delete** button (FIG. 180).
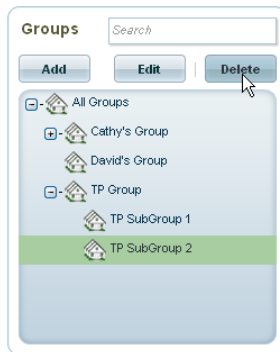
FIG. 180 Location Groups window - Delete button

NOTE: *The Delete button is only enabled if the selected Group(s) do not contain any Locations (see Editing a Location Group on page 112 for instructions on removing Locations from Groups).*

3. The system will prompt you to verify this action before the Group is deleted, via the *Delete Confirmation* dialog (FIG. 181):
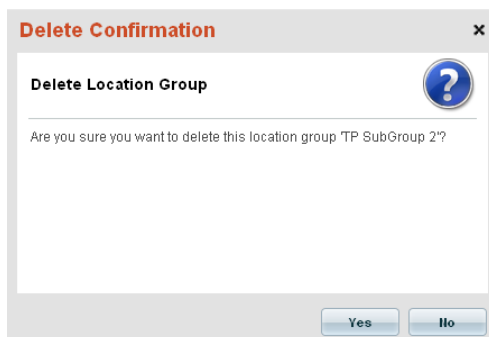
FIG. 181 Delete Location Group Confirmation dialog

4. Click **Yes** to proceed.

Moving a Location Group

RMS Enterprise supports drag-and-drop for relocating Location Groups: In the *Groups* window, click on a Location Group and drag-and-drop it onto a new parent Location Group (FIG. 182).
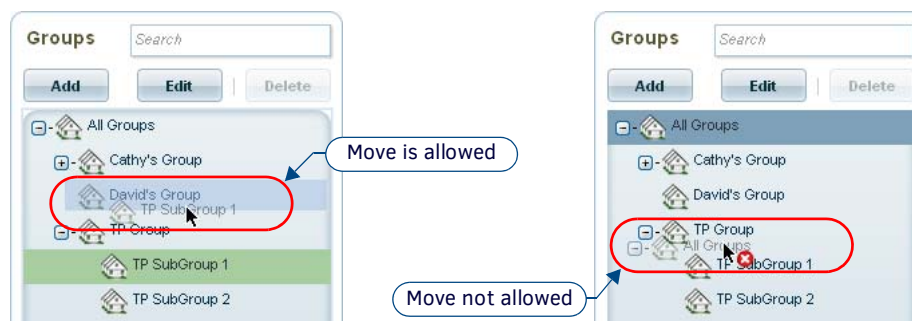
FIG. 182 Moving Location Groups via Drag-and-Drop

- The *All Groups* group cannot be relocated
- A Location Group cannot be dropped onto itself, or onto its existing parent group
- A small red "X" icon indicates when the drop target is not valid (see FIG. 182)

NOTE: *Permission implications may apply when moving a Location or Location Group. Refer to the Management - Roles (Classic UI) section on page 192 for details.*

Working With Locations

Searching for a Location

Use the *Search* tool in the Locations window to search for a specific Location (FIG. 183).
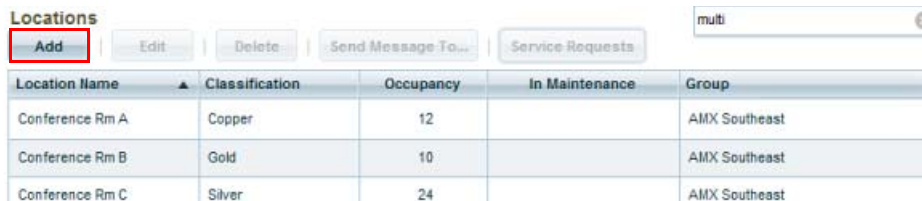
FIG. 183 Locations Table - Search window

After entering a string in the Search window, press *Enter* to filter the listing in the Locations window.

Adding a New Location

1. In the *Locations* window, click the **Add** button (FIG. 184).
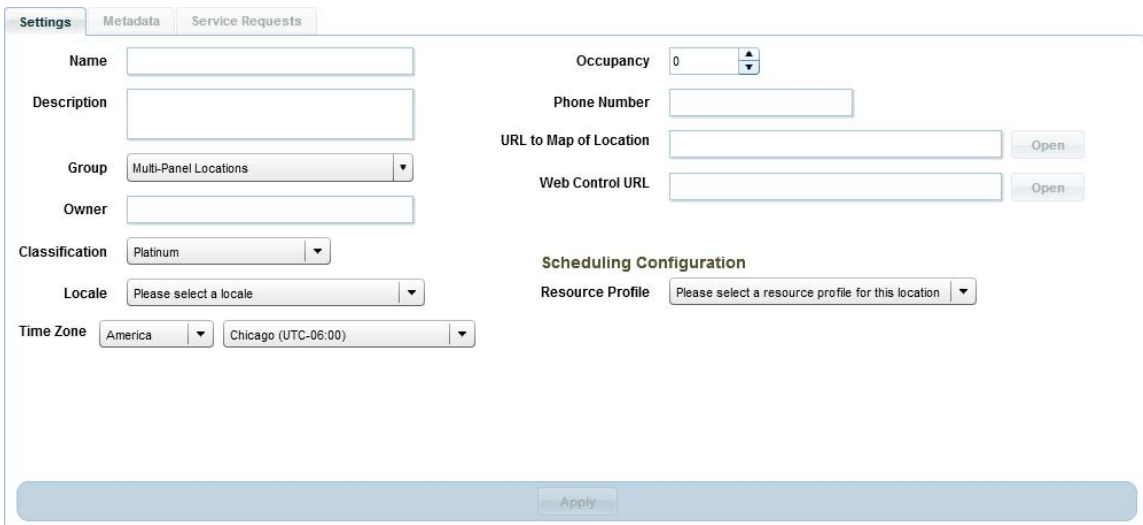
FIG. 184 Locations window - Add button

2. This opens the *Location Properties* page - **Settings** tab (FIG. 185).

FIG. 185 Location Properties page - Settings tab (new Location)

3. Fill in each field to define the new Location.

4. Click **Apply** to create this Location (enabled only after information has been entered). This action activates the other two tabs in the *Location Properties* page: *Metadata* and *Service Requests*.

5. Open the **Metadata** tab to enter metadata describing this Location. See the *Adding Location Metadata* on page 119 for details.

6. Open the **Service Requests** tab to manage service request notifications received by this Location. See the *Location Properties Page - Service Requests Tab* section on page 110 for details.

   - To view or edit this Location, select the Group to which it was added (in the *Groups* window). This Location as well as any others that belong to the selected group are listed in the table.

   - Select any Location in the table to populate the Properties window with the selected Location's Settings.

Editing a Location

1. With a Location selected in the table, click the **Edit** button (FIG. 186).

FIG. 186 Locations window - Edit button

2. This opens the *Location Properties* page - **Settings** tab (FIG. 187).
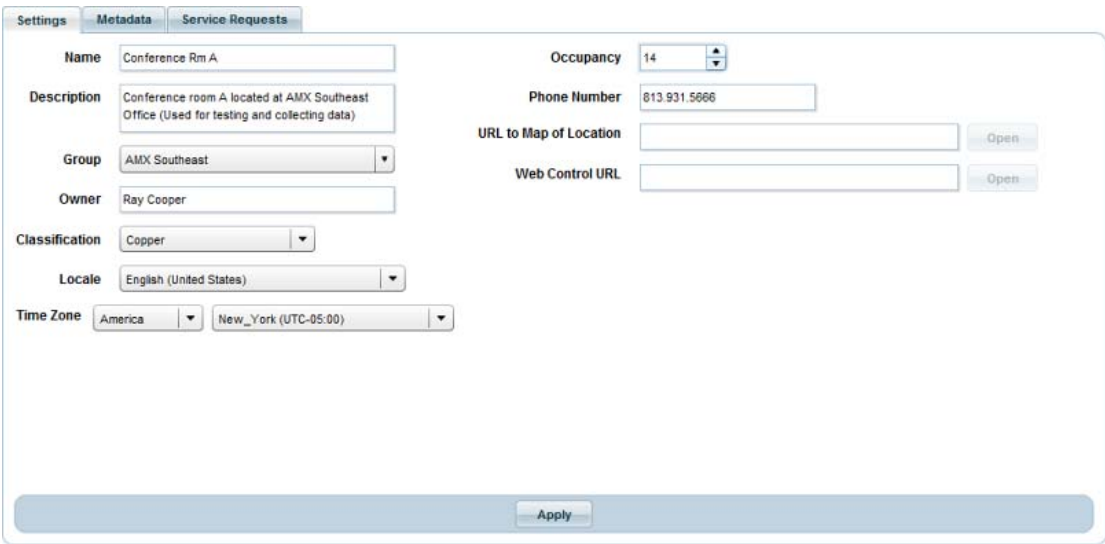
FIG. 187 Location Properties page - Settings tab (Editing Properties for an existing Location)

3. Edit the fields in this tab as necessary.

4. Click the **Apply** button to save changes.

5. Open the **Metadata** tab to enter metadata for the new Location.
   See the *Location Properties Page - Metadata Tab* section on page 109 for details.

6. Open the **Service Requests** tab to define service requests for the new Location.
   See the *Location Properties Page - Service Requests Tab* section on page 110 for details.

Deleting a Location

Use the *Delete* option in the Locations page - Locations window to delete a selected Location.

NOTE: *Deleting a Location will un-assign all Client Gateways, and delete all Assets, Asset Parameters, Asset Logging, and associated Parameter History for the deleted Location.*

1. In the Locations page - Locations window, select the Location to delete.

2. Click **Delete** (FIG. 188):
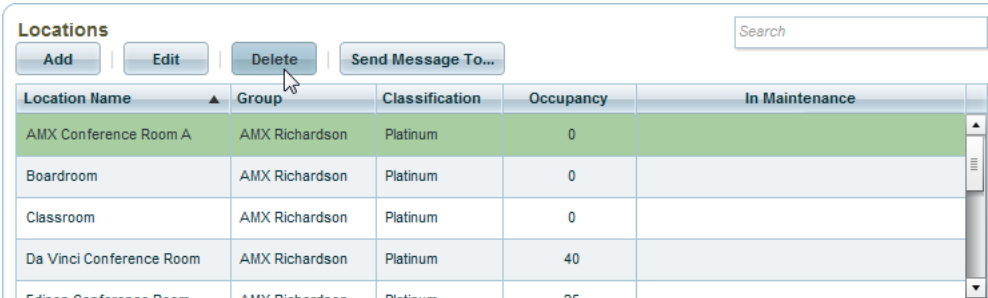
FIG. 188 Locations window - Delete button

3. The program will prompt you to verify this action before proceeding (FIG. 189):
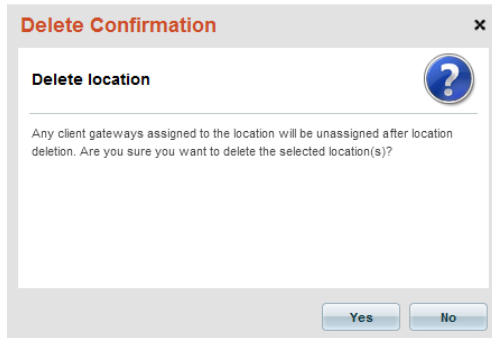
FIG. 189 Delete Confirmation dialog - Delete Location

4. Click **Yes** to proceed.

Setting a Custom Time Zone For a Location

The local time for Locations is calculated from UTC to the location's configured time zone. This calculated time includes daylight savings time shifts for the location's configured time zone. This location's property can be changed at any time by a system administrator or by each individual user in user profile management.

NOTE: *The location preferred time zone is used only to render time values to the user interface, reports, or user communications. All RMS data is stored in UTC time.*

1. In the Location Management page, select a location from the list in the *Locations* window.

2. Click **Edit** to open the *Location Properties* dialog (**Settings** tab).

3. Use the *Time Zone* drop-down menus to select a Time Zone for this location (FIG. 190).
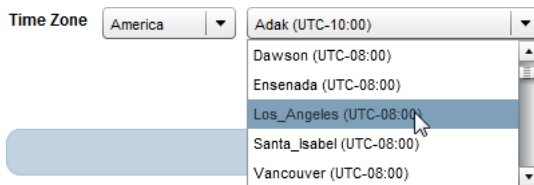
FIG. 190 Location Properties dialog (Settings tab) - Time Zone menus

4. Click **Save** to save your changes.

NOTE: *If a Location does not define a custom time zone, then the default system time zone will be used.*

Sending a Message to a Location
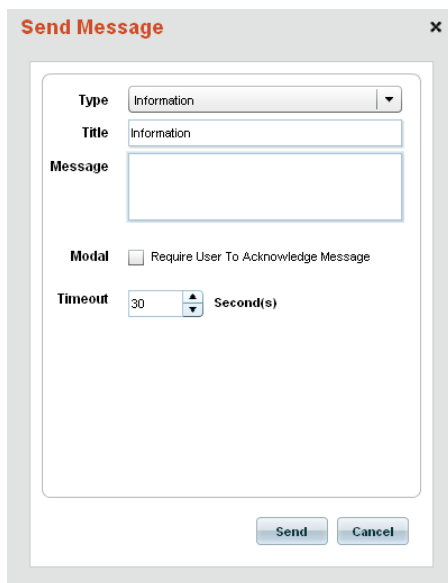
The *Send Message To* function allows you to construct a message bound to one or more selected Locations. These messages are displayed on the screen of Touch Panel(s) present in the specified Location.

1. With one or more Locations selected in the table, click the **Send Message To...** button (FIG. 191).

FIG. 191 Locations window - Send Message To button

2. This action invokes the *Send Message* dialog (FIG. 192):

FIG. 192 Send Message dialog

3. Select a message type from the **Type** drop-down menu.

    Message types are arbitrary, designed to provide distinction between the various types of messages that might be sent to a Location. Therefore there are no innate characteristics for each Message Type, assign them in any way that helps you to differentiate between types of messages.

    NOTE: *By default, new Messages are set to the Information message type.*

4. Enter a title for this message in the **Title** text field. The text is displayed as it will appear in the message in the **Message Preview** window. Note that a default title is provided for each message, based on the *Type* selected.

5. Enter the message text in the **Message** text field.

6. Click the *Require User To Acknowledge Message* option next to **Modal** to require the user to acknowledge the message dialog before it is removed from the screen (on the Touch Panel).

7. Set the **Timeout** value, in seconds (default = 30). The popup page will automatically be closed (on the Touch Panel) after the timeout period.

8. Click **Send** to send the message to the selected Location.

Moving a Location

Locations can be relocated to a different Location Group by dragging the target Location from the Locations window and dropping it on top of the new parent Group, in the *Locations Group* window (FIG. 193).
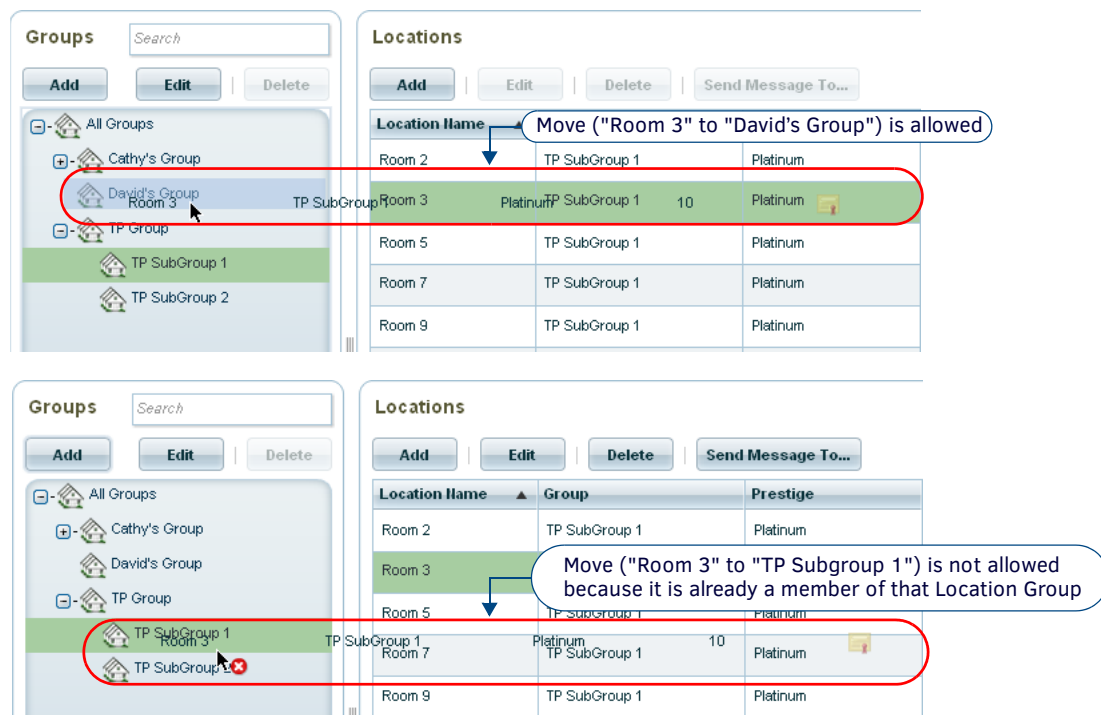
FIG. 193 Moving Locations via Drag-and-Drop

- A Location cannot be dropped onto itself, or onto its current parent Location Group.
- A small red "X" icon indicates when the drop target is not eligible (see FIG. 193).

Permissions on Moving Locations / Location Groups

Location-Level permissions can be applied to specific Location Groups or Locations via the **Location Level Permissions** tab of the Role Properties window (see FIG. 323 on page 198). For details on assigning Permissions, refer to the *Management - Roles (Classic UI)* section on page 192. When a Location Group or Location that has Location-Level permissions assigned to it is relocated to a new Location Group with it's own set of Location-Level permissions, it will automatically inherit the permissions assigned to the new parent Location Group.

The inherited permissions override any Location-Level permission associated with the Location or Location Group being moved. Therefore, note that this may result in the loss of Location-Level permissions.

Take care to understand what Location-Level permissions exist before relocating a Location Group or Location, as well as what Location-Level permissions are present in the target parent Location Group before relocating.

Working With Location Metadata

Searching for a Metadata

Use the *Search* tool in the **Metadata** tab (of the *Location Properties* page) to search for a specific Metadata entry (FIG. 194).

FIG. 194 Location Properties page - Metadata tab - Search window

This search tool searches across the data columns displayed in the **Metadata** tab.

Adding Location Metadata

Location-specific metadata can be managed via options in the Location Properties page.

NOTE: *To create metadata definitions that are available to all Locations (or to all Locations in a specific Location Group), use the options in the System Configuration - Metadata page. Refer to the Metadata section on page 225 for details.*

The authenticated user must have global Manage Clients and Locations permissions to add or edit Location Metadata.

1. With a Location selected in the *Locations* window, click the **Edit** button to open the *Location Properties* page, and click on the **Metadata** tab (FIG. 195).

FIG. 195 Location Properties page - Metadata tab

2. Click **Add** to add a new metadata definition to the selected Location. This action invokes the *Metadata Editor* dialog (FIG. 196):

FIG. 196 Metadata Editor dialog (Adding New Location Metadata)

3. Enter a name for the Metadata type in the **Name** text field.

4. Select a data type from the **Data Type** drop-down menu. See *Metadata Data Types* section on page 227 for details.

5. Enter a **Value** property, based on the selected Data Type:

    Metadata definitions must be assigned to a particular data type. The data type defines how the data will be stored and what type of UI will be presented to users when editing metadata values. The Metadata Data Types are described in the *Metadata Data Types* section on page 227.

    ● For *Strings*, enter a text string in the text field.
    ● For *Memos*, enter a text string in the expanded text field.
    ● For *Booleans*, click in the checkbox to specify *True* or *False*.
    ● For *Numbers*, use the up / down arrows (or direct edit) to set a numeric value (integer-only). Note that for the Numbers data type, decimals are automatically rounded to the nearest integer.
    ● For *Decimals*, enter a numeric (decimal) value.
    ● For *Dates*, click in the *Value* field, or click on the calendar icon to open a calendar pop-up. Select a date value.
    ● For *Times*, use the up / down arrows (or direct edit) to set Hour and Minute values, and select *AM* or *PM*.
    ● For *Hyperlinks*, enter the *Link Name* and *Link URL* in the text fields.
    ● For *Date/Times*, click in the Value field to open a calendar pop-up (select a Date value), and use the up / down arrows (or direct edit) to set *Hour* and *Minute* values, and select either *AM* or *PM*.

6. Click **OK** to save changes.

Editing Location Metadata

The authenticated user must have global Manage Clients and Locations permissions to add or edit Location Metadata.

1. With a Location selected in the *Locations* window, click the **Edit** button to open the *Location Properties* page, and click on the **Metadata** tab (FIG. 197).

FIG. 197 Location Properties page – Metadata tab

2. Click **Edit** to edit an existing metadata definition for the selected Location. This action invokes the *Metadata Editor* dialog (FIG. 198):

FIG. 198 Metadata Editor dialog (Editing Existing Location Metadata)

3. Edit the information in this dialog as desired.
4. Click **Save** to save changes.

Deleting Location Metadata

Location Metadata items that have been added to the *This Location* category (as opposed to the *All Locations* or *Location Group* category) can be deleted from this page:

1. With a Location selected in the table, click the **Edit** button to open the *Location Properties* page, and click on the **Metadata** tab (FIG. 199).

FIG. 199 Location Properties page – Metadata tab

2. Select a Metadata item with the Category listing of *This Location* and click **Delete**.
3. The program will prompt you to verify this action (FIG. 200):
4. Click **Yes** to proceed.
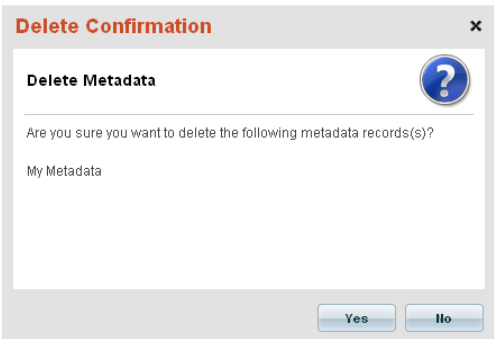
FIG. 200 Delete Confirmation dialog - Delete Metadata

Working With Location Service Requests

Searching for a Service Request

Use the *Search* tool in the **Service Requests** tab (of the *Location Properties* page) to search for a specific Service Request (FIG. 201).
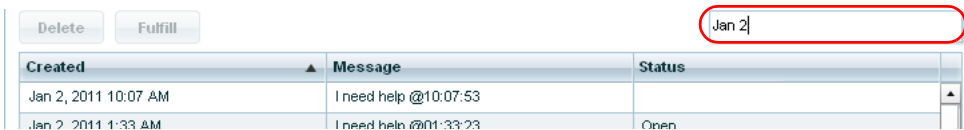
FIG. 201 Location Properties page - Service Requests tab - Search window

This search tool searches across the data columns displayed in the **Service Requests** tab:

Deleting a Service Request For a Location

Service Requests can be deleted from the list, without having been fulfilled:

1. With a Location selected in the table, click the **Edit** button to open the *Location Properties* page, and click on the **Service Requests** tab (FIG. 202).
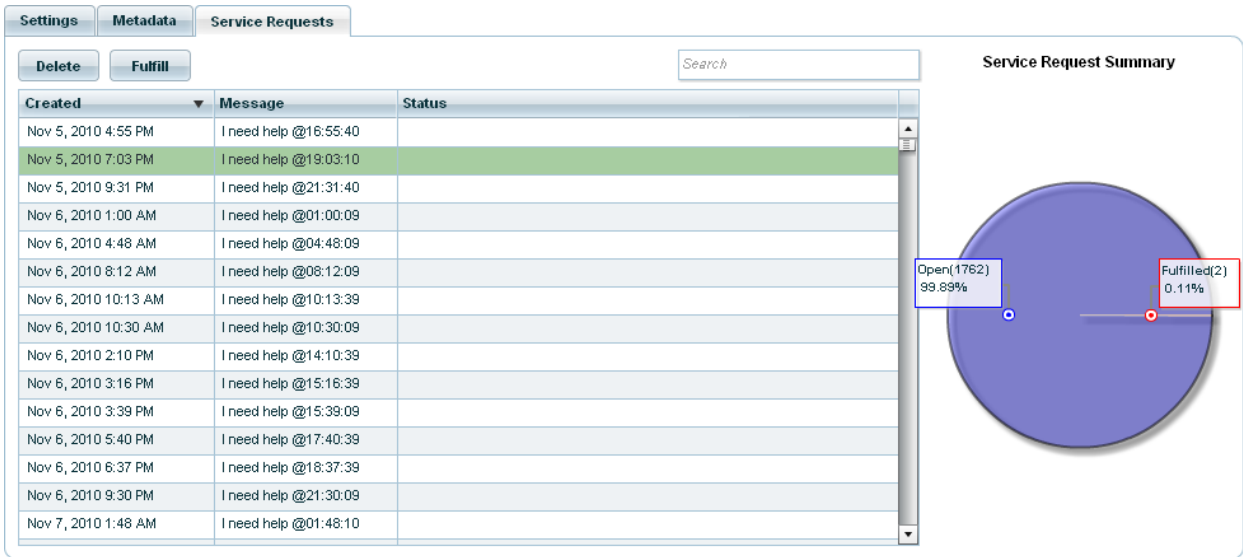
FIG. 202 Location Properties page - Service Requests tab

2. Select one or more Service Requests (*Ctrl + click* for multiple selection, *shift + click* for range select).

3. Click **Delete** to delete the selected Service Requests. The program will prompt you to verify this action (FIG. 203):
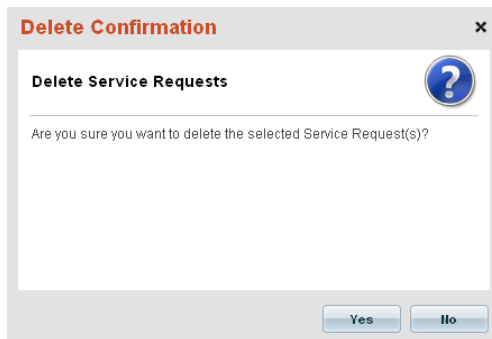
FIG. 203 Delete Confirmation dialog - Delete Service Requests

4. Click **Yes** to proceed.

Fulfilling a Service Request for a Location

Service Requests can be marked as *Fulfilled* in the list. Fulfilled implies that the Service Request has been responded to, the request has been fulfilled and no further action is expected, relative to this specific request. This option does not remove the Service Request from the list, but updates its Status from *Open* to *Fulfilled*.

1. With a Location selected in the table, click the **Edit** button to open the *Location Properties* page, and click on the **Service Requests** tab (see FIG. 202 on page 121).

2. Select one or more Service Requests (*Ctrl + click* for multiple selection, *shift + click* for range select).

3. Click **Fulfill** to mark the selected Service Requests as *Fulfilled* in the list (FIG. 204):

FIG. 204 Service Requests tab - Service Requests marked as "Fulfilled"

Maintenance Mode for Locations

When enabled for a Location, *Maintenance Mode* hides any Hotlist records for the Location and suppresses any outbound notifications for issues that occur in this Location. Maintenance Mode only suppresses Hotlist and notifications. Asset parameter changes are still accepted and applied, parameters can still be tripped, and changes are still recorded into the internal log.

When Maintenance Mode is disabled, any Hotlist records that exist for this Location are displayed. No notifications are sent for asset parameters that where tripped while in Maintenance Mode and are still tripped when Maintenance Mode is disabled. A single Hotlist record will be added to the Hotlist displaying that this location is currently in Maintenance Mode. When Maintenance Mode is disabled, this record will automatically be removed from the Hotlist.

Maintenance Mode is indicated in the location listing and the location details preview pane as an icon (FIG. 205):

FIG. 205 Maintenance Mode Enabled icon

NOTE: *Maintenance Mode can be applied to Locations, to Assets (see Maintenance Mode for Assets section on page 154), or to the entire System (see System Maintenance Mode section on page 210).*

Enabling Maintenance Mode for a Location

RMS allows users to place Locations into *Maintenance Mode*. When enabled, Location Maintenance Mode hides any Hotlist items for this Location and suppresses any outbound notifications for issues that occur in this Location while in Maintenance Mode. See *Maintenance Mode for Locations* on page 122 for more information. To enable Maintenance Mode for a Location:

1. Select a Location in the *Locations* window (see FIG. 169 on page 105).

2. Click the **Enable Maintenance** button in the *Actions* window, in the lower-right corner of the page (FIG. 206):
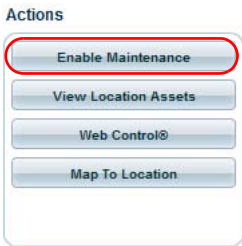
FIG. 206 Locations page – Actions window – Enable Maintenance

Alternatively, select **Enable Maintenance Mode** from the Locations window context menu (see *Locations Window Context Menu* on page 106).

3. Maintenance Mode is indicated in the Location window (in the *In Maintenance* column) and in the Properties window as an icon (FIG. 207):
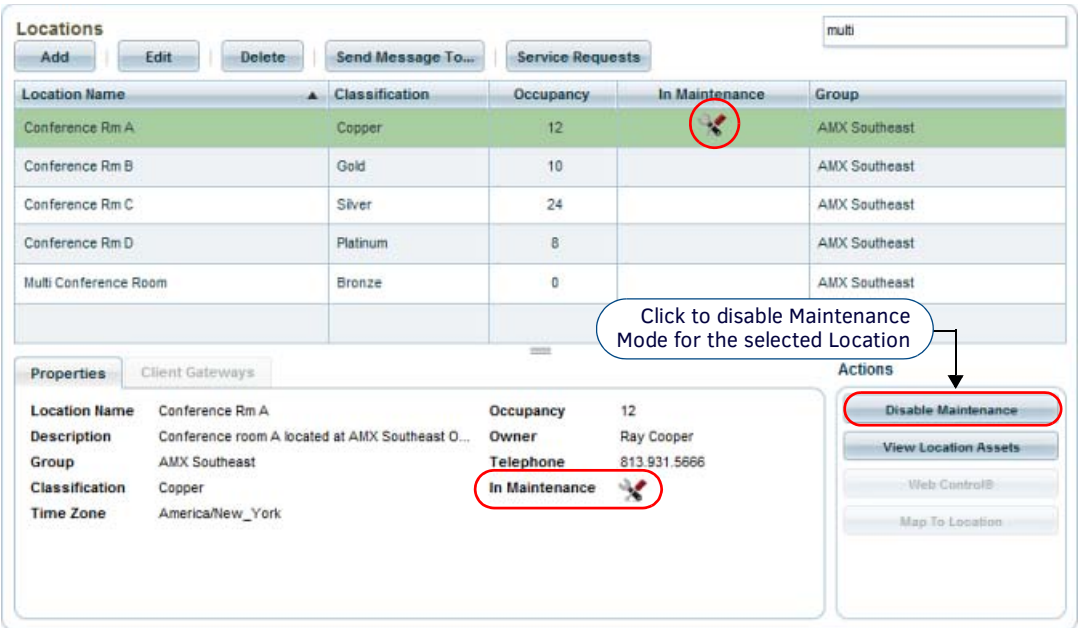
FIG. 207 Locations page – Maintenance Mode Enabled (for "AMX Conference Room A")

Disabling Maintenance Mode for a Location

1. Select a Location in the *Locations* window that currently has Maintenance Mode *Enabled*.
2. Click the **Disable Maintenance** button in the *Actions* window.

Viewing Location Assets

1. In the *Location* page, select a Location in the *Groups* window (FIG. 168 on page 104).
2. In the *Actions* window, select **View Location Assets** (FIG. 208).

Click to open the Asset Management page for the selected Location

FIG. 208 Locations page Actions window – View Location Assets

3. This action invokes the *Asset Management* page, listing all Assets contained in the selected Location (FIG. 209):

FIG. 209 Location Assets

Refer to the *Management - Assets (Classic UI)* section on page 125 for details.

Using Web Control for a Location

Web Control® provides quick access to any HTML based control panels that may have been programmed into the NetLinx system (or non-NetLinx system, such as CP-3000 keypads, which also send a web page URL). To use Web Control for a Location, the **Web Control URL** field (in the *Location Properties* page - **Settings** tab) must be filled in with a valid Web Control URL. See the *Adding a New Location* section on page 114 for details. Once a valid Web Control URL has been entered for the Location, the *Web Control* button in the *Actions* window is enabled (FIG. 210).

Click to open the URL specified in the Web Control URL field (Settings tab of the Location Properties page)
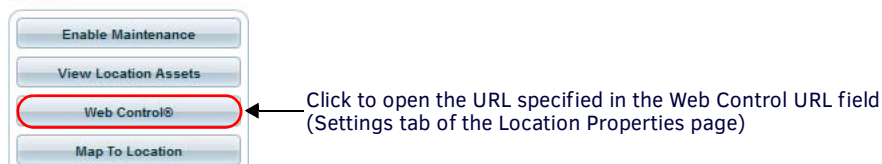
FIG. 210 Locations page - Actions window - Web Control

Click to open the Web Control URL in a new browser window. Alternatively, select **Web Control**® from the Locations window context menu (see page 106), or in the Hotlist Item Properties Window - Location tab (see page 69).

Viewing a Location Map

Map to Location represents a link to a URL that provides a map of the Location. This feature is provided so users can access a map of the facility if you have access to such a map. To associate a Map with a Location, the **URL to Map of Location** field (in the *Location Properties* page - **Settings** tab - see FIG. 173 on page 108) must be filled in with a valid URL for a page that displays a map of the Location. Once a valid URL has been entered for the Map of Location, the *Map To Location* button in the *Actions* window is enabled (FIG. 211).

Click to open the URL specified in the URL to Map of Location field (Settings tab of the Location Properties page)
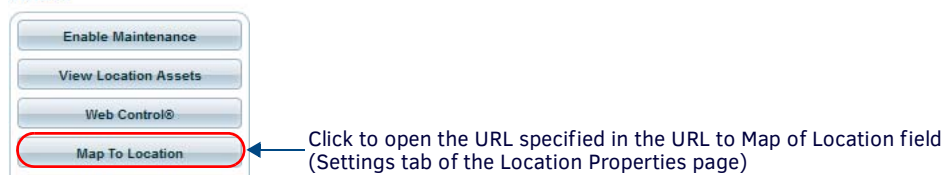
FIG. 211 Locations page - Actions window - Map To Location button

Click to open the *Map To Location* URL in a new browser window.

Management - Assets (Classic UI)

Overview

Click inside the **Management** tab (Classic UI) to access the *Management* menu. The options in this menu allow you to configure Locations/Systems, manage Assets, and manage Users & Notifications, as described in the following sections.

The options in the **Asset Management** category of the (Classic UI) *Management* menu allow you to configure *Assets* and *Control Macros* (FIG. 212):
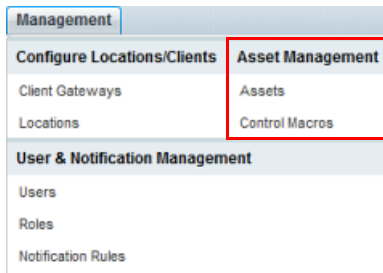
FIG. 212 Management menu - Asset Management

NOTE: *To access the RMS Classic UI described in this section, select "Classic UI" from the RMS Enterprise HTML interface menu bar.*

Asset management in RMS includes managing *Assets*, as well as *Asset Parameters* and *Control Macros*. These instructions are provided in the following sections:

- *Working With Asset Parameters* on page 158.
- *Management - Control Macros (Classic UI)* on page 165.

Assets

All monitored devices, virtual devices, and un-monitored physical devices in the RMS system are *Assets*.

NOTE: *Un-monitored devices include flip charts, white boards etc.*

An Asset is any device or object assigned to a Location and tracked by the RMS system.

- All Assets are configured and managed via options in the **Asset Management** page.
- To open the *Asset Management* page, select **Assets** under *Asset Management* in the Management menu (FIG. 213).
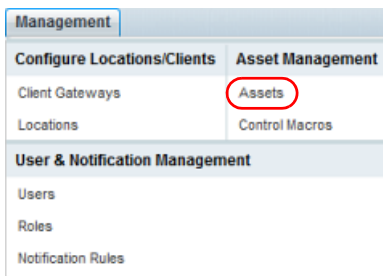
FIG. 213 Management > Asset Management > Assets

Asset Management Page

Select **Assets** under *Asset Management* in the Management menu to open the *Asset Management* page. The features of this page are organized into several windows (FIG. 214): The *Locations* window on the left, and the *Assets* window on the right.

- Use the **Locations** window to view and select Locations - see page 127.
- Use the **Assets** window to view and manage Assets - see page 128.
- Use the **Asset Parameters** window to view details on the parameters of the selected Asset - see page 130.
- Use the **Actions** window to execute various Asset-based actions - see page 130.

FIG. 214 Asset Management page

Asset Permissions

The Asset Management UI is accessible if the authenticated user has either View or Manage locations based Asset permissions.

- If the authenticated user has *Manage Assets* permissions, the user can edit/delete all assets, asset parameters, asset metadata, asset parameter thresholds, etc.
- If the authenticated user only has *View Assets* permissions, the user can view all assets, asset parameters, asset metadata, asset parameter thresholds, etc. but not make any changes.
- The *Locations* window only displays Location Groups and Locations for which the current user has permissions.

Asset Management Page - Locations Window

Use the **Locations** window to select a Location in order to manage its Assets (FIG. 215).

Search for Location / Location Group names

"All Groups" is the top-level (click '+' to expand)

User-defined Location Groups (click '+' to expand)
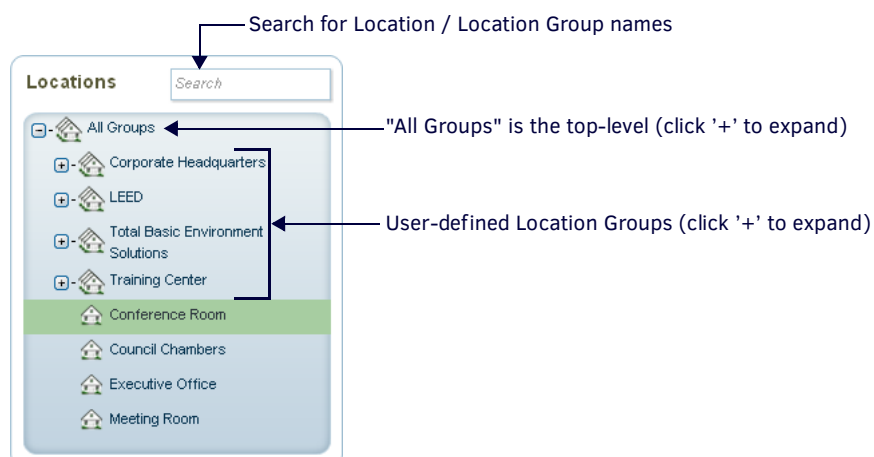
FIG. 215 Asset Management page - Locations window

- Initially, the *Locations* window indicates only the *All Groups* folder, until one or more Locations and Location Groups are defined.

  See the *Adding (Creating) a New Location Group* section on page 111.

  See the *Adding a New Location* section on page 114.

NOTE: *If there are unassigned assets present in the system, then they are listed in the Unassigned Assets folder at the top of the listing in the Locations window.*

- The Locations view shows all current Groups, Parent Groups and Locations in a hierarchical tree structure, in the same way as does the Groups window in the *Location* page. See the *Location Page - Groups Window* section on page 104 for details.
- Use the *Search* field to perform a search for Location / Location Group names. See the *Searching For Location Groups* section on page 111 for details.

Locations Window Context Menu

Right-click inside the *Locations* window (in the Asset Management page) to access the Locations window context menu. The options in this menu are described below:

Locations Window Context Menu Options	
Edit Group	Click to edit the selected Location Group, in the *Location Group* dialog. • This option is only visible if a Location Group is selected, and the user has the global permissions for Manage Clients and Locations (see the *Management - Roles (Classic UI)* section on page 192). • See the *Editing a Location Group* section on page 112 for details.
Edit Location	Click to edit the selected Location, in the *Location Properties* page (see page 108). • This option is only visible if a Location is selected, and the user has the global permissions for Manage Clients and Locations (see the *Management - Roles (Classic UI)* section on page 192). • See the *Editing a Location* section on page 115 for details.
Send Message to Locations/Group	Click to send a message to the selected Location(s) and Location Group(s). Note that when a Group containing sub-Groups and or Locations is selected, this option will send a message to all sub-Groups and Locations contained therein. See *Sending a Message to a Location* on page 116 for details.
Refresh	Click to refresh the Location Group tree.

Asset Management Page - Assets Window

Use the **Assets** window in the *Asset Management* page to view and manage Assets. The listing of Assets displayed in this window (in the *Assets Table*) represent the Assets that have been assigned to the Location selected in the *Locations* window, or the Assets returned via Asset search results. Initially, the Assets Table is empty, until a Location that has Assets defined is selected in the *Locations* window, or until a search for Assets is performed. FIG. 216 shows the Assets window indicating several sample Assets:
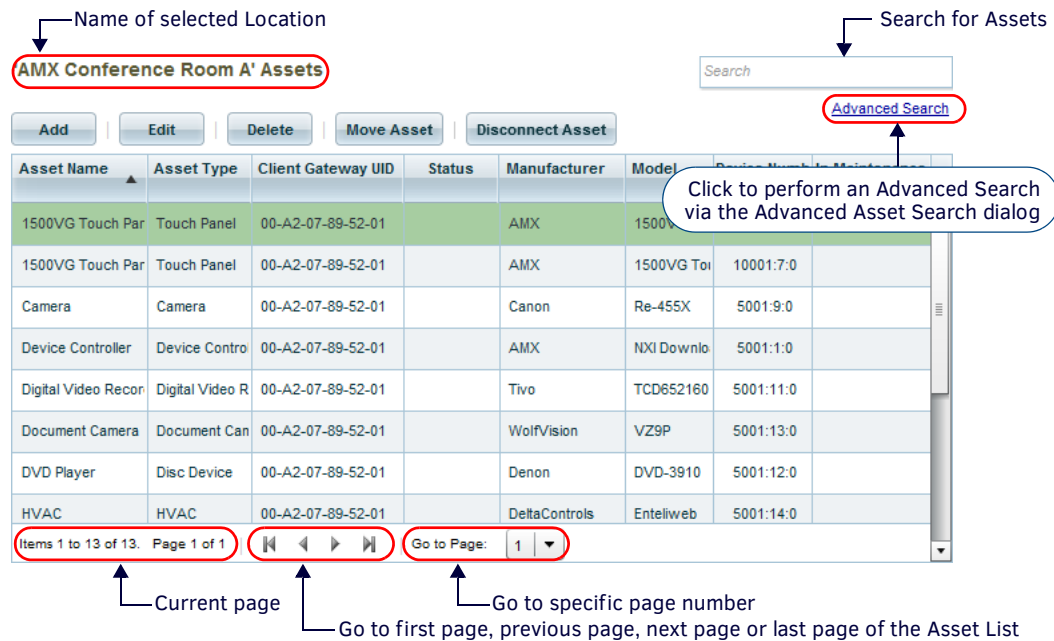
FIG. 216 Asset Management page - Assets window

The options in the *Assets* window are described below.

Assets Window Options	
Search	Use this search field to perform a search for asset names. See *Searching for Assets* on page 153.
Advanced Search	Click to invoke the *Advanced Asset Search* dialog. See *Performing an Advanced Asset Search* on page 153 for details.
Add	Click to invoke the *Add Asset* dialog, in which you can define a new Asset. See *Adding an Asset to a Location* on page 149 for details.
Edit	For users that have Edit Assets permissions, this button invokes the *Asset Management* page, in which you can view/edit a selected Asset. See *Editing an Asset* on page 149 for details. If the current User does not have Edit Assets permissions, then the *Asset Management page* is read-only. See the *Management - Roles (Classic UI)* section on page 192 for details on Roles and Permissions.
Delete	Click to delete the selected Asset. See *Deleting an Asset* on page 149 for details.
Move Asset	Click to move the selected Asset to a different Location, via the *Move Asset to another location* dialog. See *Moving an Asset (via the Move Asset Button)* on page 150 for details. *Note: This availability of this option is permission-dependant. See the* Management - Roles (Classic UI) *section on page 192 for details on Roles and Permissions.*
Disconnect Asset	This option is useful in cases where an asset needs to be temporarily removed from it's Location, with the intention of replacing it later (without losing the Asset's historical information). Unlike deleting an Asset, disconnecting an Asset will not delete Parameters, Metadata, Control Methods or Location History associated with that Asset. When the disconnected Asset is re-connected, all Asset information will be available. See *Disconnecting Assets* on page 152 for details.
Assets Table	The Assets Table lists each asset that is included in the selected Location or Search operation, providing basic asset information (*Asset Name, Asset Type, Client Gateway UID, Status, Manufacturer, Model, Device Number, In Maintenance*). *Note: These properties are defined in the Asset Management page, when the asset is added or edited. See the Adding an Asset to a Location section on page 149.* • Click any column heading to sort the table by that column. Clicking the same column heading again will reverse the direction of the sort. • Double-click an Asset to open the multi-tabbed *Asset Management* page for the selected asset. The options in the *Asset Management* page allow editing of the selected Assets' properties (see the *Asset Properties Page* section on page 131). • See *Editing an Asset* on page 149, see *Deleting an Asset* on page 149.

Assets Window Context Menu

Right-click inside the *Assets* window (in the Asset Management page) to access the Assets window context menu. The options in this menu are described below:

Assets Window Context Menu Options	
Add Asset	Click to create (add) a new Asset. This action invokes the *Add Asset* dialog. See *Adding an Asset to a Location* on page 149 for details.
Edit Asset	Click to edit the selected Asset in the *Edit Assets* page. *Note: Alternatively, double-click on an Asset to edit.* See *Editing an Asset* on page 149 for details.
Delete Asset	Click to delete the selected Asset. *Note: Deleting an Asset will also delete all Asset Parameters and Asset History.* See *Deleting an Asset* on page 149 for details.
Move Asset	Click to move the selected Asset to another Location. This action invokes the *Move Asset to another location* dialog. See *Moving an Asset (via the Move Asset Button)* on page 150 for details.
Disconnect Asset	The Disconnect Asset option is useful in cases where an asset needs to be temporarily removed from it's Location, with the intention of replacing it later (without losing the Asset's historical information). Unlike deleting an Asset, disconnecting an Asset will not delete Parameters, Metadata, Control Methods or Location History associated with that Asset. When the disconnected Asset is re-connected, all Asset information will be available. See *Disconnecting Assets* on page 152 for details.
Refresh	Click to refresh the listing in the Assets window.
Select All Assets	Click to select all Assets in the Assets window.
Select None	Click to de-select all Assets in the Assets window.
Web Link - Manufacturer	Click to open the web link that was defined for the Manufacturer of the selected Asset (if applicable). The *Manufacturer* web link URL is defined in the *Edit Manufacturer* dialog. See the *Manufacturers/Models* section on page 246 for details.
Web Link - Model	Click to open the Model web link that was defined for the selected Asset (if applicable). The *Model* web link URL is defined in the *Add Model* dialog. See the *Manufacturers/Models* section on page 246 for details.
Enable/Disable Maintenance Mode	Click to enable Maintenance Mode on the selected Asset. This is the same as clicking the **Enable/Disable Maintenance** button in the *Actions* window (see FIG. 218 on page 130). When Maintenance is enabled for a Location: • This button changes to "*Disable Maintenance*" (click to disable Maintenance) • The Maintenance icon is displayed in the *In Maintenance* column of the Locations window. • See *Enabling / Disabling Asset Maintenance Mode* on page 154 for details.
Execute Control Methods	Click to execute any Control Method that has been defined for the selected Asset. This is the same as clicking the **Execute Control Methods** button in the *Actions* window (see FIG. 218 on page 130). • Clicking this button opens the *Control Methods* dialog, in which you can select a Control Method to execute. • See *Executing a Control Method* on page 162 for details.
Reset all Tripped Parameters	Click to reset all tripped parameters for the selected Asset. This is the same as clicking the **Reset all Tripped Parameters** button in the *Actions* window (see FIG. 218 on page 130). See *Resetting Tripped Parameters* on page 160 for details.
Reset all Source Usages	Click to reset all Source Usage statistics for the selected Asset(s). This action is the same as clicking the **Reset** button in the *Source Usage* widget (see the *Source Usage Widget* section on page 81), or the **Reset All Source Usages** button in the *Actions* window (see FIG. 218 on page 130). See *Resetting Source Usage Statistics for an Asset* section on page 161 for details.

Asset Management Page - Asset Parameters Window

The *Asset Parameters* window lists all Parameters associated with the selected Asset, indicating the *Parameter Name*, *Asset Name*, *Current Value* and *Status* of each parameter (FIG. 217).

Asset Parameters

Parameter Name ▲	Asset Name	Current Value	Status
Active Window	Monitor	Left	
Device Data Initialized	Monitor	true	
Display Usage	Monitor	0 Hours	
Input Source	Monitor	VGA	
Module Debug State	Monitor	Error	
Online Status	Monitor	Online	
Power Consumption Rate	Monitor	0.42 W	

FIG. 217 Asset Parameters window

Double-click on any Parameter to edit the selected parameter via the *Asset Parameter Properties Page*. See the *Asset Parameter Properties Page* section on page 139 for details.

Asset Parameters Window - Context Menu

Right-click inside the *Locations* window (in the Locations page) to access the Locations window context menu. The options in this menu are described below:

Asset Parameters Window Context Menu Options	
Edit Asset Parameter	Click to edit the selected Asset Parameter, in the *Asset Parameter Properties* page. See the *Asset Parameter Properties Page* section on page 139 for details.
Delete Asset Parameter	Click to delete the selected Asset Parameter.
Reset Asset Parameter	Click to reset the selected Asset Parameter to its default value.
Select All Parameters	Click to select all Asset Parameters in the list.
Refresh	Click to refresh the Asset Parameters list.
Select None	Click to de-select all Asset Parameters in the list.

Asset Management Page - Actions Window

The options in the *Actions* window allow you to perform several basic actions on the selected Asset without having to leave the *Asset Management* page (FIG. 218).

Actions

- Enable Maintenance
- Execute Control Methods
- Reset All Tripped Parameters
- Reset All Source Usages

FIG. 218 Asset Management page - Actions window

Actions Window Options	
Enable/Disable Maintenance	Click to enable maintenance mode on the selected Asset. When Maintenance is enabled for a Asset: • This button changes to "*Disable Maintenance*" (click to disable Maintenance) • The Maintenance icon is displayed in the *In Maintenance* column of the Locations window. • See the *Enabling / Disabling Asset Maintenance Mode* section on page 154 for details.
Execute Control Methods	Click to execute any Control Method that has been defined for the selected Asset. This is the same as selecting **Execute Control Methods** in the *Assets* window context menu (see page 129). Clicking this button opens the *Control Methods* dialog, in which you can select a Control Method to execute. See *Executing a Control Method* on page 162 for details.
Reset All Tripped Parameters	Click to reset all tripped parameters for the selected Asset. This is the same as selecting **Reset all Tripped Parameters** in the *Assets* window context menu (see page 129). See *Resetting Tripped Parameters* on page 160 for details.
Reset All Source Usages	Click to reset all Source Usage statistics for the selected Asset(s). This action is the same as clicking the **Reset** button in the *Source Usage* widget (see the *Source Usage Widget* section on page 81), or selecting **Reset all Source Usages** in the *Assets* window context menu (see page 129). See *Resetting Source Usage Statistics for an Asset* section on page 161 for details.

Asset Properties Page

The *Asset Properties* page is invoked when you either **Add** (create) or **Edit** an Asset. The options on this page allow you to define detailed device information for each Asset in the RMS system.

NOTE: *Users must have "Manage" permission for a specific location to Edit an asset. The "Apply" button and all editable fields will be disabled if users only have "View" permission.*

The options in the *Asset Properties* page are separated into several tabs:

- **Asset Setting**: The options in this tab allow you to view/enter basic information on the selected Asset. See *Asset Properties page - Asset Setting Tab* on page 131 for details.
- **Asset Metadata**: The options in this tab allow you to enter and edit metadata for the selected Asset. See *Asset Properties page - Asset Metadata Tab* on page 133 for details.
- **Parameters**: The options in this tab allow you to edit (and delete) parameters for the selected Asset. See *Asset Properties page - Parameters Tab* on page 134 for details.
- **Control Methods**: The options in this tab allow you to view the Control Methods associated with the selected Asset, and send a selected Control Method to the Asset for immediate execution. See *Asset Properties page - Control Methods Tab* on page 135 for details.
- **Asset Log**: The options in this tab allow you to view, annotate and delete Asset Logs for the selected Asset. See *Asset Properties page - Asset Log Tab* on page 136 for details.
- **Location History**: The options in this tab allow you to view the location history for the selected Asset. See *Asset Properties page - Location History Tab* on page 137 for details.
- **Firmware History**: This tab provides a history of firmware updates made to the selected Asset. See *Asset Properties page - Location History Tab* on page 137 for details.

Asset Properties page - Asset Setting Tab

The **Asset Setting** tab of the *Asset Properties* page displays the settings for the selected Asset (FIG. 219):

FIG. 219 Asset Properties page - Asset Setting tab

The options in this tab are described below:

Asset Setting Tab Options	
INFO	
Location	This is the name (read-only) of the Location selected in the *Locations* window (see FIG. 215 on page 127).
Asset Name	This is the name displayed in the *Asset Name* column of the *Assets* window (see FIG. 216 on page 128).
Description	This field allows you to enter a brief description of the selected Asset.
Asset Type	This is the type displayed in the *Asset Type* column of the *Assets* window (see FIG. 216 on page 128). Asset types are managed via options in the *Asset Type* page. See the *Asset Configuration (Classic UI)* section on page 246 for details.

Asset Setting Tab Options (Cont.)	
Manufacturer	This is the name of the Manufacturer displayed in the *Manufacturer* column of the *Assets* window (see FIG. 216 on page 128). • Manufacturer names are managed via options in the *Manufacturer/Models* page. See the *Asset Configuration (Classic UI)* section on page 246 for details. • Click the *Add Manufacturer* link to access the Add Manufacturer dialog, in which you can define a new Manufacturer that can be associated with this or any other Asset. See the *Adding a New Manufacturer* section on page 247.
Model	This is the name of the Model displayed in the *Model* column of the *Assets* window (see FIG. 216 on page 128). • Model names are managed via options in the *Manufacturer/Models* page. See the *Asset Configuration (Classic UI)* section on page 246 for details. • Click the *Add Model* link to access the Add Model dialog, in which you can define a new Model that can be associated with this or any other Asset. See the *Adding a New Model* section on page 249.
Serial Number	This field allows you to enter a serial number for the selected Asset.
Client Gateway	This is the name (read-only) of the Client Gateway assigned to the Location selected in the *Locations* window (see FIG. 215 on page 127). Client Gateways are managed via options in the *Client Gateway Management* page (see the *Management - Client Gateways (Classic UI)* on page 93 for details).
Firmware Version	This is the firmware version (read-only) of the Client Gateway assigned to the Location selected in the *Locations* window (see FIG. 215 on page 127).
Image	This is the image associated with the selected asset's Asset Type and Model. Asset types are managed via options in the *Asset Type* page. See the *Asset Configuration (Classic UI)* section on page 246 for details.

RMS Module

This section describes the RMS SDK version of the connecting device module (either *Legacy Client 3.x* or *RMS Client 4.x*). Note that this does not relate to a specific device, only the client connection.

Module Name	This is the name (read-only) of the SDK that is loaded on the NetLinx Master
Module Version	This is the release version number (read-only) of the SDK.

RFID Asset Tracking

This section is enabled only if *RFID Tracking* is enabled (in the *RFID Asset Tracking* page. See the *RFID Asset Tracking* section on page 262 for details.

Note that Assets with an RFID Tag ID enabled automatically inherit several RFID asset parameters.

As RFID tag change notifications are received by the RMS server these asset RFID parameters will be updated accordingly:
• RFID Tag Battery Level
• RFID Tag Online
• RFID Tag Signal Strength
• RFID Tag Detected Location

Tag ID	Select a Tag ID from the drop-down list of available RFID Tag IDs.
Enabled	Click to enable RFID Tracking for this Asset using the selected RFID Tag ID. If disabled, RFID tracking will be ignored.
Portable	Click to make RFID Tag tracking for this device *Portable*: when enabled, the device will automatically move to different locations depending on which Anterus RFID Reader has the strongest signal strength (RSSI). *Note: If this option is not selected, RMS will not automatically relocate the tagged asset (but will continue RFID tracking).*

NetLinx Device Information

If the selected asset is a NetLinx Device, the following information is displayed in this window (read-only):

• Serial Number	• Device Address
• Device Type	• Device Address Type
• Device Version	• Device:Port:System
• Firmware ID	

Apply button	Click to apply all changes.

Asset Properties page - Asset Metadata Tab

The options in the **Asset Metadata** tab of the *Asset Properties* page allow users to create user-defined properties to store additional information for the selected Asset in the RMS database (FIG. 220):

FIG. 220 Asset Properties page - Asset Metadata tab

NOTE: *The authenticated user must have the location level View Asset permissions to see asset metadata or the Manage Asset permissions to add/edit asset metadata. See the Management - Roles (Classic UI) section on page 192 for details.*

The options in this tab are described below:

Asset Metadata Tab Options	
Add	Click to create a new asset metadata type, via the *Metadata Editor* dialog. See *Adding a Metadata Entry to an Asset* on page 156 for details.
Edit	Click to edit an existing asset metadata type, via the *Metadata Editor* dialog. See *Editing an Asset Metadata Entry* on page 157 for details.
Delete	Click to delete an asset metadata type. See *Deleting an Asset Metadata Entry* on page 157 for details.
Search Window	The Search window allows you to perform a search for Asset Metadata entries.
Asset Metadata table	• *Category*: This is the Asset Category that was selected when this Metadata type was defined (in the *Metadata Setting* dialog - see FIG. 373 on page 229). • *Name*: This is the Name that was defined when this Metadata type was defined (in the *Metadata Setting* dialog). • *Value*: This is the current value of the Metadata. • *Editable*: A checkmark in this column indicates that this metadata entry is editable by the current user. This setting depends on the way that the asset metadata is registered from the SDK: If an asset metadata property is registered from the SDK (NetLinx master) then the NetLinx programmer has the option to declare the asset metadata property as "read only" if they do not want the value editable via the RMS UI. See the RMS Enterprise NetLinx Programmer's Guide for details. • *Description*: This is the Description that was entered when this Metadata definition was created (in the *Metadata Setting* dialog).

Asset Properties page - Parameters Tab

The **Parameters** tab of the *Asset Properties* page displays a listing of parameters associated with the selected Asset (FIG. 221):

Name ▲	Description	Current Value	Status	Parameter Type	Parameter Data Type
Online Status	Current asset online or offline state	Online		Asset Online	Enumeration
Power Consumption Rate	Last reported power consumption rate for this asset	46.40 W		Power Consumption	Decimal
Power Status	Current asset power state	On		Asset Power	Enumeration

FIG. 221 Asset Properties page - Parameters tab

Since asset parameters are intended to be monitored and tracked in the RMS system, they are only "registered" (added) via the RMS SDK running on the Client Gateways. Use the options in this tab to edit or delete Asset Parameters.

- Each parameter may have multiple thresholds. If any of the thresholds are tripped, The corresponding threshold status type images are displayed in the Status column.
- Double-click an Asset Parameter to display the *Asset Parameter Properties* page to edit the parameter (see the *Editing Asset Parameter Settings* section on page 159 for details).

The options in this tab are described below:

Parameters Tab Options	
Edit	Click to edit a selected parameter. • See *Editing Asset Parameter Settings* on page 159 for details. • See the *Editing Asset Parameter Thresholds* on page 159 for details.
Delete	Click to delete a parameter. See *Deleting Asset Parameters* on page 159 for details.
Search window	The Search window allows you to perform a search for Asset Parameter entries.
Parameters table	The table in this tab presents Parameter data for each Asset, as specified in the Asset Properties tabs. The data presented in this table depends on the selected Asset. For example, Assets that have an RFID Tag ID enabled present several columns that are specific to the RFID tag (*RFID Tag Battery Level*, *RFID Tag Online*, *RFID Tag Signal Strength*, *RFID Tag Detected Location*).

Parameters Tab Context Menu

Right-click on a parameter inside the **Parameters** tab to access the following context menu:

Parameters Tab Context Menu Options	
Edit Asset Parameter	Click to edit the selected parameter. • See *Editing Asset Parameter Settings* on page 159 for details. • See the *Editing Asset Parameter Thresholds* on page 159 for details.
Delete Asset Parameter	Click to delete a parameter. See *Deleting Asset Parameters* on page 159 for details.
Reset Asset Parameter	Click to reset the selected parameter.
Select All Parameters	Click to select all parameters in the list.
Refresh	Click to refresh the parameters list.
Select None	Click to de-select all parameters in the list.

Asset Properties page - Control Methods Tab

The **Control Methods** tab of the *Asset Properties* page displays a listing of control methods associated with the selected Asset (FIG. 223).

FIG. 222 Asset Properties page - Control Methods tab

Since Control Methods (like Asset Parameters) are intended to be monitored and tracked in the RMS system, they are only "registered" (added) via the RMS SDK running on the Client Gateways. The options in the **Control Methods** tab allow you to manually activate system events or functions (such as turning on power, switching inputs, or playing a DVD):

Control Methods Tab Options	
Select Control Method	The Control Methods defined for the selected Asset are listed here, organized in a tree structure. • Each folder in the tree represents a Control Method Group. • Click the plus sign (+) next to each Control Method Group folder to expand the list to show all sub-folders or Control Methods. • Click the minus sign (-) next to each folder to collapse each folder. • Click to select a Control Method to display in the *Control Method Details* window.
Control Methods Details	This window displays detailed information on the selected Control Method. • Control methods that have with editable Arguments, will present these arguments here as well. • Click the **Execute Control Method** button to manually send the selected Control Method for immediate execution.

Asset Properties page - Asset Log Tab

The **Asset Log** tab of the *Asset Properties* page displays a listing of internal log records for all parameter updates, for the selected Asset (FIG. 223):

FIG. 223 Asset Properties page - Asset Log tab

The options in this tab are described below:

Asset Log Tab Options	
Delete	Click to delete the selected Asset Log entries (shift + click to multi-select). See the *Deleting Asset Logs* section on page 164 for details.
Asset Log table	The columns in the Asset Log table display the following properties for each Asset Log: • Status Type • Local Time • Parameter • Threshold • Value • Notes • Log Message See the *Adding a Note to an Asset Log* section on page 163 for instructions on annotating Asset Logs.

Asset Properties page - Location History Tab

The **Location History** tab of the *Asset Properties* page displays a historical record of relocations for the selected Asset (FIG. 224).

Asset Setting	Asset Metadata	Parameters	Control Methods	Asset Log	Location History	Firmware History

Location ▲	Time In	Time Out	Auto Relocated
Multi-Panel 01	Apr 20, 2015 3:14 PM		☐

FIG. 224 Asset Properties page - Location History tab

The options in this tab are described below:

Location History Tab Options	
Search window	The Search window allows you to perform a search for Location History entries.
Asset Location History table	• *Location*: This is the name of the Locations in which the selected Asset has been. • *Time In*: This is the time that the selected Asset was moved into the Location. • *Time Out*: This is the time that the selected Asset was moved out of the Location. • *Auto Relocated*: A check in this column indicates that this Asset is configured as a Portable device in an Anterus RFID tracking system. See the *RFID Asset Tracking* options in the **Asset Setting** tab (page 131) for details.

Asset Properties page - Firmware History Tab

The **Firmware History** tab of the *Asset Properties* page displays a historical record of firmware updates for the selected Asset (FIG. 224).

FIG. 225 Asset Properties page - Firmware History tab

The options in this tab are described below:

Firmware History Tab Options	
Search window	The Search window allows you to perform a search for Firmware History entries.
Firmware History table	• Name: Indicates the name of each firmware file. • Version: Indicates the version of each firmware file. • Installed Date: Indicates the date on which each firmware file was applied to the selected Asset.

Asset Parameter Properties Page

Use the options in the *Asset Parameter Properties* page to view/edit Asset Parameter settings and define thresholds for a selected parameter. To access this page, double-click on any parameter in the *Asset Parameters* window of the *Asset Management* page (see FIG. 217 on page 130). This page contains two tabs (*Asset Parameter Setting* and *Parameter Threshold*), as described in the following sections.

Asset Parameter Properties Page - Asset Parameter Setting Tab

This tab displays the current settings (read-only) for the selected parameter. Some of the items presented in this tab will vary, depending on the select Parameter's Parameter Data Type. However, several are common to all Parameter data types. The following (read-only) properties are presented for all Asset Parameters, based on the information registered for each Asset via the RMS SDK:

Asset Parameter Setting Tab - Common Parameters	
Parameter Name	The name of the selected Asset Parameter.
Location Name	The name of the Location of the Asset associated with the selected Parameter.
Asset Name	The name of the Asset associated with the selected Parameter.
Description	The description of the selected Asset Parameter.
Parameter Type	The Parameter Type of the selected Asset Parameter.
Parameter Data Type	The Data Type of the selected Asset Parameter. See the *Metadata Data Types* section on page 227 for details.
Min / Max	Use these fields to specify the allowed range for this Asset Parameter (number types only).
Value	The current value of the selected Asset Parameter (varies, depending on the Data Type of the selected Asset Parameter).
Track Changes	Select this option to track all changes to this parameter, in the **Asset Log** tab (see *Asset Properties page - Asset Log Tab* on page 136). Note that changing this option enables the **Apply** button.
Bargraph Enabled	Click to display this Asset Parameter as a bargraph. Selecting this option invokes a list of available bargraph types. Click to select a bargraph type to use to display this Asset Parameter. RMS provides a set of pre-configured Bargraphs. The list of Bargraphs presented here for selection are managed in the *Bargraph Management* page (FIG. 419 on page 259). See the *Asset Parameter Bargraphs* section on page 161 for details on adding, editing and deleting Bargraphs.
Reset Value	This option is presented only if the selected Asset Parameter registers as resettable in the RMS SDK. • Enter the reset value in the field provided. • Click **Reset** to reset the current value to the Reset Value.
Apply	Click to save all changes.

Asset Parameter Setting Tab - Boolean

The options in the *Asset Parameter Setting* tab for **Boolean** type Parameters are shown in FIG. 226:

FIG. 226 Asset Parameter Setting tab - Boolean Parameter Type

Asset Parameter Setting Tab - Decimal

The options in the *Asset Parameter Setting* tab for **Decimal** type Parameters are shown in FIG. 227:

FIG. 227 Asset Parameter Setting tab - Decimal Parameter Type

Asset Parameter Setting Tab - Enumeration

The options in the *Asset Parameter Setting* tab for **Enumeration** type Parameters are shown in FIG. 228:

FIG. 228 Asset Parameter Setting tab - Enumeration Parameter Type

Asset Parameter Setting Tab - Level

The options in the *Asset Parameter Setting* tab for **Level** type Parameters are shown in FIG. 229:

FIG. 229 Asset Parameter Setting tab - Level Parameter Type

Asset Parameter Setting Tab - Number

The options in the *Asset Parameter Setting* tab for **Number** type Parameters are shown in FIG. 230:

FIG. 230 Asset Parameter Setting tab – Number Parameter Type

Asset Parameter Setting Tab - String

The options in the *Asset Parameter Setting* tab for **String** type Parameters are shown in FIG. 231:

FIG. 231 Asset Parameter Setting tab – String Parameter Type

Asset Parameter Properties Page - Parameter Threshold Tab

The **Parameter Threshold** tab provides a listing of asset parameter thresholds for the selected Asset Parameter.

Use the options in this tab to *Add*, *Edit*, or *Delete* thresholds for the selected Asset Parameter (FIG. 232):

FIG. 232 Asset Parameter Properties page - Parameter Threshold tab

The items in this tab are described in the following table:

Parameter Threshold Tab Options	
Search	Use this search field to perform a search for Parameter Threshold names.
Add	Click to add a Parameter Threshold, via the *Parameter Threshold Editor* dialog (FIG. 233 on page 143). See *Adding Parameter Thresholds* on page 160 for details.
Edit	Click to edit a selected Parameter Threshold, via the *Parameter Threshold Editor* dialog (FIG. 233 on page 143). See *Editing Parameter Thresholds* on page 160 for details.
Delete	Click to delete one or more selected Parameter Thresholds. See *Deleting Parameter Thresholds* on page 160 for details.
Parameter Threshold Table	The Parameters Table lists the following information for all thresholds associated with the selected Asset Parameter: • Name • Status Type • Compare Operator • Threshold • Threshold Tripped • Time Delayed

Parameter Threshold Tab Context Menu

Right-click inside the **Parameter Threshold** tab to access the following context menu:

Parameter Threshold Tab Context Menu Options	
Add	Click to add a parameter threshold, via the *Parameter Threshold Editor* dialog (FIG. 233 on page 143). See the *Adding Parameter Thresholds* section on page 160 for details.
Delete	Click to delete a selected parameter threshold. See the *Deleting Parameter Thresholds* section on page 160 for details.
Edit	Click to edit the selected parameter threshold, via the *Parameter Threshold Editor* dialog (FIG. 233 on page 143). See the *Editing Parameter Thresholds* section on page 160 for details.
Refresh	Click to refresh the parameter thresholds list.
Select All Thresholds	Click to select all parameter thresholds in the list.
Select None	Click to de-select all parameter thresholds in the list.

Parameter Threshold Editor Dialog

The options in the *Parameter Threshold Editor* dialog allow the user to define the threshold bounding rules for a selected asset parameter. The options in the *Parameter Threshold Setting* area of this dialog will vary, depending on the Parameter Data Type of the selected Asset Parameter. However, the options in the *Template*, *Trip Macro* and *Restore Macro* options are common to all Parameter data types (FIG. 233).

FIG. 233 Parameter Threshold Editor dialog

This dialog is accessed via either the **Add** or **Edit** buttons in the **Parameter Threshold** tab of the *Asset Parameter Properties* page (see FIG. 232 on page 142).

- If this dialog is accessed via the **Add** button, all fields are empty, or populated with default values.
- When accessed via the **Edit** button, the selected Threshold's properties are displayed.

NOTE: *Users must have Manage permission for a specific Location to edit a Parameter Threshold. The Save button and all editable fields are disabled if users only have View permission. See the Management - Roles (Classic UI) section on page 192 for details.*

The options in the *Parameter Threshold Editor* dialog are described in the following table:

Parameter Threshold Editor Dialog Options	
Parameter Threshold Setting	
These options vary depending on the *Parameter Data Type* of the selected Asset Parameter. Refer to the following sections for details on threshold settings for each parameter data type: • **Boolean**: See *Asset Parameter Setting Tab - Boolean* on page 139. • **Decimal**: See *Asset Parameter Setting Tab - Decimal* on page 140. • **Enumeration**: See *Asset Parameter Setting Tab - Enumeration* on page 140. • **Level**: See *Asset Parameter Setting Tab - Level* on page 140. • **Number**: See *Asset Parameter Setting Tab - Number* on page 141. • **String**: See *Asset Parameter Setting Tab - String* on page 141.	
Template	
Trip when parameter exceeds threshold	Select this option to specify to use an overriding notification template for trip actions on the selected parameter threshold. • Default = *Disabled* If this option is enabled, the Notification Template drop-down menu is activated. Select a notification template for trip actions.
Restore when parameter returns to normal range	Select this option to specify to use an overriding notification template for restore actions on the selected parameter threshold. • Default = *Disabled* If this option is enabled, the Notification Template drop-down menu is activated. Select a notification template for restore actions.

Parameter Threshold Editor Dialog Options (Cont.)

Trip Macro

Execute Global Control Macro	Select this option to assign a *Global* Control Macro to trip actions to be executed when these occur. When this option is selected, the drop-down menu is populated with a listing of Global Control Macros to select from.
Execute Control Macro in Location	Select this option to assign a *Location* Control Macro to the trip actions to be executed when these occur. When this option is selected, the drop-down menu is populated with a listing of Control Macros available to the selected Location. Note that the currently selected Location is indicated in the upper-left corner of this dialog (see FIG. 233 on page 143).

Restore Macro

Execute Global Control Macro	Select this option to assign a *Global* Control Macro to the restore actions to be executed when these occur. When this option is selected, the drop-down menu is populated with a listing of Global Control Macros to select from.
Execute Control Macro in Location	Select this option to assign a *Location* Control Macro to the restore actions to be executed when these occur. When this option is selected, the drop-down menu is populated with a listing of Control Macros available to the selected Location. Note that the currently selected Location is indicated in the upper-left corner of this dialog (see FIG. 233 on page 143).
Save	Click to save all changes and close this dialog.

Parameter Threshold Settings - Boolean Parameters

When the *Parameter Threshold Editor* dialog is accessed with a Boolean type parameter, the following options are presented under **Parameter Threshold Settings** (FIG. 234):

FIG. 234 Parameter Threshold Settings - Boolean Data Type (Parameter Threshold Editor dialog)

Parameter Threshold Settings - Boolean Parameters

Name	The name of the selected Threshold is displayed in this text field (click to edit).
Status Type	Select an appropriate Status Type for this Threshold from the drop-down menu. • Each threshold can have a unique status type assigned. • The options in this menu are provided by the RMS system.
Threshold Compare Operator	Select an appropriate Compare Operator for this Threshold from the drop-down menu. • The options in this menu are provided by the RMS system.
Threshold	Select the Threshold value from the drop-down menu.
Time Delayed	This option allows parameter trips to be delayed by a specified amount of time. • If this option is selected and a delay interval is provided, once the parameter values exceed this threshold bounds, then the parameter will be placed into the tripped state only after the elapsed number of minutes. • If the parameter value is restored to a value within the threshold bounds prior to the trip time delay, then no trip action will occur, thus no hotlist record or outbound notifications. • Default = *Disabled*. If this option is enabled, the *Time Delay Interval* field is activated.
Time Delay Interval	Use the up and down arrow to specify the number of minutes in the Time Delay Interval. Default = *0*.

Parameter Threshold Settings - Decimal Parameters

When the *Parameter Threshold Editor* dialog is accessed with a Decimal type parameter, the following options are presented under **Parameter Threshold Settings** (FIG. 235):

FIG. 235 Parameter Threshold Settings - Decimal Data Type (Parameter Threshold Editor dialog)

Parameter Threshold Settings - Decimal Parameters	
Name	The name of the selected Threshold is displayed in this text field (click to edit).
Status Type	Select an appropriate Status Type for this Threshold from the drop-down menu. • Each threshold can have a unique status type assigned. • The options in this menu are provided by the RMS system.
Threshold Compare Operator	Select an appropriate Compare Operator for this Threshold from the drop-down menu. • The options in this menu are provided by the RMS system.
Parameter	This read-only field indicates the allowed range for this parameter. The *Min* and *Max* values can be edited via the *Asset Parameter Properties* page for the appropriate parameter data type. See the *Asset Parameter Properties Page - Asset Parameter Setting Tab* section on page 139 for details).
Threshold	Enter the Threshold value in the text field.
Time Delayed	This option allows parameter trips to be delayed by a specified amount of time. • If this option is selected and a delay interval is provided, once the parameter values exceed this threshold bounds, then the parameter will be placed into the tripped state only after the elapsed number of minutes. • If the parameter value is restored to a value within the threshold bounds prior to the trip time delay, then no trip action will occur, thus no hotlist record or outbound notifications. • Default = *Disabled*. If this option is enabled, the *Time Delay Interval* field is activated.
Time Delay Interval	Use the up and down arrow to specify the number of minutes in the Time Delay Interval. Default = *0*.

Parameter Threshold Settings - Enumeration Parameters

When the *Parameter Threshold Editor* dialog is accessed with a Enumeration type parameter, the following options are presented under **Parameter Threshold Settings** (FIG. 236):

FIG. 236 Parameter Threshold Settings - Enumeration Data Type (Parameter Threshold Editor dialog)

Parameter Threshold Settings - Enumeration Parameters	
Name	The name of the selected Threshold is displayed in this text field (click to edit).
Status Type	Select an appropriate Status Type for this Threshold from the drop-down menu. • Each threshold can have a unique status type assigned. • The options in this menu are provided by the RMS system.
Threshold Compare Operator	Select an appropriate Compare Operator for this Threshold from the drop-down menu. • The options in this menu are provided by the RMS system.

Parameter Threshold Settings - Enumeration Parameters (Cont.)	
Threshold	Select the Threshold value from the drop-down menu.
Time Delayed	This option allows parameter trips to be delayed by a specified amount of time. • If this option is selected and a delay interval is provided, once the parameter values exceed this threshold bounds, then the parameter will be placed into the tripped state only after the elapsed number of minutes. • If the parameter value is restored to a value within the threshold bounds prior to the trip time delay, then no trip action will occur, thus no hotlist record or outbound notifications. • Default = *Disabled*. If this option is enabled, the *Time Delay Interval* field is activated.
Time Delay Interval	Use the up and down arrow to specify the number of minutes in the Time Delay Interval. Default = *0*.

Parameter Threshold Settings - Level Parameters

When the *Parameter Threshold Editor* dialog is accessed with a Level type parameter, the following options are presented under **Parameter Threshold Settings** (FIG. 237):

FIG. 237 Parameter Threshold Settings - Level Data Type (Parameter Threshold Editor dialog)

Parameter Threshold Settings - Level Parameters	
Name	The name of the selected Threshold is displayed in this text field (click to edit).
Status Type	Select an appropriate Status Type for this Threshold from the drop-down menu. • Each threshold can have a unique status type assigned. • The options in this menu are provided by the RMS system.
Threshold Compare Operator	Select an appropriate Compare Operator for this Threshold from the drop-down menu. • The options in this menu are provided by the RMS system.
Parameter	This read-only field indicates the allowed range for this parameter. The *Min* and *Max* values can be edited via the *Asset Parameter Properties* page for the appropriate parameter data type. See the *Asset Parameter Properties Page - Asset Parameter Setting Tab* section on page 139 for details).
Threshold	Select the Threshold value from the drop-down menu.
Time Delayed	This option allows parameter trips to be delayed by a specified amount of time. • If this option is selected and a delay interval is provided, once the parameter values exceed this threshold bounds, then the parameter will be placed into the tripped state only after the elapsed number of minutes. • If the parameter value is restored to a value within the threshold bounds prior to the trip time delay, then no trip action will occur, thus no hotlist record or outbound notifications. • Default = *Disabled*. If this option is enabled, the *Time Delay Interval* field is activated.
Time Delay Interval	Use the up and down arrow to specify the number of minutes in the Time Delay Interval. Default = *0*.

Parameter Threshold Settings - Number Parameters

When the *Parameter Threshold Editor* dialog is accessed with a Number type parameter, the following options are presented under **Parameter Threshold Settings** (FIG. 238):

FIG. 238 Parameter Threshold Settings - Number Data Type (Parameter Threshold Editor dialog)

Parameter Threshold Settings - Number Parameters	
Name	The name of the selected Threshold is displayed in this text field (click to edit).
Status Type	Select an appropriate Status Type for this Threshold from the drop-down menu. • Each threshold can have a unique status type assigned. • The options in this menu are provided by the RMS system.
Threshold Compare Operator	Select an appropriate Compare Operator for this Threshold from the drop-down menu. • The options in this menu are provided by the RMS system.
Parameter	This read-only field indicates the allowed range for this parameter. The *Min* and *Max* values can be edited via the *Asset Parameter Properties* page for the appropriate parameter data type. See the *Asset Parameter Properties Page - Asset Parameter Setting Tab* section on page 139 for details).
Threshold	Select the Threshold value from the drop-down menu.
Time Delayed	This option allows parameter trips to be delayed by a specified amount of time. • If this option is selected and a delay interval is provided, once the parameter values exceed this threshold bounds, then the parameter will be placed into the tripped state only after the elapsed number of minutes. • If the parameter value is restored to a value within the threshold bounds prior to the trip time delay, then no trip action will occur, thus no hotlist record or outbound notifications. • Default = *Disabled*. If this option is enabled, the *Time Delay Interval* field is activated.
Time Delay Interval	Use the up and down arrow to specify the number of minutes in the Time Delay Interval. Default = *0*.

Parameter Threshold Settings - String Parameters

When the *Parameter Threshold Editor* dialog is accessed with a String type parameter, the following options are presented under **Parameter Threshold Settings** (FIG. 239):

FIG. 239 Parameter Threshold Settings - String Data Type (Parameter Threshold Editor dialog)

Parameter Threshold Settings - String Parameters	
Name	The name of the selected Threshold is displayed in this text field (click to edit).
Status Type	Select an appropriate Status Type for this Threshold from the drop-down menu. • Each threshold can have a unique status type assigned. • The options in this menu are provided by the RMS system.
Threshold Compare Operator	Select an appropriate Compare Operator for this Threshold from the drop-down menu. • The options in this menu are provided by the RMS system.
Threshold	Enter the Threshold value in the text field.
Time Delayed	This option allows parameter trips to be delayed by a specified amount of time. • If this option is selected and a delay interval is provided, once the parameter values exceed this threshold bounds, then the parameter will be placed into the tripped state only after the elapsed number of minutes. • If the parameter value is restored to a value within the threshold bounds prior to the trip time delay, then no trip action will occur, thus no hotlist record or outbound notifications. • Default = *Disabled*. If this option is enabled, the *Time Delay Interval* field is activated.
Time Delay Interval	Use the up and down arrow to specify the number of minutes in the Time Delay Interval. Default = *0*.

Working With Assets

Adding an Asset to a Location

In RMS Enterprise, users can add an asset (as described below), but it will have no parameters & cannot be monitored by RMS.

NOTE: *Users must have Manage permission for the specific location to add an Asset to a Location. The Add button will be disabled if users only have View permission for a Location. See the Management - Roles (Classic UI) section on page 192 for details.*

1. Select the Location to which you want to add a new Asset, in the *Locations* window.
2. In the Assets window, click the **Add** button to invoke the *Add Asset* dialog (FIG. 240):

Add Asset ✕

Location Name	Room 1
Asset Name	
Asset Type	Please select an asset type ▼

Save   Cancel

FIG. 240 Add Asset dialog

Note that the name of the selected Location is indicated in the **Location Name** field (read-only).

3. Enter a name for the new asset in the **Asset Name** text field.
4. Select an asset type that best matches this asset (device) from the **Asset Typ**e drop-down menu.
5. Click **Save** to save changes and close this dialog. This action also invokes the *Asset Management* page, **Asset Setting** tab (see the *Asset Properties Page* section on page 131 for details).
6. Fill in the fields in each tab.
    *   It is not required that you fill out all of the information on all tabs. However, it is recommended that you enter as much detailed information as possible in order to maximize the amount of data that RMS is able to return on each Asset in the system.
    *   Each of tabs in the *Asset Management page* are described in the following sections:
        Asset Properties page - Asset Setting Tab on page 131
        Asset Properties page - Asset Metadata Tab on page 133
        Asset Properties page - Parameters Tab on page 134
        Asset Properties page - Control Methods Tab on page 135
        Asset Properties page - Asset Log Tab on page 136
        Asset Properties page - Location History Tab on page 137
7. Click **Apply** to save your changes.

The new Asset is now listed in the Assets Table for the selected Location.

Editing an Asset

1. In the *Locations* window, select the Location that contains the Asset that you want to edit. This populates the Assets Table with the Assets assigned to the selected Location.
2. In the Assets Table, select an Asset to edit .
3. Click the **Edit** button to open the *Asset Management page*.

    NOTE: *Alternatively, double-click an Asset in the Assets Table to open the Asset Management page.*

4. Fill in the fields in each tab. See the *Asset Properties Page* section on page 131 for details.
5. Click **Apply** to save your changes.

Deleting an Asset

Users must have *Manage* permission for a specific location to delete an Asset. The **Delete** button is disabled if the current user only has *View* permission.

NOTE: *Deleting an Asset will also delete all Parameters, Metadata, Control Methods and Location History associated with that Asset.*

1. In the *Locations* window, select the Location that contains the Asset that you want to delete. This populates the Assets Table with the Assets assigned to the selected Location.
2. In the Assets Table, select the Asset(s) to delete (ctrl + click to multi-select).
3. Click the **Delete** button.
4. The system will prompt you to verify this action before the Asset is deleted, via the *Delete Confirmation* dialog (FIG. 241):
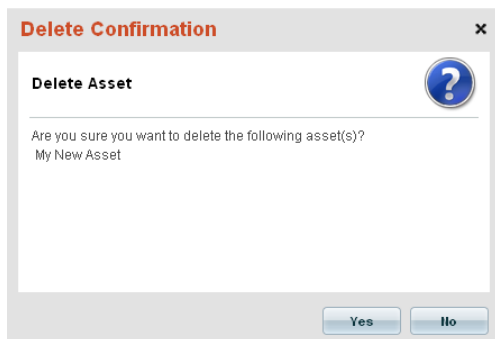
FIG. 241 Delete Confirmation dialog - Assets

5.   Click **Yes** to proceed.

Moving an Asset (via the Move Asset Button)

To move an Asset to a different Location:

NOTE: *The authenticated user must have the Location Level Manager Asset permissions to move Assets to a new Location. See the Management - Roles (Classic UI) section on page 192 for details.*

1.   In the *Locations* window, select the Location that contains the Asset(s) that you want to move. This populates the Assets Table with the Assets assigned to the selected Location.

2.   In the Assets Table, select the Asset(s) to move (ctrl + click to multi-select).

3.   Click the **Move Asset** button. This action invokes the *Move Asset to another location* dialog (FIG. 242):
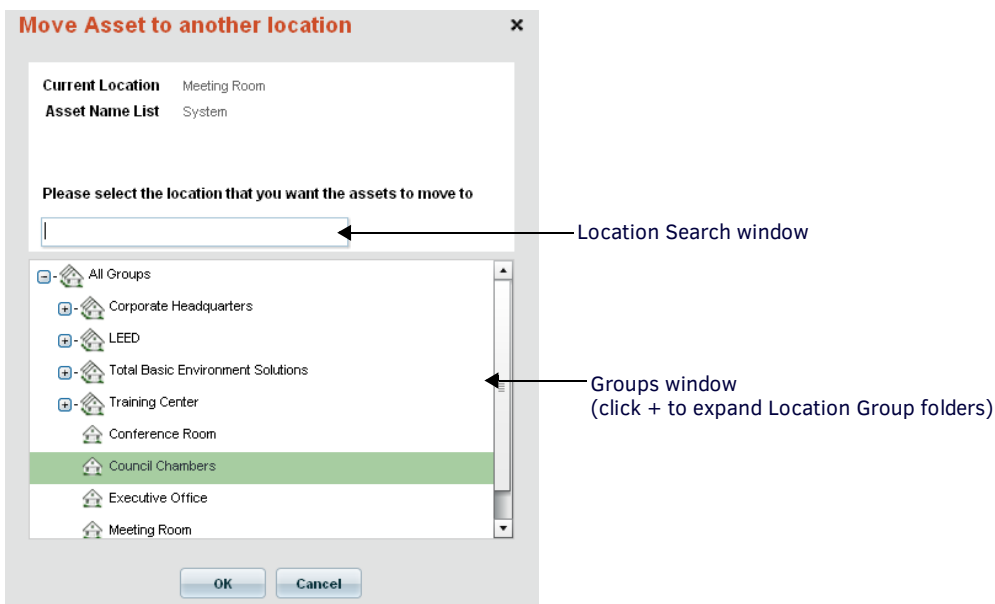
FIG. 242 Move Asset to another location dialog

4.   Specify the target Location for the selected Asset(s) using either of the two methods provided in this dialog:
   ● Use the *Search* window to perform a search for Location names
   ● In the *Groups* window, select the desired target Location for the selected Asset(s) (click the plus (+) symbol to expand each Group folder) expand the Location Groups.

5.   Click **OK** to move the selected Assets to the specified Location.

Moving an Asset (via Drag and Drop)

NOTE: *The authenticated user must have the Location Level Manager Asset permissions to move Assets to a new Location. See the Management - Roles (Classic UI) section on page 192 for details.*

Assets can be relocated to a different Location by dragging an Asset from the Assets window and dropping it on top of the new Location, in the *Locations* window (FIG. 243).

FIG. 243 Moving Assets via Drag-and-Drop

- An Asset cannot be dropped into its current Location or into a Group
- A small red "X" icon indicates when the drop target is not eligible (see FIG. 243)

NOTE: *Permission implications may apply when moving a location or location group. See the Management - Roles (Classic UI) section on page 192 for details.*

Disconnecting Assets

The **Disconnect Asset** option is useful in cases where an asset needs to be temporarily removed from it's Location, with the intention of replacing it later (without losing the Asset's historical information). For example, an Asset may need to be removed for maintenance purposes and replaced with another asset until the original equipment can be replaced.

Unlike *deleting* an Asset (see *Deleting an Asset* on page 149), disconnecting an Asset will *not* delete Parameters, Metadata, Control Methods or Location History associated with that Asset. When the disconnected Asset is re-connected, all Asset information will be available. When as asset is disconnected, the asset is taken offline, and the RMS Server stops sending/receiving requests and updates to that device.

- Users must have *Manage* permission for a specific location to disconnect an Asset. The *Disconnect Asset* button is disabled if the current user only has *View* permission.
- Each asset must be registered with a unique global ID in order to use the Disconnect Asset feature. Asset registration is managed via the SDK; some customization of the SDK is necessary in order to ensure unique global keys.

Disconnecting Assets - Workflow

The typical and expected workflow for disconnecting Assets is as follows:

1. The Asset is taken offline (and often physically removed from it's Location).
2. The Asset is disconnected according the instructions below, and temporarily replaced with a similar device.
3. When the Asset is ready to be used again, it is returned to it's Location and re-connected to the network.

Disconnecting an Asset

1. In the *Locations* window, select the Location that contains the Asset that you want to disconnect. This populates the Assets Table with the Assets assigned to the selected Location.
2. In the Assets Table, select the Asset(s) to disconnect (ctrl + click to multi-select).
3. Click the **Disconnect Asset** button.
4. The system will prompt you to verify this action (FIG. 244). Click **Yes** to proceed.
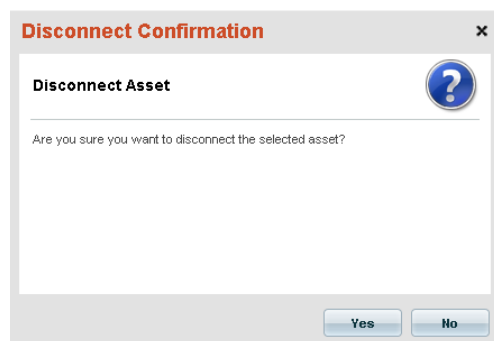
FIG. 244 Disconnect Asset Confirmation dialog

The selected device is taken Offline (indicated in the *Status* column) and is Disconnected (indicated in the *Client Gateway UID* column):

FIG. 245 Assets window - CV17 Touch Panel is Offline and Disconnected

Re-Connecting Disconnected Assets

Typically, the Disconnect Asset option is used for devices that have been (or will be) physically disconnected from the network and potentially removed from their Location. To re-connect a disconnected device, simply plug it back into the network in the same Location. The re-connected asset will go online and the "Disconnected" message will be cleared from the *Client Gateway UID* column (in the Assets window):

FIG. 246 Assets window - CV17 Touch Panel is Offline and Disconnected

Searching for Assets

Use the *Search* field in the Assets window to search for Assets by *Asset Name*, *Asset Type*, *Location Name*, *Manufacturer*, *Model*, *Device Number* (FIG. 247).
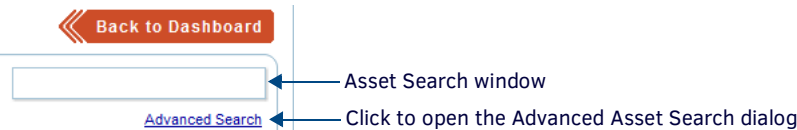
FIG. 247 Groups window - Search window

Performing an Advanced Asset Search

Click the **Advanced Search** link on the *Asset Management* page (FIG. 214 on page 126) to invoke the *Advanced Asset Search* dialog (FIG. 248).
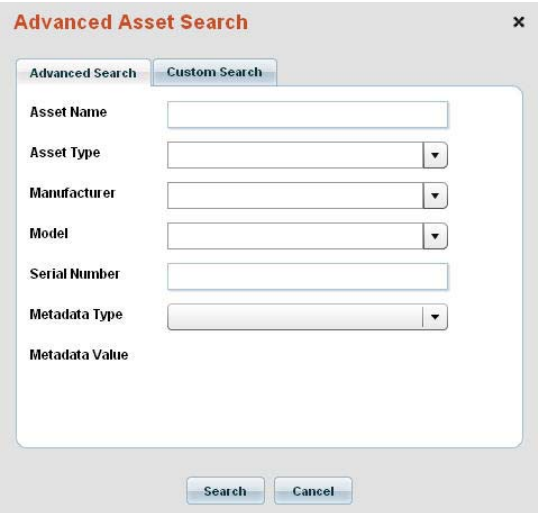
FIG. 248 Advanced Asset Search dialog - Advanced Search tab

Use this feature to search for Assets based on the detailed information provided by the *Asset Management* page (see the *Asset Properties Page* section on page 131). The options in the Advanced Asset Search dialog (*Advanced Search* tab) are described below:

Advanced Asset Search Dialog - Advanced Search Tab Options	
Asset Name	Enter a text string in this text field to search by Asset Name.
Asset Type	Click the down-arrow to filter the search by the selected Asset Type. The list of Asset Types is system-generated.
Manufacturer	Click the down-arrow to filter the search by the selected Manufacturer name. The list of Manufacturers is user-created - Manufacturer names are entered in the *Asset Management* page - **Asset Setting** tab (see *Adding an Asset to a Location* on page 149).
Model	Click the down-arrow to filter the search by the selected Model name. Model names are entered in the *Asset Management* page - **Asset Setting** tab (see *Adding an Asset to a Location* on page 149).
Serial Number	Enter a text string in this text field to search by Serial Number.
Metadata Type	Click the down-arrow to filter the search by the selected Metadata Type. The list of Metadata Types is system-generated.
Metadata Value	Use this field to specify a metadata value. *Note: The options presented here depend on the Metadata Type selection.*
Search button	Click Search to perform an asset search based on the specified search parameters.

Maintenance Mode for Assets

The **Enable Maintenance Mode** option in the *Actions* window allows users to place Assets into *Asset Maintenance Mode*. When enabled, Asset Maintenance mode hides any Hotlist records for the selected Asset, and suppresses outbound notifications for issues that occur in this Asset while in maintenance mode. Maintenance mode only suppresses Hotlist and Notifications - asset parameter changes are still accepted and applied, parameters can still be tripped, and changes are still recorded into the internal log.

- When maintenance mode is enabled for the Asset, any Hotlist records that exist for this Asset will not be displayed. No notifications will be sent for Asset Parameters that where tripped while in maintenance mode and are still tripped when maintenance mode it disabled.
- When maintenance mode is enabled for the Asset, a single Hotlist record is added to the Hotlist to indicate that this Asset is currently in Asset Maintenance Mode.
- When Asset Maintenance Mode is disabled, this Hotlist record is automatically removed and all pending notifications for the Asset are restored to the Hotlist.

Maintenance mode is indicated in the asset listing as an icon in the *In Maintenance* column of the Assets window (FIG. 249):

Asset Name	Asset Type	Status	Manufacturer	Model	Device Number	In Maintenance ▼	Client Gateway UID
Conf Rm DVD	Disc Device		Philips	BPD3020	0:4:0	⚒	00-60-9F-93-3D-7B
Conf Rm Video Proje	Video Projector		NEC	NP1350	0:3:0		00-60-9F-93-3D-7B

FIG. 249 Assets window - Asset Maintenance Mode enabled for "Conf Rm DVD"

NOTE: *Maintenance Mode can be applied to Locations (see Maintenance Mode for Locations section on page 122), to Assets, or to the entire System (see System Maintenance Mode section on page 210).*

Enabling / Disabling Asset Maintenance Mode

Actions	Actions
Enable Maintenance	Disable Maintenance
Execute Control Methods	Execute Control Methods
Reset All Tripped Parameters	Reset All Tripped Parameters
Reset All Source Usages	Reset All Source Usages

FIG. 250 Action window - Enable / Disable Maintenance

1. Select an Asset in the *Assets* window (*Asset Management* page - see FIG. 216 on page 128).
2. Click **Enable Maintenance** in the *Actions* window.
3. To disable Asset Maintenance Mode, select the Asset in the Assets window and click **Disable Maintenance** in the Actions window.

Working With Asset Settings

Enabling RFID Tracking for an Asset

In order to use RFID Asset tracking, the Anterus RFID Asset Tracking System must be installed, and Anterus RFID Asset tags must be configured in the Anterus system as well as physically installed on any Assets to be tracked.

- RFID Asset Tracking must be enabled in RMS. By default, RFID Tracking is *disabled* in RMS. See the *RFID Asset Tracking* section on page 262 for details.
- RFID Tag Assignments in RMS are managed in the *RFID Tag Assignments* page. See the *RFID Tag Assignments* section on page 263 for details.

1. Select **Assets** under *Asset Management* in the Management menu to open the *Asset Management* page (see FIG. 214 on page 126).
2. In the *Locations* window, select the Location that contains the Asset that you want to edit.
3. In the Assets Table, select an Asset on which you want to enable RFID Tracking.
4. Click the **Edit** button to open the *Asset Management* page (**Asset Settings** tab*)*.

   NOTE: *Alternatively, double-click an Asset in the Assets Table to open the Asset Management page.*

5. In the **RFID Asset Tracking** section of the page (FIG. 251), select the **Tag ID** associated with the selected Asset from the drop-down list of available RFID Tag IDs.

FIG. 251 RFID Asset Tracking options (Asset Management page - Asset Setting tab)

6. Click **Enabled** to enable the selected RFID tag for tracking this Asset.
7. Click **Portable** to make RFID Tag tracking for this device Portable: when enabled, the device will automatically move to different locations depending on which Anterus RFID Reader has the strongest signal strength (RSSI).
8. Click **Apply** to save your changes.

Working With Asset Metadata

Adding a Metadata Entry to an Asset

When a metadata entry is added to a selected Asset via the Add option in the *Asset Management* page - **Asset Metadata** tab, the metadata applies specifically to the selected Asset, and is not available for other Assets in the system.

NOTE: *To create metadata definitions that are available to all Assets (or to all Assets of a specific Asset Type), use the options in the System Configuration > Metadata page. Refer to the Metadata section on page 225 for details.*

1. Select **Assets** under *Asset Management* in the Management menu to open the *Asset Management* page (see FIG. 214 on page 126).

2. In the *Locations* window, select the Location that contains the Asset that you want to edit.

3. In the Assets Table, select an Asset that contains the metadata entry that you want to edit.

4. Click the **Edit** button to open the *Asset Management* page (**Asset Settings** tab*)*.

NOTE: *Alternatively, double-click an Asset in the Assets Table to open the Asset Management page.*

5. Open the **Asset Metadata** tab, and click the **Add** button (FIG. 252).
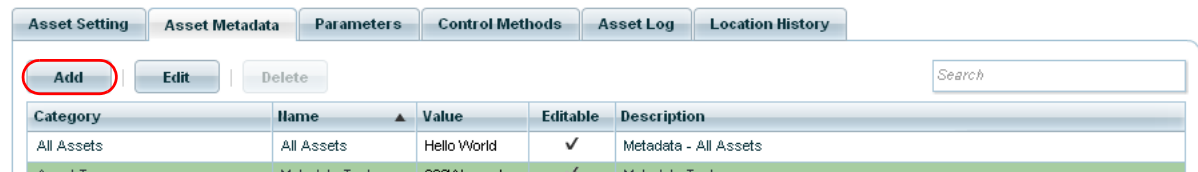
FIG. 252 Asset Metadata tab - Add button

       This action invokes the *Metadata Editor* dialog (FIG. 253).

FIG. 253 Metadata Editor dialog

6. Enter a Name for this Asset metadata entry in the **Name** field.

7. Select a data type from the **Data Type** drop-down menu. Note that the properties presented in this dialog change based on this selection.

       The following table describes the different types of Value property supported by each Data Type:

Metadata Properties / Data Types	
Data Type	**Value**
String	Text field
Memo	Text field
Boolean	Drop-down menu: Select *True* or *False* (default = *False)*.
Number	Number field: Use the up/down arrows to adjust the value (default = 0).
Decimal	Text field (numeric entry).
Date	Calendar: Click inside the field to access a pop-pop calendar, and select a date.
Time	Number fields: Click the up/down arrows to adjust the Hour and Minutes (default = 12hr / 00mins), click the radio buttons to specify AM or PM (default = AM).
Hyperlink	Enter the Link Name and Link URL (web address) in the text fields.
Date/Time	Calendar: Click inside the field to access a pop-pop calendar, and select a date. Number fields: Click the up/down arrows to adjust the Hour and Minutes (default = 12hr / 00mins), click the radio buttons to specify AM or PM (default = AM).

       See the *Metadata Data Types* section on page 227 for additional details.

8. Enter a value for the new metadata type in the *Value* field.

9. Click **OK** to save your changes.

The new Metadata Entry is added to the list in the **Asset Metadata** tab.

Editing an Asset Metadata Entry

1. In the *Asset Management* page - **Asset Metadata** tab, select an entry in the Asset Metadata table, and click the **Edit** button (FIG. 254).
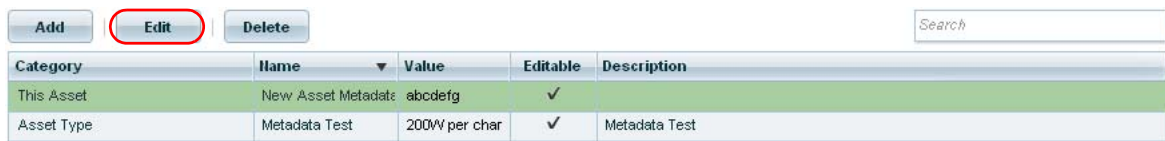
FIG. 254 Asset Management page - Edit button

Alternatively, double-click on any editable Metadata item in the list to edit.

NOTE: *Note that only Metadata items marked as Editable (indicating a checkmark in the Editable column) can be edited. Some Metadata items are specified in the SDK as being non-editable.*

2. This action invokes the *Metadata Editor* dialog, indicating the selected metadata entry's current properties (FIG. 253).
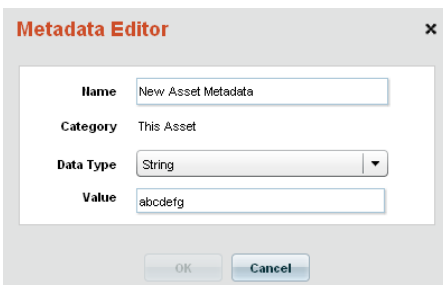
FIG. 255 Metadata Editor dialog

3. Edit the fields as desired.
4. Click **OK** to save your changes and close this dialog.

Deleting an Asset Metadata Entry

Only metadata entries that were added specifically to the selected Asset can be deleted via the *Asset Metadata* page. If you select a metadata type defined in the **System Configuration > Metadata** page, the *Delete* button is disabled. Any metadata items sent from the client cannot be deleted. Refer to the *Metadata* section on page 225 for details.

1. In the *Asset Management* page - **Asset Metadata** tab, select on or more metadata entries in the Asset Metadata table (Ctrl + click to multi-select), and click the **Delete** button (FIG. 256).
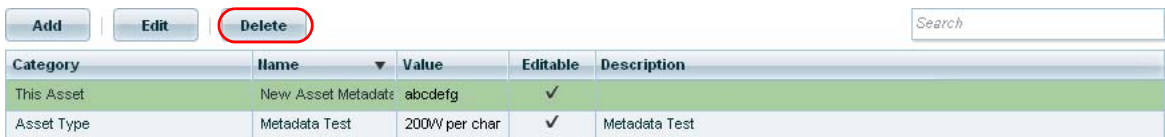
FIG. 256 Asset Management page - Delete button

2. The system will prompt you to verify this action via the *Delete Confirmation* dialog before the selected Asset Metadata Types are deleted (FIG. 257).
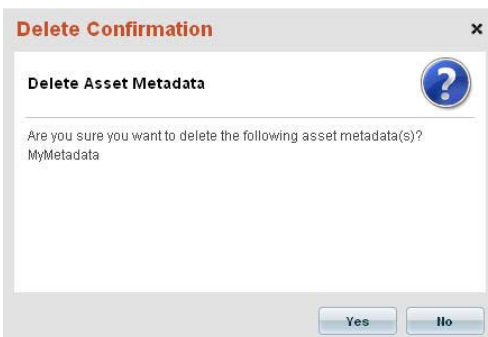
FIG. 257 Delete Confirmation dialog - Asset Metadata

3. Click **Yes** to proceed.

Searching for Asset Metadata Entries

Use the *Search* tool in the **Asset Metadata** tab to search for a specific Location (FIG. 258).
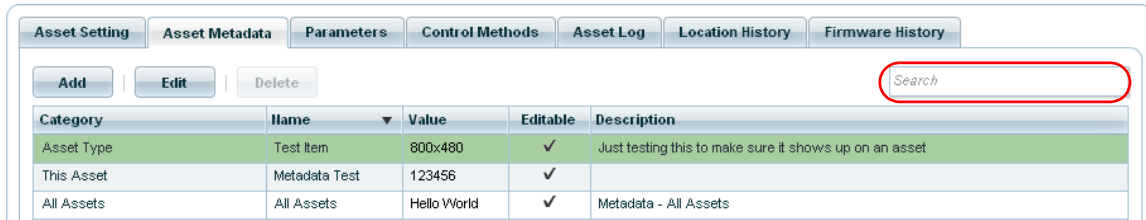
FIG. 258 Asset Metadata tab - Search window

This search tool searches text in all columns displayed in the **Asset Metadata** tab (*Category*, *Name*, *Value*, *Description*).

Working With Asset Parameters

Since asset parameters are intended to be monitored and tracked in the RMS system, they are only "registered" (added) via the RMS SDK running on the Client Gateways. Therefore, Asset Parameters cannot be added via the RMS UI, but they can be viewed, edited or deleted.

Viewing Asset Parameter Settings

1. Select a Location in the *Locations* window of the Asset Management page (FIG. 259).
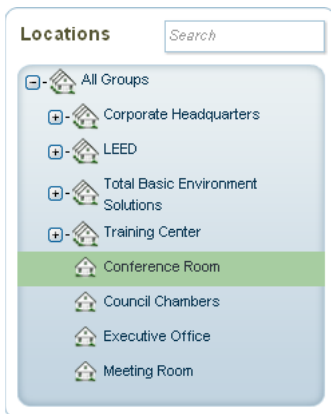
FIG. 259 Location selected in the Asset Management page (Locations window)

2. Select an Asset in the Assets Table.
3. This action populates the Asset Parameters table (FIG. 260).

FIG. 260 Asset Parameters data for a selected Asset (Asset Parameters window)

Note that this list reflects the list of parameters presented in the *Parameters* tab of the *Asset Management* page for the selected Asset.

NOTE: *Shift + click to select multiple Assets in the Assets table. In the case of multi-select, the parameters for all selected Assets are listed in the Asset Parameters table.*

4. Double-click on any parameter in the Asset Parameter window (or right-click on a parameter and select **Edit Asset Parameter** from the context menu).
5. This action opens the *Asset Parameter Properties* page in it's initial view - the **Asset Parameter Setting** tab.
   - Note that the *Asset Parameter Properties* page can also be accessed via the **Edit** button in the *Parameters* tab of the *Asset Management* page (see FIG. 221 on page 134).
   - Use the options in the *Asset Parameter Properties* page to view and edit Asset Parameter properties.

NOTE: *Users must have Manage permission for a specific Location to edit an Asset Parameter. The Apply button and all editable fields are disabled if users only have View permission. See the Management - Roles (Classic UI) section on page 192 for details.*

Editing Asset Parameter Settings

NOTE: *When an Asset parameter setting (i.e: the Max value for a graph) is changed, it will remain the new value - even if the Master is rebooted. To reset the parameter to the original default value, the client gateway must be re-initialized. Refer to Re-Initializing a Client Gateway on page 102 for details.*

1. Select **Assets** under *Asset Management* in the Management menu to open the *Asset Management* page (see FIG. 214 on page 126).
2. In the *Locations* window, select the Location that contains the Asset that you want to edit.
3. In the *Assets* window (see FIG. 216 on page 128), select an Asset that contains the parameter entry that you want to edit.

    NOTE: *Shift + click to select multiple Assets in the Assets table. In the case of multi-select, the parameters for all selected Assets are listed in the Asset Parameters table.*

4. In the *Asset Parameters* window (see FIG. 217 on page 130), double-click on the Asset Parameter that you want to edit (or right-click on a parameter and select **Edit Asset Parameter** from the context menu). This action opens the *Asset Parameter Properties* page in it's initial view - the **Asset Parameter Setting** tab.
5. Use the options in this tab to view basic properties for the selected Asset Parameter.
6. Click in the **Track Changes** checkbox to track changes to this Asset Parameter.
7. Click **Apply** to save your changes.

Editing Asset Parameter Thresholds

The options in the **Parameter Threshold** tab of the Asset Parameter Properties page allow you to edit threshold values for a selected Asset Parameter:

1. Select **Assets** under *Asset Management* in the Management menu to open the *Asset Management* page (see FIG. 214 on page 126).
2. In the *Locations* window, select the Location that contains the Asset that you want to edit.
3. In the *Assets* window (see FIG. 216 on page 128), select an Asset that contains the parameter entry that you want to edit.

    NOTE: *Shift + click to select multiple Assets in the Assets table. In the case of multi-select, the parameters for all selected Assets are listed in the Asset Parameters table.*

4. In the *Asset Parameters* window (see FIG. 217 on page 130), double-click on the Asset Parameter that you want to edit (or right-click on a parameter and select **Edit Asset Parameter** from the context menu). This action opens the *Asset Parameter Properties* page.
5. Click on the **Parameter Threshold** tab (see FIG. 232 on page 142).
6. Use the options in this tab to view/edit threshold properties for the selected Asset Parameter:
    - Click **Add** to add a new threshold to this Asset Parameter, via the *Parameter Threshold Editor* dialog (see FIG. 233 on page 143).
    - Click **Edit** to edit a selected threshold for this Asset Parameter, via the *Parameter Threshold Editor* dialog (see FIG. 233 on page 143).
    - Click **Delete** to delete a selected threshold for this Asset Parameter.

Adding a Threshold To an Asset Parameter

With an Asset selected in the Assets window:

1. In the *Asset Parameters* window (see FIG. 217 on page 130), double-click on the Asset Parameter that you want to edit (or right-click on a parameter and select **Edit Asset Parameter** from the context menu). This action opens the *Asset Parameter Properties* page.
2. Click on the **Parameter Threshold** tab (see FIG. 232 on page 142).
3. Click **Add**. This action opens the *Parameter Threshold Editor* dialog (see FIG. 233 on page 143).
4. Enter the information for the new parameter (see the *Parameter Threshold Editor Dialog* section on page 143 for details).
5. Click **Save** to save your changes and close the *Parameter Threshold Editor* dialog.

The new parameter is listed in the **Parameter Threshold** tab of the *Asset Parameter Properties* page.

Editing a Threshold For an Asset Parameter

With an Asset Parameter selected in the **Parameter Threshold** tab of the *Asset Parameter Properties* page:

1. Click **Edit**. This action opens the *Parameter Threshold Editor* dialog (see FIG. 233 on page 143).
2. Edit the information for the new parameter (see the *Parameter Threshold Editor Dialog* section on page 143 for details).
3. Click **Save** to save your changes and close the *Parameter Threshold Editor* dialog.

Deleting Asset Parameters

NOTE: *Users must have Manage permission for a specific location to delete a Parameter. The Delete button is disabled if users only have View permission. See the Management - Roles (Classic UI) section on page 192 for details.*

With an Asset selected in the Assets window:

1. In the *Asset Parameters* window (see FIG. 217 on page 130), right-click on a parameter and select **Delete Asset Parameter** from the context menu (or press the Delete key).

2. The program will prompt you to verify this action before the parameter is deleted from the system (FIG. 261):
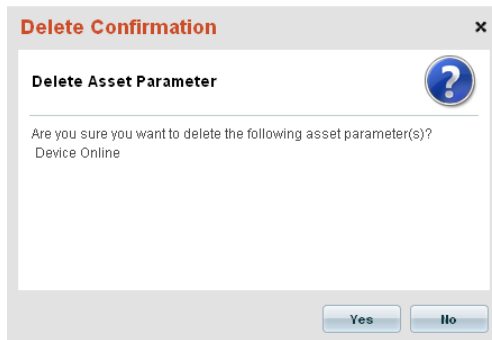
FIG. 261 Delete Confirmation dialog - Delete Asset Parameter

3. Click **Yes** to proceed.

Resetting Tripped Parameters

1. In the *Assets* window, select an Asset that has one or more Asset Parameters assigned. Asset Parameters are defined in the *Asset Management* page - **Parameters** tab (see FIG. 221 on page 134). Refer to the *Asset Properties page - Parameters Tab* section on page 134 for details on managing Asset Parameters.
2. In the *Actions* window, click the **Reset All Tripped Parameters** button.

Adding Parameter Thresholds

1. In the **Parameter Threshold** tab of the Asset Management - Parameter Settings page (FIG. 232 on page 142), click **Add**. This action invokes the *Parameter Threshold Editor* dialog (FIG. 233 on page 143).
2. Specify the threshold settings as desired.
3. Click **Save** to save your changes and close this dialog.

Editing Parameter Thresholds

1. In the **Parameter Threshold** tab of the *Asset Management - Parameter Settings* page (FIG. 232 on page 142), select a Parameter Threshold, and click **Edit**. This action invokes the *Parameter Threshold Editor* dialog (FIG. 233 on page 143).
2. Edit the threshold settings as desired.
3. Click **Save** to save your changes and close this dialog.

Deleting Parameter Thresholds

1. In the **Parameter Threshold** tab of the *Asset Management - Parameter Settings* page (FIG. 232 on page 142), select one or more Parameter Thresholds (ctrl + click for multi-select), and click **Delete**.
2. The system will prompt you to verify this action via the *Delete Confirmation* dialog before the selected Parameter Thresholds are deleted (FIG. 262).
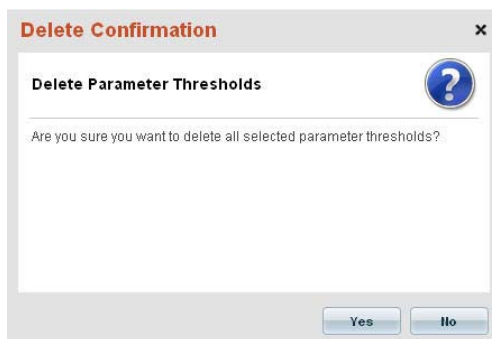
FIG. 262 Delete Confirmation dialog - Parameter Thresholds

3. Click **Yes** to proceed.

Asset Parameter Bargraphs

Parameters that are of the data type *Level*, *Number* or *Float* and that have a maximum value that is greater than the minimum value can be represented in the GUI with a *Bargraph*.

Select the **Bar Graph Enabled** checkbox (in the *Asset Parameter Properties* page - **Asset Parameter Setting** tab) to select from the list of available bargraph types (FIG. 263):


FIG. 263 Asset Parameter Setting tab - Select a Bar Graph option enabled

RMS provides a set of pre-configured Bargraphs. The list of Bargraphs presented here for selection are managed in the *Parameter Bargraphs* page (FIG. 419 on page 259).

See the *Parameter Bar Graphs* section on page 259 for details on adding, editing and deleting Bargraphs.

Enabling Asset Parameter Bargraphs

1. In the *Asset Management page*, double-click on a parameter in the *Asset Parameters* window (or right-click on a parameter and select **Edit Asset Parameter** from the context menu) to access the *Asset Parameter Properties* page - **Asset Parameter Setting** tab.

2. Select the **Bar Graph Enabled** checkbox to display the *Select a Bar Graph* window. This option is only provided for parameters with a data type of *Number* or *Float*.

3. Click to select the Bargraph that best applies to the selected parameter.

4. Click **Apply** to save your changes.

5. The selected Bargraph appears in the *Asset Parameters* window, indicating the parameter's run time value (FIG. 264):

FIG. 264 Asset Parameters window - Bar Graph enabled for "Battery Level"

Resetting Source Usage Statistics for an Asset

1. In the *Assets* window, select an Asset that has one or more Asset Parameters assigned. Asset Parameters are defined in the *Asset Management* page - **Parameters** tab (see FIG. 221 on page 134).

    Refer to the *Asset Properties page - Parameters Tab* section on page 134 for details on managing Asset Parameters.

2. In the *Actions* window, click the **Reset All Source Usage** button.

Working With Control Methods

The **Control Methods** tab of the *Asset Management* page displays a listing of control methods associated with Assets (see FIG. 222 on page 135). The **Execute** option in this tab allows you to manually activate system events or functions.

NOTE: *The control methods associated with each Asset are registered (per Asset) in the 4.6 SDK*

Executing a Control Method

1. In the *Assets* window, select an Asset that has one or more Asset Parameters assigned.
2. Click the **Edit** button. Alternatively, double-click the Asset (or right-click and select **Edit Asset** from the context menu). This action opens the *Asset Management* page.
3. Click on the **Control Methods** tab.
4. In the *Select Control Method* window, drill down through the Category directories to select the Control Method that you want to execute.
5. In the *Control Method Details* window, click on the **Execute** button.
6. The application returns a message at the bottom of this window indicating that the selected Control Method was sent (FIG. 265):
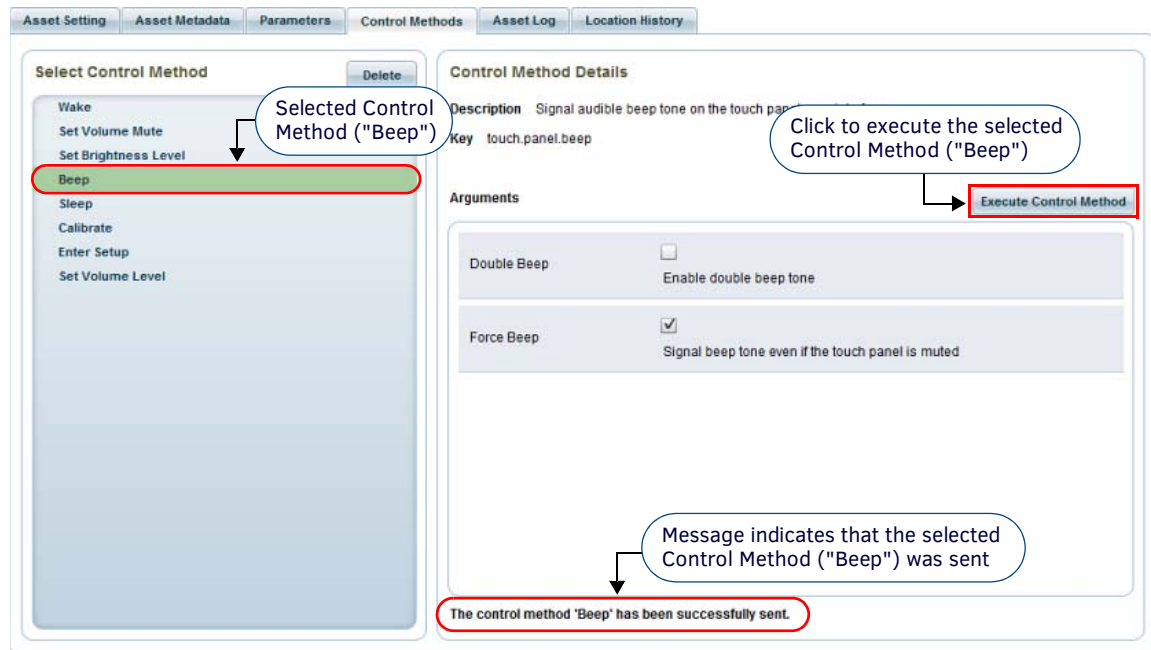
FIG. 265 Asset Management page - Control Methods tab

Duplicate Control Method Entries

If you have upgraded the RMS System from v4.x to v4.6 you may notice that some Control Methods for DVX and Touch Panels devices are listed twice in the Control Methods tab. Potential duplicate Control Method entries are a result of upgrading to the v4.6 SDK, and do not cause any problems. However, it recommended that the duplicate entries are removed, as described below.

NOTE: *Refer to the RMS Enterprise (v4.6 or higher) Installation Guide for details on upgrading from RMS v4.x to RMS v4.6.*

Removing Duplicate DVX and Touch Panel Control Method Entries

If there are duplicate entries for any DVX and/or Touch Panel Control Methods, they can be removed via the *Control Methods* tab of the Asset Management page:

1. In the *Assets* window, select a **DVX** or **Touch Panel** asset.
2. Click the **Edit** button to open the *Asset Management* page.
3. Open the **Control Methods** tab.
4. In the *Select Control Method* window, look for a duplicate Control Method entry. The potential duplicate Control Method entries for both DVX and Touch Panel assets are listed below:

DVX Assets - Potential Duplicate Control Methods	Touch Panel Assets - Potential Duplicate Control Methods
Select Audio Source	Beep
Select Video Source	Enter Setup
Set Audio Mic State	Sleep
Set Audio Mute	Set Brightness Level
Set Front Panel Lockout	Set Volume Level
Set Power	Set Volume Mute
Set Video Mute	
Set Volume	

5. Select a duplicate Control Method entry, and check the **Key** parameter in the *Control Methods Details* window.

6. Look for the term "**mutator**" or "**function**" in the control method Key (for example "asset.front.panel.lockout.*mutator*"):
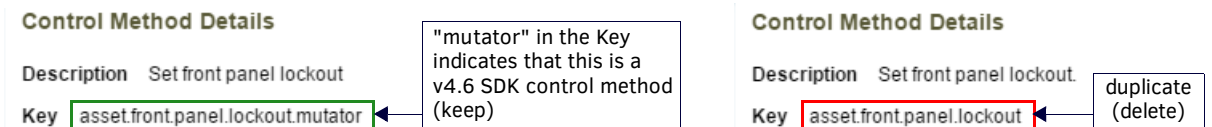
FIG. 266 Asset Management page - Control Methods tab (Control Method Details: Key)

- If the term "mutator" or "function" is included in the Key, then **do not delete**. The inclusion of *mutator* or *function* in the Key indicates that this Control Method is from the v4.6 SDK.
- If the selected duplicate Control Method does *not* include "mutator" or "function" in the Key, then it is a duplicate and should be deleted.

7. Select the duplicate duplicate Control Method entry and click **Delete**.

8. Repeat this process to remove all duplicate Control Method entries.

Working With Asset Logs

The **Asset Logs** tab of the *Asset Management* page (see FIG. 223 on page 136) tracks when thresholds are tripped or when values are returned to a level below the trip point.

The **Delete** option in this tab allows you to manually delete Asset Logs from the system.

Adding a Note to an Asset Log

The **Add Note** feature on this tab allows you to append one or more notes to each Asset Log entry (FIG. 267):
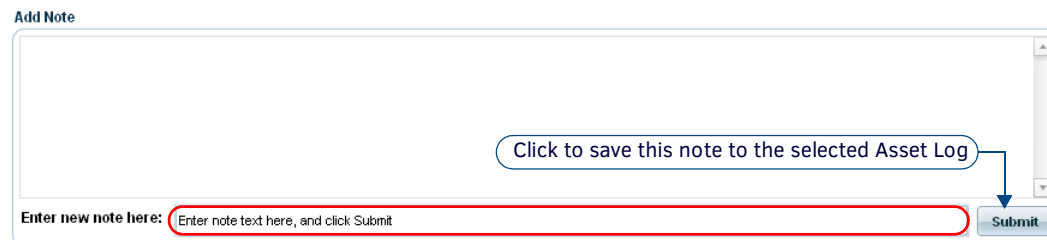
FIG. 267 Asset Logs tab - Add Note window

1. In the *Assets* window, select an Asset that has one or more Asset Parameters assigned.

2. Click the **Edit** button. Alternatively, double-click the Asset (or right-click and select **Edit Asset** from the context menu). This action opens the *Asset Management* page.

3. In the **Asset Log** tab, select an entry in the Asset Log table.

4. In the *Add Note* window, click in the **Enter new note here:** text field, and type.

5. Click **Submit** to save the note to the selected Asset Log.
   - The note is displayed in the *Add Note* window (FIG. 268):
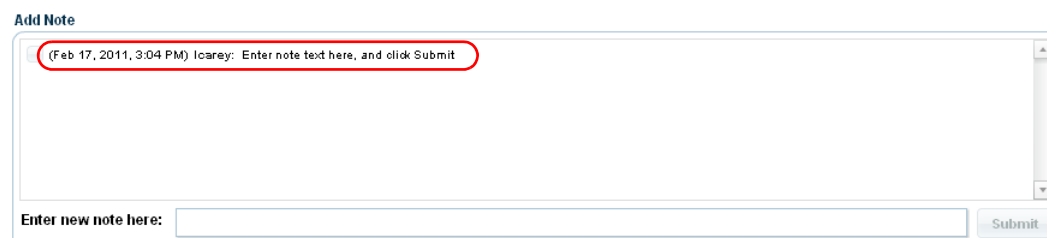
FIG. 268 Add Note window indicating a note for the selected Asset Log

- The icon in the *Notes* column of the Asset Log table indicates that a note has been saved to the Asset Log (FIG. 269):

FIG. 269 Asset Logs table indicating notes for two Asset Logs

Deleting Asset Logs

1. In the *Assets* window, select an Asset that has one or more Asset Parameters assigned.
2. Click the **Edit** button. Alternatively, double-click the Asset (or right-click and select **Edit Asset** from the context menu). This action opens the *Asset Management* page.
3. In the **Asset Log** tab, select one or more entries in the Asset Log table (shift + click to multi-select).
4. Click the **Delete** button.
5. The program will prompt you to verify this action before the Logs are deleted (FIG. 270):
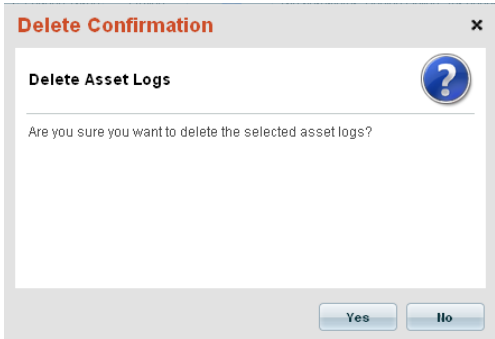
FIG. 270 Delete Confirmation - Asset Logs

6. Click **Yes** to proceed.

Management - Control Macros (Classic UI)

Overview

Click inside the **Management** tab (Classic UI) to access the *Management* menu. The options in this menu allow you to configure Locations/Systems, manage Assets, and manage Users & Notifications, as described in the following sections.

The options in the **Asset Management** category of the *Management* menu allow you to configure *Assets* and *Control Macros* preferences (FIG. 271):
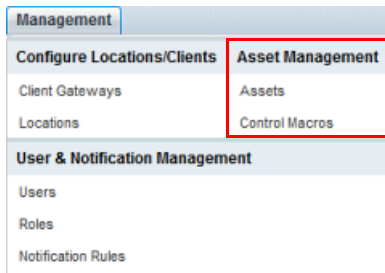
FIG. 271 Management Menu - Asset Management

NOTE: *To access the RMS Classic UI described in this section, select "Classic UI" from the RMS Enterprise HTML interface menu bar.*

Control Macros

Control macros represent sets of control methods for a selected set of Assets.

- The options in the *Control Macro Management* page allow users to create and manage control macros.
- To open the *Control Macro Management* page, select **Control Macros** under *Asset Management* in the Management menu (FIG. 272).
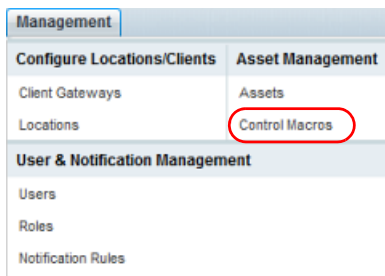
FIG. 272 Management > Configure Locations/Clients > Locations

NOTE: *To access the Control Macros Management UI, the authenticated user must have the global permission: Manage Control Macros. See the Management - Roles (Classic UI) section on page 192 for details.*

This features on this page are organized into several windows (FIG. 273):

- Use the **Control Macro** window to add, execute and delete control macros. - see page 166.
- Use the **Macro Methods** window to define control macro methods - see page 167.
- Use the **Macro Schedules** window to add, edit and delete macro schedules - see page 168.
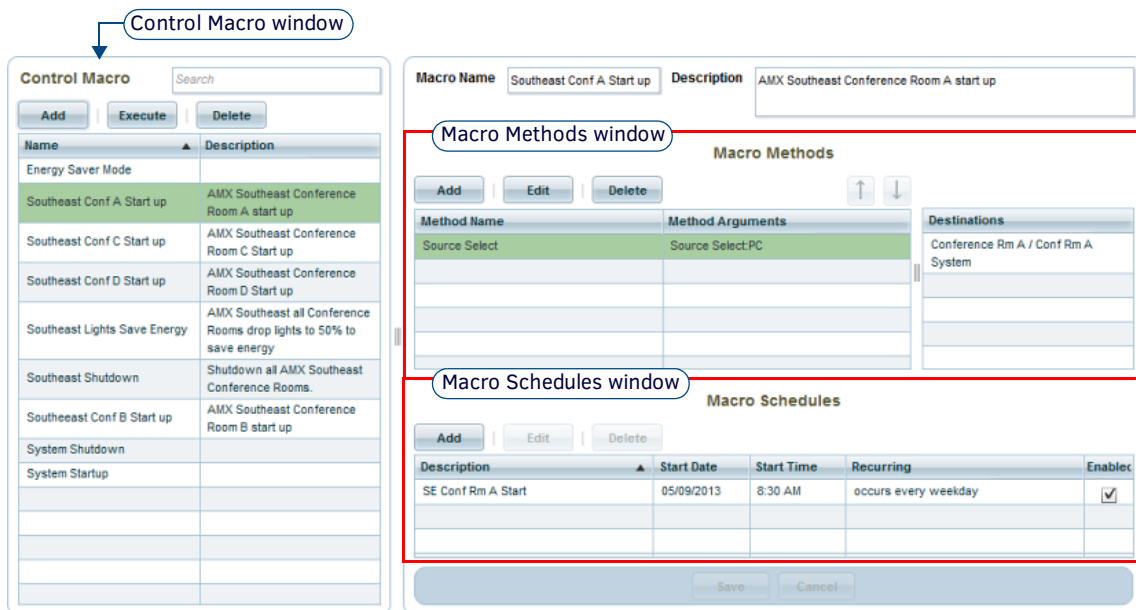
FIG. 273 Control Macro Management page

Control Macro Management Page - Control Macro Window

The **Control Macro** window lists the named control macros in a table, indicating the *Name* and *Description* assigned to each macro. Use the options in the *Control Macro* window to add a new macro, or to select a control macro to execute or delete, as well as search for control macros (FIG. 274).
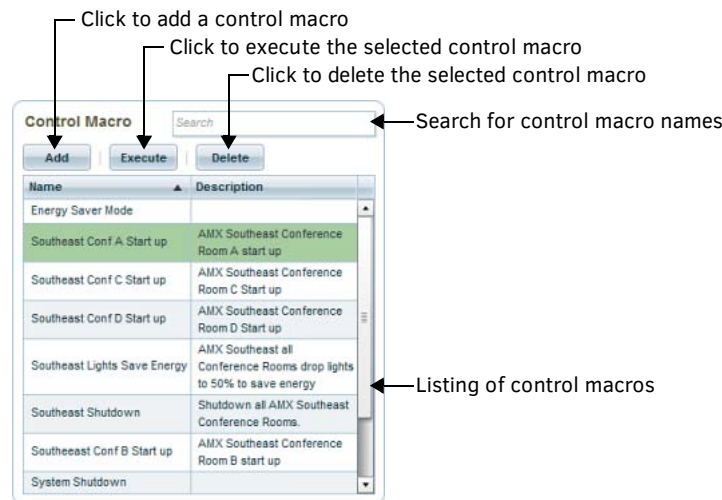
FIG. 274 Control Macro Management Page - Control Macro Window

The options in the *Control Macro* window are described below:

Control Macro Window Options	
Search:	Use this search field to perform a search for control macro names. See *Searching for a Control Macro* on page 172.
Add:	Click to add (create) a new control macro. This action invokes two new fields in the Control Macro window: *Macro Name* and *Description.* Once you have created and saved a new control macro using these fields, click Add in the *Macro Methods* window to launch the Control Macro Wizard to define methods and arguments. See *Adding (Creating) a New Control Macro* on page 172 for details.
Execute:	Click to execute the selected control macro. See *Executing a Control Macro* on page 172 for details.
Delete:	Click to delete the selected control macro. See *Deleting a Control Macro* on page 173 for details.
Control Macros Table:	The Control Macros table lists each control macro that is present in the RMS system providing *Name* and *Description*). Click either column heading to sort the table by that column. *Note: These properties are defined in the Macro Properties window, when the control macro is created or edited.* • See *Control Macros Management Page - Macro Schedules Window* on page 168. • See *Executing a Control Macro* on page 172. • See *Deleting a Control Macro* on page 173.

Control Macro Window Context Menu

Right-click inside the *Control Macro* window to access the following context menu:

Control Macro Window Context Menu Options	
Add	Click to add (create) a new control macro. This action invokes two new fields in the Control Macro window: *Macro Name* and *Description*. See *Adding (Creating) a New Control Macro* on page 172.
Execute	Click to execute the selected control macro. See *Executing a Control Macro* on page 172 for details.
Delete	Click to delete the selected control macro. See *Deleting a Control Macro* on page 173 for details.
Refresh	Click to refresh the data in the *Control Macro* window.

Control Macro Management Page - Macro Methods Window

Macro methods represent explicit asset control methods included in a control macro. When a control macro is selected in the *Control Macros* window, the properties of the selected macro are displayed in the **Macro Methods** window. Use the options in the *Macro Methods* window to define a new macro control method for the selected control macro, or to edit or delete a selected macro control method (FIG. 275). See the *Working With Macro Methods* section on page 174 for details.
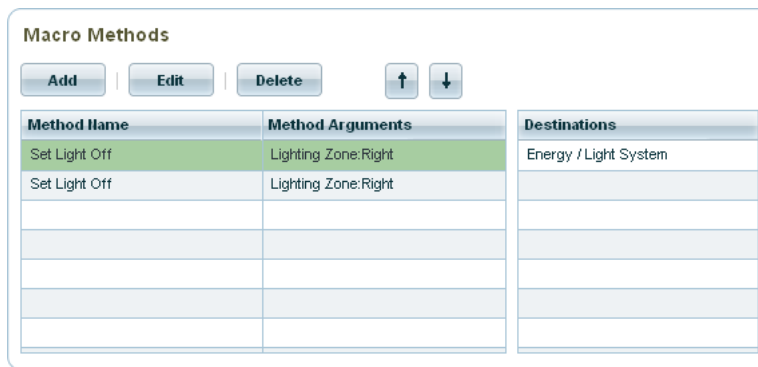
FIG. 275 Control Macro Management Page - Macro Methods Window

The options in the *Macro Methods* window are described below:

Macro Methods Window Options	
Add	Click to add control methods to the selected macro. This action invokes the *Control Macro Wizard* - a series of dialogs that step you through the process of creating a new control macro method. See the *Control Macro Wizard* section on page 169 for details.
Edit	Click to edit the control methods for the selected macro. This action opens the *Edit Control Macro Method* dialog (see FIG. 290 on page 174). The options in this dialog allow addition or removal of specific assets as well as changes to control method arguments. See *Editing a Macro Method* on page 174 for details.
Delete	Click to delete the selected control macro method from the selected control macro. *Note: The selected control macro method will be deleted immediately, in this case the system will not prompt you to verify this action. The deleted method can be retrieved if the user clicks the 'Cancel' button before clicking the 'Apply' button*
Up/Down	These buttons move the selected control macro method up or down in the *Macro Methods* table. *Note: Macros execute methods in the order shown in the Macro Methods table.*
Macro Methods table	The main table in the *Macro Methods* window lists all defined control macro methods, providing basic information for each macro. The information displayed here is defined when each control macro method is defined: • **Method Name**: This column displays a list of all control macro methods that are part of the selected control macro. • **Method Arguments**: This column displays all control method arguments that will be applied to the control macro method in the *Method Name* column.
Destinations table	This table lists all Locations and Assets included in the selected control macro method.

Macro Methods Window Context Menu

Right-click inside the *Macro Methods* window to access the following context menu:

Macro Methods Window Context Menu Options	
Add	Click to add control methods to the selected macro. This action invokes the *Control Macro Wizard* - a series of dialogs that step you through the process of creating a new control macro method. See the *Control Macro Wizard* section on page 169 for details.
Edit	Click to edit the control methods for the selected macro. This action opens the *Edit Control Macro Method* dialog (see FIG. 290 on page 174). The options in this dialog allow addition or removal of specific assets as well as changes to control method arguments. See *Editing a Macro Method* on page 174 for details.

Macro Methods Window Context Menu Options (Cont.)	
Delete	Click to delete the selected control macro method from the active control macro. *Note: The selected control macro method will be deleted immediately, in this case the system will not prompt you to verify this action.*
Move Up Move Down	These options move the selected control macro method up or down in the *Macro Methods* table. *Note: Macros execute methods in the order shown in the Macro Methods table.*

Control Macros Management Page - Macro Schedules Window

Control macros can be configured for automated execution based on **Macro Schedules**. The options in the *Macro Schedules* window allow you to add, edit and delete Schedules for the selected control macro (FIG. 276). See the *Working With Macro Schedules* section on page 175 for details.

FIG. 276 Control Macros Management Page - Macro Schedules Window

The options in the *Macro Schedules* window are described in the following table:

Macro Schedules Window Options	
Add	Click to add (create) a new macro schedule, via the *Macro Schedule Editor* dialog. See *Adding (Creating) a New Control Macro* on page 172 for details.
Edit	Click to edit the selected macro schedule. See *Editing a Macro Schedule* on page 176 for details.
Delete	Click to delete the selected macro schedule. See *Deleting a Macro Schedule* on page 176 for details.
Macro Schedules table	The *Macro Schedules* table lists all scheduled execution instances for the selected control macro. Check the *Enabled* option to enable/disable the selected macro schedule.

Macro Schedules Window Context Menu

Right-click inside the *Macro Schedules* window to access the following context menu:

Macro Schedules Window Context Menu Options	
Add	Click to add (create) a new macro schedule, via the *Macro Schedule Editor* dialog. See *Adding (Creating) a New Control Macro* on page 172 for details.
Edit	Click to edit the selected macro schedule. See *Editing a Macro Schedule* on page 176 for details.
Delete	Click to delete the selected macro schedule. See *Deleting a Macro Schedule* on page 176 for details.

Control Macro Wizard

The *Control Macro Wizard* is a series of dialogs that step you through the process of creating a new control macro method. To invoke the *Control Macro Wizard*:
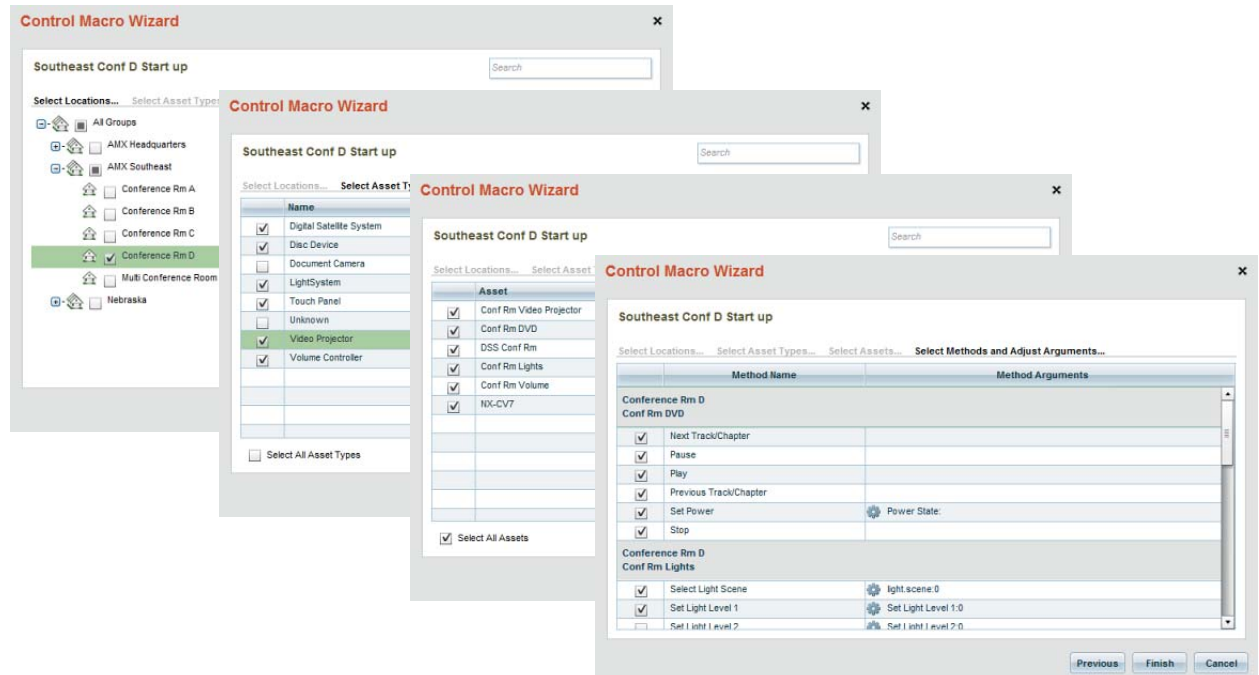
FIG. 277 Control Macro Wizard dialogs

1. Select a control macro in the *Control Macros* window.
2. Click **Add** in the *Macro Methods* window (see FIG. 275 on page 167) to invoke the *Control Macro Wizard*.

Using the Control Macro Wizard

With a macro selected in the *Control Macros* window, click **Add** in the *Macro Methods* window to invoke the *Control Macro Wizard*. The initial view is the **Select Locations** page.

1) Select Locations

1. Select one or more Locations and/or Location Groups to which this control macro will be applied.
    Initially, the only entry displayed is the top-level Location Group called **All Groups**.
2. Click the **+** sign next to the All Groups level to display all Locations and Location Groups.
3. Click the **+** sign next to each Location Group to display all Locations and Location Groups contained within .
4. Click to select the Locations and Location Groups to include in this control macro (FIG. 278):
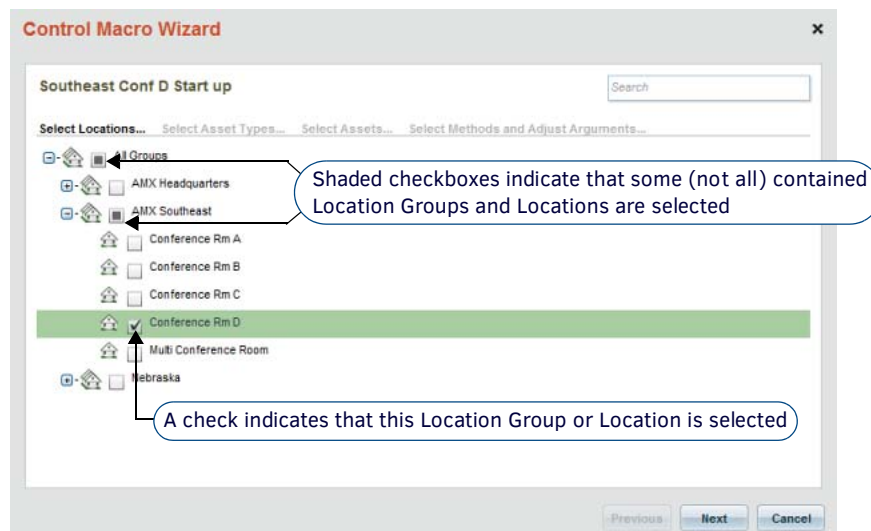
FIG. 278 Control Macro Wizard - Select Locations

5.   Click **Next** to proceed to the *Select Asset Types* page.

NOTE: *At any point in the Control Macro Wizard, you can click Cancel (or click the "X" in the upper-right corner of the dialog) to cancel the process without saving any changes.*

2) Select Asset Types

This page lists either all Asset Types defined in the RMS system (if a Location Group was selected in the previous page) or only the Asset Types related to individual Locations selected on the previous page.

1.   Select one or more Asset Types to be included in this control macro (FIG. 279).

FIG. 279 Control Macro Wizard - Select Asset Types

2.   Click **Next** to proceed to the *Select Assets* page.

3) Select Assets

All Assets of the selected Asset Type present in the selected Location are listed in this page.

1.   Select one or more Assets to be included in this control macro (FIG. 280).

FIG. 280 Control Macro Wizard - Select Assets

2.   Click **Next** to proceed to the *Select Methods and Adjust Arguments* page.

4) Select Methods and Adjust Arguments

All control methods and arguments for the selected Asset(s) present in the selected Location are listed in this page. In the event of multiple assets being selected the list of methods displayed will be broken into one or more groupings: If there are methods that selected assets have in common they will be listed in a Shared grouping first, followed by groupings of each Asset/Location and their non-common methods.

1.   Select one or more control methods to be included in this macro (FIG. 280).
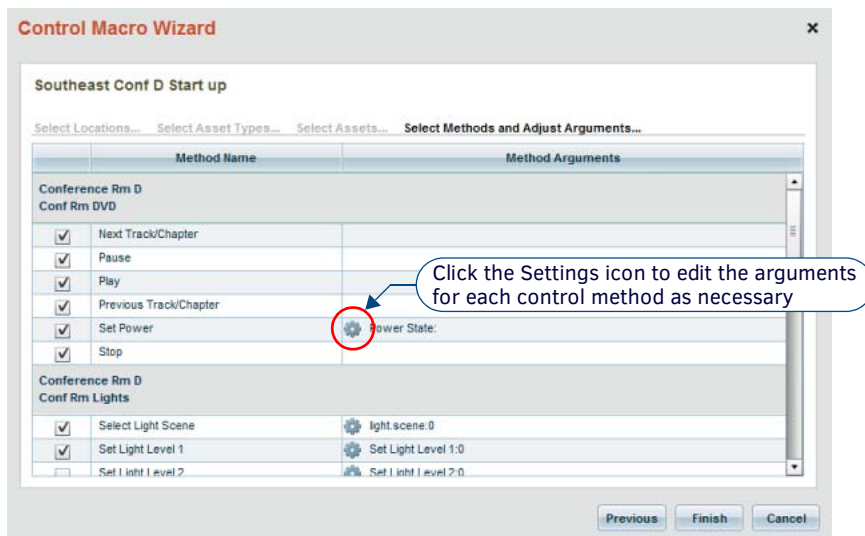
FIG. 281 Control Macro Wizard - Select Methods and Adjust Arguments

2. Click the *Settings* icon (see FIG. 281) for any control macro method to edit that method's arguments as necessary. This action invokes an additional set of fields, depending on the control method selected. An example is shown in FIG. 282:
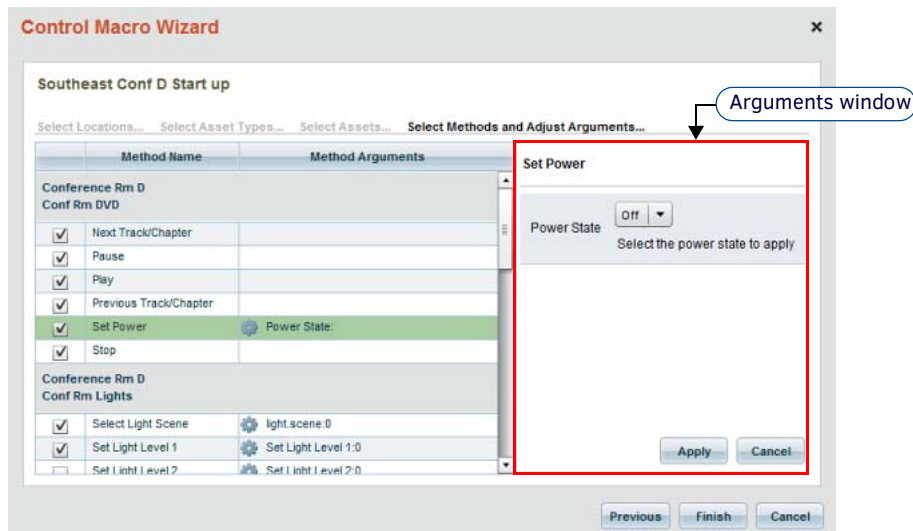
FIG. 282 Control Macro Wizard - Select Methods and Adjust Arguments - Arguments for "Set Power"

3. Click **Apply** in the *Arguments* window to save changes to arguments.

4. Click **Finish** to save changes and close the *Control Macro Wizard*. The program will prompt you to provide arguments for control methods that have none defined (FIG. 283):
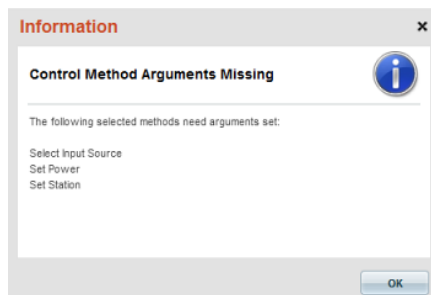
FIG. 283 Control Method Arguments Missing dialog

In this case, revisit each of the control methods listed and edit the arguments as necessary.

Working With Control Macros

Searching for a Control Macro

Use the *Search* tool in the *Control Macro* window to search for a specific control macro by name (FIG. 284).

Control Macro Search window

Control Macro list is filtered to show only search results
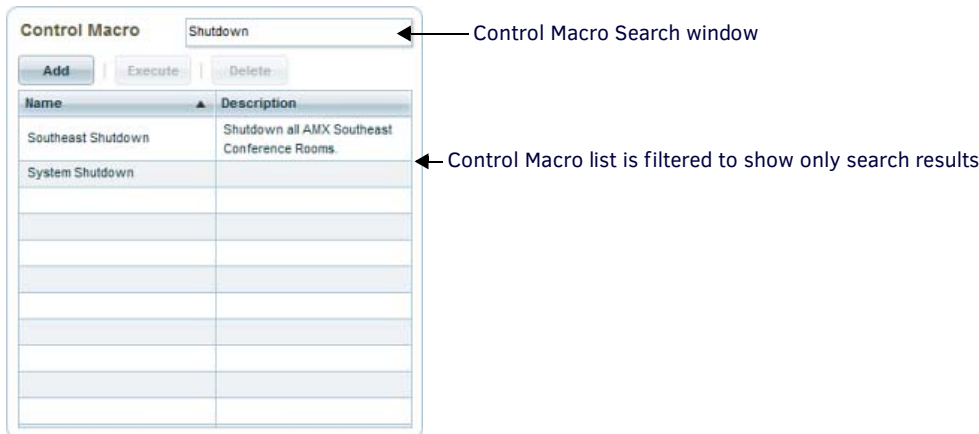
FIG. 284 Control Macro window - Search window

Adding (Creating) a New Control Macro

1.   In the *Control Macro* window, click **Add**. This action invokes two new fields above the *Macro Methods* window: *Macro Name* and *Description* (FIG. 285):
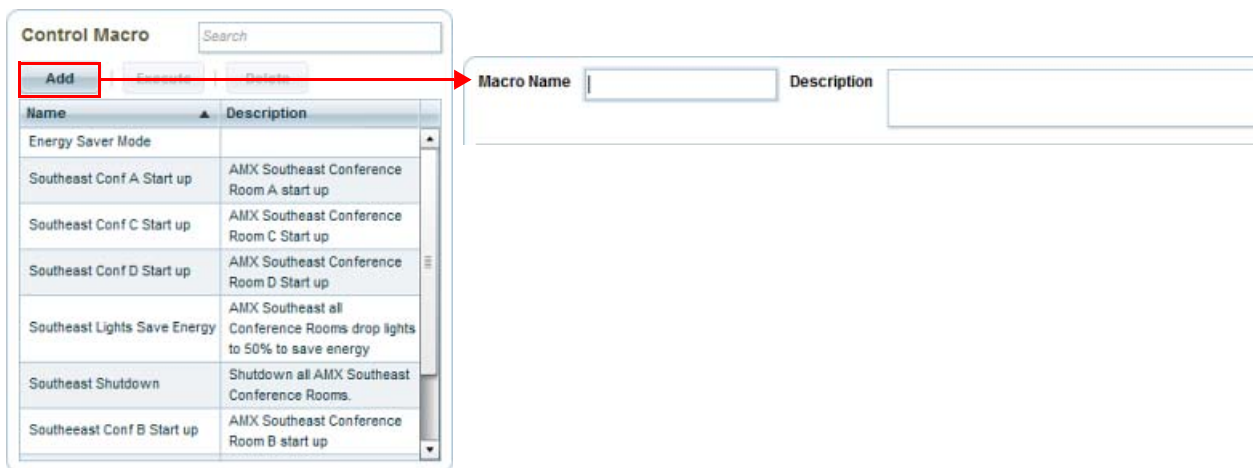
FIG. 285 Control Macro window - Add Control Macro fields

2.   In the **Macro Name** field, enter a name for the new control macro (required).
3.   In the **Description** field, enter a brief description of the new control macro (optional).
4.   Click **Finish** to accept your changes.
5.   The new macro is added to the list in the *Control Macro* window, but is not saved at this point.
6.   Use the *Control Macro Wizard* to add methods to the new macro. See the *Control Macro Wizard* section on page 169 for details.

Executing a Control Macro

1.   Select a control macro in the *Control Macro* window.
2.   Click the **Execute** button (FIG. 286).
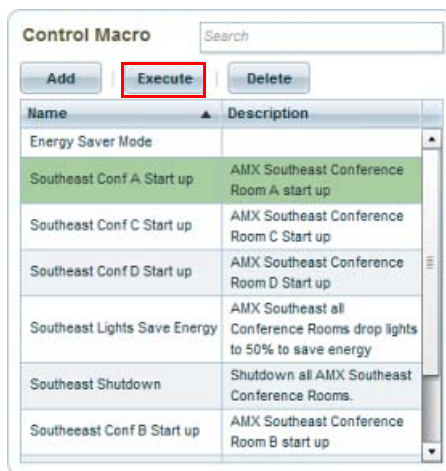
FIG. 286 Executing a Control Macro

3.   The program will indicate that the macro was successfully sent to the assets (FIG. 287).

FIG. 287 Control Macro Execution dialog

4.   Click **Close**.

Deleting a Control Macro

1.   Select a control macro in the *Control Macro* window.

2.   Click the **Delete** button (FIG. 288).
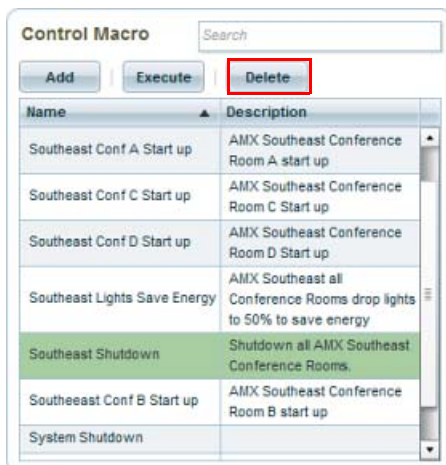
FIG. 288 Deleting Control Macro

3.   The program will prompt you to verify this action before the control macro is deleted from the system (FIG. 289).
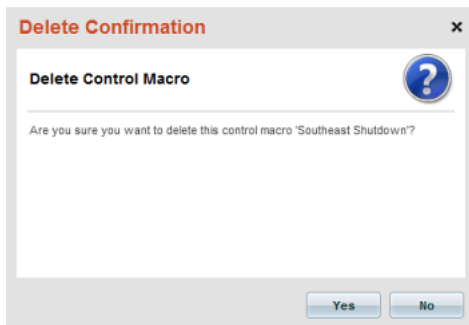
FIG. 289 Delete Confirmation dialog - Control Macro

4. Click **Yes** to proceed.

5. The deleted control macro is removed from the listing in the *Control Macros* window.

Working With Macro Methods

When a control macro is selected in the *Control Macros* window (see FIG. 274 on page 166), the methods for the selected macro are listed in the *Macro Methods* window (see FIG. 275 on page 167).

Adding a Macro Method

- Use the *Control Macro Wizard* to add methods and arguments to the selected control macro.
- See the *Using the Control Macro Wizard* section on page 169 for details.

Editing a Macro Method

Use the options in the *Edit Control Macro Method* dialog to edit a selected control macro method. The options in this dialog allow addition or removal of specific assets as well as changes to control method arguments:

1. Select a control macro in the *Control Macros* window. This populates the *Macro Methods* window with all control macro methods currently saved in the selected macro.

2. Select a control macro method in the *Macro Methods* window.

3. Click **Edit** to access the *Edit Control Macro Method* dialog (FIG. 290):
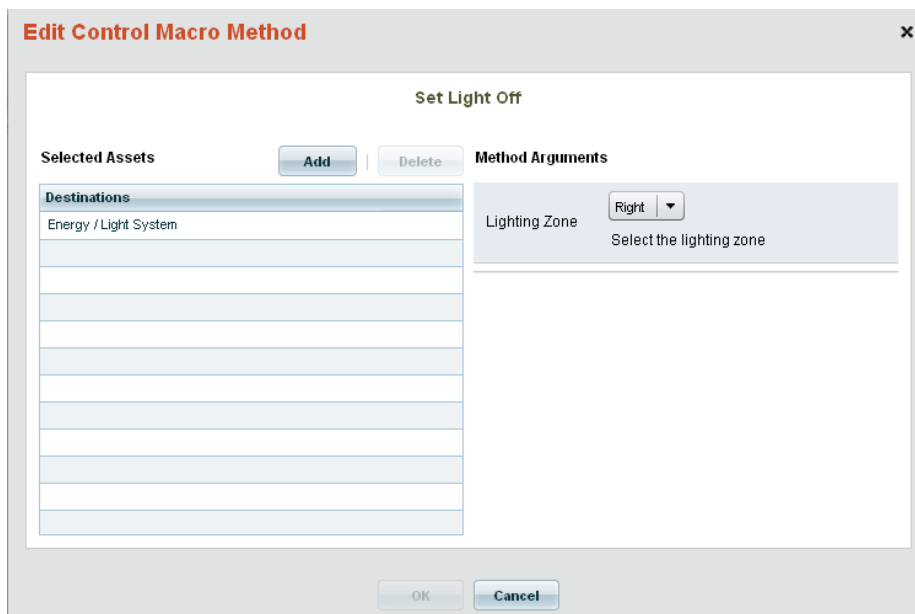
FIG. 290 Edit Control Macro Method dialog

4. Under **Selected Assets**, edit the Assets listed as destinations for this macro method:
   - Click **Add** to select additional assets that have the same Control Method.
   - Click **Delete** to remove the selected destination (Location/Asset) from the list of destinations. If there is only one Destination, the Delete option is disabled.

5. Under **Method Arguments**, edit the arguments associated with the selected control macro method. The fields presented here will depend on the method selected.

Deleting a Macro Method

1. Select a control macro in the *Control Macros* window. This populates the *Macro Methods* window with all control macro methods currently saved in the selected macro.
2. Select a control macro method in the *Macro Methods* window.
3. Click **Delete**.

Working With Macro Schedules

Macro Schedule Editor Dialog

Use the options in the *Macro Schedule Editor* dialog to add and edit macro control schedules (FIG. 291). This dialog is accessed via either the **Add** or **Edit** options in the *Macro Schedules* window.

FIG. 291 Macro Schedule Editor dialog

Macro Schedule Editor Dialog Options	
Description	Enter a descriptive name for this macro schedule.
Start Date	Enter a start date for this macro schedule. Click on the calendar icon to select a start date from a popup calendar. • Click the calendar icon in the upper-right corner of the widget. This opens a pop-up calendar. • Click on the desired date. • Click the close icon at the bottom of the calendar to close the calendar and update the Start Date.
Enabled	Click to enable this macro schedule. Default = *Enabled*.
Start Time	• Use the up and down arrows to adjust the hours and minutes fields to specify a start time for the macro schedule. • Select AM or PM.
Application Time Zone	This read-only field indicates the Application Time Zone, on which macro schedules are based. If the user time zone is different from the application time zone, the time in the user's time zone is displayed as well. *Note: The Application Time Zone is set in the System Configuration > Application Time Zone page. See the Application Time Zone section on page 211 for details.*
Execution time in selected time zones	This field lists Locations that are not in the same time zone as the system time zone, to indicate when a macro may be executing at an unexpected time.
Recurring	Click this option to define this as a recurring macro schedule. Selecting this option enables the *Pattern* and *Lifetime* options below.

Macro Schedule Editor Dialog Options (Cont.)	
Pattern	Select a pattern for the recurring schedule: **Daily**: When selected, the following daily schedule options are presented: • *Every <x> day(s)*: Specify a number of days between recurrences of the macro. • *Every Weekday*: Select to run this macro every weekday at the specified Start Time. **Weekly**: When selected, the following options weekly schedule options are presented: • *Every <x> week(s) on*: Specify a number of weeks between recurrences of the macro. • *Weekday checkboxes*: Select the day(s) on which to run this macro during the weeks specified. **Monthly**: Select one of the following Monthly schedule options: • *Day <#> of every <#> month(s)*: Use the drop-down menus to specify the day-of-month (1-31) and the month-of-year (1, 2, 3, 4, 6, or 12) on which to run this macro. • *The <ordinal #><day> of every <#> month(s)*: Use the drop-down menus to select an ordinal day option (First, Second Third, Forth or Last), a Day/Weekday option, and the month-of-year (1, 2, 3, 4, 6, or 12) on which to run this macro. **Yearly**: Select one of the following Yearly schedule options: • *Every <month><date>*: Use the drop-down menus to specify the Month and Date on which to run this macro. • *The <ordinal #><day> of <month>*: Use the drop-down menus to select an ordinal day option (First, Second Third, Forth or Last), a Day/Weekday option, and the Month on which to run this macro.

Lifetime	Select a duration for the recurring schedule:
	• *No end date*: With this option selected, the recurring macro schedule will not end on any particular date (*default setting*).
	• *End after <x> occurrences*: Select this option to end the recurring macro schedule after a specified number of occurrences (default = *10*).
	• *End by*: Select this option to end the recurring macro schedule on the specified date. Click on the calendar icon to select a start date from a popup calendar.
	  1) Click the calendar icon to open a pop-up calendar.
	  2) Click on the desired date.
	  3) Click the close icon at the bottom of the calendar to close the calendar and update the End By date.

Adding a New Macro Schedule

Use the options in the *Macro Schedule Editor* dialog to add a new schedule to a selected control macro:

1. Select a control macro in the *Control Macros* window. This populates the *Macro Methods* window with all control macro methods currently saved in the selected macro.
2. Click **Add** to access the *Macro Schedule Editor* dialog (FIG. 291). Use the fields in this dialog to define the schedule. See the *Macro Schedule Editor Dialog* section on page 175 for details.
3. Click **Finish** in the *Macro Schedule Editor* dialog to save your changes and close the dialog.

The new schedule is indicated in the *Macro Schedules* window.

Editing a Macro Schedule

Use the options in the *Macro Schedule Editor* dialog to edit a selected control macro:

1. Select a control macro in the *Control Macros* window. This populates the *Macro Methods* window with all control macro methods currently saved in the selected macro.
2. Click **Edit** to access the *Macro Schedule Editor* dialog (FIG. 291). Use the fields in this dialog to edit the schedule. See the *Macro Schedule Editor Dialog* section on page 175 for details.
3. Click **Finish** in the *Macro Schedule Editor* dialog to save your changes and close the dialog.

Deleting a Macro Schedule

1. Select a schedule in the *Macro Schedules* window.
2. Click the **Delete** button.

Management - Users (Classic UI)

Overview

Click inside the **Management** tab (Classic UI) to access the *Management* menu. The options in this menu allow you to configure Locations/Systems, manage Assets, and manage Users & Notifications, as described in the following sections.

The options in the **User & Notification Management** category of the (Classic UI) *Management* menu allow you to configure *Users* and (user) *Roles* as well as (user) *Notification Rules* (FIG. 292):
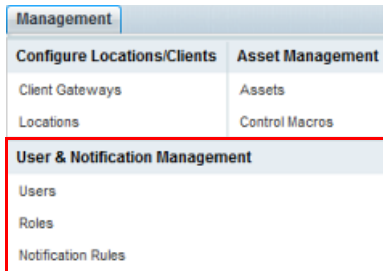
FIG. 292 Management Menu - User & Notification Management

NOTE: *To access the RMS Classic UI described in this section, select "Classic UI" from the RMS Enterprise HTML interface menu bar.*

Users

Users represent individual users of the RMS system. RMS maintains its own internal user database. Users can be created, updated, and deleted. Users can have unlimited Contacts. Users and their contacts can be associated with Notifications and Status Types. Users must be added to roles (see the *Management - Roles (Classic UI)* section on page 192) to control their access to the system.

NOTE: *See Appendix A: Using Directory Services on page 277 for details on using Microsoft Active Directory or LDAP Directory Services.*

- Each user in the RMS application must be associated with a set of Roles to establish which functions of RMS they are able to access. Refer to the *Management - Roles (Classic UI)* section on page 192 for details.
- User accounts and user Properties are managed via options in the *User Management* page. To access this page, select **Users** under *User & Notification Management* in the Management menu (FIG. 293).
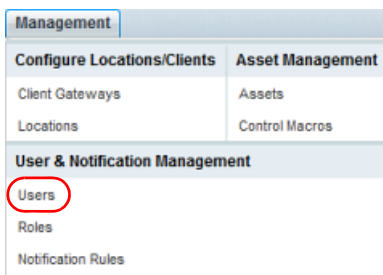
FIG. 293 Management > User & Notification Management > Users

The Users page is split into two main windows: The *Users* window on the left, and the *User Properties* window on the right (FIG. 294).

FIG. 294 User Management page

- Use the **Users** window to view and manage users. See the *User Management Page - Users Window* section on page 181 for details.
- Use the options in the **User Properties** tabs to view and manage user properties. See the *User Management Page - User Properties Window* section on page 182 for details.

NOTE: *Many options on this page are permission-dependant (see the Management - Roles (Classic UI) section on page 192 for details).*

Support For Directory Services

NOTE: *Directory Services are not supported by AMX Cloud hosted Services.*

RMS Enterprise provides support for managing users, contacts, and role membership in their existing directory.

When RMS Enterprise is configured to make use of a directory, there are two distinct modes of operation:

- In one mode, the directory performs the functions of authentication and authorization.
- In the second mode, users are pre-authenticated by a source which has a trust relationship with RMS.

In the case of pre-authentication, the directory is the authoritative source for the roles needed to make authorization decisions. In both modes the directory is the authoritative source for such things as user ID, first name, last name and email. When the RMS system is configured to use a directory server for user management, the directory will be the authoritative source for user creation and management. This means that all users (with the exception of the three special build-in users accounts: *Admin*, *Guest*, and *Client* must be managed in the directory. Refer to *Appendix A: Using Directory Services* on page 277 for details.

Default User Accounts

Several default user accounts are pre-configured in RMS: the default *Administrator* account, the default *Client User* account, the default *Transporter User* account, and the default *Guest User* account.

Default Administrator User Account

RMS includes a default Administrator account that possesses overriding access to all areas of the RMS system. During the initial installation and configuration process, the user will be prompted to enter a password for this default administrator account. This account cannot be removed or disabled from the system; however, its password can be changed. All other user profile settings can be modified.

NOTE: *The system will prompt you to change the default Administrator password on the first login (required).*

The following restrictions apply to the Default Administrator user account:

- Cannot be deleted
- Cannot be disabled
- Cannot change Username property
- Cannot be removed from "Administrators" Role (see the *Default Administrators Role* section on page 193).

Default Client User Account

RMS includes a default Client account. This account cannot be removed or disabled from the system; however, its password can be changed and all other user profile settings can be modified. The following restrictions apply to the Default Client user account:

- Cannot be deleted
- Cannot be disabled
- Cannot change Username property

Default Scheduler User Account

RMS includes a default Scheduler account which is required to support scheduling functionality, and is similar to the default Client account in that it also cannot be removed or disabled from the system; however, its password can be changed. and other user profile settings can be modified. The following restrictions apply to the Default Scheduler user account:

- Cannot be deleted
- Cannot be disabled
- Cannot change Username property
- Cannot be removed from "Scheduler" Role.

Default Transporter User Account

RMS includes a default Transporter account which is required to support transporter (Update Manager) functionality, and also cannot be removed or disabled from the system; however, its password can be changed and other user profile settings can be modified. The following restrictions apply to the Transporter user account:

- Cannot be deleted
- Cannot be disabled
- Cannot change Username property
- Cannot be removed from "Transporter" Role.

Default Anonymous / Guest User Account

Anonymous access is fulfilled with an actual account with the user name "*Guest*". The Guest account can be disabled if anonymous access is undesirable.

NOTE: *The Guest account is only available for installed RMS Servers; it cannot be enabled for AMX Cloud hosted services.*

- The default Guest account can be disabled (see *Enabling / Disabling the Guest Account*). The Guest account cannot be removed, only disabled.
- All user profile properties can be modified with the exception of the username - the username cannot be altered.

If the Guest account is enabled, any time a user visits the RMS application they will be logged in as *Guest*. They then have the option of signing into RMS with their own user account or remaining anonymous. By default, the Guest account has limited access, but through Role Management the guest account can be made as restricted or open as desired. See the *Management - Roles (Classic UI)* section on page 192 for details.

Any user preference settings (e.g. locale preference) modified while logged in on the Guest account are saved to the user's local computer (similar to a browser cookie) rather than in the RMS database. This allows for multiple people to make use of the guest account and still have a customized experience, albeit local to each physical computer.

The following restrictions apply to the Default Guest User account:

- Cannot be deleted
- Cannot change username property
- Cannot be removed from "Guest" permissions role
- Cannot be enabled for AMX Cloud hosted services

Enabling / Disabling the Guest Account

NOTE: *The Guest account is only available for installed RMS Servers; it cannot be enabled for AMX Cloud hosted services.*

1. In the *Users* window of the *User Management* page (see page 181), select the **Guest** account (FIG. 295).

Note that for AMX Cloud hosted services, the Guest account is indicated in the Users list, but cannot be enabled

FIG. 295 Users window - "Guest" Account selected

2. In the **User Profile** tab of the *User Properties* window, de-select the **Account Enabled** checkbox (FIG. 296):

FIG. 296 User Properties window - User Profile tab -"Guest" Account Disabled

> **NOTE:** *The Account Enabled option is not available for AMX Cloud hosted services.*

3. Click **Save** to save your changes.

> **NOTE:** *The Guest account can also be disabled via the Security Policy page. See the Security Policy section on page 212.*

User Authentication (Sign-In) Form

RMS provides a user authentication (Sign-In) form and associated error handling for invalid user credentials, disabled user accounts, and other login associated failures. Additionally, this user authentication form enforces user password expiration rules and failed login attempt rules (FIG. 297).

This option is displayed only if the "Enable Guest Account (Anonymous Access)" option is selected (in the Settings > Security Policy page)

FIG. 297 User Sign-In Form

- The *Sign In As Guest* option is not displayed if the system is not configured to allow anonymous guest access (see the *Security Policy* section on page 212).
- This Sign-In form will not be displayed if the user is authenticated via an external Single-Sign-On implementation such as *Windows Integrated Authentication* or *SiteMinder*.

User Profiles - Persistence

RMS persists user preferences, to provide a personalized UI for each user.   Each user account defined in the RMS system maintains its own discrete set of user preferences.

The exception is the *Guest* account. Since the "Guest" account is not a distinct user account, it instead persists its settings to a local computer cache rather than the RMS database. This allows unique "Guest" personalization on a computer basis, and prevents multiple "Guest" users from affecting the UI experience of other "Guest" users. See the *Default Anonymous / Guest User Account* section on page 179 for details.

A user's personalization settings can be reset to default in the User Management pages while editing a user's profile. This same option is also available to each user under their 'My Profile' management pages.

User Management Page - Users Window

Use the **Users** window to view and manage users. Initially, the Users window contains the default users, *Admin*, *Client*, *Guest, Scheduler* and *Transport*. FIG. 298 shows the Users window indicating several sample users:
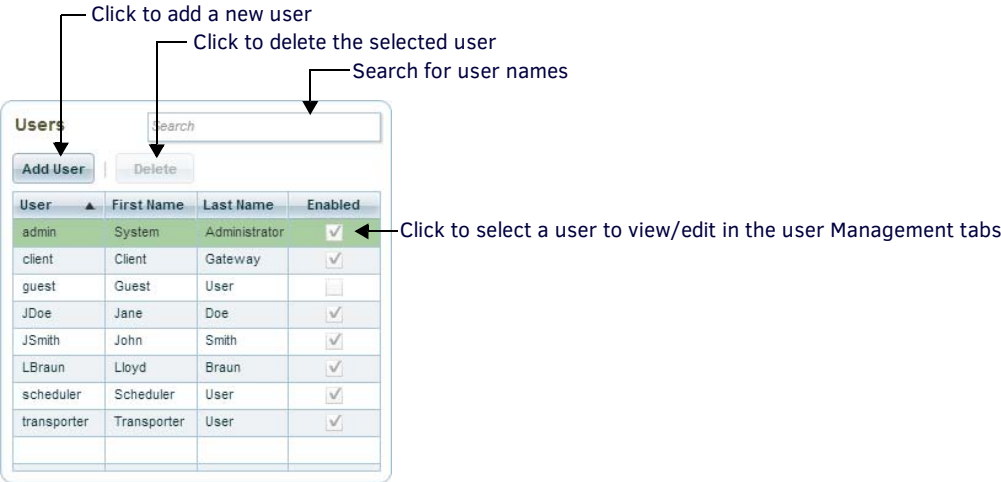
FIG. 298 User Management page - Users window

The options on the *Users* window are described below:

User Window Options	
Search	Use this search field to perform a search for user names.
Add User	Click to clear the fields in the *User Properties* window, in which you can define a new user. See *Adding a New User Account* on page 187 for details.
Delete	Click to delete the selected user. See *Deleting a User Account* on page 187 for details.
Users List	The users list shows all current users, providing the basic information for each user (*User Name*, *First Name* and *Last Name*). Note that the default *Guest* account is only available for installed RMS Servers; it cannot be enabled for AMX Cloud hosted services.

Users Window Context Menu

Right-click inside the *Users* window to access the following context menu:

Users Window Context Menu Options	
Add User	Click to generate a new set of empty tabs in the *User Properties* window. Use the options in these tabs to define (add) a new user. See the *Adding a New User Account* section on page 187 for details.
Delete User	Click to delete the selected user. • The default System Administrator, Client and Guest accounts (and the User account of the current user) cannot be deleted. • See the *Deleting a User Account* section on page 187 for details.
Refresh	This option refreshes the listing in the users window.

User Management Page - User Properties Window

Use the **User Properties** window (in the *User Management* page) to view and manage detailed properties for each individual user. This window is separated into several tabs, each described in the following sections.

User Properties Window - User Profile Tab

The options in the **User Profile** tab of the *User Properties* window allow you define, edit and view basic profile information for a selected user (FIG. 299).

FIG. 299 User Properties Window - User Profile tab

NOTE: *This page is also available to each user to self manage under the My Profile menu item. See the My Profile - My Contacts Tab section on page 87 for details.*

The options in this tab are described below:

User Profile Tab Options	
Account Enabled	A checkmark in this option indicates that this user's account is enabled, and is therefore allowed to login to the RMS system, based on the login credentials specified in this tab. • De-select this checkbox to disable the selected user's account. • Once disabled, this user will not be allowed to login to the RMS system. • The default Administrator, Client and Guest accounts cannot be disabled. • Default = *Account Enabled* See the *Enabling / Disabling a User Account* section on page 188 for details.
First /Last Name	Enter this user's first and last name (required input).
Username	Enter a username for this user (required input). The username is presented for most admin views, and is required for user Sign-In. *Note: If you edit a User's "Username", it is necessary to re-enter (and confirm) the Password before the name change can be saved.*
Password	Enter a password for this user (required input). The password entered here will be required for this user to login to the RMS system. • *Re-type Password*: Re-type the password in this text field, to verify proper entry. • *Require password change on next login*: Select this option to prompt this user to change their password, the next time they attempt to login to the RMS system (default = *disabled*). Upon a successful change, this option is reset to unchecked. *Note: The Password must be entered (and re-typed) each time that a User account is edited, in order to save changes. See Editing a User Account on page 187.*
Automatically sign out after 120 minutes of inactivity	Click this option to automatically sign this user out of the system, after 120 minutes of inactivity (default = enabled).

User Profile Tab Options (Cont.)	
Show Update Manager Badge	Click this option to enable the notification icon in the *Update Manager* tab: The Update Manager Badge notifies this user to click the Update Manager tab to manage available device firmware updates, via Update Manager (default = enabled). Refer to the *Update Manager (HTML UI)* section on page 28 for details.
Time Zone	Choose a time zone for the selected user. See the *Setting a Custom Time Zone for a User* section on page 188 for details.
Reset User's Preferences	Click this button to reset the selected user's configured preferences to their default values. *Note: This action will clear any personalization changes made to the application for this user including re-sized and re-ordered columns and dashboard customization. This action cannot be undone and all personalization will be reset to their respective 'DEFAULT' values. See the Resetting User Preferences section on page 188 for details.*

User Properties Window - User Contacts Tab

The options in the **User Contacts** tab of the *User Properties* window allow you to define, edit and view contact information for a selected user (FIG. 300).

FIG. 300 User Properties Window - User Contacts tab

NOTE: *This page is also available to each user to self manage under the My Profile menu item. See the My Profile - My Contacts Tab section on page 87 for details.*

The options in this tab are described below:

User Contacts Tab Options	
Email	
Add E-Mail	Click to add an empty E-Mail entry to the E-Mail list. See the *Adding Contact Information to a User Account* section on page 189 for details.

E-Mail information	• Delete: Click the "X" icon to delete any listed contact.
	• *Enable*: De-select this option to disable an E-Mail address for this user. By default, all E-Mail addresses are enabled.
	  Note: Disabling contact information does not delete them from the system.
	• *E-Mail address field*: Enter the E-Mail address in this text field.
	• *Location drop-down menu*: Select a Location (*Home* or *Work*) from this drop-down menu.
	• *E-Mail Format Type drop-down menu*: Select the format type of E-Mail to send to this E-Mail address from this drop-down menu. The options are:
	  HTML - This option uses HTML E-Mail to send notifications.
	  Text - This option uses text E-Mail to send notifications.
	  Short Text - This option uses a shorter text field to send brief text messages.

User Contacts Tab Options (Cont.)	
Email (Cont.)	
All Status Types/ Selected Status Types	This message indicates whether this email address will be used for email messages associated with All Status Types (default setting), or with selected status types. To select specific status types for this email address, click the *Settings* icon next to *All Status Types* to open the *Select Status Types* dialog, where you can select from a listing of supported status types. If you have selected status types in this dialog, the message changes to indicate "Selected Status Types".
Phone	
Add Phone	Click to add an empty Phone entry to the E-Mail list. See the *Adding Contact Information to a User Account* section on page 189 for details.
Phone information	Phone number contacts are for informational purposes only. RMS does not support sending SMS messages to a phone number. • *Phone number field*: Enter the Phone number in this text field. • *Location drop-down menu*: Select a Location (*Home*, *Work* or *Mobile*) from this drop-down menu.

User Properties Window - Notification Schedule Tab

The options in the **Notification Schedule** tab of the *User Properties* window allow you define, edit and view notification schedule information for a selected user (FIG. 301).

FIG. 301 User Properties Window - Notification Schedule tab

NOTE: *This page is also available to each user to self manage under the My Profile menu item. See the My Profile - Notification Schedule Tab section on page 89 for details.*

The options on this tab are described below:

Notification Schedule Tab Options	
Scheduled Notification Options	Select a scheduling option for notifications to the selected user: • *Never Send Notifications*: When this option is selected, this user will never receive notifications from RMS. • *Always Send Notifications*: When this option is selected, this user will always receive notifications from RMS (default setting). • *Only Send Notifications According to Schedule*: When this option is selected, this user will receive notifications according to the notification scheduling options defined in this tab. See *Scheduling User Notifications* on page 190 for details.
Schedule options	Use the set of Schedule options to define a Notification Schedule for this user. See *Scheduling User Notifications* on page 190 for details.

User Notification Schedule Override

Note that user notification schedules can be overridden by the **Override User Notification Schedule** option in the *Edit Notification Settings* dialog, accessible via the **Add** or **Edit** buttons in the Notification Rules window of the *Notification Rules* page (see the *Edit Notification Rule dialog* section on page 204).

User Properties Window - User Notifications Tab

The options in the **User Notifications** tab of the *User Properties* window allow you edit and delete notification schedule information for a selected user (FIG. 301). All global notifications are listed for all users, and any personal notifications will be listed per user.
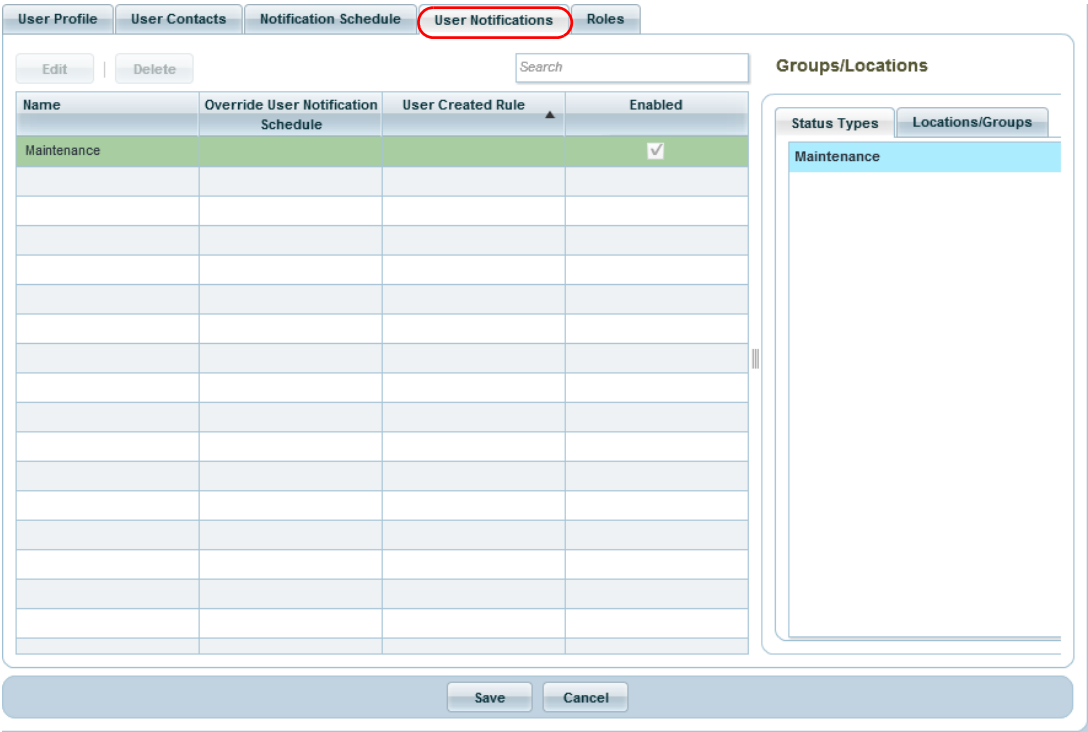
FIG. 302 User Properties Window - User Notifications tab

- The Administrator can create global notifications in the Notification Rules Management page (see the *Management - Notification Rules (Classic UI)* section on page 201).
- Users can create personal notifications in the My Profile page (see the *Dashboard - My Profile (Classic UI)* section on page 84). Users can edit or delete personal notifications.

The options in this tab are described below:

User Notifications Tab Options	
Edit	Click to edit the selected user Notification(s). *Note: This option is available only if the current user has created their own notification rules.*
Delete	Click to delete the selected user Notification(s).
Search	Click in this field to search for user Notifications - see *Searching for User Notifications* on page 191.
User Notifications table	The table in this tab presents the following properties for the selected user Notification: • Name • Override User Notification Schedule (enabled/disabled) • User Created Rule • Enabled

User Properties Window - Roles Tab

The options in the **Roles** tab of the *User Properties* window allows you define, edit and view the permissions Roles to which the selected user belongs (FIG. 303).
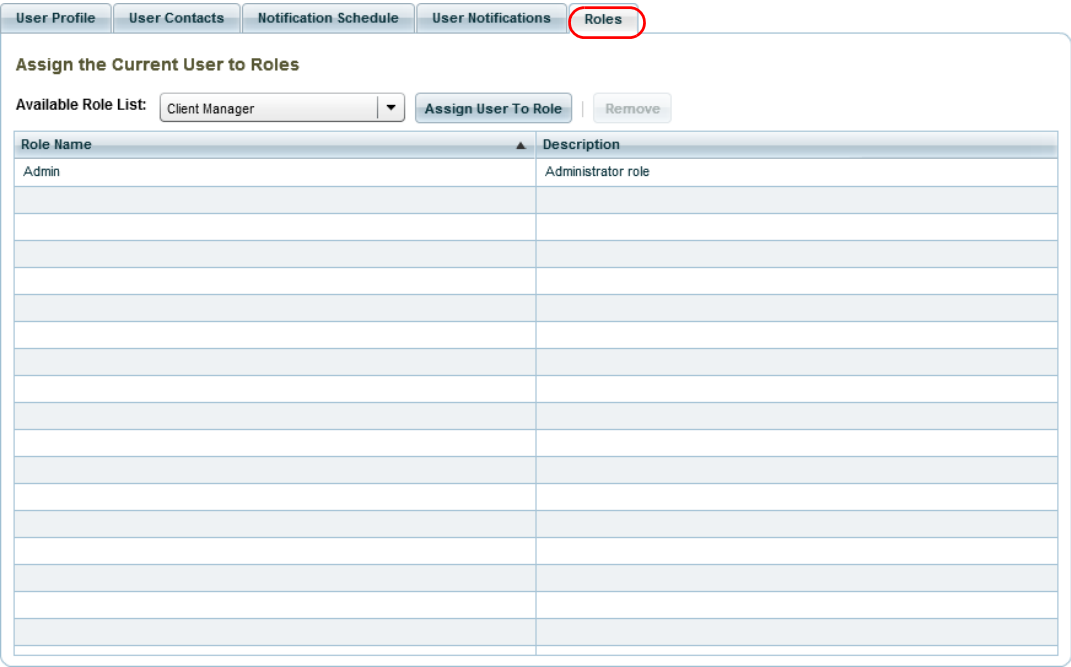
FIG. 303 User Properties Window - Roles tab

The options in this tab are described below:

Roles Tab Options	
Available Roles drop-down menu	Select which Role to add to the selected user from this drop-down menu. The default Roles are *Admin*, *Guest* and *Client*. Note: Roles are defined in the Role Management page. See the *Management - Roles (Classic UI)* section on page 192 for details.
Add Role to User	With a Role selected in the Roles drop-down menu, click this button to add the selected Role to this user. The added Role is then listed in the User Roles table.
Remove	With a Role selected in the User Roles table, click this button to remove the selected Role from this user.
User Roles table	This table lists all Roles currently assigned to the selected user, providing basic information (*Role Name* and *Description*). Double-click on a Role to edit the selected Role in the *Role Management* page. See the *Management - Roles (Classic UI)* section on page 192 for details.

Working With Users

User Profiles (User Accounts)

Adding a New User Account

1. In the *Users* window of the User Management page (FIG. 298 on page 181), click the **Add User** button. This action generates a new (empty) set of tabs in the *User Properties* window (FIG. 299 on page 182).

2. Fill in each tab to define this user account:
    *   See the *User Properties Window - User Profile Tab* section on page 182
    *   See the *User Properties Window - User Contacts Tab* section on page 183
    *   See the *User Properties Window - Notification Schedule Tab* section on page 184
    *   See the *User Properties Window - User Notifications Tab* section on page 185
    *   See the *User Properties Window - Roles Tab* section on page 186

    NOTE: *In order to create a new User Account, it is only necessary to complete the User Profile and Roles tabs. The other information can be added later.*

3. Click **Save** to save your changes. The new user is added to the Users window.

Deleting a User Account

1. In the Users window of the User Management page (FIG. 298 on page 181), select a user from the list.

2. Click the **Delete** button.

    NOTE: *Note that the Delete option is not available for the default Administrator, Client and Guest accounts. These accounts cannot be deleted from the system.*

3. The system will prompt you to verify this action before the user is deleted, via the *Delete Confirmation* dialog (FIG. 304):
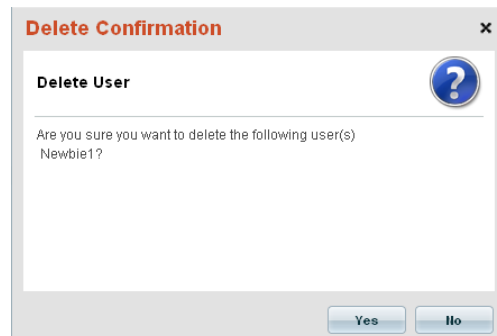
FIG. 304 Delete Confirmation dialog - User

4. Click **Yes** to proceed.

5. The selected user is deleted from the user list, and from the system.

Editing a User Account

Use the options in the tabs of the *User Properties* window to edit a selected user account:

1. In the Users window (see FIG. 298 on page 181), select a user account to edit.

2. Go through each of the tabs in the User Properties window to edit settings as desired:
    *   See the *User Properties Window - User Profile Tab* section on page 182

    NOTE: *If you edit a User's "Username", it is necessary to re-enter (and confirm) the Password before the name change can be saved.*

    *   See the *User Properties Window - User Contacts Tab* section on page 183
    *   See the *User Properties Window - Notification Schedule Tab* section on page 184
    *   See the *User Properties Window - User Notifications Tab* section on page 185
    *   See the *User Properties Window - Roles Tab* section on page 186

3. Click **Save**.

Searching For Users

Use the Search tool in the *Users* window to search for a specific user by *User Name*, *First Name* or *Last Name* (FIG. 305).
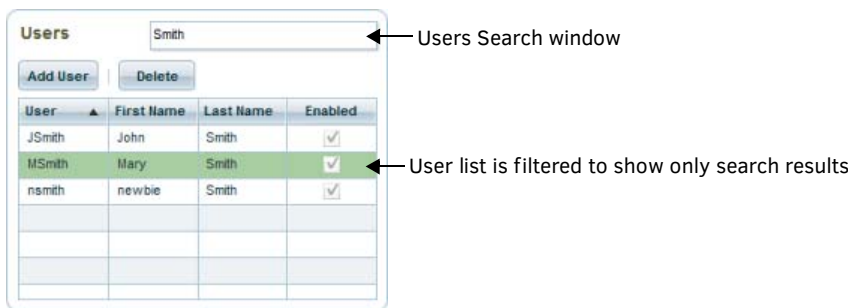
FIG. 305 Users window - Search window

Enabling / Disabling a User Account

This option is not available for the default Administrator, Client and Guest accounts. These accounts cannot be disabled.

NOTE: *The Guest account is only available for installed RMS Servers; it cannot be enabled for AMX Cloud hosted services. On AMX Cloud hosted services, the Guest account is indicated in the User list, but the option to enable the account is disabled.*

1. Select a user in the Users window.
2. In the **User Profile** tab, de-select the **Account Enabled** option. By default, this option is selected (indicating that the account is currently *Enabled*).
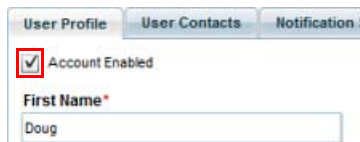
FIG. 306 Users window - Account Enabled

3. Click **Save**.

   NOTE: *User accounts can also be deleted from the system. See the Deleting a User Account section on page 187 for details.*

Editing User Profile Information

1. In the *Users* window of the *User Management* page (FIG. 298 on page 181), select a user from the list. When a user is selected, the tabs in the *User Properties* window are populated with the selected user's information.
2. Edit the fields in each tab as desired:
   ● See the *User Properties Window - User Contacts Tab* section on page 183

   NOTE: *If you edit a User's "Username", it is necessary to re-enter (and confirm) the Password before the name change can be saved.*

   ● See the *User Properties Window - Notification Schedule Tab* section on page 184
   ● See the *User Properties Window - User Notifications Tab* section on page 185
   ● See the *User Properties Window - Roles Tab* section on page 186
3. Click **Save** to save your changes.

Setting a Custom Time Zone for a User

The local time for users is calculated from UTC to the user's configured time zone. This calculated time includes daylight savings time shifts for the user's configured time zone. This user property can be changed at any time by a system administrator or by each individual user in user profile management.

NOTE: *The user preferred time zone is used to render time values to the user interface, and user communications. All RMS data is stored in UTC time.*

1. In the *Users* window of the *User Management* page (FIG. 298 on page 181), select a user from the list in the *Users* window.
2. In the **User Profile** tab, use the *Location* and *Time Zone* drop-down menus to select a Time Zone for this user account.
3. Click **Save** to save your changes.

NOTE: *If a user does not define a custom time zone, then the default Application time zone will be used (see the Application Time Zone section on page 211).*

Resetting User Preferences

1. Select **My Profile** in the Dashboard menu to open the *My Profile* page - **General Setting** tab (see FIG. 135 on page 85).
2. Click **Reset** to reset this user's configured preferences to their default values (FIG. 307):

Reset User's Preferences   **Reset**

This action will clear any personalization changes made to the application for this user including re-sized and re-ordered columns and dashboard customization. This action cannot be undone and all personalization settings will be reset to their respective 'DEFAULT' values.

FIG. 307 My Profile page - General Setting tab: Reset

User Contact Information

Adding Contact Information to a User Account

1. In the *Users* window of the *User Management* page (FIG. 298 on page 181), select a user from the list.
2. Open the **User Contacts** tab.
3. To add an E-Mail contact:
   a. Enter the user's E-Mail address in an empty **E-Mail** text field (FIG. 308):

E-Mail address text field   Location menu   E-Mail type menu

Status Types setting for this E-Mail Address

Status Types Settings icon - Click to open the Select Status Types dialog

FIG. 308 E-Mail User Contact Information

   b. Select a location (*Home* or *Work*) from the *Location* drop-down menu.
   c. Select an E-Mail format type (*HTML*, *Text* or *Shorttext*) to use for notifications to this user from the *E-Mail Type* drop-down menu.
   d. By default, E-Mail contacts are set to receive all status types. To select specific Status Types for this E-Mail address, click the Status Types Settings icon, and select from a list of supported Status Types (in the *Select Status Types* dialog - see FIG. 309).

FIG. 309 Select Status Types dialog

4. To add an Phone number contact:
   a. Enter the user's Phone number in an empty **Phone** text field (FIG. 310):

Phone number text field   Location drop-down menu

FIG. 310 Phone User Contact Information

   b. Select a location (*Home* or *Work*) from the *Location* drop-down menu.
   NOTE: *Phone number contacts are for informational purposes only. RMS does not support sending SMS messages to a phone number.*

5. Click **Save** to save your changes.

Enabling and Disabling User Contact Information

By default, all user email Contact information entries are enabled, meaning they will all receive notifications according to the Notification options defined in the **Notification Schedule** tab (see *User Properties Window - Notification Schedule Tab* on page 184).

Use the **Enable** checkbox (FIG. 311) to disable or re-enable any user Contact entry.
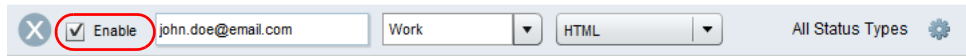
FIG. 311 Enable/Disable Contact Information

If there is not a checkmark in this checkbox, then the associated user Contact entry is disabled, and will not receive notifications (regardless of any Notification Schedule options defined).

NOTE: *Contact information entries are not deleted from the system via this option.*

Deleting User Contact Information

Click the "X" icon to delete any contact entry from the system (FIG. 312):
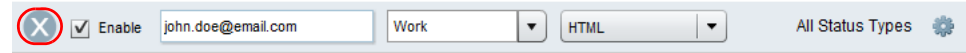
FIG. 312 Delete Contact Information

User Notification Schedules

Enabling and Disabling Notifications for a User

1. In the *Users* window of the *User Management* page (FIG. 298 on page 181), select a user from the list.
2. Open the **Notification Schedule** tab.
3. Select a *Schedule* option:
   - *Never Send Notifications*: When this option is selected, this user will never receive notifications from RMS.
   - *Always Send Notifications*: When this option is selected, this user will always receive notifications from RMS.
   - *Only Send Notifications According to Schedule*: When this option is selected, this user will receive notifications according to the notification scheduling options defined in this tab.

   Default = *Always Send Notifications*
4. Click **Save** to save your changes.

Scheduling User Notifications

1. In the *Users* window of the *User Management* page (FIG. 298 on page 181), select a user from the list.
2. Open the **Notification Schedule** tab.
3. Select the *Only Send Notifications According to Schedule* option. This action enables the notification schedule calendar (FIG. 313):
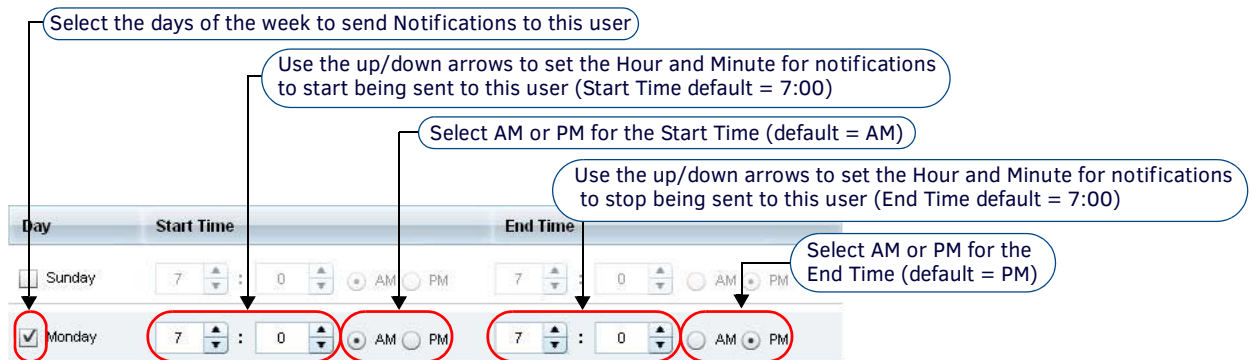
FIG. 313 Notification Schedule options

4. Click in the checkboxes in the **Day** column to specify the days that this user will receive notifications. Note that when a day is selected, the *Start Time* and *End Time* fields are activated.
5. Use the up / down arrows in the **Start Time** column to set the Hour and Minute that notification will start being sent to this user (default = *7:00*).
6. Select either **AM** or **PM** for the Start Time (default = *AM*).

   NOTE: *In some cases, the AM/PM options will not be displayed, depending on whether the selected Locale uses a 24-hour clock.*
7. Use the up / down arrows in the **End Time** column to set the Hour and Minute that notification will cease being sent to this user (default = *7:00*).
8. Select either **AM** or **PM** for the End Time (default = *PM*).
9. Click **Save** to save your changes.

User Notifications

The Administrator can create global notifications in the Notification Rules Management page (see the *Management - Notification Rules (Classic UI)* section on page 201). Users can create, edit or delete personal notifications in the My Profile page (see the *Dashboard - My Profile (Classic UI)* section on page 84).

Searching for User Notifications

Use the Search window in the **User Notifications** tab to perform a search for user Notifications (FIG. 314).

FIG. 314 User Notifications tab - Search Window

User Roles

Assigning a User to a Role

1. In the Users window of the User Management page (FIG. 298 on page 181), select a user from the list.
2. Open the **Roles** tab.
3. Select a Role to add to the selected user from this drop-down menu. The default User Roles are:
   - Admin
   - Guest
   - Client
   - Scheduler (this role is used by the Scheduling Interface, and does not apply to Users)
   - Transporter (this role is used by the RMS Enterprise Transporter Interface, and does not apply to Users)

   NOTE: *Roles are defined in the Role Management page. See the Management - Roles (Classic UI) section on page 192 for details.*

4. Click **Add Role to User**. The selected Role is added to the *User Roles* table (see FIG. 303 on page 186).
5. Click **Save** to save your changes.

Removing a Role From a User

NOTE: *Each user account must have one or more user Roles. A user will not be saved if no roles are assigned to it.*

1. In the *Users* window of the *User Management* page (FIG. 298 on page 181), select a user from the list.
2. Open the **Roles** tab.
3. Selected a Role in the *User Roles* table (see FIG. 303 on page 186).
4. Click **Remove**.
5. Click **Save** to save your changes.

Management - Roles (Classic UI)

Overview

Click inside the **Management** tab (Classic UI) to access the *Management* menu. The options in this menu allow you to configure Locations/Systems, manage Assets, and manage Users & Notifications, as described in the following sections.

The options in the **User & Notification Management** category of the (Classic UI) *Management* menu allow you to configure *Users* and (user) *Roles* as well as (user) *Notification Rules* (FIG. 315):
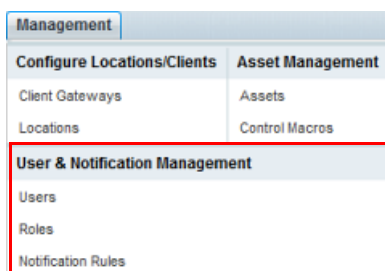
FIG. 315 Management Menu - User & Notification Management

NOTE: *To access the RMS Classic UI described in this section, select "Classic UI" from the RMS Enterprise HTML interface menu bar.*

User Permissions

User Permissions allow you to either restrict or allow users to access specific features. In RMS, user Permissions are inclusive, meaning that all permissions are designed to *grant* a user access to features and resources. Conversely, any user account that does not have user permissions assigned is *denied* access to all secured features and resources.

RMS does not support exclusive permissions or the ability to explicitly deny users access to a particular feature or resource. Restricted access is achieved by not granting user permissions to the feature or resource.

Roles

The User Permissions feature of RMS supports user *Roles*. Roles represent specific permissions granted to each user, and establish which aspects of the RMS system each user has access to, and which functions they are allowed to affect.

Roles represent sets of configured User Permissions, and a listing of which user accounts are members of the Role. Roles are the only method by which permissions can be assigned to users. Permissions cannot be assigned explicitly to individual user accounts. Roles can also be configured to apply permissions to specific Locations. Roles are non-hierarchical and do not support any inheritance model. Users can be assigned to zero or more user Roles.

- Users that belong to multiple Roles are granted the effective access of the cumulative permissions defined in each user Role.
- User accounts assigned to zero user Roles are limited to only resources and features that are unsecured (for example, pages for managing the authenticated user's account profile, contacts, and notifications).
- User accounts assigned to zero user Roles can login to the RMS UI, but they will only have access to the *My Profile* page, accessible via the **Dashboard** menu (see the *Dashboard - My Profile (Classic UI)* section on page 84).

To open the *Roles* page, select **Roles** under *User & Notification Management* in the Management menu (FIG. 316).
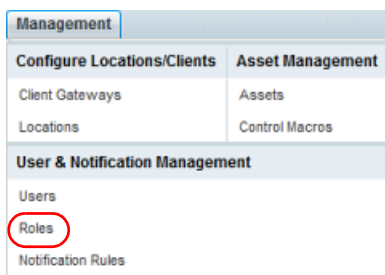
FIG. 316 Management > User & Notification Management > Roles

The features on this page are organized into several windows (FIG. 317):

- Use the **Roles** window to view and manage Roles - see the *Role Management Page - Roles Window* section on page 195.
- Use the **Role Properties** window to view and manage properties for the selected Role - see the *Role Management Page - Role Properties Window* section on page 195.

FIG. 317 Role Management page (Settings tab)

NOTE: *Access to the Role Management page is restricted to the default Administrator user account and/or to any user that is a member of a permissions role that includes the Global System Permission: Manager Users.*

Default Roles

Three default Roles are pre-configured in RMS: *Admin*, *Client*, *Guest, Scheduler* and *Transporter* . These default Roles can be renamed, but not deleted.

Default Administrators Role

RMS provides a default Administrator user account (see the *Default Administrator User Account* on page 179), and a default Administrator Role. The default administrator Role provides full access to the RMS system.

NOTE: *The default Administrator user account is a member of the default Administrator's Role and cannot be removed from the Role. The Administrator user account and Role is provided to ensure that a user account exists that has full access to the RMS system.*

The following restrictions apply to the default Administrators Role:
- Cannot change permissions settings (all access)
- Cannot remove the Administrator user account from the Role

Default Client Role

RMS provides a default Client user account (see the *Default Client User Account* on page 179), and a default Client Role. The default Client user account is a member of the default Client Role and cannot be removed from the Role.

The Default Client Role permissions are limited to *Manage Clients and Locations*.

Default Guest Role

RMS maintains a default Guest user account (see the *Default Anonymous / Guest User Account* on page 179), and a default Guest Role. The default Guest user account is a member of the default Guest Role and cannot be removed from the Role.

Note that the permissions settings for the default Guest Role can be changed if desired. See the *Role Properties Window - Settings Tab* section on page 195 for details.

Default Scheduler Role

The *Scheduler* role is used exclusively by the RMS Enterprise Scheduling Interface, and does not apply to Users. The *Scheduler* role has Global System Permissions to manage locations and clients (NetLinx systems).

The permissions settings for this role cannot be edited.

Default Transporter Role

The *Transporter* role is used exclusively by the RMS Transporter Interface, and does not apply to Users. The *Transporter* role has Location Level Permissions for Assets (All Groups).

The permissions settings for this role cannot be edited.

User Permissions in Sessions

Users are granted permissions upon user authentication, and their effective permissions are valid throughout the user's session.

- Permission changes and deletions may not be effective during a user's login session.
- Users must logout and re-login or close and restart a new browser session to obtain all updated permissions changes.

User Permissions and Report Access

Users must have certain permissions to access the various System Report types, as indicated in the table below. Only users with the permissions listed below will have access to the various report types.

See the *Reports (HTML UI)* section on page 45 for details on Report Management.

User Permissions and Report Access		
User Permissions	**Report Types**	
Manage Clients and Locations	Energy Management Reports • System-Wide Energy Usage • Location Energy Usage	Location and Client Management Reports • Location Inventory • Client Gateway Inventory
	Scheduling Events Reports • Location Web Address for QR Code Readers	
Manage Users	Administrative Reports • User Accounts • User Assigned Roles • User Audit Trail (By User) • User Audit Trail (By Date)	
View Assets Manage Assets	Service Request Reports • Service Requests • Service Request Summary	Energy Management Reports • Asset Energy Usage (by Location) • Asset Energy Usage (by Asset Type)
	Status Reports • Battery Status (by Location) • Battery Status (by Level) • Source Usage • Lamp and Display Usage • Transport Runtime • Current Temperature • Asset Parameter Status	Asset Management Reports • Asset Inventory • AMX Asset Inventory • Lamp and Display Usage History • Source Usage History • Temperature History • Asset Parameter Summary History • Asset Parameter Detailed Transaction History • Asset Tripped/Restored History (Internal Log)
	Asset Tracking Reports • RFID Detected Asset Location • Asset Relocation History (By Asset) • Asset Relocation History (By Location)	Quality of Service Reports • Location Quality of Service • Control System Quality of Service • Asset Quality of Service • Location (System) Power • Asset Power
	Scheduling Events Reports • Location Usage by Organizer • Service Request by Organizer • Source Usage by Organizer	

Role Management Page - Roles Window

Use the **Roles** window to view and manage permission Roles.

Initially, the *Roles* window (FIG. 318) indicates only the default *Admin*, *Client*, *Guest*, *Scheduler* and *Transporter* Roles, until more additional Roles are defined.
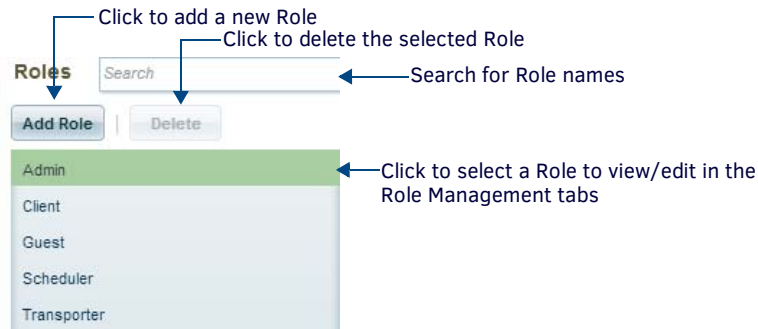
FIG. 318 Role Management page - Roles window

The options in the *Roles* window are described below:

Role Management Page - Roles Window Options	
Search	Use this search field to perform a search for Role names.
Add Role	Click to clear the fields in the Role Properties window, in which you can define a new Role. See the *Creating a New Role* section on page 200 for details.
Delete	Click to delete the selected Role. See the *Deleting a Role* section on page 200 for details. *Note: The default Roles (Admin, Client, Guest, Scheduler and Transport) cannot be deleted.*
Roles View	The Roles view shows all current Roles. The *Admin, Client* and *Guest* entries represent the three default Roles.

Role Management Page - Role Properties Window

Use the *Role Properties* window (in the *Role Management* page) to view and manage detailed properties for each individual Role. This window is separated into three tabs, described in the following sections.

Role Properties Window - Settings Tab

The options in the **Settings** tab of the *Role Properties* window allow you to define, edit and view basic information for a selected Role. Use this tab to select Global as well as Location-level permissions to include in a Role (FIG. 319).

FIG. 319 Role Properties Window - Settings tab

The options in the **Settings** tab are described below:

Role Properties Window - Settings Tab Options	
Role Name	Enter a name for the new Role.
Description	Enter a description of the new Role.
Global System Permissions	
Global System Permissions are permissions that are implemented system-wide, as opposed to Location-specific (see below). Global System Permissions include a checkbox selector for each *Permissions* item. See the *Global System Permissions* section on page 196 for descriptions of each of these permissions.	
Permissions	This column provides specific permissions that can be included in or excluded from the selected Role, at a global level.
Description	This column provides descriptions of each listed permission.
Manage	When checked, the selected Role will include full management access to the associated permission, at a global level.
Location Level Permissions for Assets	
Location Level Permissions for Assets are asset-related permissions that are implemented only for one or more specific Locations. Location-Level Permissions include a checkbox selector for each *Permissions* item. See the *Location Level Permissions* section on page 197 for details.	
Permissions	This column provides specific Asset permissions that can be included in or excluded from the selected Role, at one or more specific Locations.
Description	This column provides descriptions of each listed Asset permission.
View	When checked, the selected Role will include view-only access to the associated Asset permission, at one or more specific Locations.
Manage	When checked, the selected Role will include full management access to the associated Asset permission, at one or more specific Locations. Use the options in the **Location Level Permissions** tab to specify Locations for Location-level permissions (see below). *Note: If the Manage permission option is checked, the View option will automatically be selected, since Manage is a higher level of permission that requires View permissions. If both the Manage and View permissions are selected, and View is deselected, then the Manage permissions will also be automatically deselected as the user is required to have the View permission if Manage is selected. You can select the View permission without selecting the Manage permission.*
Location Level Permissions for Bookings	
Location Level Permissions for Bookings are scheduling-related permissions that are implemented only for one or more specific Locations. Location-Level Permissions include a checkbox selector for each *Permissions* item. See the *Location Level Permissions* section on page 197 for details.	
Permissions	This column provides specific Bookings permissions that can be included in or excluded from the selected Role, at one or more specific Locations.
Description	This column provides descriptions of each listed Bookings permission.
View	Allows the user to view booking schedule and limited meeting details (meeting name, date and time) at one or more specific Locations (see FIG. 322 on page 198).
View Booking Details	Allows the user to view booking schedule and *all* meeting details (including meeting name, date, time, organizer, attendees and description) at one or more specific Locations (see FIG. 322 on page 198).
Manage	This permission is not currently implemented, and if selected will behave the same as "*View Booking Details*".

Global System Permissions

RMS includes a set of *Global System Permissions* that grant system-wide access to certain features and functions in the RMS application. The Global System Permissions options presented in the **Settings** tab of the *Role Properties* window (see FIG. 319 on page 195) are described below:

Global System Permissions	
Permission Name	**Permission Granted to Authenticated User**
Manage Clients & Locations	• Access to view, create, modify, and delete Locations. • Access to view, create and modify Location Metadata Values. • Access to view, modify, and delete Clients (NetLinx Systems).
Manage Configuration	• Access to view and modify all system and application configuration settings. • Access to view, create, modify, and delete Location Metadata Definitions. • Access to view, create, modify, and delete Asset Metadata Definitions. • Access to view, create, modify, and delete Manufacturer, Model, and Device Definitions.
Manage Control Macros	• Access to view, create, modify, delete, and execute Control Macros. • Access to view, create, modify, and delete Control Macro Schedules.
Manage Users	• Access to view, create, modify, and delete user accounts. • Access to view, create, modify, and delete user Roles, including the ability to assign user accounts to user Roles. • Access to view, create, modify, and delete Notification Rules.
Reporting	Access to view administrative reports permission to run and export administrative reports. *Note: Administrative reports include all reports that are not based on Location.*

Location Level Permissions

Location Level Permissions grant Location-specific access to specific features and functions. Unlike Global System Permissions that grant full administrative access, Location-level permissions segment the permissions attributes into two distinct permissions types: **View** and **Manage**:

- **View** permissions grant users the ability to view resources and features in the assigned scope of locations, but not to execute, create, edit, modify, or delete.
- **Manage** permissions grant users full access to view, create, modify, and delete resources and features in the assigned scope of locations.

  Note that the Manage permission supersedes View permissions: any Role that includes Manage permissions will have full View rights as well.

RMS uses Location-level permissions for *Assets*, and for *Bookings* (scheduling information).

Location-Level Permissions for Assets

FIG. 320 Role Properties Window (Settings tab) - Location-Level Permissions for Assets

The Location-Level Permissions for Assets options are described in the following table:

Location Level Permissions for Assets	
Permission Granted to Authenticated User	
View	**Manage**
• View Location properties	• View Location properties
• View Location metadata	• View Location metadata
• Launch Location custom hyperlinks	• Launch Location custom hyperlinks
• View Asset listing	• View asset listing
• View Asset parameters	• Modify Assets
• View Asset parameter thresholds	• Add (unmanaged) Assets
• View Location tripped asset parameters in Hotlist.	• Delete (unmanaged) Assets
	• View Asset parameters
	• Edit Asset parameters
	• View Asset parameter thresholds
	• Add Asset parameter thresholds
	• Modify Asset parameter thresholds
	• Delete Asset parameter thresholds
	• Reset tripped Asset parameters
	• View Location tripped Asset parameters in Hotlist.
	• Reset Location tripped Asset parameters in Hotlist.

- Location-level permissions can be attached to both (Location) Groups and Locations (see *Management - Locations (Classic UI)* on page 103).
- Location-level permissions are inherited if no permissions are attached to a particular group or Location.

Location-Level Permissions for Bookings

The *Location-Level Permissions for Bookings* options control how scheduling information is presented on the User's mobile device when scanning a QR Code for Mobile Scheduling.

FIG. 321 Role Properties Window (Settings tab) - Location-Level Permissions for Bookings

The Location-Level Permissions for Bookings options are described below:

- **View**: This permission allows the user to view booking schedule and limited meeting details (meeting name, date and time) at one or more specific Locations (see "View" in FIG. 322)

  The *Guest* account has View privileges as a default. Therefore, if the Guest account is enabled, the user can see the booking schedule and *limited* meeting details without logging in.

  User's with *View* privileges can press a meeting entry (on their mobile device) to view *limited* meeting details.

- **View Booking Details**: This permission allows the user to view booking schedule and all meeting details (including meeting name, date, time, organizer, attendees and description) at one or more specific Locations (see "View Booking Details" in FIG. 322).

  This permission setting requires the User to login before accessing the detailed bookings view.

  User's with *View Booking Details* privileges can press a meeting entry (on their mobile device) to view *all* meeting details.

Login Screen   Meeting Schedule

View
(Limited Meeting Details)

View Booking Details
(All Meeting Details)
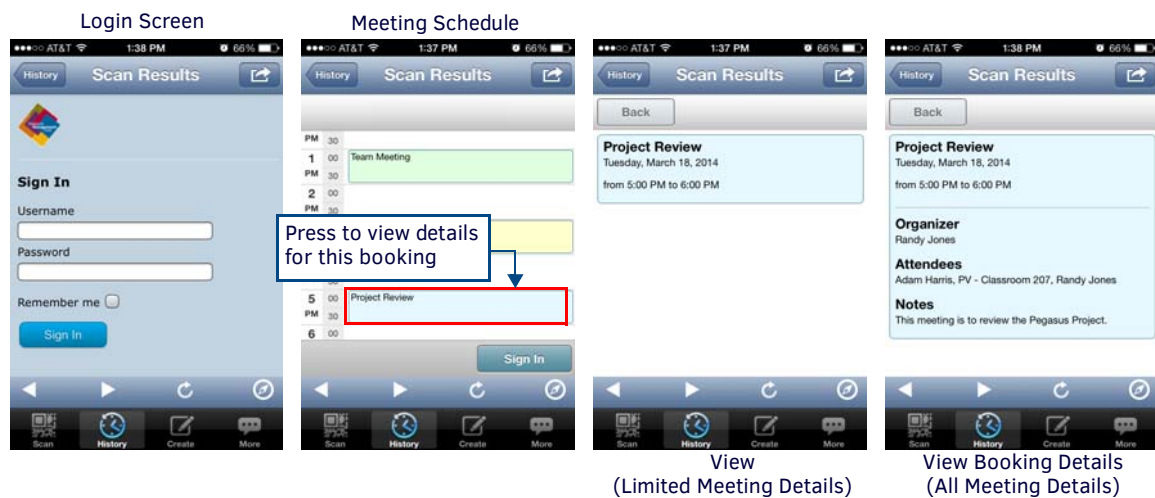
FIG. 322   Example Mobile Device Scheduling Displays

- **Manage**: *Not implemented at this time, currently behaves the same as View Booking Details.*

Remember me

Note that the Mobile Device Scheduling Login Screen features a **Remember me** option (see the Scheduling Login Screen in FIG. 322). This option is de-selected by default.

Remember-me refers to a web site's ability to remember the identity of a user between sessions. When this option is selected, the stored user identity will remain valid for the number of days specified in the *Mobile Scheduling configuration page* (default = 30 days; see the *Mobile Scheduling* section on page 214 for details).

When the specified number of days have passed, the user will be prompted to sign-in again.

Role Properties Window - Location Level Permissions Tab

The **Location Level Permissions** tab of the *Role Properties* window allows you to define and apply Role permissions specifically for selected Locations and/or Location Groups (FIG. 323).
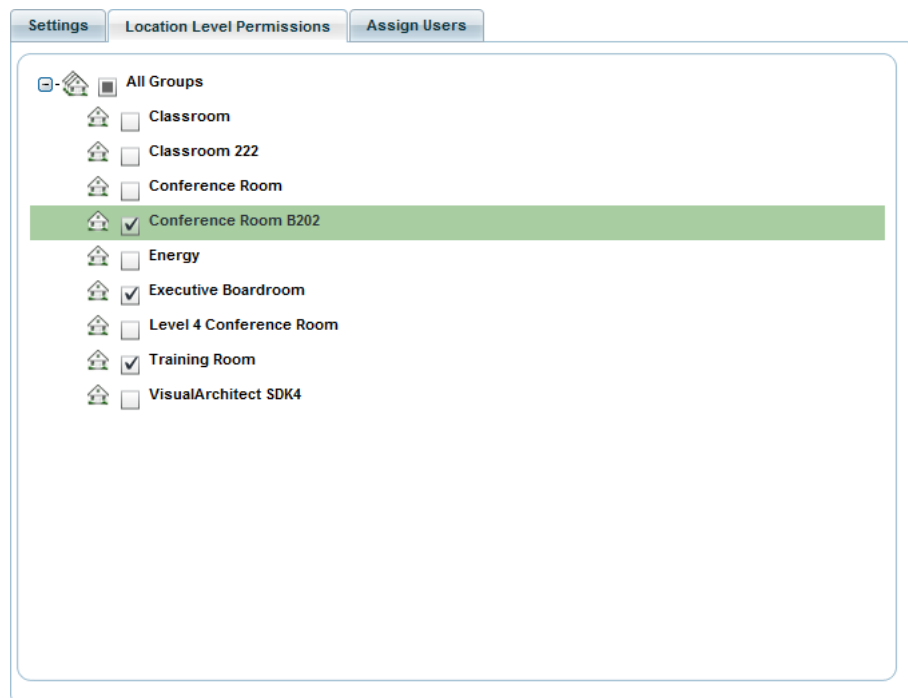
FIG. 323   Role Properties Window - Location Level Permissions tab

NOTE: *Groups and Location Groups are configured in the Location page (FIG. 167 on page 104). See Management - Locations (Classic UI) on page 103 for details.*

The options on this tab are described below:

Role Properties Window - Location Level Permissions Tab Options	
Apply Permissions to All Locations	By default, permissions are applied to all Locations. De-select this checkbox to enable the Groups/Locations window, in which you can selected specific Groups and/or Locations for the selected Role. Default = *Enabled*
Groups/Locations window	All current Location Groups and Groups are displayed in a hierarchical tree structure. The top-level entry is *All Groups*. • Click the plus sign (+) next to the *All Groups* entry to expand the list to show all Groups in the system. • Click the plus sign (+) next to any *Group* entry to expand the list to show all Locations in the Group. • Click the minus sign (-) next to each entry to collapse each Group.

Role Properties Window - Assign Users Tab

The **Assign Users** tab of the *Role Properties* window allows you assign users to the selected Role (FIG. 324).

FIG. 324 Role Properties Window - Assign Users tab

The options on this tab are described below:

Role Properties Window - Assign Users Tab Options	
Available User List	Click the down arrow to select from a drop-down list of all Users in the system.
Add Users	Click to add a selected User to the current Role.
Remove	Click to remove a selected User from the current Role.
Users Table	A listing of all Users assigned to the current Role.

Working With Roles

Searching for Role Names

Use the Search tool in the *Roles* window to search for a specific Role by *Role Name* (see FIG. 318 on page 195).

Creating a New Role

Use the tabs in the *Role Properties* window to define the permissions for a Role, as well as specify Locations to which the Role will be applied, and assign Users to the Role. See the *Role Management Page - Role Properties Window* section on page 195 for descriptions of the options presented in each tab.

1. In the *Roles* window of the *Role Management* page (FIG. 318 on page 195), click the **Add Role** button. This action opens a new set of tabs in the *Role Properties* window (the initial view is the **Settings** tab (FIG. 319 on page 195).
2. In the **Settings** tab, specify the basic properties of the Role:
   a. Enter a *Name* and *Description* for the new role in the text fields at the top of the tab.
   b. Under *Global System Permissions*, check each permission that you want to include in this role (see the *Global System Permissions* section on page 196 for details).
   c. Under *Location Level Permissions*, select **View** and/or **Manage** (see the *Location Level Permissions* section on page 197 for details).
   d. Click **Save**.
3. In the **Location Level Permissions** tab, specify the Locations to which this Role will apply:
   a. Select one or more Locations (click the + icon next to *All Groups* to expand the list).
   b. Click **Save**.
4. In the **Assign Users** tab, select Users to assign to this Role:
   a. Click the down arrow to open the Available Users drop-down list. This is a listing of all Users in the system.
   b. Click **Add User** to add the selected User to the list.
   c. Click **Save**.
5. The new Role is added to the *Roles* window.

Editing a Role

Use the options in the tabs of the *Role Properties* window to edit a selected permission Role:

1. In the *Roles* window (see FIG. 318 on page 195), select a Role to edit.
2. Go through each of the tabs in the Role Properties window to edit settings as desired:
   - See the *Role Properties Window - Settings Tab* section on page 195
   - See the *Role Properties Window - Location Level Permissions Tab* section on page 198
   - See the *Role Properties Window - Assign Users Tab* section on page 199
3. Click **Save**.

Deleting a Role

1. In the Roles window of the Role Management page (FIG. 318 on page 195), select a Role from the list.
2. Click the **Delete** button.

   NOTE: *Note that the Delete option is not available for the default (Administrator, Client and Guest) Roles. These Roles cannot be deleted from the system.*

3. The system will prompt you to verify this action before the Role is deleted, via the *Delete Confirmation* dialog (FIG. 325):
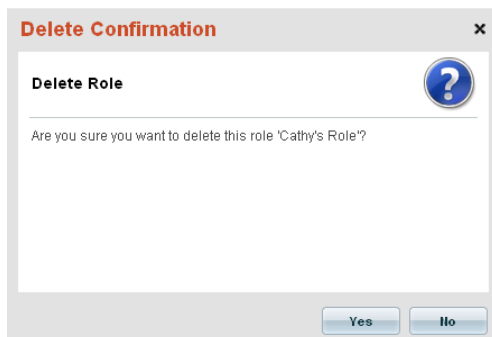
FIG. 325 Delete Confirmation dialog - Role

4. Click **Yes** to proceed.
5. The selected Role is deleted from the Roles list, and from the system.

   NOTE: *A Role can be deleted even if it is associated with a user account. If that user account has no other role assigned to it, the next time that user attempts to login to the UI, they will receive an error message indicating that they cannot login because there is no role assigned.*

Management - Notification Rules (Classic UI)

Overview

Click inside the **Management** tab (Classic UI) to access the *Management* menu. The options in this menu allow you to configure Locations/Systems, manage Assets, and manage Users & Notifications, as described in the following sections.

The options in the **User & Notification Management** category of the (Classic UI) *Management* menu allow you to configure *Users* and (user) *Roles* as well as (user) *Notification Rules* (FIG. 326):
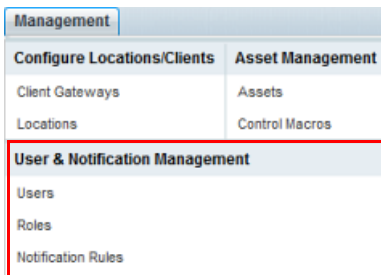
FIG. 326 Management Menu - User & Notification Management

NOTE: *To access the RMS Classic UI described in this section, select "Classic UI" from the RMS Enterprise HTML interface menu bar.*

Notification Rules

RMS Enterprise uses *Notification Rules* to specify how system notification e-mail messages will be handled for each User. Notification Messages represent SMTP e-mail messages sent by RMS to one or more Users to provide notification that a specific system event has occurred. To open the *Notification Rules* page, select **Notification Rules** under *User & Notification Management* in the Management menu (FIG. 327).
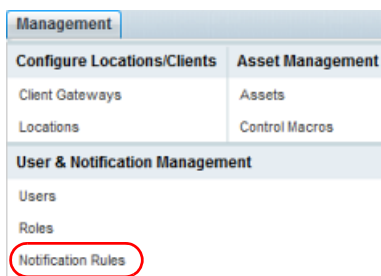
FIG. 327 Management > Configure Locations/Clients > Locations

The *Notification Rules* page provides a listing of all notification rules defined in the RMS system.   From this page, notifications can be Added, Edited, and Deleted.

NOTE: *Many options on this page are permission-dependant (see the Management - Roles (Classic UI) section on page 192 for details).*

The features on this page are organized into two windows (FIG. 328):

- Use the **Notification Rules** window to view and manage Notification Rules - see the *Notification Rules Page - Notification Rules Window* section (below) for details.
- Use the **Properties** window to view and manage properties for the selected Notification Rule - see the *Notification Rules Page - Properties Window* section on page 203 for details.
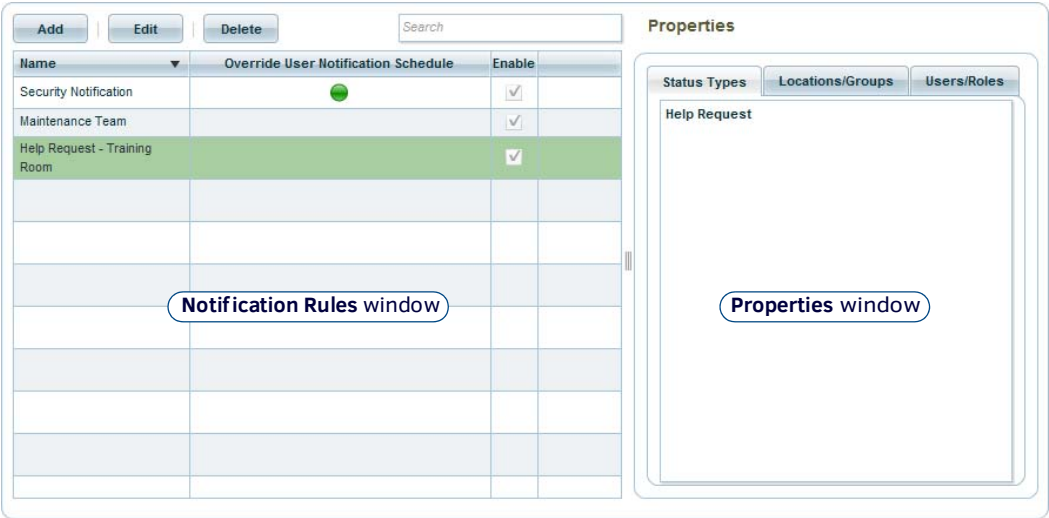
FIG. 328 Notification Rules page

Notification Rules Page - Notification Rules Window

All Notification Rules are listed in the **Notification Rules** window (FIG. 329).
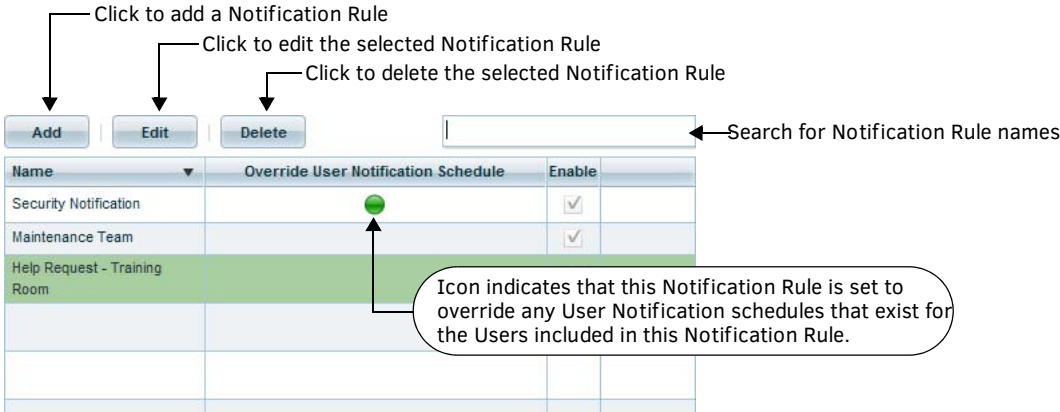
FIG. 329 Notification Rules Page - Notification Rules Window

The options in the *Notification Rules* window are described below:

Notification Rules Page - Notification Rules Window Options	
Search	Use this search field to perform a search for Notification Rule names. See the *Searching for Notification Rule Names* section on page 207 for details.
Add	Click to create a new Notification Rule, via options in the *Edit Notification Rule* dialog. See the *Creating a New Notification Rule* section on page 207 for details.
Edit	Click to edit the selected Notification Rule, in the *Edit Notification Rule* dialog. See the *Editing a Notification Rule* section on page 208 for details.
Delete	Click to delete the selected Notification Rule. See the *Deleting a Notification Rule* section on page 208 for details.
Notification Rules View	The table in this window lists all current Notification Rules.

Notification Rules Page - Properties Window

The *Properties* window provides details on the Notification Rule selected in the *Notification Rules* window. This window is separated into three tabs, as described below.

Properties Window - Status Types tab

The options in the **Status Types** tab of the *Properties* window allow you to view the Status Types included in the selected Notification Rule (FIG. 330):
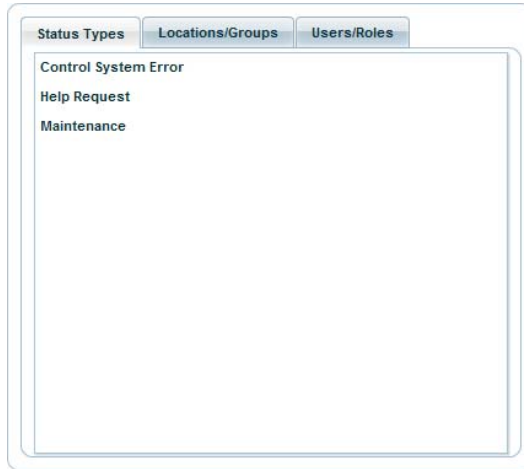
FIG. 330 Notification Rules Page - Properties Window (Status Types tab)

Status Types are selected for each Notification Rule in the *Edit Notification Rule* dialog - **Status Types** tab (see page 205 for details).

Properties Window - Locations/Groups tab

The options in the **Location/Groups** tab of the *Properties* window allow you to view the Location Groups and Locations included in the selected Notification Rule (FIG. 331):
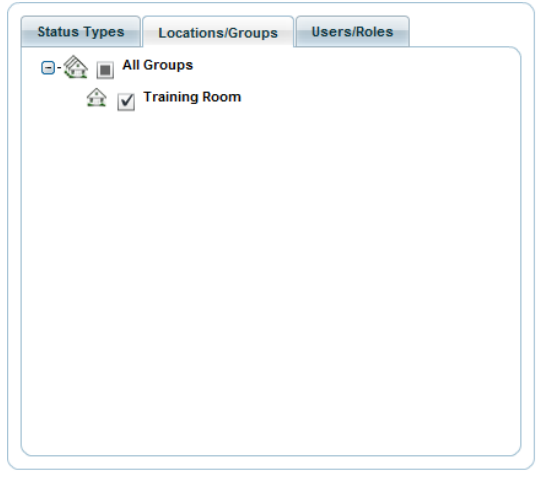
FIG. 331 Notification Rules Page - Properties Window (Locations/Groups tab)

Locations and Location Groups are selected for each Notification Rule in the *Edit Notification Rule* dialog - **Locations** tab (see page 206 for details).

Properties Window - Users/Roles tab

The options in the **Users/Roles** tab of the *Properties* window allow you to view the Users and Roles included in the selected Notification Rule (FIG. 332):
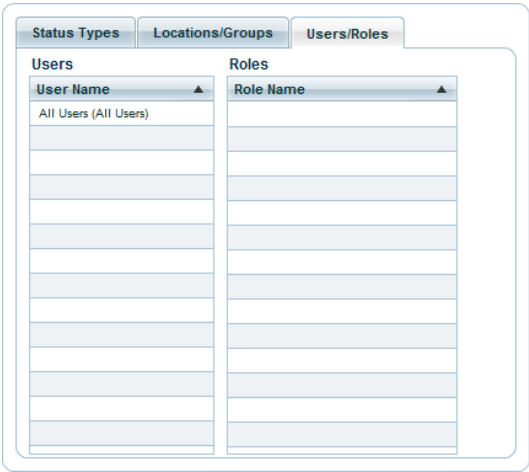
FIG. 332 Notification Rules Page - Properties Window (Users/Roles tab)

Users and Roles are selected for each Notification Rule in the *Edit Notification Rule* dialog - **Recipients** tab (see page 206 for details).

Edit Notification Rule dialog

The *Edit Notification Rule* dialog is invoked via both the **Add** and **Edit** buttons in the Notification Rules window of the Notification Rules page. This dialog consists of four tabs: *Rule*, *Status Types*, *Locations*, and *Recipients*.

- When invoked via the **Add** button, the dialog allows you to define a new Notification Rule. See the *Creating a New Notification Rule* section on page 207 for details.
- When invoked via the **Edit** button, the dialog allows you to edit the properties of the selected Notification Rule. See the *Editing a Notification Rule* section on page 208 for details.

Edit Notification Rule Dialog - Rule Tab

The **Rule** tab of the *Edit Notification Rule* dialog is shown in FIG. 333:
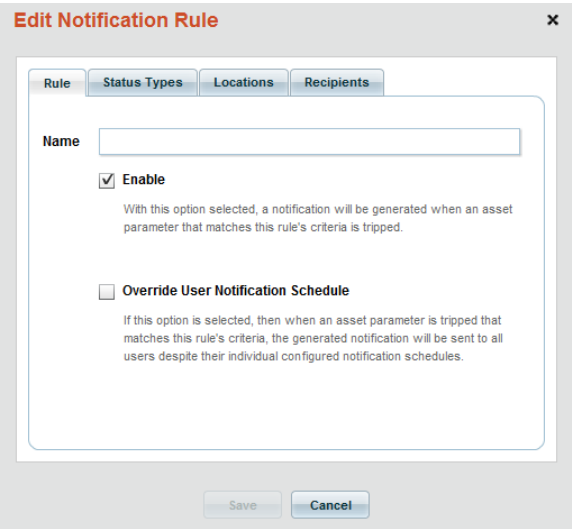
FIG. 333 Edit Notification Rule Dialog - Rule Tab

Edit Notification Rule Dialog - Rule Tab Options	
Name	This field contains the name of the selected Notification Rule. If this dialog was accessed via the **Add** button, the field is blank; if accessed via the **Edit** button, it indicates the name of the selected Rule.
Enable	With this option selected, a notification will be generated when an asset parameter that matches this rule's criteria is tripped. Default = *Enabled*.

Edit Notification Rule Dialog - Rule Tab Options (Cont.)	
Override User Notification Schedule	If this option is selected, then when an asset parameter is tripped that matches this rule's criteria, the generated notification will be sent to all users despite their individual configured notification schedules. Note that Notification Rules that are configured to use this option are indicated by a green icon in the *Override User Notification Schedule* column of the *Notification Rules* window (see FIG. 329 on page 202). Default = *Disabled*.
Save	Click to save all changes made in this dialog. *Note: Clicking Save will save changes made on all tabs - if any required data is missing, the user is presented with the tab that is missing information, with a prompt (in red) at the top of that tab indicating what required info is missing.*

Edit Notification Rule Dialog - Status Types Tab

The **Status Types** tab of the *Edit Notification Rule* dialog is shown in FIG. 334:
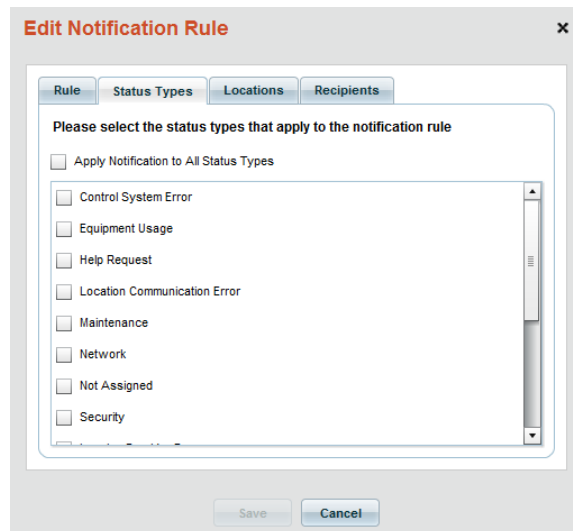
FIG. 334 Edit Notification Rule Dialog - Status Types Tab

Edit Notification Rule Dialog - Status Types Tab Options	
Apply Notification to All Status Types	Click to add all Status Types to this Notification Rule. Default = *disabled*.
Status Types	Click to select specific Status Types to include in this Rule. • Note that these options are disabled if *Apply Notification to All Status Types* is selected. • Status Types are managed via options in the *Status Types* page (see the *Status Types* section on page 251 for details).
Save	Click to save all changes made in this dialog. *Note: Clicking Save will save changes made on all tabs - if any required data is missing, the user is presented with the tab that is missing information, with a prompt (in red) at the top of that tab indicating what required info is missing.*

Edit Notification Rule Dialog - Locations Tab

The **Locations** tab of the *Edit Notification Rule* dialog is shown in FIG. 335:
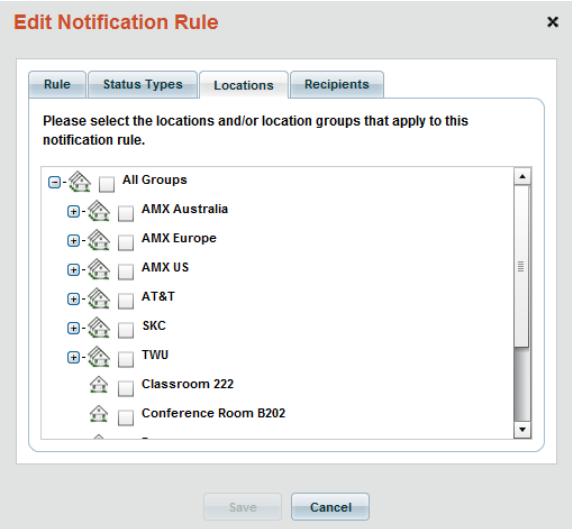
FIG. 335 Edit Notification Rule Dialog - Locations Tab

Edit Notification Rule Dialog - Locations Tab Options	
Location Groups/Locations	All Location Groups and Locations are displayed in a hierarchical tree structure. The top-level entry is *All Groups.* Select **All Groups** to include all Locations and Location Groups in this Notification Rule. • Click the plus sign (+) next to the *All Groups* entry to expand the list to show all Groups in the system. • Click the minus sign (-) next to each entry to collapse each Group. Select individual Location Groups and/or Locations to include specific Locations in this Rule. All Locations and Location Groups are configured and managed via options in the *Location* page (see the *Management - Locations (Classic UI)* on page 103).
Save	Click to save all changes made in this dialog. *Note: Clicking "Save" will save changes made on all tabs - if any required data is missing, the user is presented with the tab that is missing information, with a prompt (in red) at the top of that tab indicating what required info is missing.*

Edit Notification Rule Dialog - Recipients Tab

The **Recipients** tab of the *Edit Notification Rule* dialog contains two tabs: **Users** and **Roles** (FIG. 336).
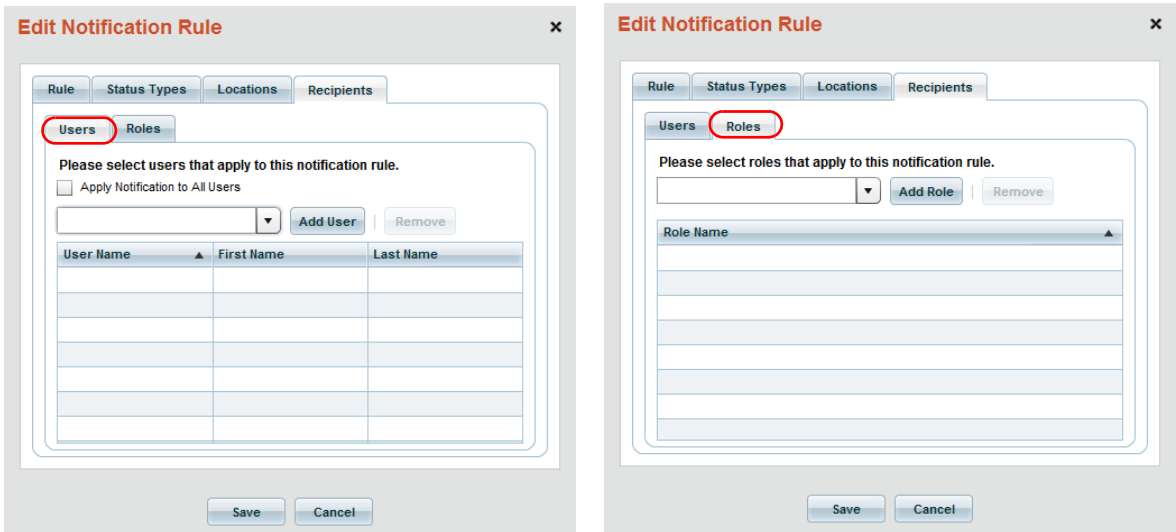

FIG. 336 Edit Notification Rule Dialog - Recipients Tab

Edit Notification Rule Dialog - Recipients Tab Options	
Users tab	
Apply Notification To All Users	Select this option to select all Users
Users drop-down menu	Click the down-arrow to open a drop-down menu of all Users in the system. User accounts and user Properties are managed via options in the *User Management* page (see the *Management - Users (Classic UI)* section on page 177 for details).
Add User	With a User selected in the *Users drop-down menu*, click to add the selected User to this Notification Rule.
Remove	With a User selected in the *Users list*, click to remove the selected User from this Notification Rule.
Users List	This is a listing of Users currently included in this Notification Rule (*User Name*, *First Name*, *Last Name*).
Roles tab	
Roles drop-down menu	Click the down-arrow to open a drop-down menu of all Roles in the system. Roles are managed via options in the *Role Management* page (see the *Management - Roles (Classic UI)* section on page 192 for details).
Add Role	With a Role selected in the *Roles drop-down menu*, click to add the selected Role to this Notification Rule.
Remove	With a Role selected in the *Roles list*, click to remove the selected Role from this Notification Rule.
Roles List	Role Name.
Save	Click to save all changes made in this dialog. *Note: Clicking Save will save changes made on all tabs - if any required data is missing, the user is presented with the tab that is missing information, with a prompt (in red) at the top of that tab indicating what required info is missing.*

Working With Notification Rules

Searching for Notification Rule Names

Use the Search tool in the *Roles* window to search for a specific Notification Rule by name (FIG. 337).
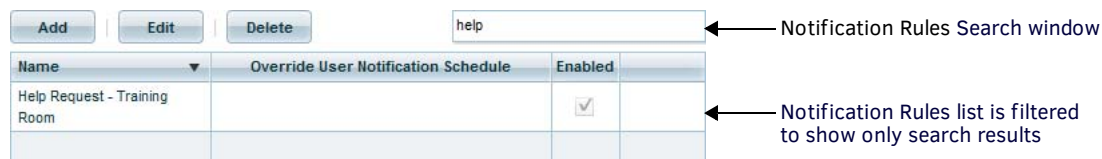
FIG. 337 Notification Rules window - Search window

Creating a New Notification Rule

Use the tabs in the *Edit Notification Rule* dialog to define new Notification Rules, as well as specify Locations to which the Role will be applied, and assign Users to the Role. See the *Edit Notification Rule dialog* section on page 204 for descriptions of the options presented in each tab.

1. In the *Notification Rules* window, click the **Add** button. This action opens the *Edit Notification Rule* dialog (the initial view is the **Rule** tab).
2. In the **Rule** tab, specify the basic properties of the Notification Rule:
   a. Enter a name for the new Rule in the *Name* field.
   b. Select the *Override User Notification Schedule* option if desired (default = disabled). When selected, when an asset parameter is tripped that matches this Rule's criteria, the generated notification will be sent to all users despite their individual configured notification schedules.
   c. Click **Save**.
3. In the **Status Types** tab, select the Status Types that apply to this Notification Rule.
   a. Use the *Apply Notification To All Status Types* option to select all.
   b. Click **Save**.
4. In the **Locations** tab, select the Locations and/or Location Groups that apply to this Notification Rule.
   a. Click the '+' icon to expand the top-level All Groups directory, use the checkboxes to select one or more Locations and/or Location Groups to include in this Rule.
   b. Use the *All Status Groups* option to select all.
   c. Click **Save**.
5. In the **Recipients** tab, select the Users and Roles that apply to this Notification Rule.
   a. In the *Users* tab:
   ● Click the **Apply Notification To All Users** option to add all Users to this Notification Rule (default = disabled).
   ● Otherwise, click the down arrow to select from the drop-down menu of Users (FIG. 338).
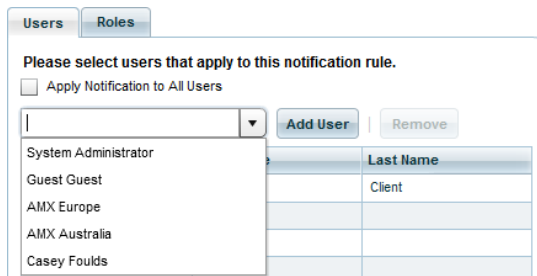
FIG. 338 Selecting Users (Edit Notification Rule dialog - Recipients tab)

      b. Click **Add User** to add the selected User to the *Users* list.

      c. In the *Roles* tab, click the down arrow to select from the drop-down menu of User Roles (FIG. 339).
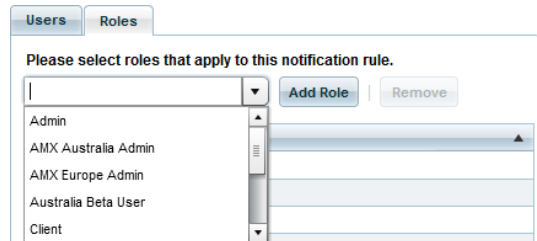
FIG. 339 Selecting Roles (Edit Notification Rule dialog - Recipients tab)

      d. Click **Add Role** to add the selected Role to the *Roles* list.

      e. Click **Save**.

6. The new Rule is added to the *Notification Rules* window.

Editing a Notification Rule

Use the options in the tabs of the *Edit Notification Rule* dialog to edit a selected permission Notification Role:

1. In the *Notification Rules* window (see FIG. 329 on page 202), select a Rule.

2. Click **Edit** to open the *Edit Notification Rule* dialog (see FIG. 333 on page 204).

3. Go through each of the tabs in the *Edit Notification Rule* dialog to edit the selected Rule as desired:
   - See the *Edit Notification Rule Dialog - Rule Tab* section on page 204
   - See the *Edit Notification Rule Dialog - Status Types Tab* section on page 205
   - See the *Edit Notification Rule Dialog - Locations Tab* section on page 206
   - See the *Edit Notification Rule Dialog - Recipients Tab* section on page 206

4. Click **Save**.

Deleting a Notification Rule

1. Select a Rule in the *Notification Rules* window (FIG. 329 on page 202).

2. Click **Delete**.

3. The program will prompt you to verify this action (FIG. 340):
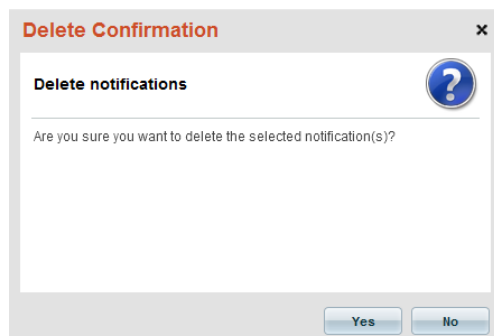
FIG. 340 Delete Confirmation dialog - Notifications

4. Click **Yes** to proceed.

5. The selected Notification Rule is deleted.

System Configuration (Classic UI)

Overview

Click inside the **Configuration** tab (Classic UI) to access the *Configuration* menu. The options in this menu allow you to configure many System-level settings, as described in the following sections. The options in the **System Configuration** category of the *Configuration* menu allow you to specify various basic system settings (FIG. 341):

FIG. 341 Configuration Menu - System Configuration options

NOTE: *To access the RMS Classic UI described in this section, select "Classic UI" from the RMS Enterprise HTML interface menu bar.*

NOTE: *Unlike the Management pages, the Settings pages do not utilize an "Apply" button. Changes made on the Settings pages are saved when you navigate away from the page on which the changes were made.*

Web Application Settings

Select **Web Application** under *System Configuration* in the Configuration menu to open the *Web Application Settings* page (FIG. 342):

FIG. 342 Web Application Settings page

Use the options on this page to customize the RMS Web Interface. The options on the Web Application page are global settings that apply to all RMS UIs.

Web Application Page Options	
Application Title	Edit the title displayed along the top of the application window via this text field. • Default = "*Resource Management Suite*" • Click *Restore to Default* to restore the default Application Title. • See the *Changing the Application Title* section on page 210 for details.
Browser Title	Edit the title displayed in the browser window via this text field. • Default = "*RMS*" • Click *Restore to Default* to restore the default Browser Title. • See the *Changing the Browser Title* section on page 210 for details.
System Maintenance Mode	Enable this setting to place all Assets and Locations in *Maintenance Mode*. • Issues will not be displayed on the Hotlist and external notifications will be suspended for all Assets and Locations. • See the *System Maintenance Mode* section on page 210 for details.
Logo Image	Preview and change the logo image displayed in the top left of the application window. Click *Select Image* to select an image to upload, in the *Select file to upload to* dialog. • Supported image types: JPG, JPEG, GIF and PNG. • Max display size = 85 x 85 (pixels). • Click *Restore to Default* to restore the default RMS logo image. • See the *Changing the Logo Image* section on page 211 for details.

Changing the Application Title

1. Select **Web Application** under *System Configuration* in the Configuration menu to open the *Web Application Settings* page (FIG. 342 on page 209).
2. Under **Application Title**, edit the name of the application in the text field:
3. Click the **Back to Dashboard** button to refresh the application window to display the new Application Title (FIG. 343):
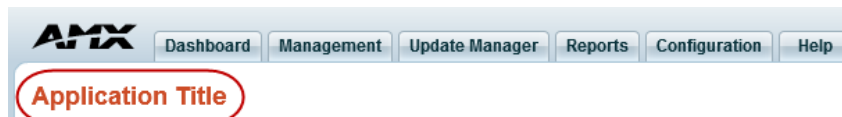
FIG. 343 Application Title

Click **Restore to Default** to remove changes and restore the default Application Title (default = *Resource Management Suite*.

Changing the Browser Title

1. Select **Web Application** (under *System Configuration*) to open the *Web Application Settings* page (FIG. 342 on page 209).
2. Under **Browser Title**, edit the browser title in the text field.
3. Click the **Back to Dashboard** button to refresh the application window to display the new Browser Title - displayed in the browser tab containing the RMS application window (FIG. 344):
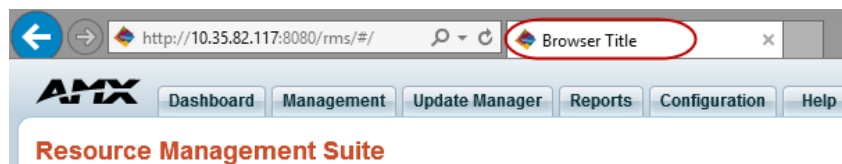
FIG. 344 Browser Title

Click **Restore to Default** to remove changes and restore the default Browser Title (default = *RMS*).

System Maintenance Mode

Click the **Enable System Maintenance Mode** checkbox to enable system maintenance mode (FIG. 345):
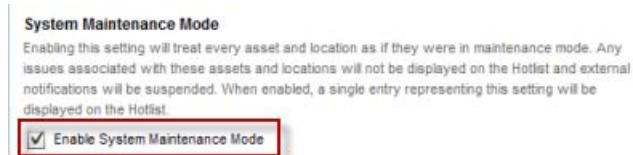
FIG. 345 System Maintenance Mode checkbox

- While in System Maintenance Mode, all issues associated with Assets and Locations will not be displayed on the Hotlist, and external notifications will be suspended.
- When enabled, a single entry representing this setting will be displayed on the Hotlist (FIG. 346):

Status	Occurrence	Classification	Location	Asset	Summary
✗	10:27 AM CST				The system has been placed into maintenance mode. Any issues associated with assets or locations will not be displayed on the Hotlist and external notifications will be suspended.

FIG. 346 Hotlist - System Maintenance Mode enabled

To disable System Maintenance Mode, de-select the *Enable System Maintenance Mode* checkbox n the Web Application page.

Changing the Logo Image

1. Select **Web Application** (under *System Configuration*) to open the *Web Application Settings* page (FIG. 342 on page 209).
2. Under **Logo Image**, click **Select Image**. This action invokes the *Select File To Upload* dialog.
3. Locate and select the image file to use as the new logo image for the RMS application and click **Open**.
   - Supported image types: JPG, JPEG, GIF and PNG.
   - Max display size = 85 x 85 (pixels).
   - Click *Restore to Default* to restore the default RMS logo image.

   NOTE: *RMS will scale the image to the proper resolution for the image category. For best results, prepare the image to be 85 x 85 pixels before uploading, to avoid scaling or stretching of the image when it is displayed in RMS.*

4. A preview of the selected image is displayed on the page(FIG. 347):

FIG. 347 Logo Image preview window

5. Click the **Back to Dashboard** button to refresh the application window to display the custom Logo (FIG. 348):
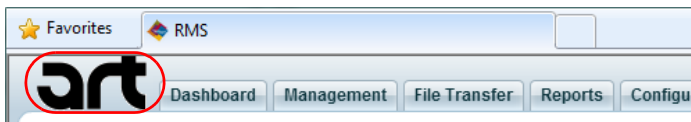
FIG. 348 Logo Image

Click **Restore to Default** to remove changes and restore the default logo image (default = *AMX Logo*, see FIG. 344 on page 210).

Application Time Zone

Select **Application Time Zone** under *System Configuration* in the Configuration menu to open the *Application Time Zone* page (FIG. 349):

FIG. 349 Application Time Zone page

Use the options on this page to specify the default application time zone settings:

Application Time Zone Page Options

Default Application Time Zone:	These settings establish the default region and time zone setting from the drop-down menu. • Default Region and Time Zone: By default, the region and time zone are set according to the settings established for the server upon which RMS is installed. • Default Application Locale: See the *Setting the Default Application Time Zone and Locale (Language)* section on page 212 for details.
Default Application Locale:	This setting establishes the default language localization setting for the RMS UI. By default, the Default Application Locale setting is *English (US)*.

NOTE: *The options on this page represent global settings that apply to all RMS UIs.*

Setting the Default Application Time Zone and Locale (Language)

Application Time Zone represents time calculated from UTC to the Time Zone specified as the default *System Time Zone*. This calculated time includes daylight savings time shifts in the application time zone.

- System Time Zone is used to render time values to the UI, reports, or user communications.
- All RMS data is stored in UTC time.
- Default = The time zone established for the server upon which RMS is installed.

To change the default application time zone:

1. Select **Application Time Zone** (under *System Configuration*) to open the *Application Time Zone* page (FIG. 349 on page 211).

2. Under **Default System Timezone**, select the desired application default time zone from the drop-down menus (FIG. 350):

FIG. 350 Default System Timezone drop-down menu

- The left drop-down menu allows you to select a region.
- The right drop-down menu allows you to select a time zone. The time zone options presented are based on the region selection.

3. Under **Default Application Locale**, select the desired application default language setting from the drop-down menus (FIG. 350):

FIG. 351 Default Application Locale drop-down menu

Security Policy

Select **Security Policy** under *System Configuration* in the Configuration menu to open the *Security Policy* page (FIG. 352):

FIG. 352 Security Policy page

The RMS system can provide anonymous user access to the RMS UI. Use the options on this page to enable/disable security features, and specify how to manage system login credentials.

Security Policy Page Options	
Enable Guest Account (Anonymous Access):	The Guest account provides anonymous access (no login credentials required to login). By default, this option is disabled. Refer to the *Enabling / Disabling the "Guest" Account* section on page 213 for details. *Note: The Guest account is only available for installed RMS Servers; it cannot be enabled for AMX Cloud hosted services.*

Security Policy Page Options (Cont.)	
User Password Policy	
Enable password complexity requirements:	Check this option to require the degree of password complexity specified in the following options. When enabled, the *Number of characters required and Password complexity* options are activated. See the *Configuring the User Password Policy* section on page 213 for details. • Default = *Disabled*
Number of characters required	Click the up/down arrows (or type) to set the minimum number of characters required when creating a new password. This option is enabled only if the *Enable password complexity requirements* option is enabled. See the *Configuring the User Password Policy* section on page 213 for details. • Range = 5-50 • Default = *6*
Password complexity	Move the slider to adjust the level of required password complexity: • *Low* - Any mixture of letters and digits will be accepted • *Medium* - A combination of single case letters and digits are required • *High* - A combination of mixed case letters and digits are required. • Default = *Low* See the *Configuring the User Password Policy* section on page 213 for details.
Disable User after number of invalid login attempts	Click this option to disable the user after the number of invalid login attempts specified in the *Maximum number of login attempts* field (below). • Default = *disabled* See the *Configuring the User Password Policy* section on page 213 for details.
Maximum number of login attempts	Click the up/down arrows (or type) to set the maximum number of invalid login attempts allowed before the user is locked out of the RMS system. This option is enabled only if the *Disable User after number of invalid login attempts* option is enabled (this option is disabled by default). • Range = *1-100* • Default = *3* If this option is disabled, then this rule will not be enforced, and user accounts will not be disabled regardless of the number of invalid attempts. See the *Configuring the User Password Policy* section on page 213 for details.

Enabling / Disabling the "Guest" Account

The Guest account provides anonymous access (no login credentials required to login).

NOTE: *The Guest account is only available for installed RMS Servers; it cannot be enabled for AMX Cloud hosted services.*

Disable the Guest account to disable anonymous access:

1. Select **Security Policy** under *System Configuration* in the Configuration menu to open the *Security Policy* page (FIG. 352 on page 212).
2. Under **Security Policy**, select the **Enable Guest Account (Anonymous Access)** option to enable the "Guest" user account on the RMS Server.
   ● The Guest account provides anonymous access (no login credentials required to login)
   ● By default, the **Enable Guest Account (Anonymous Access)** option is selected.

   NOTE: *The Guest account can also be disabled via options in the User Management page - see the Management - Users (Classic UI) section on page 177 for details.*

Configuring the User Password Policy

NOTE: *Password policy requirements must be set prior to creating a user's password in order to ensure the user password meets complexity requirements.*

1. Select **Security Policy** under *System Configuration* in the Configuration menu to open the *Security Policy* page (FIG. 352 on page 212).
2. Under **User Password Policy**, de-select the **Enable password policy requirements** option to disable password policy requirements for users logging into the RMS Server.
   ● By default, the **Enable password policy requirements** option is selected.
   ● Note that when this option is deselected, all fields in this section of the page are disabled.
3. In the **Number of characters required** field, use the up and down arrows to specify the minimum number of characters that must be present in a password in order for it be accepted by the system.
   ● Range = *5-50*
   ● Default = *6*
4. In the **Password Complexity** field, use the slider to select a level of complexity (FIG. 353).
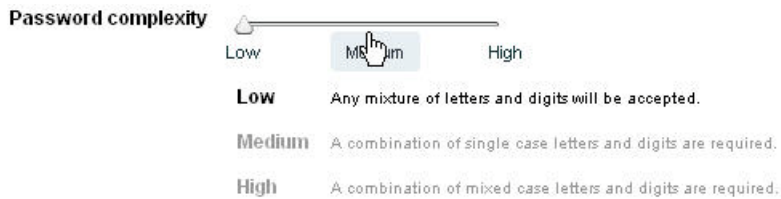
FIG. 353 Password Complexity Slider

- **Low** - any mixture of letters and digits will be accepted (*default setting*).
- **Medium** - a combination of single case letters and digits are required.
- **High** - A combination of mixed case letters and digits are required.

5. De-select the **Disable User after number of invalid login attempts** option to allow users an unlimited number of invalid login attempts.

   By default, the **Disable User after number of invalid login attempts** option is de-selected.

   Note that when this option is selected, the **Maximum number of login attempts** option is enabled. Use the up and down arrows to set the number of login attempts that will be allowed, after which the user will be locked out of the RMS system.

   - Range = *1 - 100*
   - Default = *2*

   NOTE: *If the Password Complexity settings are changed after a user account password has been created, the new Password Complexity settings will not apply until the password is changed while the new Password Complexity policy is in effect.*

Mobile Scheduling

RMS utilizes QR Codes for *Mobile Scheduling*. With Mobile Scheduling, a *RMS-ENT-QR RMS QRS Quick Response Scheduling* Door Sign (**FG3004-51**) is physically mounted outside the meeting room. This Door Sign features a QR Code that will provide the current schedule information for the meeting room when scanned with a mobile device. An example RMS-ENT-QR is shown below (FIG. 354):
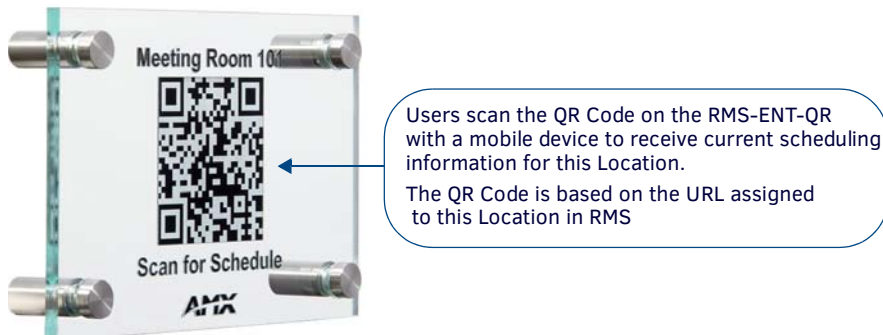
FIG. 354 RMS-ENT-QR RMS QRS Quick Response Scheduling Door Sign

The QR Code (as well as both labels) on the Door Sign are custom-engraved to order by AMX.

The process of enabling Mobile Scheduling in RMS, and specifying the custom engraving for RMS-ENT-QR (*RMS Quick Response Scheduling*) Door Signs is described in the following sections:

Step One - Enable Mobile Scheduling

To use QR Codes and Mobile Scheduling, you must enable the *Mobile Scheduling* feature in RMS:

1. In the RMS Enterprise UI, select the **Configuration** tab.
2. Select **System Configuration > Mobile Scheduling** (FIG. 355):
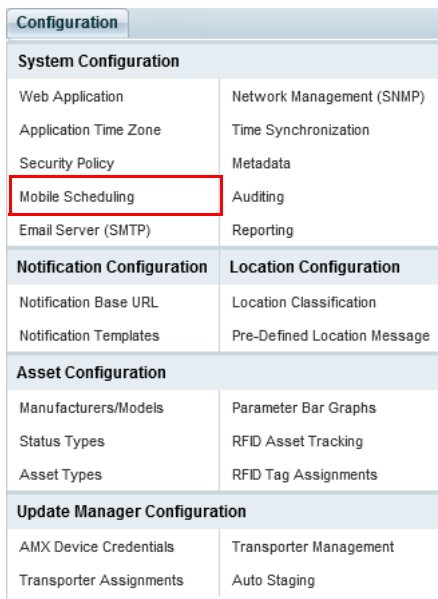
FIG. 355 Configuration Menu (System Scheduling > Mobile Scheduling)

> This opens the *Mobile Scheduling* configuration page (FIG. 356):
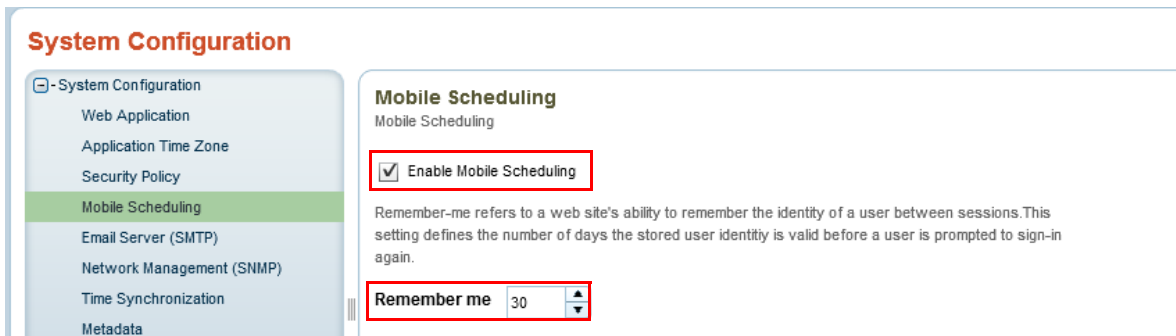
FIG. 356 System Configuration - Mobile Scheduling Page

3. In the *Mobile Scheduling* configuration page, select the **Enable Mobile Scheduling** option.

4. Optionally, use the up and down arrows to adjust the **Remember me** value as desired. *Remember-me* refers to a web site's ability to remember the identity of a user between sessions. This setting defines the number of days the stored user identity is valid before a user is prompted to sign-in again.

   Note that this value relates to the *Remember me* option on the RMS Mobile Scheduling login page. This page may be invoked when a user attempts to access scheduling information on a mobile device via QR code (FIG. 357):
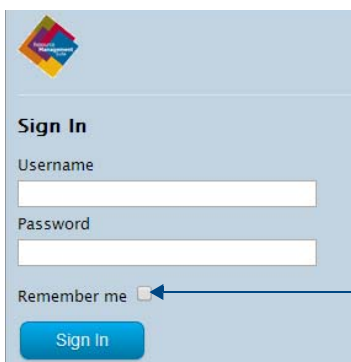
When selected, the Remember me option on the RMS Mobile Scheduling page will remember this user's login information for the number of days specified in the Mobile Scheduling configuration page.

FIG. 357 RMS Mobile Scheduling login page

- The default setting is **30** (days). The maximum setting is **750**.
- If the **Remember Me** option is de-selected on the RMS Mobile Scheduling login page, the login information is still automatically saved for *30 minutes.*

Step Two - Establish the URLs for Locations to Use Mobile Scheduling

The QR Code that is engraved on each RMS-ENT-QR (RMS QRS Quick Response Scheduling plaque) represents the URL assigned to each Location in RMS. The URLs assigned to Locations in your system are determined via the *Location Web Address for QR Code Readers* report.

NOTE: *Refer to the Reports (HTML UI)* section on page 45 *for details on working with Reports.*

To determine the Location Web Address (URL) associated with each Room in the RMS system, run the *Location Web Address for QR Code Readers* report:

1.   In the RMS HTML interface (see page 20), select **Reports** (FIG. 358):

FIG. 358 RMS Enterprise HTML interface - Reports option

2.   In the *Reports* page, select **Location Web Address for QR Code Readers** (FIG. 359):
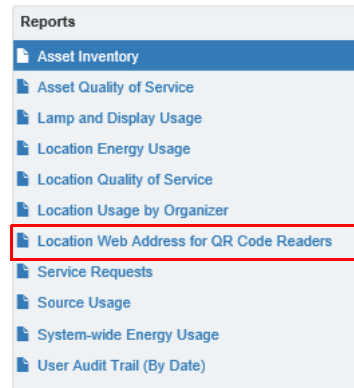
FIG. 359 Report Manager menu (Scheduling Event Reports > Location Web Address...)

This opens the *Location Web Address for QR Code Readers* report page - **General** tab (FIG. 360):
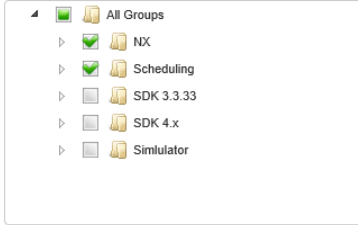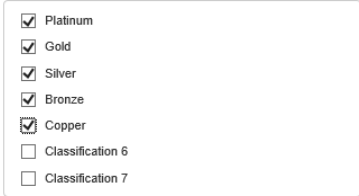
FIG. 360 Location Web Address for QR Code Readers report page (General tab)

3.   In the **URL** field, enter the base URL for the location(s) that will use mobile scheduling. This base URL can be either internal or external and must be determined by the System Administrator.

This input is required (as indicated by the red asterisk).

Click *Reset All Parameters* to clear the URL field.

4.   In the **Location** tab, select the Locations to include in Mobile Scheduling (FIG. 361):

FIG. 361 Location Web Address for QR Code Readers report page (Location tab)

Location Web Address for QR Code Readers - Location Options	
Select Location:	Select **Any** to include all Locations (no filter applied) Select **Selected** to select Location Groups or individual Locations from a Location Groups window. The Location Groups view shows all current Locations and Parent Location Groups in a hierarchical tree structure. • The top-level entry is *All Groups*. • Click the plus sign (+) next to the All Groups entry to expand the list to show all Location Groups in the system. • Click the minus sign (-) next to each entry to collapse each Location Group: • Click the checkboxes to select the Location Groups or individual Locations to include in mobile scheduling.
Location Name:	Enter a Location Name to serve as a filter for the Locations list. Only Locations with the specified name will be included in the Locations list.
Select Time Zone:	Select a Time Zone to serve as a filter for the Locations list. Only Locations with the specified Time Zone will be included in the Locations list.
Owner:	Select an Owner (name) to serve as a filter for the Locations list. Only Locations with the specified Owner will be included in the Locations list.
Select Classification:	Select a level of Classification to serve as a filter for the Locations list. Only Locations with the specified Classification will be included in the Locations list. • Click *Select All* to select all Classification levels. • Click *Select None* to de-select all Classification levels
Reset All Parameters	Click to clear all fields and return all selections to their default settings.

5. In the **Schedule** tab, specify a schedule for Mobile Scheduling (FIG. 361):
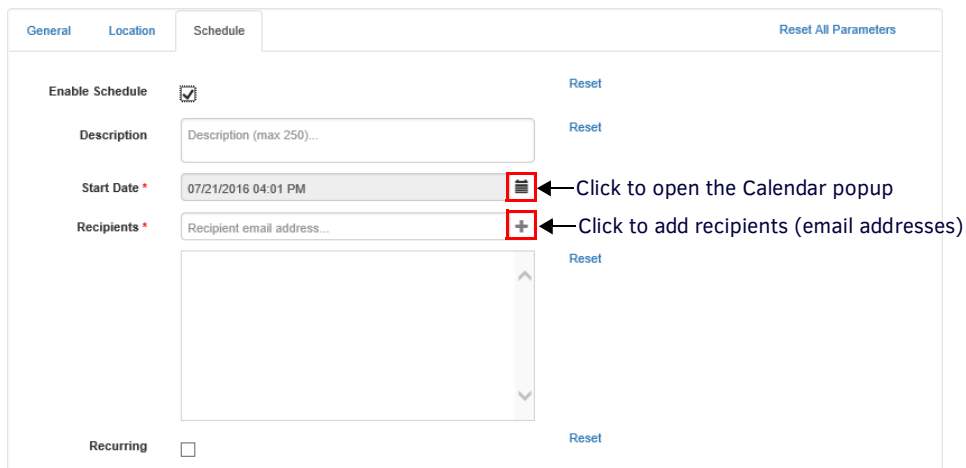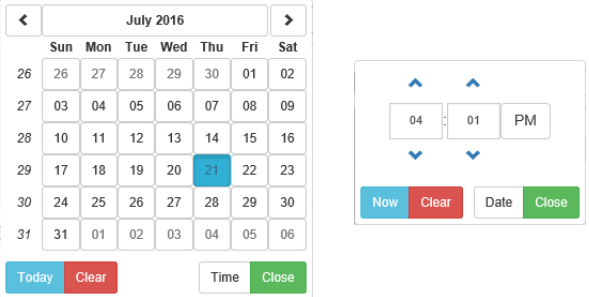
FIG. 362 Location Web Address for QR Code Readers report page (Schedule tab)

Location Web Address for QR Code Readers - Schedule Options	
Enable Schedule	Click to enable scheduling for Mobile Scheduling.
Description	Enter a description in this text field (max 250 characters).
Start Date	*Required Input* - Click the Calendar icon to open the Calendar popup: Click to select a Start Date for this schedule. • Click *Today* to select the current day as the Start Date. • Click *Clear* to clear the current selection. • Click *Time* to open the Time popup. Click *Date* in the Time popup (shown above) to return to the Calendar.
Recipients	*Required Input* -
Recurring	Select this option to save this schedule as a recurring schedule.
Reset All Parameters	Click to clear all fields and return all selections to their default settings.

Click **Run Report** (at the top of the page) to run the run the report using the selected options (FIG. 363):
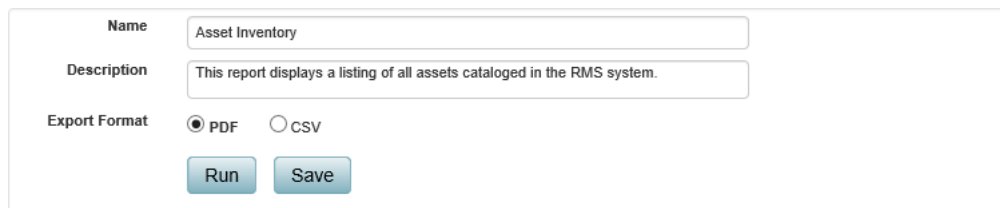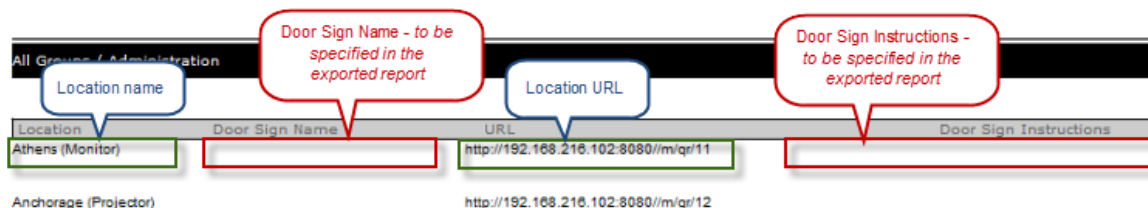
FIG. 363 Reports Page - Report Options Window

Note that *Name* and *Description* are editable fields.

- The **Export Format** options are *PDF* (default selection) and *CSV.*
- Click **Run** to generate the selected export, in the selected file format.
- Click **Save** to save the selected report as a user-defined *Saved Report*. Note that user-defined reports are listed under *Saved Reports* in the Report Selection window.

The resulting report is titled "*Location Web Address for QR Code Readers*".

An example report (with just two entries) is shown in FIG. 364. The URL column provides the URL for each Location included in the report:

FIG. 364 Example Location URLs Mapping Report page

Note that the report indicates that the *Door Sign Name* and *Door Sign Instructions* fields are blank. These fields represent the upper and lower labels for the door sign (FIG. 365):
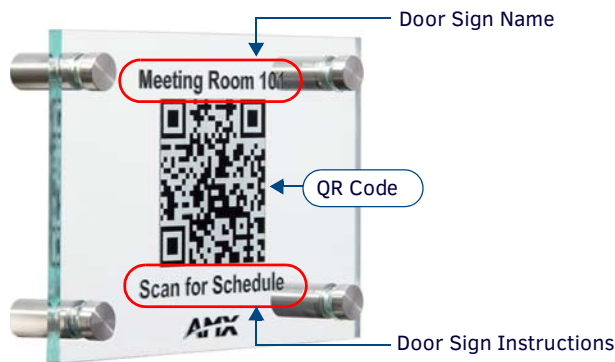
FIG. 365 Example RMS-ENT-QR RMS Door Sign

The text for these fields must be specified in the last page of the *Location Web Address for QR Code Readers* report, as described below:

Step Three - Specify the "Door Sign Name" and "Door Sign Instructions" Text

1. Export the *Location Web Address for QR Code Readers* report as a Microsoft Word 2007 document.
    a. Click **Export Report** to open a drop-down menu of export format options (FIG. 366):
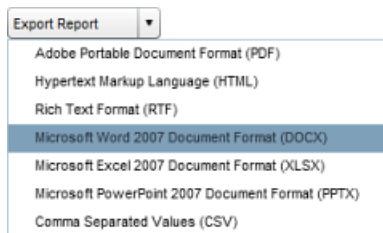
FIG. 366 Export Report menu

    b. Select **Microsoft Word 2007 Document Format (DOCX)**.
    c. When prompted, specify a target directory for the exported report.
    d. The program will indicate when the report has been exported (FIG. 367):

FIG. 367 Download File (Report Exported) dialog

2. Open the exported report and enter the text to be displayed on the Door Sign:

    NOTE: *Both the Door Sign Name and Door Sign Instruction text can have up to 23 characters (including spaces).*

    - Enter the **Door Sign Name** for each location if different (example: *Meeting Room 104*)
    - Enter the **Door Sign Instructions** for each location if different (example: *Scan for Schedule*)
    - Please note locations that do not require door signs.

3. Save the exported report, and email a copy along with your purchase order.

AMX will custom engrave your Door Sign with the Door Sign Name QR Code and Door Sign Instructions.

Email Server (SMTP)

Select **Email Server (SMTP)** under *System Configuration* in the Configuration menu to open the *Email Server (SMTP)* page (FIG. 368):

FIG. 368 Email Server (SMTP) page

RMS can send notification messages to subscribed users via a SMTP server. Use the options on this page to configure your SMTP server and define access credentials:

Email Server (SMTP) Page Options	
Enable/Disable	Click to enable or disable the SMTP notification provider in the RMS system. Default = *Enabled* • If *Disabled*, RMS will not send any notification emails. • If *Disabled*, the UI will disable all user interface input fields. See the *Enabling/Disabling SMTP Messaging* section on page 221 for details.

SMTP Server	Address/Port: Specify the SMTP server's hostname or IP Address / Port assignment. Address and Port are both required for RMS to send email notifications:
	• *Address* - Specify the SMTP server's hostname or IP address (default = "*email-smtp.us-east-1.amazonaws.com*").
	• *Port* - Specify the SMTP server's IP port. The default Port assignment depends on the *SMTP Encryption* option selected in this dialog:
	  With *No Encryption* selected, the default is port **25**
	  With *SSL/TLS* selected (the default setting), the default is port **465**
	  With *TLS* selected, the default is port **587**

SMTP Encryption	Specify if the SMTP server requires secure communication to send email messages. If no encryption method is required, this option should remain disabled. • No Encryption (default port: 25) • *SSL/TLS (default port: 465)* - default setting • TLS (default port: 587)
Server Requires Authentication	Specify if the SMTP server requires user authentication (Username/Password) to send email messages. • Enable/Disable - default = *enabled* • *Username* - If SMTP communication requires user authentication, this field is used to store the username for accessing the SMTP server. This will be a single username for the entire RMS application. All email communication will be sent using this username account. The username is stored (encrypted) in the RMS database. • *Password* - If SMTP communication requires user authentication, this field is used to store the user's password for accessing the SMTP server. The password is stored (encrypted) in the RMS database. *Note: If no user authentication credentials are required, this option should remain disabled.*
SMTP Email Configuration	Configure SMTP email send from address, friendly name, and reply-to address This information is used to send email notifications: • Email Address (required): Enter the RMS Server's sender email address (default = "*rms@amxservice.com*"). • Friendly Name (required): This option is required for RMS to send email notifications. Enter the RMS Server's sender name (default = "*RMS Administrator*"). • Reply Address (optional): Enter the SMTP server's sender reply-to address (default = "*rms@amxservice.com*"). If this field is left empty, then the RMS Server will use the sender email address as the reply-to address for all outbound email messages.

Email Server (SMTP) Page Options (Cont.)	
Send Test Email Message	Click *Send Test Message* to send a SMTP test message to a specific e-mail address, to test the configured SMTP server settings. See *Sending a Test SMTP Email Message* on page 221.

Enabling/Disabling SMTP Messaging

1. Select **Email Server (SMTP)** under *System Configuration* in the Configuration menu to open the *Email Server (SMTP)* page (FIG. 368 on page 220).
2. Under **SMTP Settings**, de-select the **Enable SMTP Message** option to disable SMTP Messaging on the RMS Server.
   By default, the **Enable SMTP Services** option is selected (enabled).
   Note that when this option is deselected, all fields in this page are disabled.

Configuring an SMTP Server

1. Select **Email Server (SMTP)** under *System Configuration* in the Configuration menu to open the *Email Server (SMTP)* page (FIG. 368 on page 220).
2. Verify that the **Enable SMTP Services** option is selected.
3. Under **SMTP Server**, enter the IP Address of the SMTP server in the text field under **Address/Port**, and use the up and down arrows to specify the port used for SMTP messaging
   - This setting is required for RMS to send email notifications.
   - Default = *25*
4. Under **SMTP Email Configuration**, fill in the text fields (*Email Address*, *Friendly Name*, *Reply Address*)
5. Under **SMTP Encryption**, select either *No Encryption* or *SSL/TTS* (default = *No Encryption*).
6. Under **Server Requires Authentication**, click in the *Enable* checkbox to require user authentication in order to send SMTP Email messages.
   - If this option is checked, the *Username* and *Password* text fields are enabled. Enter the username and password that will be required to send SMTP Email in these fields.
   - Default = *disabled*.

Sending a Test SMTP Email Message

1. Select **Email Server (SMTP)** under *System Configuration* in the Configuration menu to open the *Email Server (SMTP)* page (FIG. 368 on page 220).
   The options under **SMTP Email Configuration** on this page allow you to send a test SMTP Email message to a specified set of recipients.
2. Verify that **SMTP** is enabled, and that the SMTP Server and SMTP Names & Addresses are configured correctly.
3. Under **SMTP Settings**, click **Send Test Message** to open the *SMTP Test Message* dialog (FIG. 369):

FIG. 369 SMTP Test Message dialog

4. Enter a valid email address for the recipient, and enter the message text.
5. Click **Send** to send the message.

Network Management (SNMP)

RMS supports both SNMP queries and SNMP trap notifications. Select **Network Management (SNMP)** under *System Configuration* in the Configuration Menu to open the *Network Management (SNMP)* page (FIG. 370):

FIG. 370 Network Management (SNMP) page

NOTE: *Network Management (SNMP) is only available for installed RMS Server; this service is not available through AMX Cloud hosted services.*

Notes on RMS Enterprise SNMP Support

RMS Enterprise supports SNMPv1 only, and provides information regarding client gateways, locations, assets, parameters and thresholds. The following table indicates the information provided by RMS Enterprise on monitored devices:

SNMP Information Provided on Monitored Devices		
Client Gateways	• The number of client gateways registered in RMS. • Info about each client gateway:	
	clientGatewayIndex (or primary key) clientGatewayClientUID clientGatewayName clientGatewayIPAddress clientGatewayProtocol	clientGatewayProtocolVersion clientGatewayMACAddress clientGatewaySDKVersion clientGatewayLocationIndex
Locations	• The number of locations in RMS. • Info about each location:	
	locationIndex locationName locationGroup locationMapURL	locationPrestigeLevel locationNumberSeats locationPhone
Assets	• The number of assets registered in RMS. • Info about each asset	
	assetIndex assetLocationIndex assetClientGatewayIndex assetAssetType assetName assetDescription assetManufacturer	assetModel assetSerialNumber assetDPS assetNLDeviceVersion assetNLDeviceAddressType assetNLDeviceAddress

SNMP Information Provided on Monitored Devices (Cont.)	
Parameters	There is an extra number needed to GET these values. It is because "*assetParameterEntry*" has an index defined by two values: INDEX { assetParameterAssetIndex,assetParameterIndex }. The *assetParameterAssetIndex* value doesn't matter because the second number is a primary key to the parameter. You must simply provide some value. • The number of parameters registered in RMS. • Info about each parameter

assetParameterAssetIndex	assetParameterValue
assetParameterIndex	assetParameterCanReset
assetParameterName	assetParameterResetValue
assetParameterType	assetParameterTripped

Thresholds	Similar to parameters, the thresholds have an index defined by more than a single value: INDEX {assetParameterThresholdAssetIndex, assetParameterThresholdParameterIndex, assetParameterThresholdIndex } • The number of thresholds registered in RMS. • Info about each threshold

assetParameterThresholdAssetIndex	assetParameterThresholdThreshold
assetParameterThresholdParameterIndex	assetParameterThresholdCompare
assetParameterThresholdIndex	assetParameterThresholdStatusType
assetParameterThresholdName	assetParameterThresholdTripped
assetParameterThresholdEnabled	

Notifications	Traps are generated for the following events:

• new client gateway registered • new location created • new asset registered • new parameter registered • parameter tripped • parameter restored

Responses to SNMP Queries

See the amx.mib for details: it is located at :

> **C:\Program Files\AMX\Resource Management Suite\Server\doc\snmp\amx.mib**

NOTE: *Nothing in the way of code or configuration can be done to tailor the responses provided by RMS.*

The options on the *Network Management (SNMP)* page allow you to specify SNMP Community credentials settings for sending trap notifications and responding to queries:

Network Management (SNMP) Page Options	
SNMP General Settings	
Enable/Disable	Click to enable or disable the SNMP management system in RMS. This option must selected (*Enabled*) for RMS to support SMTP queries and trap notifications. Default = *Disabled*.
SNMP Community	This option defines the group to which devices and management stations running SNMP belong (usually a "friendly" name). If the inbound query does not specify this same community identifier string, RMS will ignore the query.
SNMP Agent Port	Use the up/down arrows to change the assigned SNMP Agent Port. Default = *30161*
SNMP Trap Port	Use the up/down arrows to change the assigned SNMP Trap Port. Default = *30162*
SNMP Trap Recipients	This option defines a listing of SNMP trap message recipients. If no recipients are defined, then RMS will send a generic broadcast trap message on the network. However, if trap recipients are defined, RMS will send the trap messages only to these defined addressed. Each trap recipient defines an IP address or hostname to a SNMP monitoring agent.

Enabling/Disabling SNMP Services

1. Select **Network Management (SNMP)** under *System Configuration* in the Configuration menu to open the *Network Management (SNMP)* page (FIG. 370 on page 222).
2. Under **SNMP General Settings**, de-select the **Enable SNMP Services** option to disable SNMP Services on the RMS Server.
   By default, the **Enable SNMP Services** option is de-selected. Note that when this option is deselected, all fields in this page are disabled.

Configuring SNMP Trap Settings

1. Select **Network Management (SNMP)** under *System Configuration* in the Configuration menu to open the *Network Management (SNMP)* page (FIG. 370 on page 222).
2. Verify that the **Enable SNMP Services** option is selected.
3. In the **SNMP Community** text field, enter the address of the target SNMP Community for SNMP messaging.

4. Under **SNMP Agent Port**, use the up / down arrows to change the assigned SNMP Agent Port, if necessary (default = *30161*).

5. Under **SNMP Trap Port**, use the up / down arrows to change the assigned SNMP Trap Port, if necessary (default = *30162*).

6. Under **SNMP Trap Recipients**, enter one or more SNMP Trap Recipients addresses (IP address or hostname).
   - Click **Add** to add each address to the list. To remove a Trap Recipient, select an address and click **Remove**.
   - Each Trap Recipient defines an IP address or hostname to a SNMP monitoring agent.
   - If no Trap Recipients are defined, then RMS will send a generic broadcast trap message on the network.
   - If Trap Recipients are defined, RMS will send the trap messages only to the defined addresses.

Time Synchronization

Select **Time Synchronization** under *System Configuration* in the Configuration menu to open the *Time Synchronization* page (FIG. 371):

Time Synchronization

The RMS system enforces time synchronization across all connected clients. RMS will use the date/time of the server and calculate the offset based on the location's configured time zone and send time synchronization instructions to the connected clients. This option should be disabled if using an alternate network time synchronization method for the connected clients.
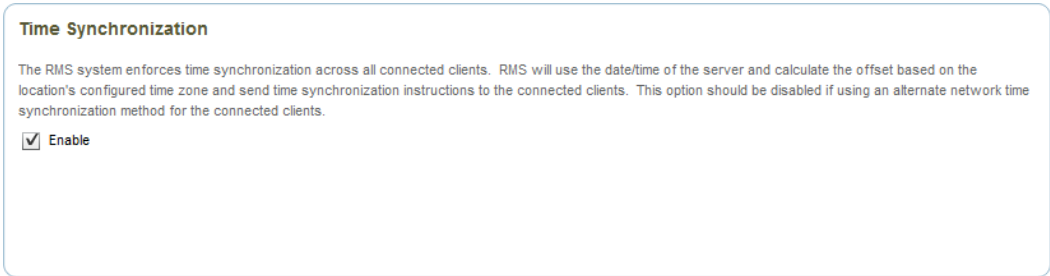
☑ Enable

FIG. 371 Time Synchronization page

The RMS system can enforce time synchronization across all connected clients. RMS uses the date/time of the server, calculates the offset based on the Location's configured time zone and sends time synchronization instructions to the connected clients.

NOTE: *This option should be disabled if using an alternate network time synchronization method for the connected control systems.*

Use the options on this page to enable and disable Control System Time Synchronization:

Time Synchronization Page Options
Enable	Click this option to enable / disable Control System Time Synchronization for the RMS system. Default = *Disabled*

Enabling / Disabling Control System Time Synchronization

1. Select **Time Synchronization** under *System Configuration* in the Configuration menu to open the *Time Synchronization* page (FIG. 371 on page 224).

2. Deselect the **Enable Control System Time Synchronization** option to disable Control System Time Synchronization on the RMS Server.

   NOTE: *By default, the Enable Control System Time Synchronization option is de-selected.*

Metadata

Select **Metadata** under *System Configuration* in the Configuration menu to open the *Metadata* page (FIG. 372):

Metadata			
Category	**Name** ▲	**Data Type**	**Default Value**
All Assets	Metadata 02	Boolean	True
All Locations	Metadata 03	Number	1234
Asset Type	Metadata 04	Numeric Range	55
All Locations	Metadata 05	Decimal	1.23456
Location Group	Metadata 06	Date	03/02/2015
All Assets	Metadata 07	Time	2:15 PM
Location Group	Number (Location Group)	Number	42
Asset Type	Number (Touch Panel)	Number	42
Location Group	Number Range (Location Group)	Numeric Range	25
Asset Type	Number Range (Touch Panel)	Numeric Range	50
All Locations	Power State	Boolean	True
Location Group	String (Location Group)	String	Location group string
Asset Type	String (Touch Panel)	String	Asset type string
Location Group	Test	Memo	FOLSOM LAKE (CBS13) — A Northern California reservoir ran dry
Location Group	Time (Location Group)	Time	2:15 PM
Asset Type	Time (Touch Panel)	Time	1:15 PM

FIG. 372 Metadata page

NOTE: *The authenticated user must have the global permission of Manage Configuration to access and manage metadata definitions using this configuration page. See the Management - Roles (Classic UI) section on page 192 for details.*

Use the options on this page to manage metadata definitions (including adding, editing and deleting Descriptor properties) for Locations and Assets in the RMS database.

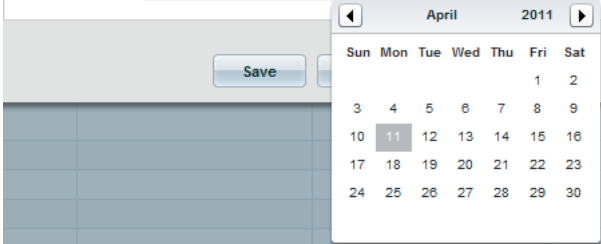| Metadata Page Options	
Add	Click to add a new metadata definition. This action invokes the *Metadata Setting* dialog. Use this dialog to define the new metadata definition. • See *Adding a New Metadata Definition* on page 229.
Edit	Click to edit the selected metadata definition, via the *Metadata Setting* dialog. • This option is only enabled when a metadata entry is selected. • See *Editing a Metadata Definition* on page 229.
Delete	Click to delete the selected metadata definition. The System will prompt you to verify this action before the selection is deleted - Click **Yes** in the *Delete Confirmation* dialog to proceed. • This option is only enabled when a metadata entry is selected. • See *Deleting a Metadata Definition* on page 229.
Search	Use this field to search for a specific Metadata by *Category*, *Name*, *Data Type* and/or *Default Value*.
Metadata Table	The table on this page provides a listing of all metadata definitions currently in the RMS database. The columns in this table present the following data for each metadata definition: • Category: This column indicates the scope of each metadata definition (*All Locations*, *Location Group*, *All Assets* or *Asset Type*. See the *Metadata Categories* section (below) for details. • Name: This column indicates the name of each metadata definition. • Data Type: This column indicates the data type (*String*, *Memo*, *Boolean*, *etc.*) of each metadata definition. See the *Metadata Data Types* section on page 227 for details. • Default Value: This column indicates the default value of each metadata definition. See the *Adding a New Metadata Definition* section on page 229.

Metadata Categories

In the *Metadata Setting* dialog (see FIG. 373 on page 229), click the **Category** field to open a drop-down menu of application Categories that can be applied to a metadata definition. The Category selection defines the scope of the metadata definition, as described in the following table:

Metadata Categories	
All Locations	Select this option to make this metadata entry available for use in all Locations. Use this category to define a global Location property to store custom information for each Location in the RMS system. **Note**: This is the default setting.
Location Group	Select this option to make this metadata entry available for use only in a specific Location Group. Use this category to define a Location property to store custom information for each Location in a particular Location Group. When this option is selected, an additional field is provided - **Select Location Group**. • Click this field to open a drop-down menu of Location Groups. • Select a Location Group to which this metadata entry will apply from the list.
All Assets	Select this option to make this metadata entry available for use with all Assets. Use this category to define a global Asset property to store custom information for each Asset in the RMS system. Metadata definitions assigned to the *All Assets* category are automatically inherited by new Assets (indicated on the *Asset Properties* page - **Asset Metadata** tab (see FIG. 220 on page 133). The defined metadata property will be listed with its default value. This metadata value can be edited to override the default value and assign an asset specific instance value to the metadata property. *Note: Metadata properties inherited by global definition cannot be deleted from the asset instance. If an overriding value has been applied for the asset instance, that value can be reverted back to the definitions default value.*
Asset Type	Select this option to make this metadata entry available for use only with a specific Asset type. Use this category to define an Asset property to store custom information for each Asset of a particular asset type. Metadata definitions assigned to the *Asset Type* category are automatically inherited on the each assets metadata listing page who is a member of the configured asset type (indicated on the *Asset Properties* page - **Asset Metadata** tab (see FIG. 220 on page 133). The defined metadata property will be listed with its default value. This metadata value can be edited to override the default value and assign a location specific instance value to the metadata property. When this option is selected, an additional field is provided - **Select Asset Group**. • Click this field to open a drop-down menu of Asset Types. • Select an Asset Type to which this metadata entry will apply from the list. *Note: These Asset instance metadata properties can be deleted from the asset metadata listing page.*

Metadata Data Types

In the *Metadata Setting* dialog (see FIG. 373 on page 229), click the **Data Type** field to open a drop-down menu of Data Types that can be applied to a metadata definition. The supported metadata Data Types are defined in the following table:

Metadata - Data Types	
String	This data type is the base for all string and character types. When this option is selected, the *Default Value* field is provided: **Data Type** String **Default Value** • **Default Value**: Enter the default value for String metadata entries (200 characters max).
Memo	This data type is used to store large notes, etc. • Text is provided as ASCII (no formatting). • Variable length. When this option is selected, the *Default Value* field is provided: **Data Type** Memo **Default Value** • **Default Value**: Enter the default value for Memo metadata entries (200 characters max).
Boolean	This data type is used to represent one of two values: *true* or *false*. When this option is selected, the *Default Value* field is provided: **Data Type** Boolean **Default Value** False False True • **Default Value**: Click in this checkbox to set the default value for boolean metadata entries to *True*. Un-check this option to set the default value to *False*. • Default = *False*.
Number	This data type is used to represent a number (fixed). When this option is selected, the *Default Value* field is provided: **Data Type** Number **Default Value** 0 • **Default Value**: Use the up and down arrows to set the default value for numeric metadata entries. • Range = *-1,000,000* to *1,000,000* • Default = *0*
Numeric Range	This data type is used to represent a range of numbers (fixed). When this option is selected, the following fields are provided: **Data Type** Numeric Range **Lower Bounds** 0 **Upper Bounds** 100 **Default Value** 0 100 0 • Range = *-1,000,000* to *1,000,000* • Lower Bounds: Set the lower boundary for the allowed numeric range (*default = 0*). • Upper Bounds: Set the upper boundary for the allowed numeric range (*default = 100*). • **Default Value**: Use the slider to set the default value for numeric metadata entries. *Note: The Lower Bounds value can never be greater than the Upper Bounds value, and the Upper Bounds value can never be less than the Lower Bounds value.*

Metadata - Data Types (Cont.)	
Decimal	This data type is used to represent a decimal number (floating-point). When this option is selected, the following field is provided: **Data Type** Decimal ▼ **Default Value** 0 • **Default Value**: Use the up and down arrows to set the default value for decimal metadata entries. • Range = *-100,000,000,000* to *100,000,000,000* • Default = *0*
Date	This data type is used to represent a calendar date. When this option is selected, the following fields are provided: **Data Type** Date ▼ **Default Value** 04/11/2011 🗓 – Click to open the calendar ◀ April 2011 ▶ Sun Mon Tue Wed Thu Fri Sat 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 • **Default Value**: Select a default date from the calendar (click the Calendar icon to access the Calendar). • Default = *today's date*.
Time	This data type is used to represent a specific time (Hour / Minute). When this option is selected, the following fields are provided: **Data Type** Time ▼ **Default Value** 12 ▲▼ : 00 ▲▼ ○ AM ● PM • **Default Value**: Use the up and down arrows to specify default Hour and Minute values, and select either AM or PM. • Default = *12:00/PM*.
Enumeration	This data type is used to represent an enumeration set. *Note: An enumeration is a data type consisting of a set of named values that represent integral constants, known as enumeration constants. Enumerations require that you list (enumerate) each of the values in creating a name for each of them. In addition to providing a way of defining and grouping sets of integral constants, enumerations are useful for variables that have a small number of possible values.* When this option is selected, the following fields are provided: **Data Type** Enumeration ▼ **Enumeration** [ ] Add / Remove / ▲ / ▼ **Default Value** Please select enumeration value ▼ • **Add**: Click to add an entry to the Enumeration list. See *Defining a Enumeration Metadata Type* on page 230 for details. • **Remove**: Click to remove a selected entry from the Enumeration list. • **Up/Down Arrows**: Use these buttons to move a selected Enumeration entry up or down in the Enumeration list. • **Default Value**: Click inside this field to select a default Enumeration value from the drop-down menu.
Hyperlink	This data type is used to represent a hyperlink. When this option is selected, the following fields are provided: **Data Type** Hyperlink ▼ **Default Value** **Link Name** [ ] **Link URL** [ ] • **Default Value**: Use the *Link Name* and *Link URL* text fields to define the default hyperlink value.

Metadata - Data Types (Cont.)	
Date/Time	This data type is used to represent a calendar date as well as a specific time (Hour / Minute). This option combines the Date and Time Enumeration types: when this option is selected, the following fields are provided: **Data Type** [Date/Time ▾] **Default Value** [04/11/2011 🗓] [12 ▲▼] : [00 ▲▼] ○ AM ⦿ PM • **Default Value**: Select a default date from the calendar (click the Calendar icon to access the Calendar), use the up and down arrows to specify default Hour and Minute values, and select either AM or PM. • Default = *today's date, 12:00/PM*

Adding a New Metadata Definition

1. Select **Metadata** under *System Configuration* in the Configuration menu to open the *Metadata* page (FIG. 372 on page 225).

2. Click the **Add** button. This action invokes the *Metadata Setting* dialog (FIG. 373):

Metadata Setting ✕

Name [   ]
Description [   ]
Category [All Locations ▾]
Data Type [String ▾]
Default Value [   ]

[OK]   [Cancel]

FIG. 373 Metadata Setting dialog

3. Use the fields in this dialog to define the new metadata definition:
   a. In the **Name** field, enter a name for this metadata definition.
   b. In the **Description** field, enter a brief description for this metadata definition.
   c. Click the **Category** field to open a drop-down menu of application categories that can be applied to the new metadata definition. The supported categories are described in the *Metadata Categories* section on page 226.
   d. Click the **Data Type** field to open a drop-down menu of Data Types that can be applied to the new metadata definition. The supported data types are described in the *Metadata Data Types* section on page 227.
   e. Enter a default value for this metadata definition in the **Default Value** field (optional).
   f. Click **OK** to save your changes and close the *Metadata Setting* dialog.

4. The new metadata definition is represented in the Metadata table (on the *Metadata* page).

Editing a Metadata Definition

1. Select **Metadata** under *System Configuration* in the Configuration menu to open the *Metadata* page (FIG. 372 on page 225).

2. Select a metadata definition in the Metadata table.

3. Click the **Edit** button. This action invokes the *Metadata Setting* dialog (FIG. 373 on page 229).

4. Edit the fields as necessary (see *Adding a New Metadata Definition* on page 229 for details), and click **OK** to save your changes and close the dialog.

Deleting a Metadata Definition

1. Select **Metadata** under *System Configuration* in the Configuration menu to open the *Metadata* page (FIG. 372 on page 225).

2. Select a metadata definition in the Metadata table.

3. Click the **Delete** button. The system will prompt you to verify this action before the selected metadata definition is deleted, via the *Delete Confirmation* dialog (FIG. 374):
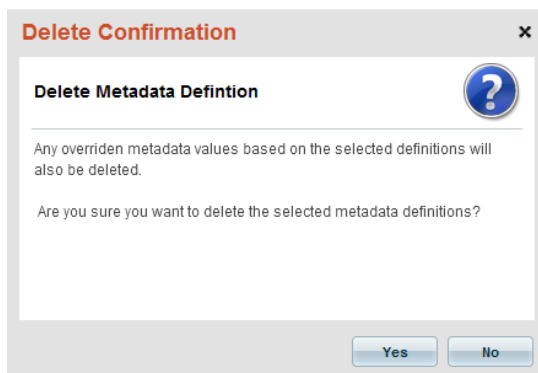
FIG. 374 Delete Confirmation dialog - Metadata Definition

4. Click **Yes** to proceed.

Defining a Enumeration Metadata Type

1. Select **Metadata** under *System Configuration* in the Configuration menu to open the *Metadata* page (FIG. 372 on page 225).

2. Click the **Add** button. This action invokes the *Metadata Setting* dialog (FIG. 373 on page 229).

3. Fill in the **Name**, **Description** fields, and select a **Category**.

4. In the **Data Type** field, select **Enumeration** from the drop-down menu.

5. Click **Add** to insert a new (empty) entry into the Enumeration list (FIG. 375):
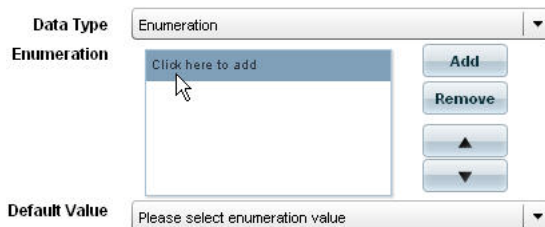
FIG. 375 Adding an Enumeration Entry

6. Click on the new entry (*Click here to add*) to assign a name to this Enumeration entry.

7. Click outside of the new entry to apply the name.

8. Repeat steps 5-7 to add more Enumeration entries.
   - To remove a selected entry from the Enumeration list, click **Remove**.
   - Use the up and down arrows to move a selected entry up or down in the Enumeration list.

9. Click **OK** to save your changes and close the *Metadata Setting* dialog.

Searching For Metadata Definitions

Use the *Search* tool in the *Metadata* page to search for a Metadata Definition by *Category*, *Name*, *Data Type* and/or *Default Value* (FIG. 376).

Metadata Definition Search window
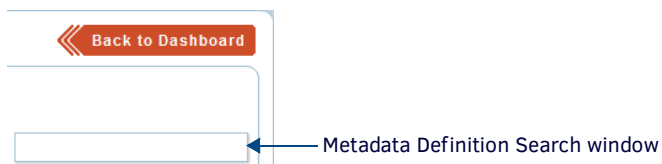
FIG. 376 Metadata Definition page - Search window

Auditing

Select **Auditing** under *System Configuration* in the Configuration Menu to open the *Auditing* page (FIG. 377):

FIG. 377 Auditing page

The RMS system can track all user activity and record user interaction with the RMS system for auditing purposes. All auditing history is stored in the RMS database. Use the options on this page to enable/disable Auditing services, and specify how to manage purging audit report entries from the database:

Auditing Page Options	
Enable Auditing:	Click to enable system auditing and tracking. • Default = *Enabled*. See the *Enabling/Disabling System Auditing* section on page 233 for details.
Auditing Automatic Cleanup	
Limit the number of days to keep audit records	Check this option to limit the number of days to keep audit record entries in the database. When enabled, the *Maximum Number of Days* field is activated. • Default = *Enabled*.
Maximum number of days:	Click the up/down arrows (or type) to set the maximum number of days to keep audit report entries in the database. This option is enabled only if the *Limit the number of days to keep audit records* option is enabled. • Range = *1-1500* • Default = *180* See the *Configuring Automatic Audit Record Cleanup Settings* section on page 233 for details.
Purge Auditing Records	
Delete all auditing records:	Select this option to delete all auditing records in the RMS database when the *Delete* button is clicked. See the *Purging Audit Records* section on page 234 for details.
Delete only the auditing records before this date:	Select this option to delete all auditing records before the date selected in the calendar when the *Delete* button is clicked. When this option is selected, the calendar is activated. Click to select a date; use the left and right arrow buttons to scroll back and forward through months and years as necessary. • Default = *Disabled*.
Delete button:	Click to delete system reporting entries from the database, according to the *System Log Maintenance* options selected. This button is enabled only if one or more system log entries exist in the database, relative to the *Purge Auditing Records* options selected.

Auditable Items

The auditable items for RMS Enterprise are limited to user-invoked actions. An audit record consists of the following fields:

Auditable Items	
Created (Datetime)	Timestamp when the action took place
Action (String)	A verb describing the nature of the action that took place.
User (String)	The username of the user invoking the action.
Target (String)	Describes the subject of the action.
Location (String)	A fully qualified location path/name where an action took place. i.e. "*Building A.Floor 4.Engineering Lab.Workroom 34*"
Description (String)	A textual description of the auditable action.

The audit record records an action that typically follows this pattern:

[**USER**] performs an [**ACTION**] on or against a [**TARGET**] {optionally to a [**LOCATION**]}

FIG. 378 provides a few of examples of auditable items:
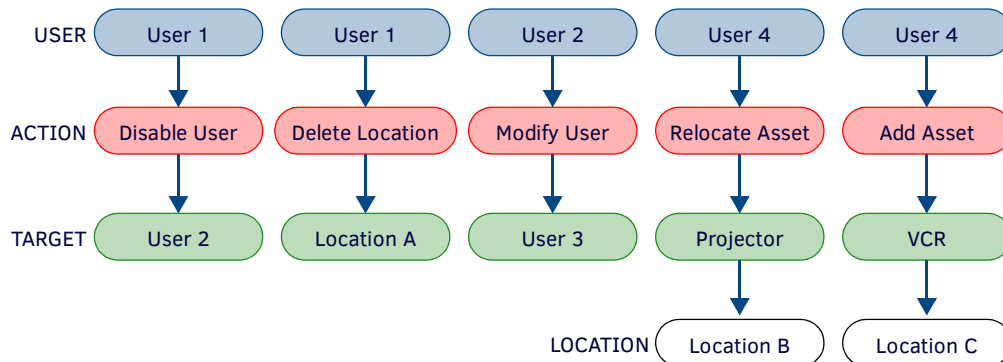
FIG. 378 Typical pattern for Audit Record records on an Action

Auditable Actions

The following table provides a listing of all auditable actions:

Auditable Actions		
User Management		
User:	• Add User • Delete User • Modify User	• Enable User • Disable User • Reset User Password
User Contact:	• Add User Contact • Delete User Contact • Modify User Contact	• Enable User Contact • Disable User Contact
User Notification:	• Add User Notification • Delete User Notification • Modify User Notification	• Enable User Notification • Disable User Notification
User Role:	• Add User Role • Delete User Role • Modify User Role	
Location Management		
Location Group:	• Add Location • Delete Location Group • Modify Location Group	
Location:	• Add Location • Delete Location • Modify Location	• Enable Location Maintenance Mode • Disable Location Maintenance Mode

Auditable Actions (Cont.)		
Asset Management		
Client (System):	• Delete Client	
Asset:	• Add Asset • Delete Asset • Modify Asset	• Relocate Asset • Enable Asset Maintenance Mode • Disable Asset Maintenance Mode
Asset Parameter:	• Modify Asset Parameter • Reset Asset Parameter	
Asset Parameter Threshold:	• Add Asset Parameter Threshold • Delete Asset Parameter Threshold • Modify Asset Parameter Threshold	
Asset Control Method:	• Execute Asset Control Method	
Asset Manufacturer:	• Add Asset Manufacturer • Delete Asset Manufacturer • Modify Asset Manufacturer	
Asset Model:	• Add Asset Model • Delete Asset Model • Modify Asset Model	
System Configuration		
• Modify System Configuration		
Notification Rule		
• Add Notification Rule • Delete Notification Rule • Modify Notification Rule • Enable Notification Rule • Disable Notification Rule		
Notification Template		
• Add Notification Template • Delete Notification Template • Modify Notification Template		
Status Type		
• Add Status Type • Delete Status Type • Modify Status Type		
Classification Level		
• Modify Classification Level • Enable Classification Level • Disable Classification Level		
Control Function Macro		
• Add Control Function Macro • Delete Control Function Macro • Modify Control Function Macro • Execute Control Function Macro • Schedule Control Function Macro		
Source Usage		
• Reset Source Usage		

Enabling/Disabling System Auditing

When Auditing is enabled / disabled, the new setting will be propagated across all RMS servers.

1. Select **Auditing** under *System Configuration* in the Configuration menu to open the *Auditing* page (FIG. 377 on page 231).
2. Under **System Auditing**, de-select the **Enable Auditing** option to disable system auditing on the RMS Server.
   By default, the **Enable Auditing** option is selected. Note that when this option is deselected, all fields in this page are disabled.

Configuring Automatic Audit Record Cleanup Settings

RMS can automatically remove auditing records that are older than the specified number of days:

1. Select **Auditing** under *System Configuration* in the Configuration menu to open the *Auditing* page (FIG. 377 on page 231).
2. Under **Auditing Automatic Cleanup**, de-select the **Limit the number of days to keep audit records** option to keep auditing records in the database forever.

By default, the **Limit the number of days to keep audit records** option is selected. Note that when this option is selected, the **Maximum number of days** option is enabled. Use the up and down arrows to set the number of days that the auditing records will be saved in the database, after which they will automatically be deleted.

- Range = *1 - 1500*
- Default = *180*

Purging Audit Records

1. Select **Auditing** under *System Configuration* in the Configuration menu to open the *Auditing* page (FIG. 377 on page 231).

2. Under **Purge Auditing Records**, select an option:
   - **Delete all auditing records**: Select this option to delete all auditing records when the *Delete* button is clicked (default setting).
   - **Delete only the auditing records entries before this date**: Select this option to delete all auditing records before the date selected in the calendar when the *Delete* button is clicked:

     When this option is selected, the calendar is activated (FIG. 379).

FIG. 379 Auditing Records Maintenance Calendar

Click to select a date; use the left and right arrow buttons to scroll back and forward through months and years as necessary.

Reporting

Select **Reporting** under *System Configuration* in the Configuration menu to open the *Reporting* page (FIG. 380):

FIG. 380 Reporting page

The RMS system tracks multiple data points for historical reporting and analysis. All reporting metrics are stored in the RMS database. Use the options on this page to specify how to manage purging report entries from the database in order to help limit database growth and manage database size.

Reporting Page Options	
Reporting Data Automatic Cleanup	
Maximum days to keep detailed history	Use the up/down arrows to adjust the maximum number of days to maintain detailed historical transaction records in the RMS database. • Range = 1-750 • Default = *90*
Maximum time to keep summary history (Year(s)):	Use the up/down arrows to adjust the maximum number of years to maintain summarized historical records in the RMS database. • Range = 1-15 • Default = *2*
Purge Historical Reporting Records	
Delete all historical reporting records:	Select this option to delete all reporting records when the *Delete* button is clicked. This option will delete all historical reporting records in the RMS database. This includes both detailed historical transaction records and reporting summary records.
Delete only the historical reporting entries before this date:	Select this option to delete all reporting records before the date selected in the calendar when the *Delete* button is clicked. This includes both detailed historical transaction records and reporting summary records. When this option is selected, the calendar is activated. Click to select a date; use the left and right arrow buttons to scroll back and forward through months and years as necessary. • Default = *Disabled*.
Delete:	Click to delete system reporting entries from the database, according to the *System Log Maintenance* options selected. This button is enabled only if one or more system log entries exist in the database, relative to the *Purge Historical Reporting Records* options selected. *Note: Deleting history records in RMS is a permanent deletion. There is no way to restore deleted history records in RMS once they have been purged. See the Deleting Report History Records section on page 235 for details.*

Configuring Automatic Report History Record Cleanup Settings

RMS can automatically remove report history records that are older than the specified number of days:

1. Select **Reporting u**nder *System Configuration* in the Configuration menu to open the *Reporting* page (FIG. 380 on page 234).
2. Use the up and down arrow next to the **Maximum number of days** to set the number of days that the System Reports will be saved in the database, after which they will automatically be deleted.
   - Range = *0 - 750*
   - Default = *90*

Deleting Report History Records

NOTE: *Deleting history records in RMS is a permanent deletion. There is no way to restore deleted history records in RMS once they have been purged.*

1. Select **Reporting** under *System Configuration* in the Configuration menu to open the *Reporting* page (FIG. 380 on page 234).
2. Under **Purge Historical Reporting Records**, select an option:
   - **Delete all historical reporting records**: Select this option to delete all historical reporting records in the RMS database (including both detailed historical transaction records and reporting summary records) when the *Delete* button is clicked (default setting).
   - **Delete only historical reporting entries before this date**: Select this option to delete all system report entries before the date selected in the calendar when the *Delete* button is clicked. When this option is selected, the calendar is activated (FIG. 381).
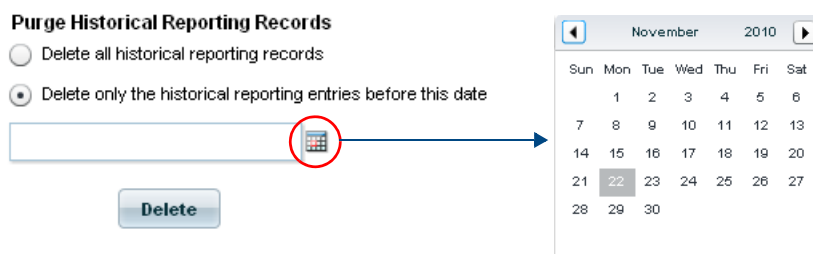

FIG. 381 System Report Maintenance Calendar

Click to select a date; use the left and right arrow buttons to scroll through months and years as necessary.

3. Click **Delete.**

Notification Configuration (Classic UI)

Overview

RMS Enterprise uses system-defined Notification Templates to define the notification message associated with each event type. Use the options in the *Notification Templates* page to create new templates, or edit the system-defined templates if desired. Furthermore, a user created template can be set as the new default for a particular event type.

The options in the **Notification Configuration** category of the (Classic UI) *Configuration* menu allow you to specify a RMS Base URL Address as well as manage Notification Templates, as described in the following sections (FIG. 382):
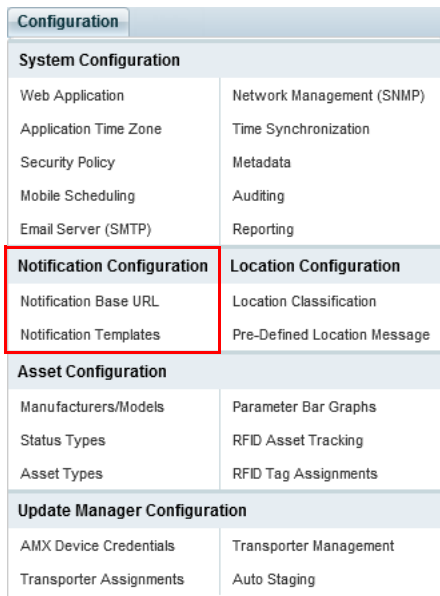
FIG. 382 Configuration Menu - Notification Configuration options

Notification Base URL

Select **Notification Base URL** under *Notification Configuration* in the Configuration menu to open the *Notification Base URL* page (FIG. 383):

FIG. 383 Notification Base URL page

RMS Base URL Address - This option is intended for use in multi-server installations. Enter the base address for accessing this site in a multi-server installation, to allow delivery of notification emails to the specified URL.

Changing the Base URL Address

1. Select **Notification Base URL** under *Notification Configuration* in the Configuration menu to open the *Notification Base URL* page (FIG. 383 on page 236).

2. Under **RMS Base URL Address,** edit the base URL for accessing this site in the field.

Click **Restore to Default** to remove changes and restore the default Base URL (default = *RMS*).

Notification Templates

Select **Notification Templates** under *Notification Configuration* in the Configuration menu to open the *Notification Templates* page (FIG. 384):

Template Type	Template Name	Description	Default
Asset Parameter Trip	Asset Parameter Trip	System-Defined Asset Parameter Trip	✓
Asset Parameter Restore	Asset Parameter Restore	System-Defined Asset Parameter Restore	✓
New Client Gateway	New Client Gateway	System-Defined New Client Gateway	✓
Notification Message Delivery Failure	Notification Message Delivery Failure	System-Defined Notification Message Delivery Failure	✓
Service Provider Request	Service Provider Request	System-Defined Service Provider Request Template	✓
Location Maintenance Mode Change	Location Maintenance Mode Change	Location Maintenance Mode Template	✓
Asset Maintenance Mode Change	Asset Maintenance Mode Change	Asset Maintenance Mode Template	✓
Troller Error	Troller Communication Error	Troller Communication Error Template	✓
Resource Profile Synchronization Failure	Resource Profile Synchronization Failure	Resource Profile Synchronization Failure Template	✓
Scheduling Error	Scheduling Error	Scheduling Error Template	✓
System Maintenance Mode Change	System Maintenance Mode Change	System Maintenance Mode Change Template	✓
Transporter Error	Transporter Communication Error	Transporter Communication Error Template	✓

FIG. 384 Notification Templates page

Use the options on this page to manage Notification Templates:

Notification Templates Options	
Add	Click to add a new Notification Template. This action invokes the *Notification Template Editor* dialog. • See the *Creating a Notification Template* on page 239.
Edit	Click to edit the selected Notification Template, via the *Notification Template Editor* dialog. • This option is only enabled when a Notification Template is selected. • See the *Editing a Notification Template* on page 240.
Delete	Click to delete the selected Notification Template. The System will prompt you to verify this action before the selection is deleted - Click **Yes** in the *Delete Confirmation* dialog to proceed. • This option is only enabled when a non-default Notification Template is selected. Templates that are marked as 'default' cannot be deleted. • See the *Deleting a Notification Template* on page 241.
Copy Template	Click to create a copy of the selected Notification Template. A copy of the selected template is added to the list, directly beneath the selected template. See the *Copying a Notification Template* section on page 240.
Notification Template Table	The table on this page provides a listing of all Notification Templates currently in the database.

Notification Template Editor Dialog

The *Notification Template Editor* dialog is accessed via either the **Add** or **Edit** buttons in the *Notification Templates* window. FIG. 385 shows the *Notification Template Editor* dialog populated with example data from a selected Notification Template.
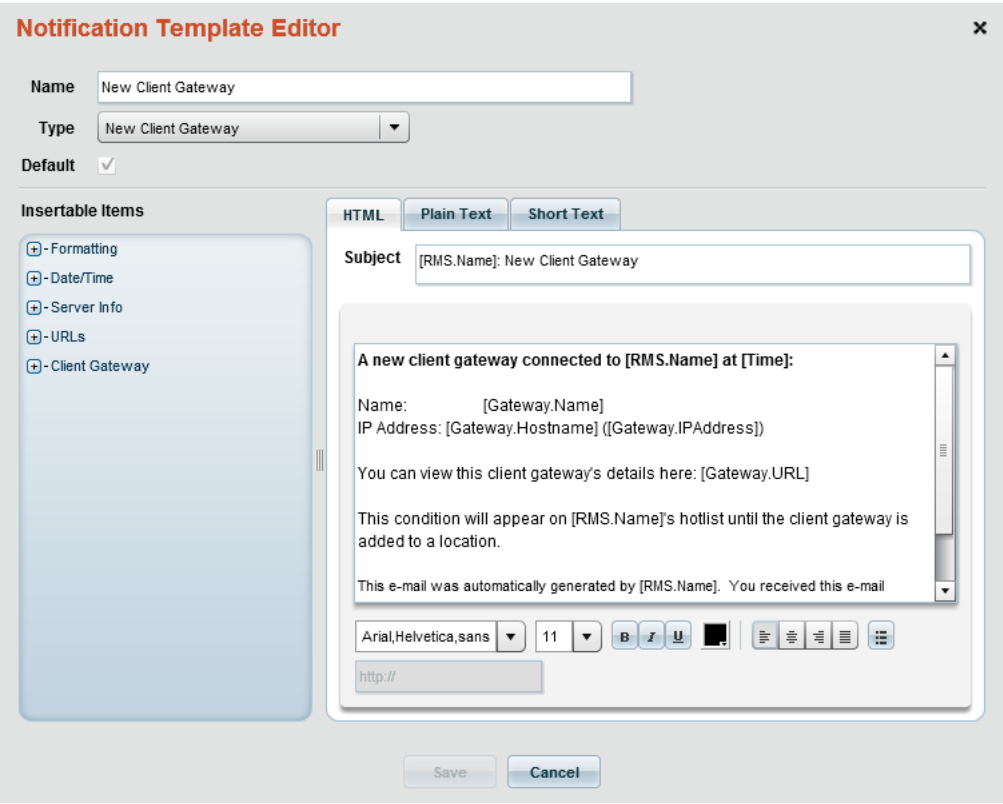

FIG. 385 Notification Template Editor dialog

The options in this dialog are described below:

Notification Template Editor Dialog Options	
Name	Enter or edit the Name for the selected Notification Template.
Type	Select an event type to associate with this Notification Template from the **Type** drop-down menu: • Asset Parameter Trip • Asset Parameter Restore • New Client Gateway • Notification Message Delivery Failure • Service Provider Request
Default	When checked, this Notification Template is set as the default notification template for the selected (Event) Type. • Note that this option is enabled only when a user-created Notification Template is selected for editing. • If a system default Notification Template is selected, this option is pre-selected, and cannot be de-selected.
Insertable Items	Select which data items to insert into this Notification Template. • The items presented in this window depend on the Type selected. • Click the + sign next to each Category to expand the view to show all contained items. • Double-click on any Item to add it to the template. As each Item is added it is represented in either the *Subject* field, or the *Body* field of the Message window (at the location of the cursor).
Message Window	The Message contains three tabs, allowing you to configure the notification template in three formats (*HTML*, *Plain Text* and *Short Text*). Each tab contains a subject and body field. The HTML tab also contains a set of text formatting tools. • Enter the Subject for Notification Messages that utilize this template in the *Subject* field. • Enter the text for Notification Messages that utilize this template in the *Body* field. • When an item is selected in the *Body* field of the Message window, the URL field is enabled. Enter a URL for the selected item (to provide a link to a manufacturer's website, operation manual, etc.), if desired.
Save	Click to save all changes to the current Notification Template and close this dialog.
Cancel	Click to close the dialog without saving any changes.

Creating a Notification Template

1. In the *Notification Templates* window, click the **Add** button. This invokes the *Notification Template Editor* dialog (FIG. 385).

2. In the **Name** field, type a name for the new Notification Template.

3. Select an event type to associate with this Notification Template from the **Type** drop-down menu.

4. In the **Insertable Items** window (FIG. 386), select which data items to insert into this Notification Template. The items presented in this window depend on the *Type* selected.

Asset Parameter Trip, Asset Parameter Restore	New Client Gateway	Notification Message Delivery Failure	Service Provider Request
Location Maintenance Mode Change	Asset Maintenance Mode Change	Troller Error, Resource Profile Synchronization Failure, Scheduling Error	
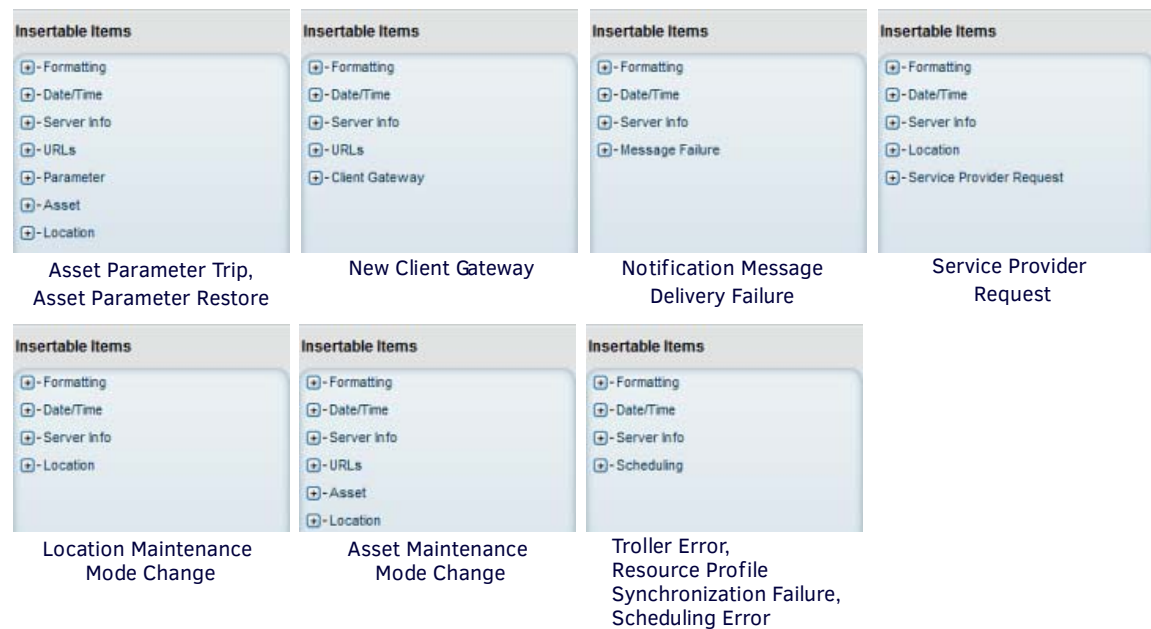
FIG. 386 Modify Template Settings dialog - Insertable Items window

- Click the + sign next to each Category to expand the view to show all contained items.
- Data items can be added to the *Subject* field, or inside the *Body* field by placing the cursor in the field, and double-clicking on an item in the in the *Insertable Items* window.
- Click in the *Subject* field, or inside the *Body* field, depending on where you want to insert the data Item.
- Double-click on any item in the *Insertable Items* window to add it to the template. As each Item is added it is represented in either the *Subject* field, or the *Body* field (at the location of the cursor).

5. In the **Subject** field, enter a subject header for this Notification Template. Data items can be added by placing the cursor in this field and double-clicking on an item in the in the *Insertable Items* window.

6. Select the **HTML**, **Plain Text** or **Short Text** tab to choose the text format for this template.
   - If *HTML* is selected, a set of text formatting tools as well as a URL field is provided (FIG. 387):
   - Data items can be added by placing the cursor in this field and double-clicking on an item in the in the *Insertable Items* window.
   - When an Item is selected in the *Body* field, the **URL** field is enabled. Enter a URL for the selected Item if desired.
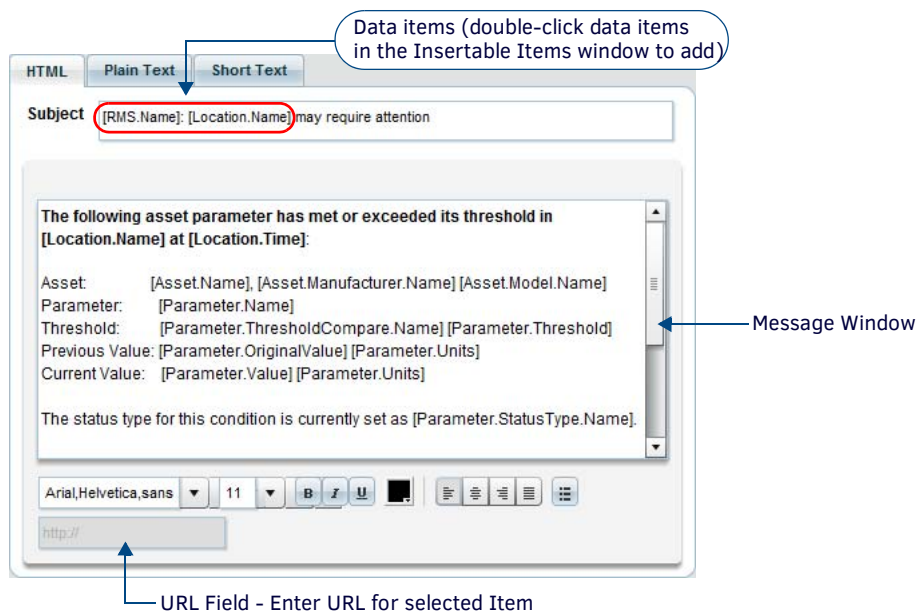
FIG. 387   Modify Template Settings dialog - Message Window (HTML)

7.   Click **Save** to save your changes.

The new Notification Template is added to the listing in the *Notification Templates* page (FIG. 384 on page 237).

Editing a Notification Template

1.   In the *Notification Templates* window, select the template from the list table that you want to edit.

2.   Click the **Edit** button. This invokes the *Notification Template Editor* dialog (FIG. 385 on page 238).

3.   Edit the fields as desired. See the *Notification Template Editor Dialog* section on page 238 for details.

4.   Click **Save** to save your changes.

Setting a User-Defined Notification Template as the Default

1.   Select a user-defined Notification Template in the list table.

2.   Click the **Edit** button. This invokes the *Notification Template Editor* dialog (FIG. 385 on page 238).

3.   Click in the **Default** checkbox.

When checked, this Notification Template is set as the default notification template for the selected (Event) Type.

- Note that this option is enabled only when a user-created Notification Template is selected for editing.
- If a system default Notification Template is selected, this option is pre-selected, and cannot be de-selected.

Copying a Notification Template

1.   With a template selected in the *Notification Templates* window, click the **Copy** button.

2.   A copy of the selected template is added to the list, directly beneath the selected template (FIG. 388):

FIG. 388   Copy of "New Client Gateway" template

Note the differences between the original template and the copied template:

- The *Template Name* is the name of the original template with "*Copy of*" prepended to it.
- The copied template does not indicate a *Template Type*.
- The copied template is not designated as the default template.

3.   Edit the copied template as desired, in the *Notification Template Editor* dialog. See the *Notification Template Editor Dialog* section on page 238 for details.

Deleting a Notification Template

1. With a template selected in the *Notification Templates* window, click the **Delete** button.

   NOTE: *The Notification Template to be deleted cannot be a system default template.*

2. The program will prompt you to verify this action before the template is deleted:

Delete Confirmation ✕

Delete Notification Template

Are you sure you want to delete the selected notification template(s)?

[Yes]   [No]
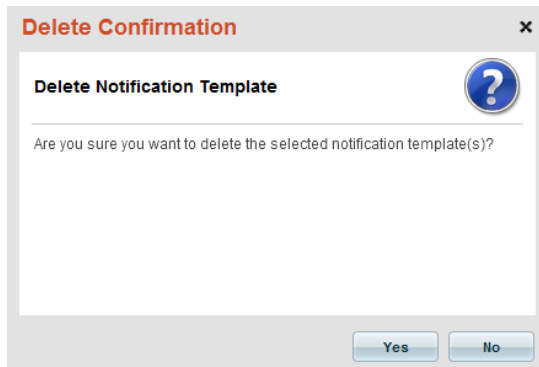
FIG. 389 Notification Templates page – Search window

3. Click **Yes** to proceed.

Location Configuration (Classic UI)

Overview

The options in the **Location Configuration** category of the (Classic UI) *Configuration* menu allow you to view and manage Classification Levels for Locations (FIG. 390):

FIG. 390 Configuration Menu - Location Configuration options

NOTE: *A "Location" is any physical or virtual space that is configured to be monitored or serviced by RMS (such as a classroom, conference room, lecture hall, foyer, network closet, basement, etc). Locations are managed in the Location Page - see the Management - Locations (Classic UI) section on page 103 for details.*

Location Classification

The *Location Classification* option in the **Location Configuration** category of the *Configuration* menu allows you to view and manage *Classification Levels* for Locations.

Classification Levels classify Locations based on your own criteria. Classification Levels are arbitrary, designed to provide distinction between Locations in searches. Hotlist records can also be sorted by Classification Levels.

There are no inherit characteristics for each Classification Level. They can be assigned in any way that helps to differentiate between types of Locations.

The number of Classification Levels is fixed to 10 levels in escalating order.

By default, RMS presents the following Classification Levels:

- Platinum
- Gold
- Silver
- Bronze
- Copper
- Classification 6-10

NOTE: *A Classification Level must be applied to every Location. Each Location can only be assigned to one Classification Level.*

Select **Location Classification** under *Location Configuration* in the Configuration menu to open the *Location Classification* page (FIG. 391):

FIG. 391 Location Classification page

You can enable/disable as well as rename Classification Levels via options in the *Location Classification* page:

Location Classification Options	
Classification Levels Table	The table on this page provides a listing of all Classification Levels currently in the system. The columns in this table present the following data for each Classification Level: • Level: The numbers in this column indicate the relative level of each Classification Level (read-only) • Name: This column presents the name of each Classification Level (click to edit) • Description: By default, this column is empty. Click to enter a brief description for each Classification Level as desired. See *Editing a Classification Level* on page 243 for details. • Enabled: By default, all system-defined Classification Levels are enabled (indicated by a check in each checkbox in this column). De-select these checkboxes to disable up to nine of the ten Classification Levels. See *Enabling / Disabling a Classification Level* on page 243 for details.

Editing a Classification Level

1. Select **Location Classification** under *Location Configuration* in the Configuration menu to open the *Location Classification* page (FIG. 391 on page 243).
2. Select a Classification level definition in the Classification Level table.
3. Click inside the **Name** cell to edit the name of the selected classification level.
4. Click inside the **Description** cell to edit the description of the selected classification level.

Enabling / Disabling a Classification Level

When a Classification Level has been disabled, it will not be available for selection when you add a new Location.

1. Select **Location Classification** under *Location Configuration* in the Configuration menu to open the *Location Classification* page (FIG. 391 on page 243).
2. Select a classification level definition in the Classification Level table.
3. Click to de-select the checkbox in the **Enabled** cell.

Pre-Defined Location Messages

RMS allows you to define and save messages (for example, help request responses) that are to be sent to Locations. These messages are displayed on the touch panel(s) in the specified Location. *Pre-Defined Location Messages* can be sent via the **Send Message To** option in the *Location* page (see the *Location Page - Locations Window* section on page 105). *Pre-Defined Location Messages* can be also sent via the Message feature on the Dashboard (see the *Sending a Message to a Location* section on page 116).

Select **Pre-Defined Location Message** under *Location Configuration* in the Configuration menu to open the *Pre-Defined Location Message* page (FIG. 392):

FIG. 392 Pre-Defined Location Message page

Use the options in this page to add or edit pre-defined location messages:

Pre-Defined Location Message Options	
Search	Use this search field to perform a search for message text. See *Searching For Pre-Defined Location Messages* on page 244 for details.
Add	Click to create a new pre-defined location message, via options in the *Edit Pre-Defined Location Message* dialog. See *Creating a New Pre-Defined Location Message* on page 244 for details.
Edit	Click to edit the selected message, in the *Edit Pre-Defined Location Message* dialog. See *Editing a Pre-Defined Location Message* on page 245 for details.
Delete	Click to delete the selected message. See *Deleting a Pre-Defined Location Message* on page 245 for details.
Pre-Defined Location Messages Table	The table on this page provides a listing of all Predefined Messages currently in the system. The columns in this table present the following data for each message. A checkmark in the *Modal* column indicates that the user must dismiss the message. This property is set in the *Edit Pre-Defined Location Message* dialog.

Searching For Pre-Defined Location Messages

Use the *Search* window in the *Pre-Defined Location Message* page (see FIG. 392) to search for a message by name.

Creating a New Pre-Defined Location Message

1. In the *Pre-Defined Location Message* page, click the **Add** button. This action opens the *Edit Pre-Defined Location Message* dialog (FIG. 393).

FIG. 393 Edit Pre-Defined Location Message dialog

2. Select the type message to create, from the **Message Type** drop-down menu. The message types available to choose from are: *Information*, *Warning*, *Security*, *Critical* or *Question*.

3. Enter a title for the message in the **Title** text field.

4. Enter the body text of the message in the **Message** text field.

5. Select the **Modal** checkbox to set this message so that the recipient user must specifically dismiss the message on the touch panel(s) in order to close it (as opposed to a timeout - see below).
    Default = *disabled*.

6. Use the Up/Down arrows next to **Timeout** to set a timeout value for this message in seconds. By default, pre-defined location messages timeout on the touch panel(s) after 30 seconds.

7. Click **Save** to save your changes, close this dialog, and add the new message to the *Pre-Defined Messages* list.

Editing a Pre-Defined Location Message

1. In the *Pre-Defined Location Message* page, select a message in the *Pre-Defined Messages* list.

2. Click **Edit** to open the *Edit Pre-Defined Location Message* dialog, populated with the selected message's information.

3. Edit the fields as desired.

4. Click **Save** to save your changes, close this dialog, and update the selected message in the *Pre-Defined Messages* list.

Deleting a Pre-Defined Location Message

1. In the *Pre-Defined Location Message* page, select one or more messages in the *Pre-Defined Messages* list.

2. Click **Delete**.

3. The program will prompt you to verify this action (FIG. 394):
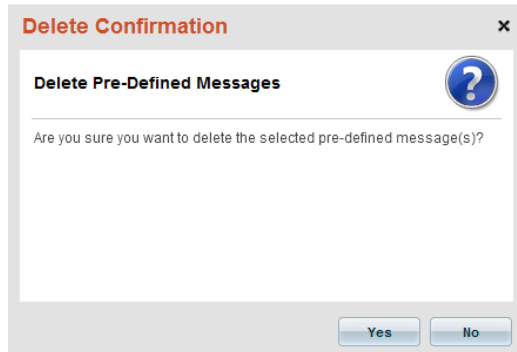
FIG. 394 Delete Confirmation dialog

4. Click **Yes** to proceed.

Asset Configuration (Classic UI)

Overview

RMS utilizes a common catalog for shared Asset manufacturers and models. This allows the user to define records for Asset manufacturers and models, which can later be used in searches and reporting to view related assets. URLs can be assigned to manufacturers and models and are made available in the Hotlist detail pane for quick access to more information on the manufacturer or model. Asset model images are stored and displayed when viewing an asset.

The options in the **Asset Configuration** category of the (Classic UI) *Configuration* menu allow you to view and manage Assets (FIG. 395):

FIG. 395 Configuration Menu - Asset Configuration options

Manufacturers/Models

Select **Manufacturers/Models** under *Asset Configuration* in the (Classic UI) *Configuration* menu to open the *Manufacturers/Models* page (FIG. 396):

FIG. 396 Manufacturers/Models page

Use the options in this page to manage assets by Manufacturer and Model information:

Manufacturers/Models Options	
Manufacturers window	
Search	Use this field to perform a search for Manufacturer names. • See *Searching for Manufacturers* on page 248.
Add	Click to add a new device Manufacturer entry. This action invokes the *Add Manufacturer* dialog. Use this dialog to define the new Manufacturer entry. • See *Adding a New Manufacturer* on page 247.
Edit	Click to edit the selected Manufacturer entry, via the *Edit Manufacturer* dialog. • This option is only enabled when a Manufacturer entry is selected. • See *Editing a Manufacturer* on page 248.
Delete	Click to delete the selected Manufacturer entry. The System will prompt you to verify this action before the selection is deleted – Click **Yes** in the *Delete Confirmation* dialog to proceed. • This option is only enabled when a Manufacturer entry (containing zero Models) is selected. • See *Deleting a Manufacturer* on page 248.
Manufacturers List	This is the listing of all manufacturer's names in the RMS system.
Models window	
Search	Use this field to perform a search for Model names. See *Searching for Models* on page 251 for details.
Add	Click to add a new device Model entry. This action invokes the *Add Model* dialog. Use this dialog to define the new Model entry. • See *Adding a New Model* on page 249.
Edit	Click to edit the selected Manufacturer entry, via the *Edit Manufacturer* dialog. • This option is only enabled when a Manufacturer entry is selected. • See *Editing a Model* on page 250.
Delete	Click to delete the selected Manufacturer entry. The System will prompt you to verify this action before the selection is deleted – Click **Yes** in the *Delete Confirmation* dialog to proceed. • This option is only enabled when a Model entry is selected. • See *Deleting a Model* on page 250.
Models Table	This is the listing of all model names associated with the selected Manufacturer name.

NOTE: *Changes made on this page will take effect when you leave the page.*

Adding a New Manufacturer

A *Manufacturer* represents the manufacturer of one or Models (devices) in the system.
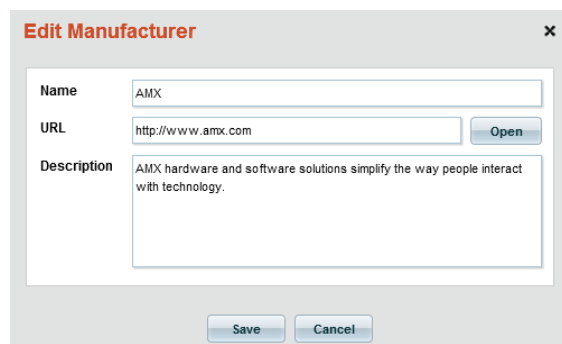
1. Select **Manufacturers/Models** under *Asset Configuration* in the Configuration menu to open the *Manufacturers/Models* page (FIG. 396 on page 246).

2. In the *Manufacturers* window, click the **Add** button. This action invokes the *Add Manufacturer* dialog (FIG. 397):

FIG. 397 Add Manufacturer dialog

3. Fill in the fields in this dialog:
   a. Enter the manufacturer's name in the **Name** field.
   b. Enter the URL of the manufacturer's website in the **URL** field.
      Once a URL has been entered, click the **Open** button to open the specified URL in a browser window. This feature allows you to verify that the specified URL opens the intended website.
   c. Enter a brief description of this manufacturer in the **Description** text field.
4. Click **Save** to save your changes and close this dialog.
5. The new manufacturer is listed in the *Manufacturers* list.

Editing a Manufacturer

1. Select **Manufacturers/Models** under *Asset Configuration* in the Configuration menu to open the *Manufacturers/Models* page (FIG. 396 on page 246).
2. In the *Manufacturers* window, select a manufacturer.
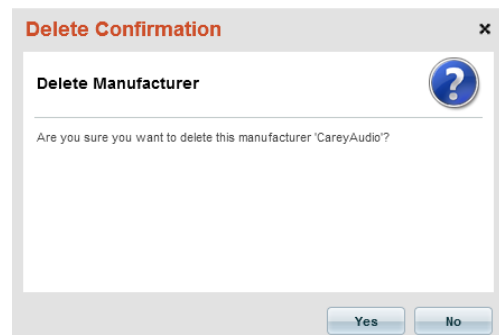3. Click the **Edit** button. This action invokes the *Edit Manufacturer* dialog (FIG. 398):

FIG. 398 Edit Manufacturer dialog

4. Edit the fields as desired.
5. Click **Save** to save your changes and close this dialog.

Deleting a Manufacturer

NOTE: *RMS will not allow you to delete Manufacturers that are currently referenced in the System.*

1. Select **Manufacturers/Models** under *Asset Configuration* in the Configuration menu to open the *Manufacturers/Models* page (FIG. 396 on page 246).
2. In the *Manufacturers* window, select a manufacturer.
3. Click the **Delete** button.
4. The system will prompt you to verify this action before the manufacturer is deleted, via the *Delete Confirmation* dialog (FIG. 399):

FIG. 399 Delete Confirmation dialog - Manufacturer

5. Click **Yes** to proceed.
6. The Manufacturer is removed from the *Manufacturers* list.

Searching for Manufacturers

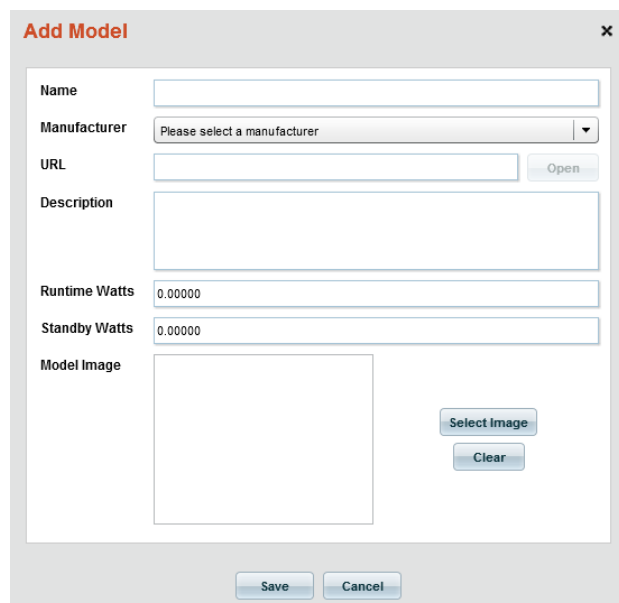Use the *Search* tool in the Manufacturers window to search for a specific Manufacturer by name (FIG. 400).

FIG. 400 Manufacturers window - Search window

Adding a New Model

A *Model* represents a specific device in the system.

1. Select **Manufacturers/Models** under *Asset Configuration* in the Configuration menu to open the *Manufacturers/Models* page (see FIG. 396 on page 246).

2. In the *Manufacturers* window, select the manufacturer of the model that you are adding.

3. In the *Models* window, click the **Add** button. This action invokes the *Add Model* dialog (FIG. 401):

FIG. 401 Add Model dialog

NOTE: *The only required entry in this dialog is "Name". However, provide as much information as possible for each Model so that RMS can provide this information to users.*

4. Fill in the fields in this dialog:
   a. Enter the model's name in the **Name** field.
   b. Enter the URL of the manufacturer/model website in the **URL** field. Once a URL has been entered, click the **Open** button to open the specified URL in a browser window. This feature allows you to verify that the specified URL opens the intended website.
   c. Enter a brief description of this model in the **Description** text field.
   d. Enter the current draw (Watts) for this model when the device is active in the **Runtime Watts** field.
   e. Enter the standby current draw (Watts) for this model when the device is in standby mode in the **Standby Watts** field.

   NOTE: *Runtime and Standby Watts specifications have to be provided by the Manufacturer of each device.*

5. Select an image to associate with this model:
   a. Click **Select Image**. This action invokes the *Select File to Upload* dialog.
   b. Locate and select an image file to associate with this model.
   ● Supported image types: JPG, JPEG, GIF and PNG.
   ● The *Model Image* window is 125 x 125 pixels.
   ● A preview of the selected image is displayed in the preview window.
   ● Click **Clear** to remove the model image.

   NOTE: *RMS will scale the image to the proper resolution for the image category. For best results, prepare the image to be 125 x 125 pixels before uploading, to avoid scaling or stretching of the image when it is displayed in RMS.*

6. Click **Save** to save your changes and close this dialog.

7. The new model is listed in the *Models* list (FIG. 402).

FIG. 402 New Model Added to Models List

Editing a Model

1. Select **Manufacturers/Models** under *Asset Configuration* in the Configuration menu to open the *Manufacturers/Models* page (FIG. 396 on page 246).
2. In the *Manufacturers* window, select the manufacturer of the model that you wish to edit.
3. In the *Models* window, select a model, and click **Edit**. This action invokes the *Add Model* dialog, indicating the selected model's information (FIG. 403):

FIG. 403 Add Model dialog (editing an existing model)

4. Edit in the fields in this dialog as desired.
5. Click **OK** to save your changes and close this dialog.

Deleting a Model

NOTE: *RMS will not allow you to delete Models that are currently referenced in the System.*

1. Select **Manufacturers/Models** under *Asset Configuration* in the Configuration menu to open the *Manufacturers/Models* page (FIG. 396 on page 246).
2. In the *Manufacturers* window, select the manufacturer of the model that you wish to delete.
3. In the *Models* window, select a model, and click **Delete**.
4. The system will prompt you to verify this action before the model is deleted, via the *Delete Confirmation* dialog (FIG. 404):

FIG. 404 Delete Confirmation dialog - Model

5. Click **Yes** to proceed.
6. The deleted Model is removed from the *Models* list.

Searching for Models

Use the *Search* tool in the Models window to search for a specific Model (FIG. 405).

FIG. 405 Models window - Search window

This search tool searches across the data columns displayed in the Models window (*Name*, *Description*, *URL*).

Status Types

Status Types get assigned to asset parameter thresholds and other trigger events in the system, and are used to route notifications to appropriate recipients. Status Types are displayed in the Status column of the Hotlist data grid to indicate the current status of each Hotlist item.

Select **Status Types** under *Asset Configuration* in the (Classic UI) *Configuration* menu to open the *Status Types* page (FIG. 406):

FIG. 406 Status Types page

The table on this page provides a listing of all Status Types available in the RMS System. The columns in this table present data for each Status Type, as defined in the Add & Edit Status Type dialogs. Refer to the *Default Status Types* section on page 252 for detailed descriptions of each of the default Status Types. Use the options in this page to configure and manage Status Types:

Status Types Page Options	
Search	Use this field to perform a search across all columns in the Status Types table. See *Searching For Status Types* on page 254.
Add	Click to add a new device Status entry. This action invokes the *Add Status Type* dialog. Use this dialog to define the new Status entry. See *Adding a New Status Type* on page 252.
Edit	Click to edit the selected Status entry, via the *Edit Status Type* dialog. This option is only enabled when a Manufacturer entry is selected. See *Editing a Status Type* on page 254.
Delete	Click to delete the selected Status entry. The System will prompt you to verify this action before the selection is deleted – Click **Yes** in the *Delete Confirmation* dialog to proceed. This option is only enabled when a Status entry is selected. See *Deleting a Status Type* on page 254.

NOTE: *Changes made on this page will take effect when you leave the page.*

Default Status Types

RMS is pre-configured with many default Status Types, as described in the following table:

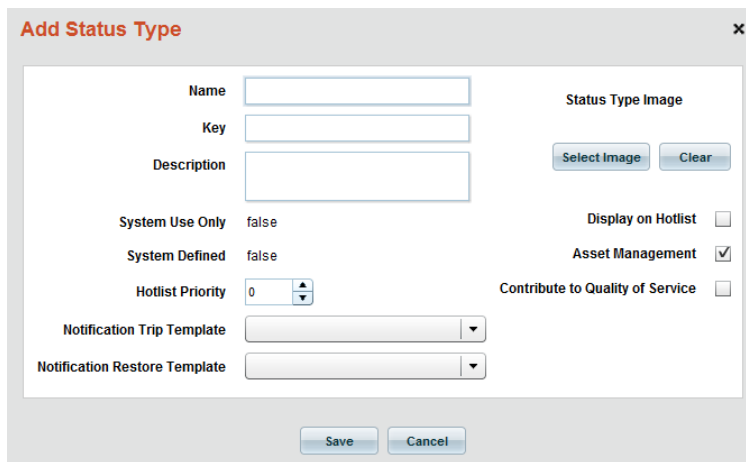| Default Status Types		
Internal Application Status Types The following *internal application* status types are used to route application specific events and messages. *Note: Internal application status types are implemented by the RMS application only and they are not exposed for user assignment for asset parameters.*		
Icon	**Name**	**Description**
	New Client Gateway	Invoked anytime a new RMS client gateway is attached to the RMS server. This status type can be used to notify users of new client systems wishing to participate in the RMS system.
	Notification Message Delivery Failure	Invoked anytime a notification provider encounters an error condition preventing a single notification (i.e. SMTP e-mail notification) from being delivered.
	Notification Provider Error	Invoked anytime a notification provider encounters an error condition preventing all notifications from being delivered (i.e. is the SMTP notification provider is unable to establish a connection to the SMTP server).
	Scheduling Resource Synchronization Failure	Invoked anytime a scheduling resource encounters a synchronization error. Check the scheduling provider and verify the RMS Legacy Troller configuration settings.
	System Maintenance Mode	Invoked anytime a location or asset is placed into maintenance mode. This status type can notify users/administrators of the system if anyone disables a locations or assets monitoring using the maintenance mode feature.
	Transporter Communication Error	Invoked anytime that communication between the RMS Server and the RMS Transporter Service has failed.
	Troller Communication Error	Invoked anytime the troller process encounters a scheduling error. Check the scheduling provider and verify the RMS Legacy Troller configuration settings.
Asset Parameter-Specific Status Types RMS defines the following system predefined status types used to route asset parameter specific events and messages. The status types are exposed for user assignment for asset parameters and are assignable from the RMS SDK. *Note: Users may not delete or change these system defined status types.*		
Icon	**Name**	**Description**
	Control System Error	Invoked anytime an asset parameter assigned as a Control System Error status type exceeds its threshold value.
	Equipment Usage	Invoked anytime an asset parameter assigned as a Equipment Usage status type exceeds its threshold value.
	Help Request	Invoked anytime an asset parameter assigned as a Help Request status type exceeds its threshold value.
	Location Communication Error	Invoked anytime an asset parameter assigned as a Location Communication Error status type exceeds its threshold value.
	Maintenance	Invoked anytime an asset parameter assigned as a Maintenance status type exceeds its threshold value.
	Network	Invoked anytime an asset parameter assigned as a Network status type exceeds its threshold value.
	Security	Invoked anytime an asset parameter assigned as a Security status type exceeds its threshold value.

Adding a New Status Type

Custom (user-defined) Status Types can be assigned to asset parameters via the RMS GUI and are assignable from the asset parameter registration in the RMS SDK.

NOTE: *Custom (user-defined) Status Types can be edited (see Editing a Status Type on page 254) or deleted (see Deleting a Status Type on page 254) at any time.*

1. Select **Status Types** under *Asset Configuration* in the Configuration menu to open the *Status Types* page (see FIG. 406 on page 251).
2. Click the **Add** button to open the *Add Status Type* dialog (FIG. 407):

FIG. 407 Add Status Type dialog

3. Fill in the fields in this dialog to define the new status type;

Add Status Type Dialog Options	
Name	Enter a descriptive name for the new status type in the text field.
Key	Enter a key for the new status type in the text field. The Key entry allows this Status Type to be programmatically hooked to a threshold. Typically, the Key entry should be the same as the *Name* entry, but in all uppercase and with underscores in place of spaces. For example, the Key for the "Help Request" Status Type is "HELP_REQUEST".
Description	Enter a brief description of the new status type in the text field.
System Use Only	This read-only field indicates wether this Status Type is reserved for System Use (*True* or *False*). • "*True*" indicates that this Status Type is reserved for system use; therefore it is unavailable for users to associate it with a parameter threshold. • "*False*" indicates that this Status Type is available to be associated with a threshold.
System Defined	This read-only field indicates wether this Status Type is one of the pre-defined Status Types that come with RMS Enterprise (*True* or *False*).
Hotlist Priority	Use the up and down arrows to specify the Hotlist Priority for the new status type. This property allows you to sort items in the Hotlist according to Status.
Notification Trip Template	Click the down arrow to select a Notification Trip Template from the drop-down menu of available templates: • Asset Parameter Trip • Asset Parameter Restore • New Client Gateway • Notification Message Delivery Failure • Service Provider Request
Notification Restore Template	Click the down arrow to select a Notification Restore Template from the drop-down menu of available templates (same options as are available for *Notification Trip Template*).
Status Type Image	• *Select Image*: Click to open the *Select file to upload* dialog, to locate and select an image file to associate with this parameter status type. 　Supported image types: JPG, JPEG, GIF and PNG. 　Max display size = 32 x 32 (pixels). • *Clear*: Click to clear the Status Type Image. *Note: RMS will scale the image to the proper resolution for the image category. For best results, prepare the image to be 32 x 32 pixels before uploading, to avoid scaling or stretching of the image when it is displayed in RMS.*
Display on Hotlist	Check this option to display this Status Type in the Hotlist. Default = *Disabled*
Asset Management	Check this option to include this Status Type notification in *Asset Management* reports. Default = *Enabled*
Contribute To Quality of Service	Check this option to include this Status Type notification in *Quality of Service* reports. Default = *Disabled*

4. Click **Save** to save your changes and close this dialog.

5. The new Status Type is added to the Status Types list (FIG. 408):
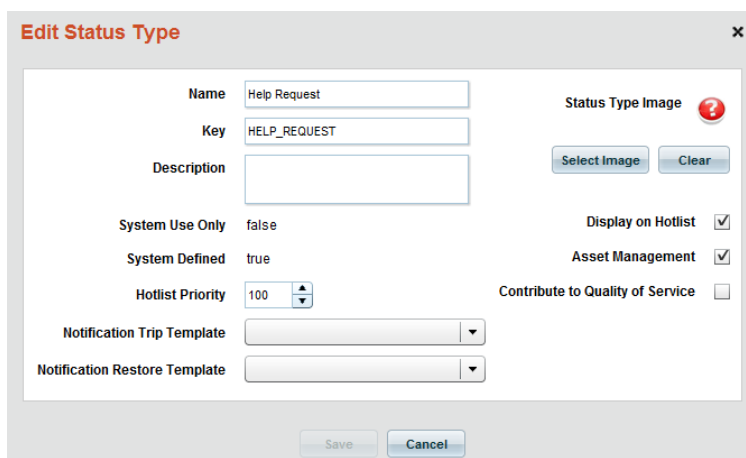
FIG. 408 New Status Type Added to Status Types List

Editing a Status Type

1. Select **Status Types** under *Asset Configuration* in the Configuration menu to open the *Status Types* page (see FIG. 406 on page 251).
2. Select the Status Type that you want to edit.
3. Click the **Edit** button. This action invokes the *Edit Status Type* dialog (FIG. 409):

FIG. 409 Edit Status Type dialog

4. Edit the fields in this dialog as desired.
5. Click **Save** to save your changes and close this dialog.

Deleting a Status Type

NOTE: *RMS will not allow you to delete Status Types that are currently referenced in the System.*

1. Select **Status Types** under *Asset Configuration* in the Configuration menu to open the *Status Types* page (see FIG. 406 on page 251).
2. Select the Status Type that you wish to delete.
3. Click **Delete**.
4. The system will prompt you to verify this action before the Status Type is deleted, via the *Delete Confirmation* dialog (FIG. 410):

FIG. 410 Delete Confirmation dialog - Status Type

5. Click **Yes** to proceed.
6. The deleted Status Type is removed from the *Status Types* list.

Searching For Status Types

Use the *Search* tool in the Status Types window to search for a specific Status Type (FIG. 411).

FIG. 411 Status Types Window - Search window

Asset Types

Assets can be assigned as *Asset Types* to group common assets, extend metadata asset type definitions, and to provide generic asset images based on type. Select **Asset Types** (under *Asset Configuration*) to open the *Asset Types* page. This page has two tabs: **Asset Type** and **NetLinx Device Type.**

Asset Types - Asset Types Tab

Use the options in the **Asset Types** tab to configure and manage Asset Types (FIG. 412):

FIG. 412 Asset Types page (Asset Type tab)

Asset Types (Asset Types tab) Options	
Search	Use this field to perform a search for Asset Types. See *Searching for Asset Types* on page 258.
Add	Click to add a new Asset Type entry. This action invokes the *Asset Type Editor* dialog. Use this dialog to define the new Asset Type entry. See *Adding a New Asset Type* on page 256.
Edit	Click to edit the selected Asset Type entry, via the *Status Type Editor* dialog. • This option is only enabled when an Asset Type entry is selected. • See *Editing an Asset Type* on page 257.
Delete	Click to delete the selected Asset Type entry. The System will prompt you to verify this action before the selection is deleted - Click **Yes** in the *Delete Confirmation* dialog to proceed. • This option is only enabled when an Asset Type entry is selected. • See *Deleting an Asset Type* on page 257.
Asset Types Table	The table on this page provides a listing of all Assets Types available in the RMS System. The columns in this table present data for each Asset Type, as defined in the *Edit Status Type* dialog. • See *Editing an Asset Type* on page 257.

NOTE: *Changes made on this page will take effect when you leave the page.*

Asset Types - NetLinx Device Types Tab

The **NetLinx Device Types** tab provides a listing of all pre-defined NetLinx device types. Use the options in the **NetLinx Device Types** tab to configure and manage NetLinx device types (FIG. 413):

FIG. 413 Asset Types page (NetLinx Device Types tab)

Asset Types (NetLinx Device Types) Options	
Search	Use this field to perform a search for NetLinx Device Types.
Edit	Click to edit the selected NetLinx Device Type entry. via the *Edit NetLinx Device Type* dialog. • This option is only enabled when a NetLinx Device Type entry is selected. • See *Editing NetLinx Device Types* on page 258.
NetLinx Device Type Table	The table on this page provides a listing of all NetLinx Device Types available in the RMS System. • **Name**: Each (pre-defined) NetLinx Device Type is listed in this column. • **Asset Type**: The (pre-defined) Asset Type for each NetLinx Device Type is listed in this column.

Adding a New Asset Type

1. Select **Asset Types** under *Asset Configuration* in the Configuration menu to open the *Asset Types* page (see FIG. 412 on page 255).

2. In the **Asset Type** tab, click the **Add** button to open the *Asset Type Editor* dialog (FIG. 414):

FIG. 414 Asset Type Editor dialog

NOTE: *The only required entry in this dialog is "Name" and "Key". However, provide as much information as possible for each Asset Type so that RMS can provide this information to users.*

3.   Fill in the fields in this dialog to define the new asset type;

Asset Type Editor Dialog Options	
Name	Enter a descriptive name for the new asset type in the text field.
Description	Enter a brief description of the new asset type in the text field.
Key	Enter a key for the new asset type in the text field. The Key entry allows this Status Type to be programmatically hooked to a threshold. Typically, the Key entry should be the same as the *Name* entry, but in lowercase and without spaces. For example, the Key for the "Audio Conferencer" Asset Type is "audioconferencer".
System Defined	This read-only field indicates wether this Asset Type is one of the pre-defined Asset Types that come with RMS Enterprise (*True* or *False*).
Runtime Watts	Enter the current draw (Watts) for this Asset Type when the device is active in this field. *Note: Runtime and Standby Watts specifications have to be provided by the Manufacturer of each asset type.*
Standby Watts	Enter the current draw (Watts) for this Asset Type when the device is in standby mode in this field. *Note: Runtime and Standby Watts specifications have to be provided by the Manufacturer of each asset type.*
Asset Type Image	• *Select Image*: Click to open the *Select file to upload* dialog, to locate and select an image file to associate with this parameter status type. Supported image types: JPG, JPEG, GIF and PNG. Max display size = 32 x 32 (pixels). • *Clear*: Click to clear the Status Type Image. *Note: RMS will scale the image to the proper resolution for the image category. For best results, prepare the image to be 32 x 32 pixels before uploading, to avoid scaling or stretching of the image when it is displayed in RMS.*

4.   Fill in the fields in this dialog:

5.   Select an image to associate with this asset type:
    a.   Click **Select Image**. This action invokes the *Select File to Upload* dialog.
    b.   Locate and select an image file to associate with this Asset Type.
    ● Supported image types: JPG, JPEG, GIF and PNG.
    ● The *Asset Image* window is 125 x 125 pixels.
    ● A preview of the selected image is displayed in the preview window.
    ● Click **Clear** to remove the Asset Type image.

    NOTE: *RMS will scale the image to the proper resolution for the image category. For best results, prepare the image to be 125 x 125 pixels before uploading, to avoid scaling or stretching of the image when it is displayed in RMS.*

6.   Click **OK** to save your changes and close this dialog.

7.   The new asset is listed in the *Asset Types* list (FIG. 415).

Image	Name	Description	Key	System Defined	Runtime Watts	Standby Watts
	New Asset	New Asset Description	New Asset Key	☐	12	2
	Pool Spa		PoolSpa	✓	0	0

FIG. 415 New Asset Type Added to Asset Types List

Editing an Asset Type

1.   Select **Asset Types** under *Asset Configuration* in the Configuration menu to open the *Asset Types* page (see FIG. 412 on page 255).

2.   In the **Assets Type** tab, select the Asset Type that you want to edit.

3.   Click the **Edit** button to open the *Asset Type Editor* dialog (see FIG. 414 on page 256).

4.   Edit in the fields in this dialog as desired.

5.   Click **OK** to save your changes and close this dialog.

Deleting an Asset Type

NOTE: *RMS will not allow you to delete Asset Types that are currently referenced in the System.*

1.   Select **Asset Types** under *Asset Configuration* in the Configuration menu to open the *Asset Types* page (see FIG. 412 on page 255).

2.   In the **Assets Type** tab, select the Asset Type that you want to delete.

3.   The system will prompt you to verify this action before the Asset Type is deleted, via the *Delete Confirmation* dialog (FIG. 416):

4.   Click **Yes** to proceed.

5.   The deleted Asset Type is removed from the *Asset Types* list.
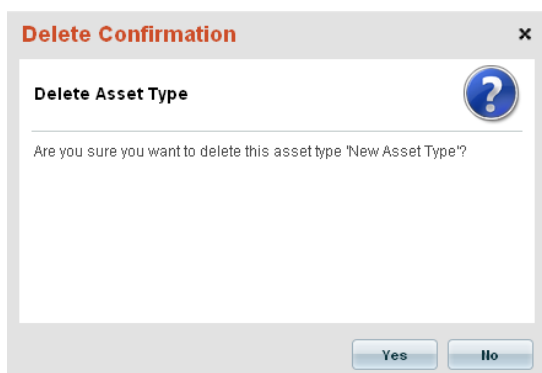
FIG. 416 Delete Confirmation dialog - Asset Type

Searching for Asset Types

Use the *Search* tool in the Asset Types window to search for a specific Asset Type (FIG. 417).

FIG. 417 Asset Types Window - Search window

This search tool searches across the data columns displayed in the Status Type window (*Name*, *Description*, *Key*).

Editing NetLinx Device Types

1. Select **Asset Types** under *Asset Configuration* in the Configuration menu to open the *Asset Types* page.

2. In the **NetLinx Device Types** tab (FIG. 413 on page 256), select the NetLinx Device Type that you want to edit.

3. Click the **Edit** button to open the *Edit NetLinx Device Type* dialog (FIG. 418):
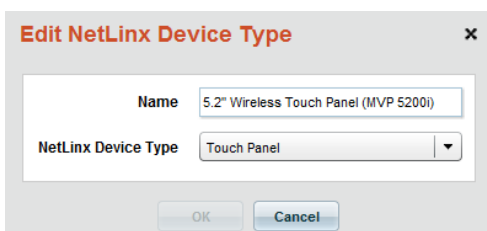
FIG. 418 Edit NetLinx Device Type dialog

4. To edit the name of the selected NetLinx Device Type, type directly in the **Name** field.

5. To change the device type, select from the **NetLinx Device Type** drop-down menu.

6. Click **OK** to save your changes and close this dialog.

Parameter Bar Graphs

Bar Graphs can be assigned to Asset Parameters of numeric type (ie: Lamp Hours), to graphically represent their current value

- Bar Graphs can be percent based or a specific range of values. The Bar Graph Key allows new NetLinx Masters to register a parameter with a Bar Graph directly.
- Asset Parameters allow Bar Graph selection in the Asset Management portion of the application.

Select **Parameter Bar Graphs** under *Asset Configuration* in the Configuration menu to open the *Parameter Bar Graphs* page (FIG. 419):

FIG. 419 Parameter Bar Graphs page

Use the options in this page to configure and manage the Bar Graphs that can be applied to Asset Parameters that are of the *Number* or *Float* data type (see *Parameter Bar Graphs* on page 259):

Parameter Bar Graphs Options	
Add	Click to add a new Bar Graph entry. This action invokes the *Edit Bar Graph* dialog. Use this dialog to define the new Bar Graph entry. See *Adding a New Bar Graph* on page 259.
Edit	Click to edit the selected Bar Graph entry, via the *Edit Bar Graph* dialog. • This option is only enabled when a Bar Graph entry is selected. • See *Editing a Bar Graph* on page 261.
Delete	Click to delete the selected Bar Graph entry. The System will prompt you to verify this action before the selection is deleted - Click **Yes** in the *Delete Confirmation* dialog to proceed. • This option is only enabled when a Bar Graph entry is selected. • See *Deleting a Bar Graph* on page 261.
Bar Graph Table	The table on this page provides a listing of all Bar Graphs available in the RMS System. The columns in this table present the properties for each Bar Graph, as defined in the *Edit Bar Graph* dialog (see FIG. 420 on page 260):

NOTE: *Changes made on this page will take effect when you leave the page.*

Adding a New Bar Graph

1. Select **Parameter Bar Graphs** under *Asset Configuration* in the Configuration menu to open the *Parameter Bar Graphs page* - see FIG. 419 on page 259).

2. Click **Add** to invoke the *Edit Bar Graph* dialog (FIG. 420):

FIG. 420 Edit Bar Graph dialog

3. Enter a *Name* and *Description* in the first two text fields.

4. Enter a *Bar Graph Key*. The *Bar Graph Key* is a symbol (text) that SDK programmers can use to associate a defined Bar Graph to a parameter at the time of asset registration (i.e. "battery.level").

5. Specify a range for this bargraph:

    By default, the *Percent Based* option is selected. With this option selected, the Min and Max fields are set to 0 and 100, and are read-only (as shown in FIG. 420).

    To define custom limits other than 0-100:

    a. De-select the *Percent Based* option to enable the **Min** and **Max** fields (FIG. 421):

FIG. 421 Edit Bar Graph dialog (Min and Max fields)

    b. Enter the *Min* and *Max* limits for this Bar Graph.

    c. Click **Recalibrate** to reset the preview bargraph in the dialog to represent the new limits. FIG. 422 shows the preview Bar Graph set with a range of 0 - 50:

FIG. 422 Edit Bar Graph dialog (Min and Max fields set to "0" and "50")

6. Specify the colors to use in this Bar Graph:

    By default, Bar Graphs are configured to display in two colors - green (for the 0-50% region) and yellow (for the 50-100% region), as shown in FIG. 422.

    To define custom colors to for each region in the bar graph:

    a. Click and drag the slider to beneath the Bar Graph to the point on the graph that you want to see a change in color. By default, the slider is positioned at the 50% point on the Bar Graph. FIG. 423 shows that the slider has been moved to the 90% point:

Slider moved to the 90% point

FIG. 423 Edit Bar Graph dialog (Min and Max fields set to "0" and "50")

    b. Click inside the preview Bar Graph, within one of the color fields. This invokes the Color Selector popup window (FIG. 424):
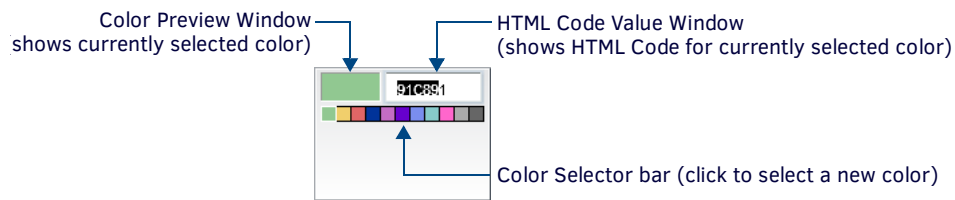
FIG. 424 Edit Bar Graph dialog - Color Selector popup window

    c.   Click in the Color Selector bar to select a new color for the selected region of the Bar Graph.

        Alternatively, enter the HTML code for the new color in the HTML Code Value window. Use this feature to add custom colors to the Color Selector bar.

        FIG. 425 shows that the first region of the Bar Graph (representing 0-90%) has been changed from green to cyan:
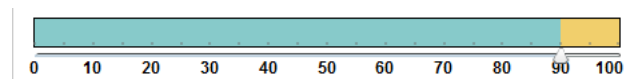
FIG. 425 Edit Bar Graph dialog (0-90% region set to Cyan)

7.   Separate the Bar Graph into additional regions if necessary:
    a.   Click **Add** to add a new slider to the Bar Graph. The new slider is always placed initially at the far-left edge of the graph.
    b.   Move the new slider to a point in the Bar Graph to define a new range (which will be represented by another color). FIG. 426 shows that a new slider has been added, and moved to the 50% point:
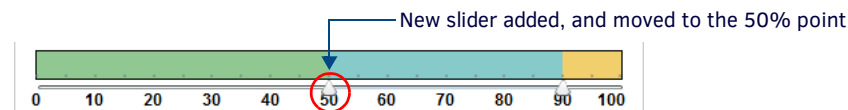
FIG. 426 Edit Bar Graph dialog - new region (0-50% in green)

        Note that new regions are always colored green by default. Click in the new region and change it's color via the Color Selector popup window (if desired), as described above.

    c.   Repeat steps 6-7 to define additional colored regions in the bargraph, as desired. FIG. 427 shows the bargraph with on more region (0 - 20%) defined (in red):
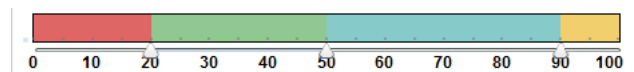
FIG. 427 Edit Bar Graph dialog - new region (0-20% in red)

8.   Click **OK** to save your changes and close this dialog. The new Parameter Bar Graph is listed in the Bar Graph table.

Editing a Bar Graph

1.   Select **Parameter Bar Graphs** under *Asset Configuration* in the Configuration menu to open the *Parameter Bar Graphs page* - see FIG. 419 on page 259).
2.   Click **Edit** to invoke the *Edit Bar Graph* dialog (FIG. 420 on page 260).
3.   Edit the fields in this dialog as desired.
4.   Click **OK** to close the dialog and save your changes.

Deleting a Bar Graph

1.   Select **Parameter Bar Graphs** under *Asset Configuration* in the Configuration menu to open the *Parameter Bar Graphs page* - see FIG. 419 on page 259).
2.   Select a Bar Graph in the Bar Graphs table.
3.   Click **Delete**.
4.   The program will prompt you to verify this action (FIG. 428):
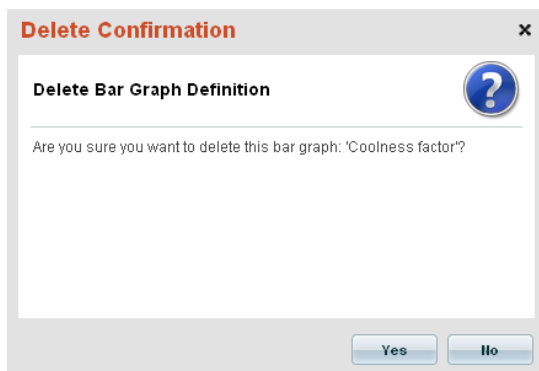
FIG. 428 Delete Confirmation dialog - Delete Bar Graph Definition

5.   Click **Yes** to proceed.

RFID Asset Tracking

RMS provide asset tracking and asset location monitoring using AMX Anterus RFID readers and RFID tags.

NOTE: *RFID historical reporting is automatically tracked with the system reporting data. RFID tracking records are part of the RMS reporting system and are purged along with reporting aging clean up maintenance tasks. See the Reports (HTML UI) section on page 45 for details.*

Select **RFID Asset Tracking** under *Asset Configuration* in the Configuration menu to open the *RFID Asset Tracking* page (FIG. 429):
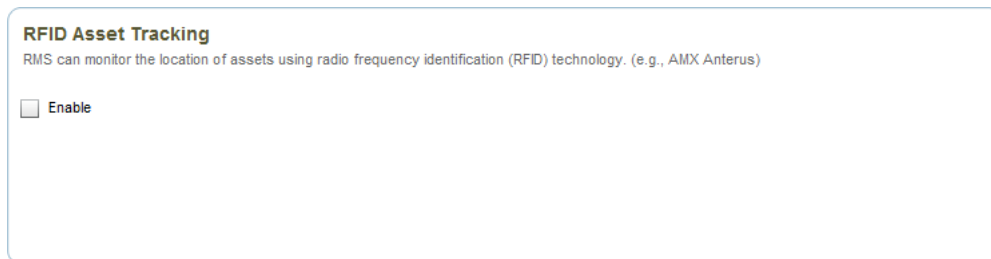
FIG. 429 RFID Asset Tracking page

The **Enable** option on the *RFID Tracking* page allow you to enable/disable RFID device tracking, and specify how to RFID historical reporting.

Enabling RFID Tracking

Enabling the RFID feature set will expose RFID settings on the Asset management page and enable RMS clients to send RFID communication messages to the RMS server
- If disabled, the RMS GUI will not display RFID asset configuration, RFID management pages, or RFID based reports.
- If disabled, RMS client will not transmit RFID updates to the RMS server.
- Default = *Disabled*.

1.   Select **RFID Asset Tracking** under *Asset Configuration* in the Configuration menu to open the *RFID Asset Tracking page* - see FIG. 429 on page 262).
2.   Select the **Enable** checkbox.

NOTE: *Changes made on this page will take effect when you leave the page.*

RFID Tag Assignments

Select **RFID Asset Assignments** under *Asset Configuration* in the Configuration menu to open the *RFID Tag Assignments* page (FIG. 430):

RFID Tag Assignments							
Assign | Unassign | Delete							Show Unassigned Only
Tag ID ▲	**Signal Strength**	**Battery Level**	**Last Update**	**Detected Location**	**Reader Address**	**Asset**	**Location**	**Enabled**
100173	0	0	Oct 13, 2015 7:23 PM	RFID-r26c01		Disc Device	djohannes3100	☑
100acc	88	–2147483648	Oct 14, 2015 2:37 PM	djohannes3100	108:1:64			☐
100b58	0	0	Oct 14, 2015 2:56 PM	djohannes3100		Document Camera	djohannes3100	☑
2001ba	152	–2147483648	Oct 14, 2015 2:30 PM	RFID-r26c01	109:1:534	Video Projector	djohannes3100	☑
200222	160	–2147483648	Oct 14, 2015 2:59 PM	RFID-r26c01	109:1:534	DVD	Room 101	☑
20022a	148	–2147483648	Oct 13, 2015 6:47 PM	RFID-r26c01	109:1:534	Display	Room 401	☐
200611	0	0	Oct 13, 2015 6:54 PM	djohannes3100		Display	Sim Group A	☑
200631	0	0	Oct 13, 2015 6:54 PM	djohannes3100		Simulated Disc Device	IDStress-01	☑
200637	0	0	Oct 13, 2015 6:55 PM	djohannes3100		Simulated Disc Device	IDStress-02	☑
20063b	120	–2147483648	Oct 14, 2015 9:59 AM	RFID-r26c01	109:1:534			☐
20065b	0	0	Oct 14, 2015 11:36 AM	RFID-r26c01		Disc Device	RFID-r26c01	☐
20066a	118	–2147483648	Oct 13, 2015 6:47 PM	RFID-r26c01	109:1:534			☐
2007b0	104	–2147483648	Oct 14, 2015	djohannes3100	108:1:64			☐

Items 1 to 17 of 17. Page 1 of 1 |◄ ◄ ► ►| Go to Page: 1 ▼

FIG. 430 RFID Tag Assignments page

This page lists all known (detected) AMX Anterus RFID tags along with their current status and location. This listing includes the ability to search the list using the *Search* tool in the upper right corner of the page. The options on the *RFID Tag Assignments page* allow you to manage RFID Tag Assignments:

RFID Tag Assignments Options	
Search	Use this field to perform a search for RFID Tag ID names. See *Searching For RFID Tag IDs* on page 264.
Assign	Click to add a new RFID Tag Assignment entry. This action invokes the *Add RFID Tag Assignment* dialog. Use this dialog to define the new RFID Tag Assignment entry. See *Assigning a RFID Tag to an Asset* on page 263.
Unassign	Click to edit the selected RFID Tag Assignment entry, via the *Edit RFID Tag Assignment* dialog. • This option is only enabled when a RFID Tag Assignment entry is selected. • See *Un-assigning a RFID Tag From an Asset* on page 264.
Delete	Click to delete the selected RFID Tag Assignment entry. The System will prompt you to verify this action before the selection is deleted - Click **Yes** in the *Delete Confirmation* dialog to proceed. • This option is only enabled when a RFID Tag Assignment entry is selected. • See *Deleting an RFID Tag Assignment* on page 264.

NOTE: *Changes made on this page will take effect when you leave the page.*

Assigning a RFID Tag to an Asset

1. In the *RFID Tag Assignments* list, select a Tag that is not currently assigned to an Asset.
2. Click the **Assign** button. This opens the *Edit RFID Tag* dialog (FIG. 431):
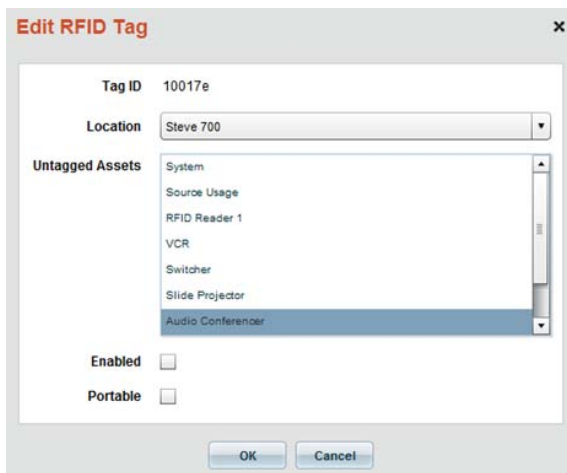
FIG. 431 Edit RFID Tag dialog

3. Select an available Location from the **Location** drop-down menu. This selection populates the *Untagged Assets* list.

4. Select the Asset that will be associated with this Tag ID from the **Untagged Assets** list.

5. Click **Enabled** to enable this RFID Tag ID.

6. Click **Portable** to make RFID Tag tracking for this Asset portable. When enabled, the Asset will automatically move to different locations depending on which Anterus RFID Reader has the strongest signal strength (RSSI).

    NOTE: *If the Portable option is not selected, RMS will not automatically relocate the tagged asset.*

7. Click **OK** to save your changes and close this dialog.

Un-assigning a RFID Tag From an Asset

1. In the *RFID Tag Assignments* list, select a Tag that is assigned to an Asset.

2. Click the **Unassign** button.

Deleting an RFID Tag Assignment

1. In the *RFID Tag Assignments* list, select a Tag that is not currently being detected by any RFID reader.

2. Click **Delete** to permanently remove the RFID tag record and all it's associated history from the RMS system.

3. The program will prompt you to verify this action before the RFID Tag is deleted (FIG. 432):

FIG. 432 Delete Confirmation - Delete RFID Tag dialog

4. Select **Yes** to proceed.

Searching For RFID Tag IDs

Use the *Search* tool in the *RFID Tag Assignments* page to search for a specific RFID Tag ID name (FIG. 433).
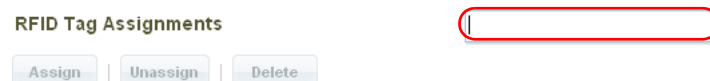
FIG. 433 RFID Tag Assignments page - Search window

Update Manager Configuration (Classic UI)

Overview

RMS Transporter is a utility for RMS Enterprise that allows the simultaneous transfer of firmware to all devices on your system's network for a given firmware file. This ensures that all devices are updated to the latest version at one time rather than making multiple trips to perform system upgrades. This tool also allows viewing of transfers to all devices in real time, so you can see at a glimpse the status of all file transfers, as well as the status of files that were transferred in previous sessions. Detailed log files are also available which allow viewing of historical data for each system or installation, whether it be one small room, or a campus wide system.

The RMS Transporter installation file (RMSTransporter.exe), must be installed in order to add *Update Manager* functionality to RMS Enterprise.The RMS Transporter installation file (*RMSTransporter.exe*) is available to download from www.amx.com. Refer to the *RMS Transporter Installation Manual* for instructions.

NOTE: *If RMS Transporter has not been installed, RMS Enterprise will prompt you to install RMS Transporter, when any of the RMS Transporter Configuration options are selected.*

The options in the **Update Manager Configuration** category of the *Configuration* menu allow you to view and manage AMX Device Credentials, Transporter Assignments and Transporter Management (FIG. 434):

FIG. 434 Configuration menu - Update Manager Configuration options

NOTE: *The Configuration pages do not utilize an Apply button. Changes made on the Configuration pages are saved when you navigate away from the page on which the changes were made.*

NOTE: *To access the RMS Classic UI described in this section, select "Classic UI" from the RMS Enterprise HTML interface menu bar.*

AMX Device Credentials

In order for Update Manager to work, communication must be established between the Transport Server and each AMX device that will receive a firmware file. If the AMX devices in the system require login credentials, the device credentials need to be entered.

Use the options on the *AMX Device Credentials* page to enter *system-wide* credentials in the case where your AMX devices have security enabled. These system-wide credentials will be saved and applied to all AMX devices in the system. Use this option when most or all of the AMX devices in the system require login credentials, and most or all device share the same credentials.

You can also enter individual AMX device credentials via the *Edit* option in the *Client Gateway* page (see *Entering/Editing AMX Device Credentials* section on page 101 for details).

NOTE: *The device credentials entered on this page are not the credentials used to connect your NetLinx master to the RMS Server.*

Select **AMX Device Credentials** under *Update Manager Configuration* in the *Configuration* menu to open the *AMX Device Credentials* page (FIG. 435):

FIG. 435 AMX Device Credentials page

AMX Device Credentials Page Options	
No Credentials Required	Select this option if no credentials are required to connect to AMX devices in the system. Note that this is the default setting, and when this option is selected, the Username and Password fields are disabled.
Credentials	Select this option to apply login credentials to the selected device, and enable the *Username* and *Password* fields.
Username	Enter the Username required to connect to the AMX devices in the system.
Password	Enter the Password required to connect to the AMX devices in the system.

Transporter Assignments

In order to use Update Manager, each Location Group needs to be assigned a *Transporter*. Transporters are defined in the Update Manager Configuration application - refer to the *Update Manager Installation Guide* for details on creating a Transporter.

NOTE: *Multiple Groups can use the same Transporter, but each Group must have a Transporter assigned via the Transporter Assignments page.*

Select **Transporter Assignments** under *Update Manager Configuration* in the *Configuration* menu to open the *Transporter Assignments* page (FIG. 435):

FIG. 436 Transporter Assignments page

Transporter Assignments Page Options	
Groups window	The Groups window indicates all Location Groups currently defined in the system. Select a Group to assign a Transporter.
Transporter Menu	Choose a Transporter from the drop-down menu to assign to the selected Location Group.

Removing Transporter Assignments

1. Select the Group for which you want to remove the current Transport assignment.

2. In the *Transporters* menu, select the blank entry at the top of the list (FIG. 437):
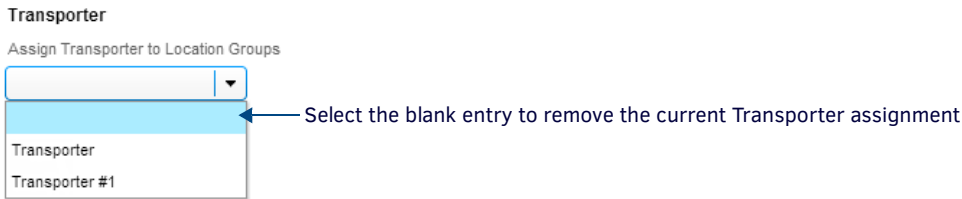
FIG. 437 Transporter Assignments page - Transporter menu

Transporter Management

Use the *Transporter Management Settings* page to delete Transporters from the system. Select **Transporter Management** under *Update Manager Configuration* in the *Configuration* menu to open the *Transporter Management* page (FIG. 438):
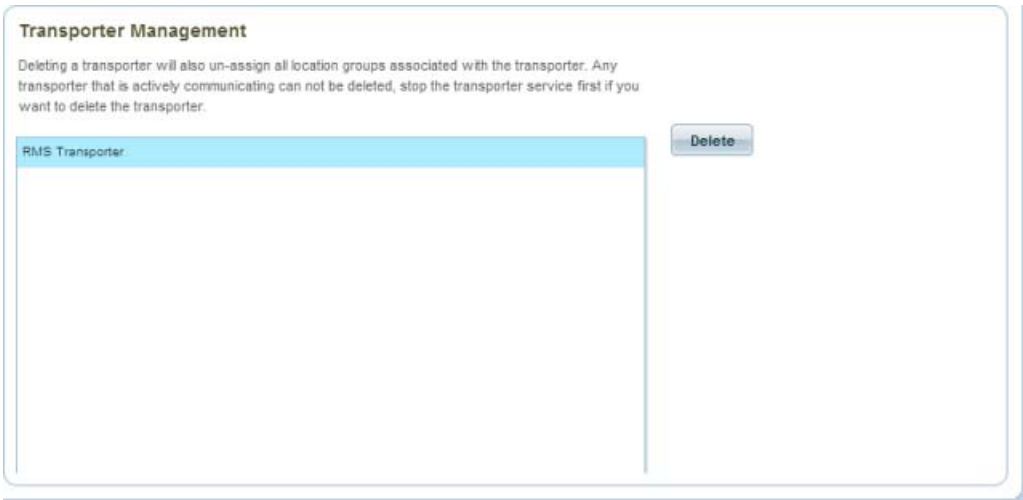
FIG. 438 Transporter Management page

Transporter Management Page Options	
Transporters List	The main window on this page is the Transporters list, which indicates every Transporter currently configured for this system.
Delete	Click to permanently delete the selected Transporter from the system.

- Deleting a Transporter will also un-assign all Location Groups associated with the Transporter.
- Any Transporter that is actively communicating can not be deleted. In this case, stop the Transporter service first in order to delete the transporter.

Stopping the Transporter Service

The Transporter Service can be managed like any other Service on the Transporter Server: via the *Stop*, *Start* and *Restart* options on the **Computer Management > Services and Applications** page.

To manually stop the Transporter Service, open the **Services and Applications** page, select the *RMS Enterprise Transporter* Service and select **Stop**.

Use the **Start** and **Restart** options to manually start or restart the service.

Auto Staging Settings

Use the *Auto Staging Settings* page to configure how RMS will automatically identify and retrieve firmware files from the AMX InConcert Resource Center on a daily basis.

NOTE: *Auto Staging checks for updated firmware, and automatically downloads firmware files that represent updates to the firmware currently detected on AMX devices in the RMS system. However, this feature does not automatically transfer firmware files to devices. The actual file transfers are managed via the options in Update Manager. Refer to the Update Manager (HTML UI) section on page 28 for details.*

Select **Auto Staging** under *Update Manager Configuration* in the *Configuration* menu to open the *Auto Staging Settings* page (FIG. 439):

FIG. 439 Auto Staging Settings page

Use the options on this page to configure

Auto Staging Settings Options	
Auto Download Firmware from AMX	Select this option to enable the auto-download function in Update Manager. By default, this option is selected (auto-updates enabled). Note that if this option is de-selected, then other settings in this page are disabled.
Start Time	With *Auto Download Firmware from AMX* selected, use the *Start Time* controls to specify the time at which Update Manager will connect to the AMX InConcert Resource Center to check for updates daily, and download new firmware files to the RMS Transporter server.
	Use the up and down arrows to adjust the hour and minute settings, and click AM or PM to set the time to start checking for updates.
	Note that the time settings configured here are relative to the Application Time Zone (see below).
Application Time Zone	This read-only field indicates the current Time Zone setting for RMS (including Update Manager).
	Note: The Application Time Zone is set in the System Configuration > Application Time Zone page. See the Application Time Zone section on page 211 for details.
Last Download Time	This read-only field indicates the time of the most recent firmware download.
	Note that the time indicated here is relative to the Application Time Zone.
Download Now	Click to manually download the "staged" firmware files immediately (as opposed to waiting for the Start Time to begin downloading files).

Configuring Auto Staging Settings

1. In the *Configuration* menu, under *Update Manager Configuration*, select **Auto Staging**.
2. Verify that the **Auto Download Firmware from AMX** option is selected.
3. To set the **Start Time** for Auto Staging operations, use the up and down arrows to adjust the hour and minute settings, and click AM or PM to set the time to start checking for updates each day.

Manually Downloading Firmware Files

1. Click **Download Now** to manually download firmware files immediately (as opposed to waiting for the *Start Time* to begin downloading files).
2. Update Manager presents a notification dialog that indicates that this download operation may take some time - click **Close** to close this dialog (FIG. 440):
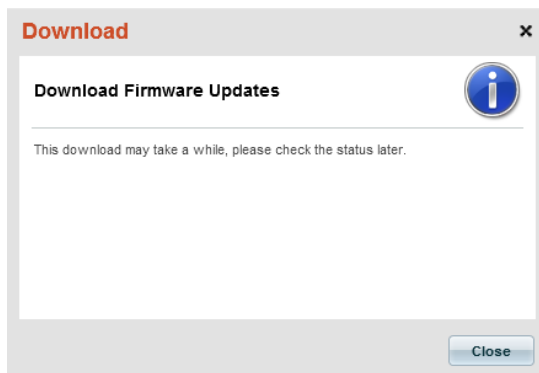
FIG. 440 Download Firmware Updates notification dialog

Note that the time required for downloading firmware files will depend on both the number of files being downloaded and the size of each file.

Help / Diagnostics (Classic UI)

Overview

The options presented in the **Help** menu provide access to RMS Documentation, Online Resources and System Information, as well as Diagnostics options (FIG. 441).

FIG. 441 Help Drop-Down Menu

RMS Documentation

The options under **RMS Documentation** in the *Help* menu (FIG. 442) provide access to online documentation:

FIG. 442 Help > RMS Documentation

Click on any of these links to access the following online documents (PDF):

- RMS Administrator's Guide

NOTE: *All RMS Enterprise documentation is also available to view/download from www.amx.com.*

Online Resources

The options under **Online Resources** in the Help menu (FIG. 443) provide access to online resources for RMS:

FIG. 443 Help > Online Resources

Click **Visit AMX Online** to access www.amx.com in a new browser window.

RMS System Information

The options under **RMS System Informations** in the *Help* menu (FIG. 444) provide access to online resources for RMS:

FIG. 444 Help > RMS System Information

Click on any of these links to access the following system information documents:

RMS Readme (Release Notes)

Click to open the current release notes file (HTML) in a new browser window.

RMS Licensing Information

Click to open the *RMS Licensing Information* dialog (FIG. 445):
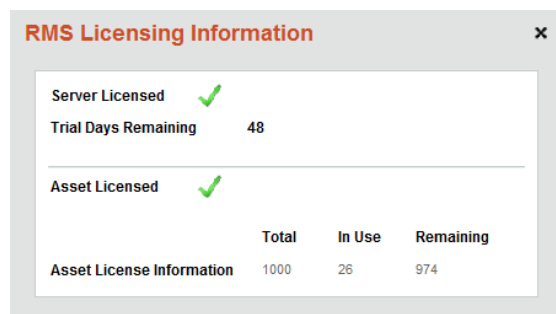
FIG. 445 RMS Licensing Information dialog

About Resource Management Suite

Click to open the *About* dialog, which indicates the versions of RMS and the RMS Database currently installed (FIG. 446).
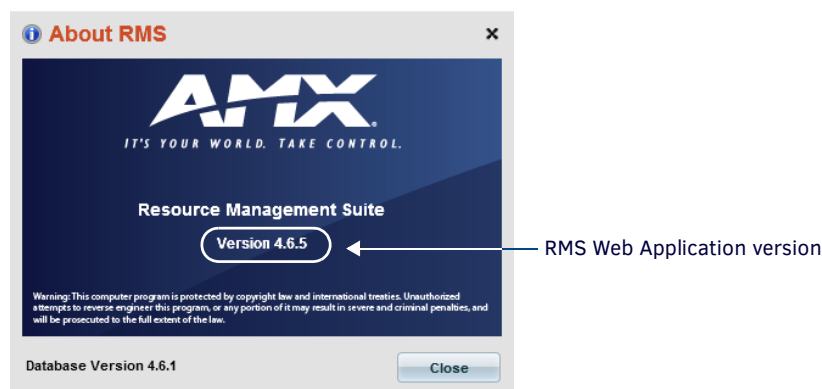
FIG. 446 Help > RMS System Information

Diagnostics

To provide engineering and technical support of the RMS system, RMS provides internal system diagnostics and logging capabilities. This allows logging of internal subsystems and runtime diagnostics information about the RMS application and its health. The options under **Diagnostics** in the *Help* menu (FIG. 447) provide access to the diagnostics options for RMS:
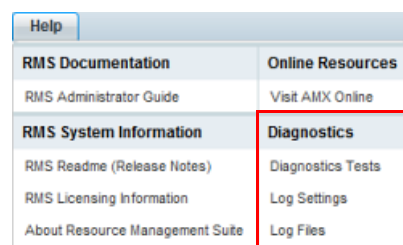
FIG. 447 Help > Diagnostics

Select an Diagnostics option from the Help menu to access the *Diagnostics* page. This page consists of three tabs, as described in the following sections:

Diagnostics Page - Diagnostics Tests Tab

Select **Diagnostics Tests** under *Diagnostics* in the Help menu to open the *Diagnostics Tests* tab of the Diagnostics page (FIG. 448):

FIG. 448 Diagnostics page – Diagnostics Tests tab

Use the options on this page to run various diagnostics to determine if the RMS server/server is configured property and contains the necessary prerequisites to run the RMS server and web application. The options on this page are described below:

Diagnostics - Diagnostics Tests tab Options	
Run All Diagnostics Tests:	Click to run each diagnostic test, in the order that they are listed. As each test is completed, the results are displayed in the *Result*, *Details* and *Last Run Time* columns.
Run Selected Diagnostics Tests:	Click to run only the selected diagnostic test(s). As each test is completed, the results are displayed in the *Result*, *Details* and *Last Run Time* columns.
Refresh:	Click to refresh the table. Refreshing the table will clear the *Result*, *Details* and *Last Run Time* columns.
Diagnostics Test List:	• *Test*: This column indicates the name of each Diagnostic Test. • *Result*: This column indicates the result of each Diagnostic Test that has run since the *Refresh* button was clicked. • *Details*: This column provides additional information on the results of each Diagnostic Test that has run since the *Refresh* button was clicked. • *Last Run Time*: This column indicates the time at which each test was run.

Diagnostics Page - Log Settings Tab

The RMS Enterprise server is automatically configured to log all errors and fatal messages to the server log files. Select **Help > Diagnostics > Log Settings** to open the **Log Settings** tab of the *Diagnostics* page (FIG. 449):

FIG. 449 Diagnostics page - Log Settings tab

Use the options presented in the **Log Settings** tab of the *Diagnostics* page to set explicit log levels for various exposed packages inside the server. The options in this tab are described below:

Diagnostics - Log Settings tab Options	
Set All Levels To	Use this option to set a common Logging Level to all Packages. Click the down arrow to access a drop-down menu of Logging Levels. • To set Logging Levels for individual Packages, use the *Level* drop-down menus in the Logging Settings table. • See *Logging Levels* on page 273 for a description of each Logging Level option.
Log Settings table	The table on this page provides a listing of all Packages currently in the database, indicating the current Logging Level setting for each. • See *Logging Levels* on page 273. • See *Configuring Logging Settings* on page 274. The columns in this table present the following data for each Package: • *Level*: The current logging level applied to each Package (click to access drop-down menu). • *Package*: The name of each package (read-only). • *Description*: Text description of each Package/Logging Level (read-only).
Apply Changes	Click to apply all changes made in the *Diagnostics* page - **Log Settings** tab.
Reset Changes	Click to discard all changes made in the *Diagnostics* page - **Log Settings** tab.

Logging Levels

Click the down arrow within any cell in the *Level* column of the Logging Settings table to select from a drop-down menu of available logging levels (FIG. 450):
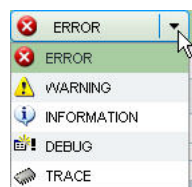
FIG. 450 Logging Levels drop-down

Logging Levels	
• ERROR:	This level designates error events that might still allow the application to continue running.
• WARNING:	This level designates potentially harmful situations.
• INFORMATION:	This level designates informational messages that highlight the progress of the application at coarse-grained level.
• DEBUG:	This level designates fine-grained informational events that are most useful to debug an application.
• TRACE:	This level designates finer-grained informational events than the DEBUG.

Configuring Logging Settings

To set logging settings for any Package listed in the Logging Settings table (*Diagnostics* page - **Logging Settings** tab):

1. In the *Package* column, select a Package.
2. In the *Level* column, select the desired Logging Level from the drop-down menu.
3. In the *Description* column, enter a text description of this Package/Logging Level (optional).
4. Click **Apply Changes**.

Diagnostics Page - Log Files Tab

Select **Help > Diagnostics > Log Files** to open the **Log Files** tab of the *Diagnostics* page (FIG. 451):

FIG. 451 Diagnostics page - Log Files tab

Use the options on this page to manage and download RMS log files:

Diagnostics - Log Files tab Options	
Log Files table	The table on this page provides a listing of all Log Files currently in the database. The columns in this table present basic file data for each Log File.
Delete	Click to delete the selected Log File(s) from the RMS server (see *Deleting Log Files* on page 275).
Refresh	Click to refresh the Log Files table.

Downloading Log Files

1. Select a Log File in the Log Files table, and click the **Download icon** (FIG. 452) to download the selected file from the RMS Server to your PC.

FIG. 452 Download Icon (Log Files Table)

NOTE: *Log Files can only be downloaded individually (multiple-selection is not supported).*

2. This action invokes the *Select location for download* dialog. Specify a target directory for the Log File and click **Save**.

3. The system will indicate when the download is complete in the *Download Log File* dialog (FIG. 453):
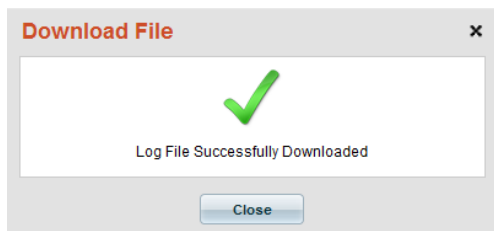
FIG. 453 Download File dialog

4. Press **Close**.

Deleting Log Files

Select a Log File in the Log Files table, and click the **Delete** button to delete the selected file from the RMS Server.

- To select multiple Log Files, press and hold the Ctrl key while selecting.
- To select a range of Log Files, click to select the first file, press and hold Shift key, and select the last file in the desired range.

The system will prompt you to verify this action before the file is deleted from the server, via the *Delete Confirmation* dialog (FIG. 454):
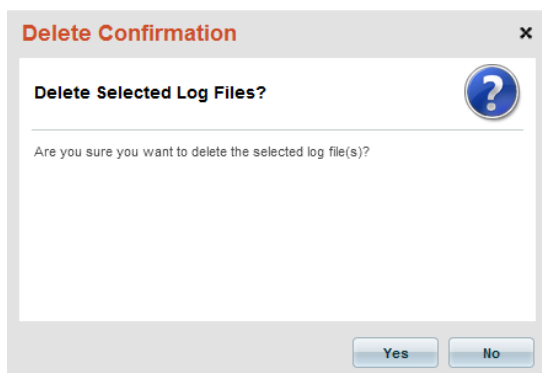
FIG. 454 Delete Confirmation dialog

- Click **Yes** to proceed.
- Click **No** to close the dialog without deleting the Log File(s).

RMS Utility Toolbox

The RMS Utility Toolbox is provided on the *Diagnostics Tests* tab of the Diagnostics page (FIG. 455).
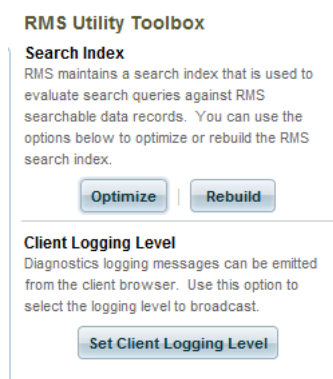
FIG. 455 RMS Utility Toolbox (Diagnostics page - Diagnostics Tests tab)

The options in the RMS Utility Toolbox allow you to manage the RMS Search Index, database housekeeping maintenance tasks, and set the client logging level for diagnostics message broadcasts. The options in the RMS Utility Toolbox are described below:

RMS Utility Toolbox Options	
Search Index	
• Optimize:	Click to optimize the Search Index (see *Optimizing the Search Index* on page 276).
• Rebuild:	Click to rebuild the Search Index (see *Rebuilding the Search Index* on page 276).

RMS Utility Toolbox Options (Cont.)	
Client Logging Level	
• Set Client Logging Level:	This function is intended for use by AMX. The "Client" in this function represents the Flex UI as opposed to client SDK logging on the master.

Optimizing the Search Index

Click the **Optimize** button in the RMS Utility Toolbox (see FIG. 455 on page 275) to optimize the Search Index. This action invokes the *Optimize Search Index* dialog (FIG. 456):
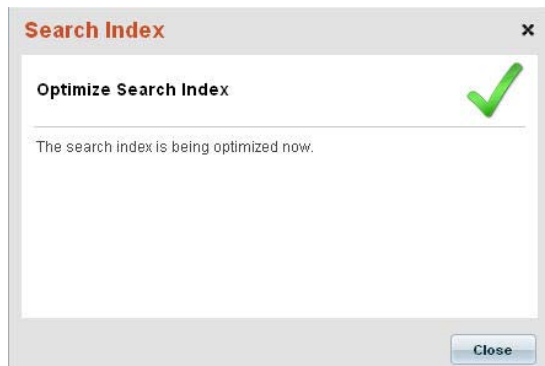
FIG. 456 Optimize Search Index dialog

- Click **Close** to close this dialog and continue optimizing the search index.
- To cancel the optimization process, close this dialog via the "X" in the upper-right corner.

Rebuilding the Search Index

Click the **Rebuild** button in the RMS Utility Toolbox (see FIG. 455 on page 275) to rebuild the Search Index. This action invokes the *Rebuild Search Index* dialog (FIG. 457):
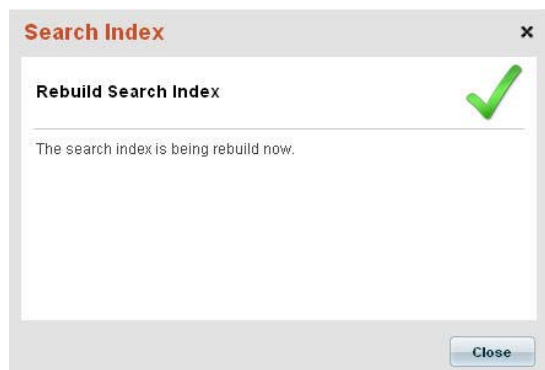
FIG. 457 Rebuild Search Index dialog

- Click **Close** to close this dialog and continue rebuilding the search index.
- To cancel the rebuild process, close this dialog via the "X" in the upper-right corner.

Appendix A: Using Directory Services

Overview

RMS Enterprise provides support for managing users, contacts, and role membership in their existing directory.

NOTE: *Directory Services are supported by installed RMS Servers only; not supported on AMX Cloud hosted services.*

When RMS Enterprise is configured to make use of a directory, there are two distinct modes of operation:

- In one mode, the directory performs the functions of authentication and authorization.
- In the second mode, users are pre-authenticated by a source which has a trust relationship with RMS.

In the case of pre-authentication, the directory is the authoritative source for the roles needed to make authorization decisions. In both modes the directory is the authoritative source for such things as user ID, first name, last name and e-mail.

When the RMS system is configured to use a directory server for user management, the directory will be the authoritative source for user creation and management. This means that all users (with the exception of the three build-in users accounts: *Admin*, *Guest*, and *Client* must be managed in the directory.

Directory Service Configuration

During the RMS Enterprise installation, the user will be given the option to enable RMS for use with a directory server. When enabled, the installer will also prompt for several other pieces of information, many of these values do not have a default value and must be provided during installation.

When RMS is configured to be directory enabled, user information can be stored in either a *LDAP version 3* server or *Active Directory*.

- For *LDAP*, the users must be '**inetOrgPerson**' objects.
- When *Active Directory* is chosen, users can be '**inetOrgPerson**' or '**user**' objects. When using Active Directory with 'user' objects, attributes must use their default LDAP names.

  In either case, the attribute used to search for users must provided at the time of installation. Frequently the attribute is '**uid**' for LDAP installations and '**SAMAccountName**' for Active Directory installations.
- Case is not important, as the directory must ignore case during user searches.
- The RMS property '**rms.directory.user.attribute.name**' will hold the attribute name after installation.

RMS has the ability to connect to a directory with or without SSL. During the installation process, a LDAP URL must be provided. The URL must contain protocol, host name and port.

An example of the URL might be *ldaps://ldapserver:636*. The use of '*ldaps*' in the URL also requires the port be a SSL port. The URL input during installation is stored in the '**rms.directory.url**' entry in the RMS properties file.

The install process also provides prompts for the following items:

- The DN of an account which RMS will use to connect to the directory. Inside the properties file, this is stored as '**rms.directory.bind.dn**'.
- Credentials for the DN above. After being input by the install process it will be encrypted and stored on the line '**rms.directory.bind.dn.password**' line in the properties file.
- The base DN used to search for users. The '**rms.directory.base**' property holds this value.
- The base DN used to search for groups. RMS uses the property '**rms.directory.group.base**' to store this value.
- The name of the attribute used by a directory for group membership. Often the attribute is 'member'. In the directory, the attribute must contain the distinguished names of users who are a member of that group. The directory must be able to perform searches based on this attribute. The group attribute name is stored in the RMS properties file as '**rms.directory.group.attribute.name**'.

Directory Server Access Credentials (Required Directory Permissions)

RMS Enterprise requires the use of a single account to connect (i.e. bind), search for and read directory information. This bind account is configured during installation and is stored in the RMS properties file. This account connects to the directory using a simple bind. For authentication, authorization and directory synchronization, the RMS bind account requires read only access to standard LDAP/Active Directory attributes for both users and groups. RMS needs read access to the attributes for last name, first name, mail, user ID, common name and object class. In order for RMS to search for users, it must have the ability to search based on the user ID attribute. Authorization requires the ability to search for and read the attribute used to define group membership. Refer to the *Directory User Authorization/Permissions Roles/Group Membership* section on page 278 for details.

Directory User Authentication

When directory services are enabled and RMS is configured to authenticate to the directory, all authentication requests, *excluding the three special built-in accounts (admin, guest and client)*, will be performed by the directory server.

- If the directory authentication attempt is unsuccessful, the request will be denied and the user will be prompted with an error message on the logon screen.
- If the authentication request is successful, then the Directory user will be queried for group membership. Refer to the *Directory User Authorization/Permissions Roles/Group Membership* section on page 278 for details.

Authentication requires the ability to search for users with standard attributes. The actual attribute used in a search, is provided during the installation process and is stored in the RMS properties file. When searching for a user, the directory must never return more than user.

Non-Directory Supported User Accounts

RMS Enterprise includes three special built-in system user accounts that are managed internally and not managed/synchronized with any external Directory server:

Non-Directory Supported User Accounts	
admin	This is the RMS system administrator account. This account provides full system administrative access to the RMS server. This account is necessary to perform initial setup and administrative tasks. In the event that a mis-configuration leads to a RMS system that all normal accounts are locked out, use this administrative account to access the RMS system.
guest	The guest account is used to allow anonymous access to the RMS system. This account can be disabled in the RMS user management configuration (see the *Enabling / Disabling the Guest Account* section on page 180). *Note: The Guest account is only available for installed RMS Servers; it cannot be enabled for AMX Cloud hosted services.*
client	The client account is used by NetLinx masters (and other RMS clients) to authenticate and communicate with the RMS server API. This user account is restricted to API access and cannot logon to the web user interface application.

Directory User Authorization/Permissions Roles/Group Membership

While directory services are enabled, RMS role permission records must be mapped to a specific directory group. Directory group mapping is accomplished by putting the distinguished name of directory group into the "Directory User Group' field on the RMS role management screen. Following authentication, the user's roles are determined by checking group memberships against the mapping role entries. If during the process of verifying a user's group memberships, a group is not mapped to a RMS role, that group will be ignored and will not be considered for authorization decisions. Any user account which does not have at least one mapped role will not be granted access.

RMS Roles are not created automatically from Directory groups. Roles must first be configured in RMS and mapped to a specific directory group prior to user authentication and authorization. The process to determine what groups a user is a member of consists of two steps:

1. Search for the user object in the directory to determine the distinguished name (DN).
2. Search for all directory groups which contain the user's DN.

The built-in users mentioned earlier are in no way affected by enabling directory services.

Directory User Contacts

RMS Enterprise user accounts may contain zero or more contact records associated with the user account. During the directory user synchronization, contact information will be synchronized from the Directory to the RMS user account. Refer to the *User Contacts* section on page 280for details.

Directory Synchronization

Following authentication, and just prior to making any authorization decisions, the complete list of roles assigned to the user will be synchronized with RMS. If the user has mapped roles and does not already exist in RMS, that user account will be created in RMS. Only after synchronization is complete will any authorization decisions be made. After the user authentication request has been approved, the user authorization has been established, and the user information has been fully synchronized, the user will be allowed to access the RMS web application with the access privileges granted via the matched RMS permission roles.

User

Upon successful authentication with a Directory server, the following user account information will be synchronized from the Directory into the RMS database:

- First Name
- Last Name

NOTE: *User authentication will fail if an Active Directory user has a blank first name or a blank last name.*

User Contacts

Upon successful authentication with a Directory server, the following user contact information will be synchronized from the Directory into the RMS database:

- User Default Email Address (Mail)

    This email account will be labeled as the "Work" email account in RMS.

User Role Membership

Following successful authentication, each group membership is checked against groups in RMS. The complete list of roles is synchronized with that user in RMS. User roles will be added or removed to ensure that RMS and the directory agree.

Directory Synchronization Flowchart

Refer to FIG. 458 for a depiction of the Directory user authentication, authorization, and synchronization process.
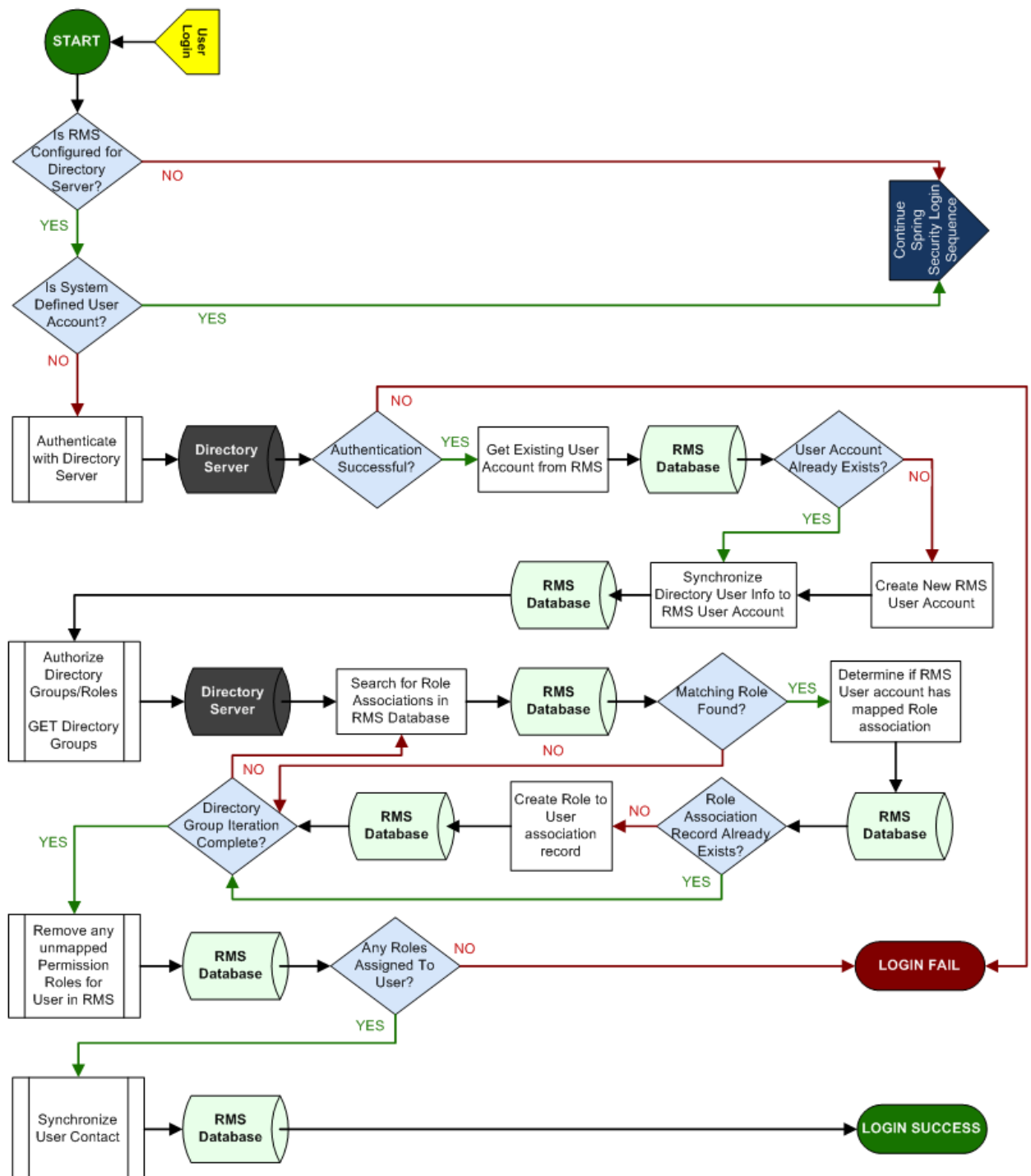
FIG. 458 RMS Enterprise LDAP Workflow

Scheduled Directory User Account Verification

When Directory services are enabled, RMS must perform a regularly scheduled task to determine if the information in RMS is consistent with the directory. Any information which differs, will be updated in RMS. Users which exist in RMS but not in the directory will be automatically removed from RMS. This account verification process will be implemented as a Quartz job in RMS. Quartz will schedule and execute the job.

Sanity Check

Prior to any accounts being removed, a basic check is performed to ensure the count of users to remove is below a fixed total and percentage of existing users. If the number of users scheduled for removal exceeds either of these values, no accounts will be removed. The purpose of this sanity check is to prevent the accidental removal of RMS user account in certain edge cases.

Sanity check thresholds are controlled by two entries in the **rms.properties file**:

- rms.jobs.missingdirectoryuserpurgejob.maxusersthreshold=100
- rms.jobs.missingdirectoryuserpurgejob.maxpercentusersthreshold=25

If during account verification the total number of user accounts to be eliminated exceeds the value assigned to "**maxusersthreshold**", no accounts will be removed from RMS. The value assigned to "**maxpercentusersthreshold**" is defined as a percentage of total RMS accounts. If the number of accounts to be purged exceeds this percentage, no accounts will be removed from RMS.

User

During the user account verification process, user accounts defined in RMS that are no longer present in the Directory will be removed from the RMS database.

User Contacts

During the user account verification process, user accounts that are purged from the RMS database must also remove any associated user contact records. For users who still exist both in RMS and the directory, if contact information in the directory differs from information stored in RMS, RMS will be updated.

User Notification Schedule

During the user account verification process, user accounts that are purged from the RMS database must also remove any associated user notification schedule records.

User Notifications

During the user account verification process, user accounts that are purged from the RMS database must also remove any associated user notification rule records.

User Role Membership

During the user account verification process, user accounts that are purged from the RMS database must also remove any associated user role membership records. For users who still exist both in RMS and the directory, if role membership in the directory differs from information stored in RMS, RMS will be updated.

User Management UI

User Profile

When the RMS system is configured for Directory based user management, the user management administrative interface in the RMS web application must limit certain fields and options. The Directory will be considered the authoritative source for user accounts. The following table indicates the accessible fields for the user profile.

LDAP Accessible Fields for User Profile	
Field Name	**Accessibility**
Account Enabled	DISABLED, READ ONLY
First Name	DISABLED, READ ONLY
Last Name	DISABLED, READ ONLY
Username	DISABLED, READ ONLY
Password	DISABLED
Require Password Change on Next Login	DISABLED
Time Zone	ENABLED, READ-WRITE
Reset User's Preferences	ENABLED

These restrictions are to only be imposed on Directory managed user accounts, not on the built in system defined RMS user accounts: *Admin*, *Guest*, and *Client*.

NOTE: *For directory users which are automatically created upon their initial login to RMS, the value assigned to the password is a random value. The random value is assigned to ensure these accounts must authenticate against the directory and prevent backdoor access.*

User Contacts

When the RMS system is configured for Directory based user management, some user contact records may be synchronized and managed in the Directory. These Directory managed contact records must limit certain administrative functions and fields in the RMS user management interface and My Profile interface.

Directory Synchronized Contact

LDAP Accessible Fields for User Contact	
Field Name	**Accessibility**
Delete Contact	DISABLED
Contact Value (String)	DISABLED, READ ONLY
Contact Type / Label	ENABLED, READ-WRITE
Contact Formatting Option	ENABLED, READ-WRITE

Additional non-Directory synchronized user contact records may be created and managed in the RMS User Management interface and the My Profile interface. Non-Directory synchronized user contact records do not impose the same limited or restricted options in the user interface. *These restrictions are to only be imposed on Directory managed user accounts, not on the built in system defined RMS user accounts (Admin, Guest, and Client).*

User Notification Schedule

The User Notification schedule administrative user interface under User Management and the My Profile interface is not limited or restricted for Directory managed user accounts.

User Notifications

The User Notification Rules administrative user interface under User Management and the My Profile interface is not limited or restricted for Directory managed user accounts.

User Role Membership

The User Role Membership administrative user interface under User Management is limited / restricted for Directory managed user accounts. The Directory user account synchronization process will be responsible for all user associated permission roles, thus this user interface must DISABLE the ability to ADD or REMOVE roles from the user account. *These restrictions are to only be imposed on Directory managed user accounts, not on the built in system defined RMS user accounts (Admin, Guest, and Client).*

Role Management UI

When the RMS system is configured for Directory based user management, the permissions Role Management administrative interface in the RMS web application must limit certain fields and options for user to role associations. The Directory is considered the authoritative source for user accounts and mapped user permissions

Role Settings

Each permission role record in RMS will require a Distinguished Name (DN) text field that is exposed (visible) only when the RMS system is configured for Directory manage users.

- The maximum length for the Distinguished Name (DN) field is: 250 characters.
- The caption label for this Distinguished Name (DN) field is: "*Directory User Group (Distinguished Name)*"

A TEST button is provided adjacent to the Distinguished Name (DN) field allowing verification that the provided DN value can be resolved against the RMS configured Directory server. Upon test completion, the results of the TEST should be provided to the user interface. Once a role is saved, the group DN will be converted to lower case and normalized for search purposes. The Role name, description, global permissions, and location level permissions fields are not limited in any way when RMS is configured for Directory based user management.

Location Level Permissions

The location level permissions assignment user interface is not limited in any way when RMS is configured for Directory based user management.

Assign Users

When the RMS system is configured for Directory based user management, the Assign User UI under Role Management must limit which user accounts that can be ADDED and REMOVED from the Role. This user listing should display all the Directory and Non-Directory user account currently assigned to the selected user Role.

- The Available User List may only include the default built-in system defined user accounts: *Admin*, *Guest*, and *Client*. No other user accounts are permitted to be added to the listing.
- Only the default built-in system defined user accounts: *Admin*, *Guest*, and *Client* can be removed from the list. No other user accounts can be manually removed from the listing.

Appendix B: RMS Enterprise Certificates

About Certificates

Certificates are files that clients and servers use to authenticate information about themselves. They can certify who they are, where they come from, and they can also be used by the parties involved to agree on a method of communication.

There are *many* different ways to implement certificates, but this document will only concentrate on a couple of different ways, Self-Signed and Certificate Authority (CA) Issued certificates.

Notes on this Document

In this document we will be using all of the commands in PowerShell since we will be working on servers. We will explain the step, the next line will be the actual command, and the next piece will be an explanation of the command (if necessary).

NOTE: *Almost all of this will require your user have Administrator Privileges on the server.*

We will be using the '*cacerts*' keystore located in the "**C:\Program Files\Java\jre8\lib\security**" folder. The main reason for this is because the cacerts keystore can be used as both a server keystore for Tomcat and a client keystore for the Java Virtual Machine (JVM) installed on the server. This enables functionality for LDAPS and secure SQL configurations. Using this keystore also allows for direct manipulation of the JVM rather than manipulating Tomcat (Tomcat runs as an instance of JVM, so you are essentially working with the puppet master rather than the puppet).

There are other ways to get this same functionality, but for this document we will focus on these methods

Self-Signed Certificate

Self-signed Certificates are created by the server and then given to a client to tell them "I certify myself as being secured". From a security point of view, this is probably the worst way you can possibly secure something. Trusting a self-signed certificate is like allowing a thief in your house and him telling you, "Don't worry, I won't take anything. I'm not a thief." Self-signed certificates should only be used as a means to test your implementation or if it is impossible to get an actual certificate from a Certificate Authority (CA).

The following steps can be used to create a self-signed certificate, connect Tomcat to the keystore that contains the certificate, and configure Tomcat to redirect to HTTPS:

1. Open PowerShell and change the directory to **C:\Program Files\Java\jre8\bin**.
   Command:
   ```
   cd "C:\Program Files\Java\jre8\bin"
   ```

2. Create a self-signed certificate.
   Command:
   ```
   .\keytool –genkey –alias Tomcat –keyalg RSA -sigalg SHA256withRSA –keypass changeit –keystore
   "C:\Program Files\Java\jre8\lib\security\cacerts" -storepass changeit –validity 365
   ```
   Explanation:
   Use the keytool to generate a key (certificate) with the alias name of **Tomcat**.
   The key's algorithm will use RSA and the signature algorithm is SHA256withRSA.
   The password to the key will be "**changeit**". Put it in the keystore cacerts located in **C:\Program Files\Java\jre8\lib\security.**
   The password for the keystore is "**changeit**". This key will last for 365 days.

3. You will be asked a series of questions at this point.
   ```
   What is your first and last name?
     [Unknown]:  Firstname Lastname
   What is the name of your organizational unit?
     [Unknown]:  Company
   What is the name of your organization?
     [Unknown]:  Org
   What is the name of your City or Locality?
     [Unknown]:  City
   What is the name of your State or Province?
     [Unknown]:  State
   What is the two-letter country code for this unit?
     [Unknown]:  CC
   Summary: CN=Firstname Lastname, OU=IT&S, O=COMPANY NAME p.l.c, L=locality, ST=state, C=country
   ```

4. Once you have answered the questions, you will be prompted to confirm your entries. It says [no], but press **Y** and then Enter to confirm your entries:
   ```
   Is CN=Firstname Lastname, OU=Company, O=Org, L=City, ST=State, C=CC correct
     [no]: Y
   ```

5. Stop the Tomcat service.

6. Open the **server.xml** file located in **C:\Program Files\Apache Software Foundation\Tomcat 7.0\conf**.

7. Locate the section in the file that says:

```
<!--
<Connector port="**8number**" protocol="HTTP/1.1"
    connectionTimeout="20000"
    redirectPort="8443" />
-->
```

Explanation:

8number will either be 80 or 8080 depending upon how you originally setup Tomcat. This is the port that people would normally reach when they type in http://URL/rms or http://URL:8080/rms.

8. Remove "**<!--**" and "**-->**". (these characters comments out the section in between them, and we want this section to run).

9. Change **redirectPort** to **443**. It is suggested you use 443 so the user doesn't have to type in https://URL:8443/rms, instead it will be https://URL/rms.

10. Locate the section in the file that says:

```
<!--
<Connector port="8443" protocol="org.apache.coyote.http11.Http11Protocol"
maxThreads="150" SSLEnabled="true" scheme="https" secure="true" clientAuth="false" sslProtocol="TLS"
-->
```

11. Remove "**<!--**" and "**-->**".

12. Change the "**8443**" to "**443**" to match the previous setting.

13. Add the following code after secure="true":

```
keystoreFile="C:\Program Files\Java\jre8\lib\security\cacerts" keystorePass="changeit"
```

Explanation:

This line redirects the Tomcat server to use the '*cacerts*' keystore and the keys located therein as the certificates it presents when a client tries to login. The password is '**changeit**' by default.

14. Save and close the server.xml file.

15. Open the **web.xml** file located in **C:\Program Files\Apache Software Foundation\Tomcat 7.0\conf**.

16. Add the following lines of text to the file between the last line that says

```
</mime-mapping> and <!-- ============= Default Welcome File List ============== -->:
```

```
<security-constraint>
    <web-resource-collection>
        <web-resource-name>RMS Web Application User Interface</web-resource-name>
        <url-pattern>/index.html</url-pattern>
        <url-pattern>/rms.swf</url-pattern>
        <url-pattern>/flex-http.crossdomain</url-pattern>
        <url-pattern>/flex-https.crossdomain</url-pattern>
        <url-pattern>/libs/*</url-pattern>
        <url-pattern>/messagebroker/*</url-pattern>
        <url-pattern>/logfile/*</url-pattern>
        <url-pattern>/resources</url-pattern>
        <url-pattern>/report/*</url-pattern>
    </web-resource-collection>
        <user-data-constraint>
            <transport-guarantee>CONFIDENTIAL</transport-guarantee>
        </user-data-constraint>
    </security-constraint>
</security-constraint>
```

17. Save the *web.xml* file and close it.

18. Start the Tomcat service.

At this point typing in **https://URL/rms** should allow you to connect via a secure connection.

NOTE: *Depending upon the name you give the certificate, you may receive warnings at this point saying that the certificate name doesn't match the server name. Even with this warning it should allow you to connect via HTTPS.*

Certificate Authority (CA) Issued Certificates

Certificates that have been created by a Certificate Authority (CA) are the best way of securing your server's security and connections. CAs provide certificates that have been digitally signed by either the company's network security team or a worldwide authorized CA (Verisign, DigiCert, Symantec, GoDaddy). The certificates will either be given based upon organizational rules, or the security team will request a Certificate Signing Request (.csr) file from the server.

In this document we will be creating and providing a .csr file. Once the CA processes the .csr file, they will return a number of certificates back to you. These include *Root* Certificates, *Intermediate* Certificates, and *Company (or Site)* Certificates. We will include all three of these in this document.

Self-signed certificates are created by the server and then given to a client to tell them "I certify myself as being secured". From a security point of view, this is probably the worst way you can possibly secure something. Trusting a self-signed certificate is like allowing a thief in your house and him telling you, "Don't worry, I won't take anything. I'm not a thief." Self-signed certificates should only be used as a means to test your implementation or if it is impossible to get an actual certificate from a Certificate Authority (CA).

The following steps can be used to create a self-signed certificate, connect Tomcat to the keystore that contains the certificate, and configure Tomcat to redirect to HTTPS.

1. Open PowerShell and change the directory to **C:\Program Files\Java\jre8\bin**.

   Command:

   ```
   cd ".\Program Files\Java\jre8\bin"
   ```

2. Generate a key on your server.

   Command:

   ```
   .\keytool -genkey -alias Tomcat -keyalg RSA -keystore
   "C:\Program Files\Java\jre8\lib\security/cacerts" -storepass changeit
   ```

   Explanation:

   Use the keytool program to generate a key with the alias name of Tomcat. The key will use the RSA algorithm and be stored in the keystore located in C*:\Program Files\Java\jre8\lib\security*, in the cacerts file, with the password of "*changeit*".

3. Generate a .csr file using the key you have just created.

   Command:

   ```
   .\keytool -certreq -keyalg RSA -alias Tomcat -file certreq.csr -keystore
   "C:\Program Files\Java\jre8\lib\security/cacerts" -storepass changeit
   ```

   Explanation:

   Use the keytool to create a certificate request using the RSA algorithm. The request is based on the Tomcat key and will be named certreq.csr. You can find the key in the *C:\Program Files\Java\jre8\lib\security* folder, in the cacerts keystore, with the password of "*changeit*".

   NOTE: *The .csr file will be generated in the C:\Program Files\Java\jre8\bin folder.*

4. Send the .csr file to the CA. They will return back several files including the Root Certificate, the Intermediate Certificate, and the Site Certificate.

5. Copy the certificates into the **C:\Program Files\Java\jre8\bin** folder.

6. Remove the self-signed certificate from the keystore.

   Command:

   ```
   .\keytool -delete -alias Tomcat -keystore "C:\Program Files\Java\jre8\lib\security/cacerts"
    -storepass changeit
   ```

   Explanation:

   Use the keytool to delete the certificate with the alias of Tomcat from the keystore located in the *C:\Program Files\Java\jre8\lib\security* folder, in the *cacerts* keystore, with the password of "*changeit*".

7. Import the **Root Certificate** to the keystore.

   Command:

   ```
   .\keytool -import -trustcacerts -alias root -file root.crt -keystore
   "C:\Program Files\Java\jre8\lib\security/cacerts" -storepass changeit
   ```

   Explanation:

   Use the keytool to import a trusted certificate named root.crt with a new alias of '**root**' into the keystore located in the *C:\Program Files\Java\jre8\lib\security* folder, in the *cacerts* keystore, with the password of "*changeit*".

8. Import the **Intermediate Certificate** to the keystore.

   Command:

   ```
   .\keytool -import -trustcacerts -alias intermediate -file intermediate.crt -keystore
   "C:\Program Files\Java\jre8\lib\security/cacerts" -storepass changeit
   ```

   Explanation:

   Use the keytool to import a trusted certificate named intermediate.crt with a new alias of '**intermediate**' into the keystore located in the *C:\Program Files\Java\jre8\lib\security* folder, in the *cacerts* keystore, with the password of "*changeit*".

9. *Import* the **Site Certificate** to the keystore.

   Command:

   ```
   .\keytool -import -trustcacerts -alias site -file site.crt -keystore
   "C:\Program Files\Java\jre8\lib\security/cacerts" -storepass changeit
   ```

   Explanation:

   Use the keytool to import a trusted certificate named site.crt with a new alias of '**site**' into the keystore located in the *C:\Program Files\Java\jre8\lib\security* folder, in the *cacerts* keystore, with the password of "*changeit*".

10. Stop the Tomcat service.

11. Open the **server.xml** file located in **C:\Program Files\Apache Software Foundation\Tomcat 7.0\conf**.

12. Locate the section that says:

    ```
    <!--
    <Connector port="**8number**" protocol="HTTP/1.1"
         connectionTimeout="20000"
         redirectPort="8443" />
    -->
    ```

Explanation:

8number will either be 80 or 8080 depending upon how you originally setup Tomcat. This is the port that people would normally reach when they type in http://URL/rms or http://URL:8080/rms.

13. Remove "**<!--**" and "**-->**". (these characters comments out the section in between them, and we want this section to run).

14. Change the redirectPort to "**443**". It is suggested you use 443 so the user doesn't have to type in https://URL:8443/rms, instead it will be https://URL/rms.

15. Locate the section in the file that says:

```
<!--
<Connector port="8443" protocol="org.apache.coyote.http11.Htp11Protocol"
maxThreads="150" SSLEnabled="true" scheme="https" secure="true" clientAuth="false" sslProtocol="TLS"
-->
```

16. Remove "**<!--**" and "**-->**".

17. Change the "**8443**" to "**443**" to match the previous setting.

18. Add the following code after `secure="true"`:

```
keystoreFile="C:\Program Files\Java\jre8\lib\security/cacerts" keystorePass="changeit"
```

Explanation:

This line redirects the Tomcat server to use the 'cacerts' keystore and the keys located therein as the certificates it presents when a client tries to login. The password is 'changeit' by default.

19. Save and close the *server.xml* file.

20. Open the **web.xml** file located in **C:\Program Files\Apache Software Foundation\Tomcat 7.0\conf**.

21. Add the following lines of text to the file between the last line that says
`</mime-mapping>` and `<!-- ============== Default Welcome File List ============== -->`:

```
<security-constraint>
    <web-resource-collection>
        <web-resource-name>RMS Web Application User Interface</web-resource-name>
        <url-pattern>/index.html</url-pattern>
        <url-pattern>/rms.swf</url-pattern>
        <url-pattern>/flex-http.crossdomain</url-pattern>
        <url-pattern>/flex-https.crossdomain</url-pattern>
        <url-pattern>/libs/*</url-pattern>
        <url-pattern>/messagebroker/*</url-pattern>
        <url-pattern>/logfile/*</url-pattern>
        <url-pattern>/resources</url-pattern>
        <url-pattern>/report/*</url-pattern>
    </web-resource-collection>
        <user-data-constraint>
            <transport-guarantee>CONFIDENTIAL</transport-guarantee>
        </user-data-constraint>
</security-constraint>
```

22. Save sand close the *web.xml* file.

23. Start the Tomcat service.

At this point typing in https://URL/rms should allow you to connect via a secure connection.

Also, if you are using these certificates to also connect to an LDAP or SQL server over SSL, this should allow you to connect to the server now.

RMS and SQL Using SSL

Once the certificates have been setup in the cacerts keystore, there are a couple of other steps that need to be completed in order for RMS to communicate with SQL via SSL.

NOTE: *This method drops the level of security to TLSv1. This is a bug in the JDBC driver that RMS uses, there is a feature request in to fix this issue, but this process is a temporary work around until that fix is implemented.*

1. Stop the Tomcat service.

2. Browse to the *rms.properties* file located in **C:\ProgramData\AMX\Resource Management Suite\Server\configuration**.

3. Edit the *rms.properties* file:
   a. Locate the line that begins with "**jbdc.url**".
   b. At the end of this line add the following string: "**;ssl=require**". Don't add the quotation marks.
   c. Save and close the *rms.properties* file.

4. Open the **Configure Tomcat** program via the Start menu.

5. Click on the **Java** tab.

6. In the **Java Options** section, add the following line: "**-Djsse.enableCBCProtection=false**". Do not add the quotation marks.

7. Start the Tomcat service.

At this point RMS should be able to communicate with SQL via SSL.

Additional Keytool and Tomcat Commands

The following is an additional list of very useful keytool and Tomcat commands. Depending upon which commands you use, some of them you may need to use before you do any of the other commands from above (i.e. the change password command).

Change a Java Keystore Password

Command:

```
.\keytool -storepasswd -new new_storepass -keystore
"C:\Program Files\Java\jre8\lib\security\cacerts" -storepass changeit
```

Explanation:

Use the keytool to create a new password as "new_storepass" for the keystore cacerts located in C:\Program Files\Java\jre8\lib\security that has the current password of "chageit".

Change a Private Key Password

Command:

```
.\keytool -keypasswd -alias Tomcat -keypass changeit -new new_password -keystore
"C:\Program Files\Java\jre8\lib\security\cacerts" -storepass password
```

Explanation:

Use the keytool to create a new password for the certificate with the alias of Tomcat with the current password of "changeit" to the new password of "new_password" located in the cacerts

Delete Certificate from a Keystore

Command:

```
.\keytool -delete -alias mydomain -keystore keystore.jks -storepass password
```

Explanation:

Use the keytool to delete the certificate with the alias mydomain from the keystore.jks keystore with the password "password".

Check Certificates in a Keystore

Command:

```
.\keytool -list -v -keystore "C:\Program Files\Java\jre8\lib\security\cacerts" -storepass changeit
```

Explanation:

Use the keytool to produce the long form list of all the keys in the cacerts keystore with the password "changeit"

Export a Certificate

Command:

```
.\keytool -export -alias Tomcat -file Tomcat.crt -keystore
"C:\Program Files\Java\jre8\lib\security\cacerts" -storepass changeit
```

Explanation:

Use the keytool to export your certificate with the alias name Tomcat to a file named Tomcat.crt. The certificate is in the cacerts keystore located in C:\Program Files\Java\jre8/lib\security with the password "changeit".

Change the Keystore Tomcat Utilizes

In the Tomcat configuration, under the Java tab, in the Java Options section you can change the keystore that Tomcat uses when it presents keys to a client. A keystore holds private keys like the self-signed certificate used for setting up HTTPS.

Command:

```
-Djavax.net.ssl.keyStore=/path/to/keystore
-Djavax.net.ssl.keyStorePassword=password
```

Explanation:

These two commands change the path to the keystore and the password to the keystore that Tomcat is using.

Change the Truststore Tomcat Utilizes

In the Tomcat configuration, under the Java tab, in the Java Options section you can change the truststore that Tomcat uses when it connects to another server. A truststore holds the public key for a remote server that you need to trust when you, for example, need to connect to an LDAP server over SSL.

Command:

```
-Djavax.net.ssl.trustStore=/path/to/truststore
-Djavax.net.ssl.trustStorePassword=password
```

Explanation:

These two commands change the path to the truststore and the password to the truststore that Tomcat uses to login to other servers.

Connecting an NX Master to an RMS Server via HTTPS

The following is a list of pre-requisites that must be satisfied before we can connect the NX Master to the RMS server via HTTPS:

- The NX Master must be running at least master FW v1.5.
- The code running in the NX Master but define the RmsNetLinxAdapter module.
- The version of NetLinx Studio installed on the host machine must be v4.4 or later.
- Java JRE/JDK keytool must be installed on the host machine.

JDK 8 can be downloaded from Oracle's website:
http://www.oracle.com/technetwork/java/javase/downloads/jdk8-downloads-2133151.html

If you just want JRE 8 it can be downloaded from here:
http://www.oracle.com/technetwork/java/javase/downloads/jre8-downloads-2133155.html

Basic Steps

1. Obtain the Root CA SSL certificate used to issue the RMS Servers SSL certificate for HTTPS.
2. Download the Duet Truststore from the NX Master.
3. Import the Root CA SSL certificate into the Duet Truststore.
4. Upload the Duet Truststore to the NX Master (and reboot).
5. Configure the NX Master to connect to the RMS server via HTTPS.

Detailed Instructions

Step 1: Obtain the Root CA SSL Certificate Used to Issue the Servers SSL Certificate for HTTPS

The following example uses Google Chrome browser v54.0.2840.71 to obtain the required SSL certificate for the sandbox RMS server hosted by avt (rms-demo.amxsambox.com/rms). The steps may be different if using a different version or another browser.

1. Browse to the RMS web server using HTTPS and click on the padlock icon (left of "**https://**" in the address bar - FIG. 459):
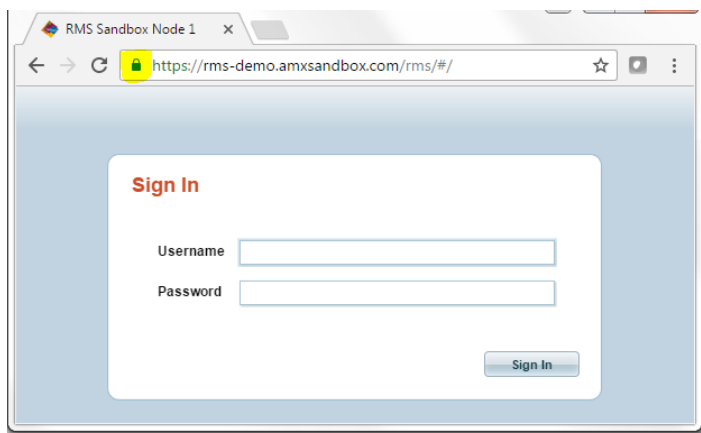
FIG. 459 RMS Enterprise Sign-In Screen - RMS web server using HTTPS

2. Click the **Details** link (FIG. 460):
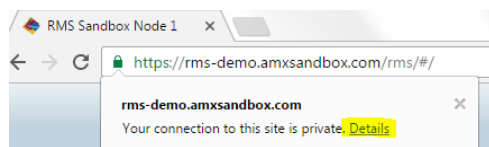
FIG. 460 Details link

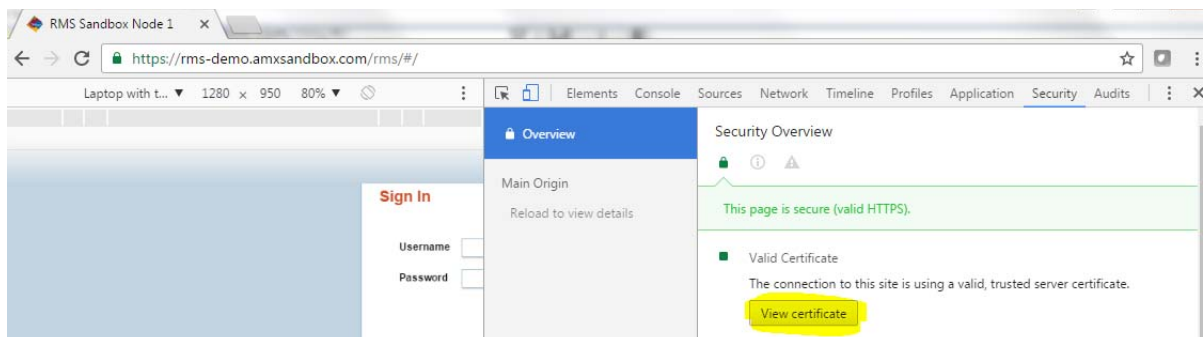3. Click **View Certificate** (FIG. 461):

FIG. 461 View Certificate button

You can then see the information about the RMS servers public key certificate including the certification path right up to the root certificate authority (Root CA). In this example we can see that the server certificate; rms-demo.amxsandbox.com; was issued by an intermediate certificate; *Let's Encrypt Authority X3*; which was issued by the root certificate, *DST Root CA X3* (FIG. 462):
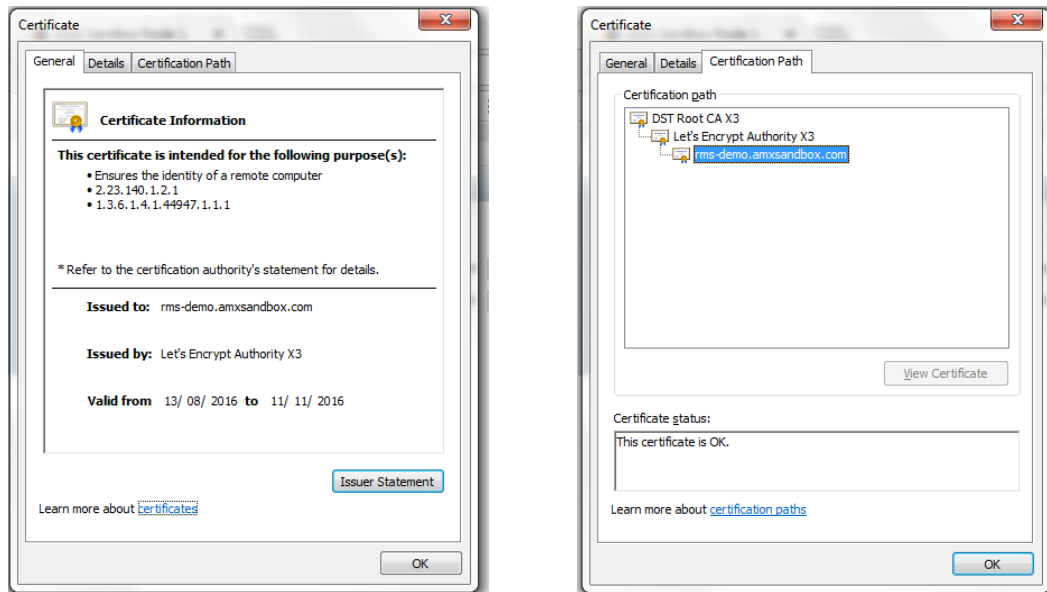

FIG. 462 Certificate Information

We only need the Root CA and can ignore both the Server and Intermediate certificates.

4. Select the Root CA at the top of the *Certification Path* tab and click **View Certificate** (FIG. 463):
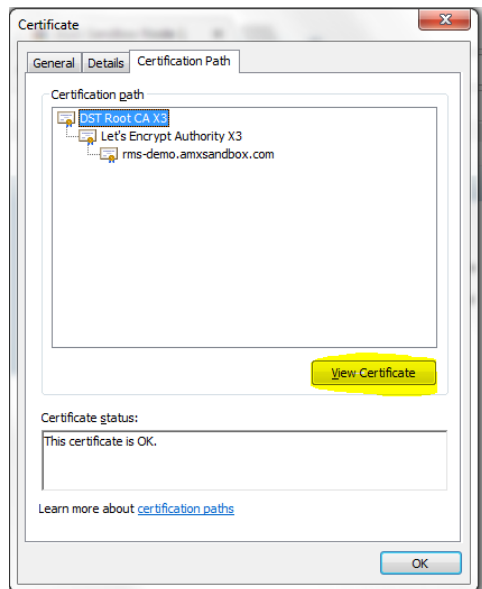
FIG. 463 Certificate Path - View Certificate

5. Go to the **Details** tab for the newly opened Certificate window and click **Copy to File ...** (FIG. 464):
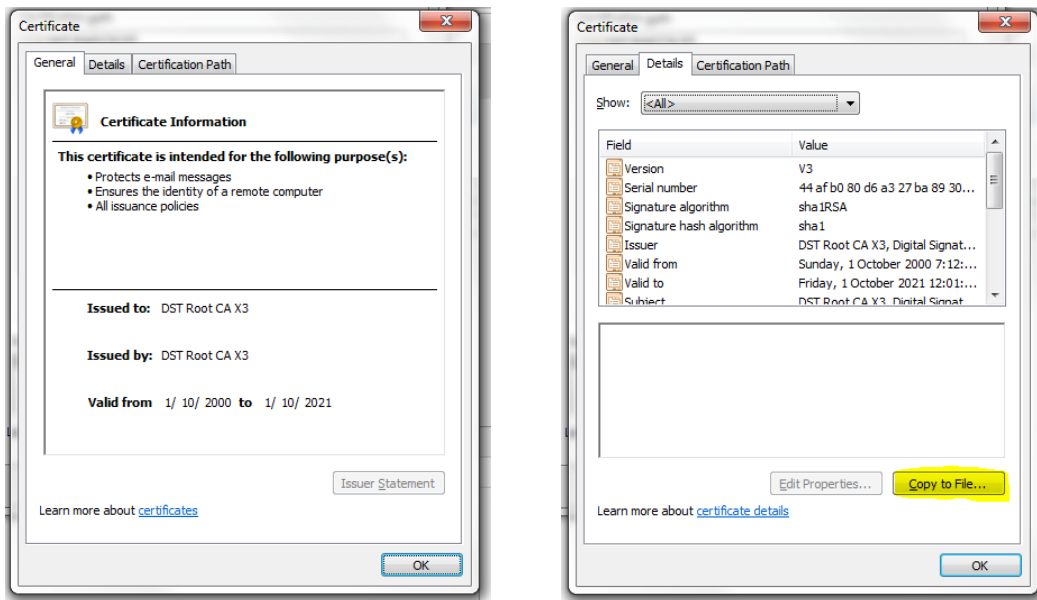
FIG. 464 Certificate Information - Copy to File

6.   This launches the *Certificate Export Wizard* - click **Next** (FIG. 465):

FIG. 465 Certificate Export Wizard

7.   Select either of the X.509 formats (DER or Base-64) to export the certificate to and click **Next** (FIG. 466):
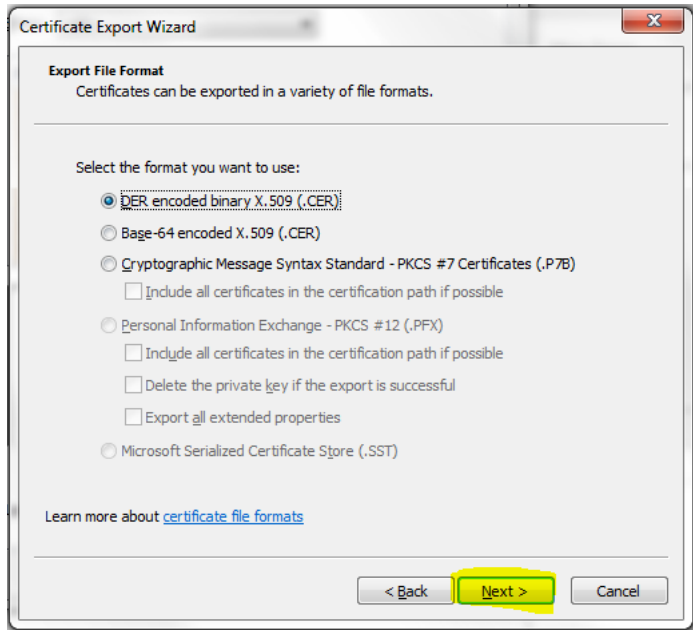
FIG. 466 Certificate Export Wizard - Export File Format

> **NOTE:** *The selected format must be in either of the X.509 formats.*
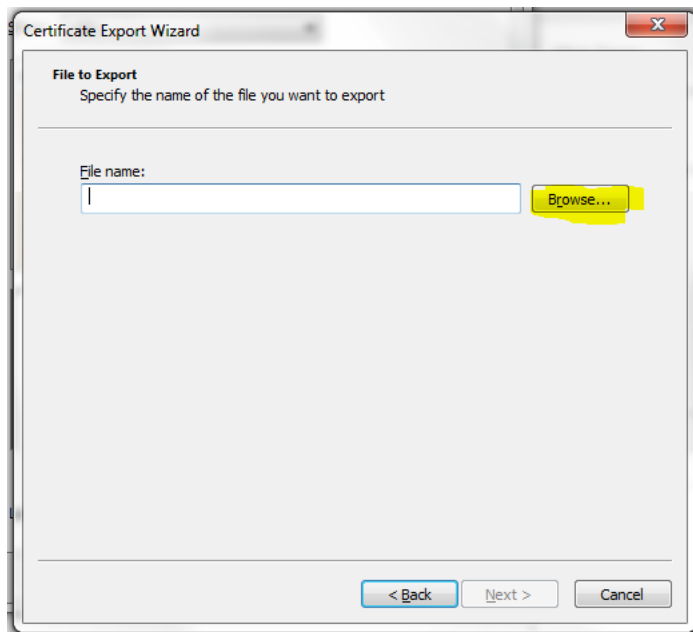
8.   Click **Browse** (FIG. 467):

FIG. 467 Certificate Export Wizard - File to Export

9. Browse to the folder you want to export the certificate to, type a filename for the certificate, and click **Save** (FIG. 468):
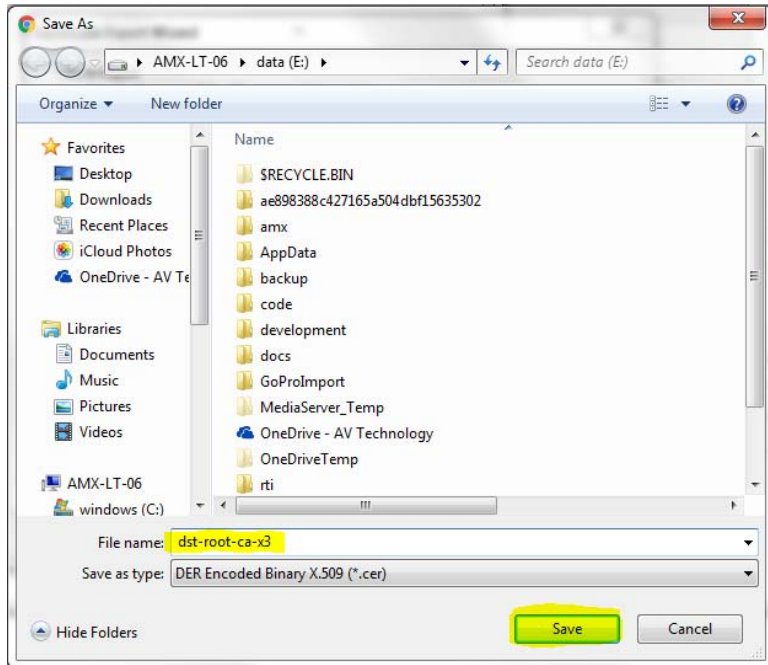
FIG. 468 Save As dialog

10. Click **Next** (FIG. 469):
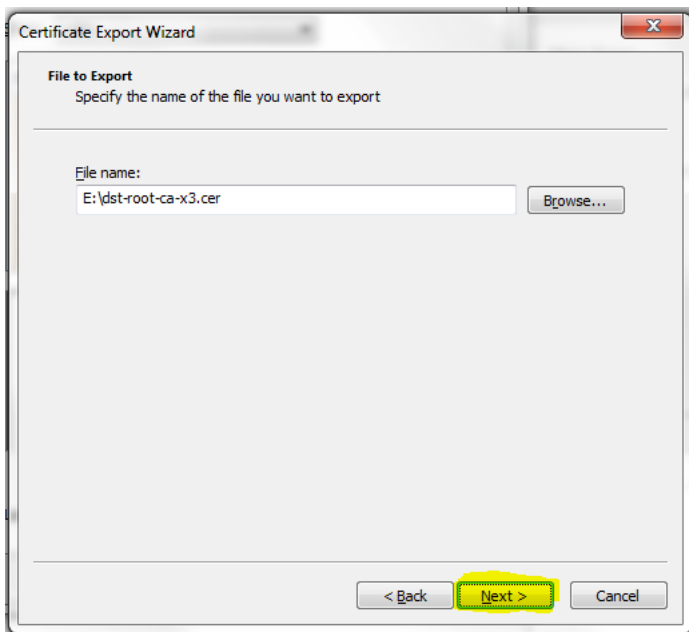
FIG. 469 Certificate Export Wizard - File To Export

11.   Click **Finish** (FIG. 470):
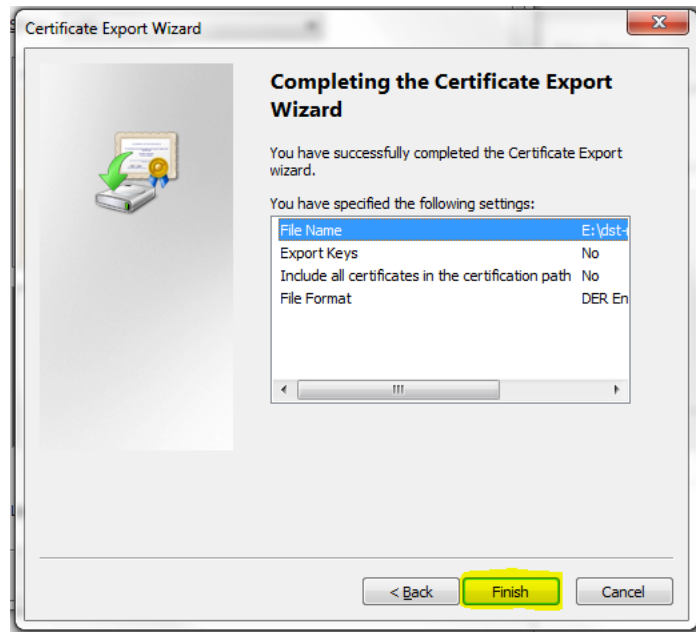
FIG. 470 Certificate Export Wizard - Completing the Certificate Export Wizard

12.   Click **OK** (FIG. 471):
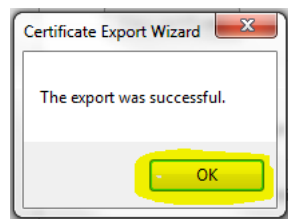
FIG. 471 Certificate Export Wizard - Export Successful

13.   The exported certificate file will now be saved in the folder of your choosing (FIG. 472):
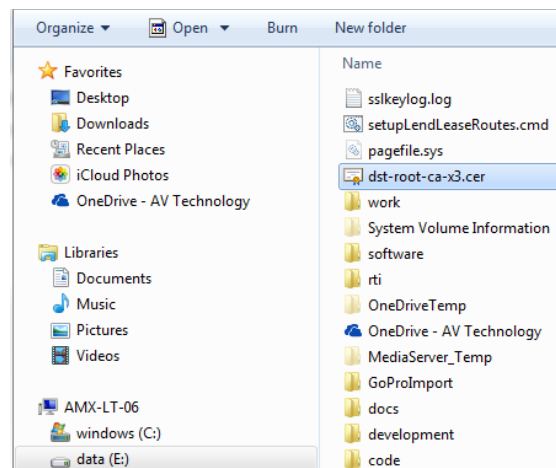
FIG. 472 Saved Certificate (.cer) File

Step 2: Download the Duet Truststore from the NX Master

1. In NetLinx Studio connect to the NX Master and select **Certificate Manager** from the Tools Menu (FIG. 473):
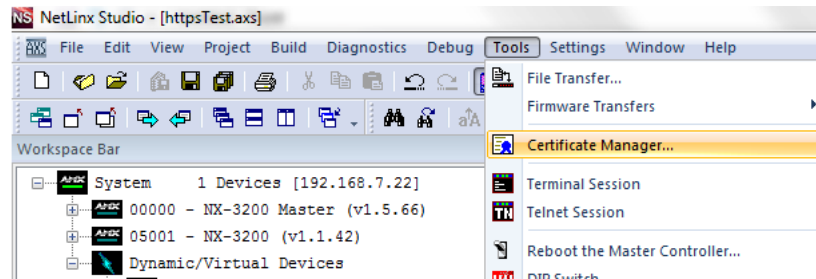
FIG. 473 NetLinx Studio

2. In the Certificate Receive tab of the Certificate Management tool, select the Duet Truststore certificate file and choose the folder to save the file before clicking **Receive Certificate(s)** (FIG. 474):
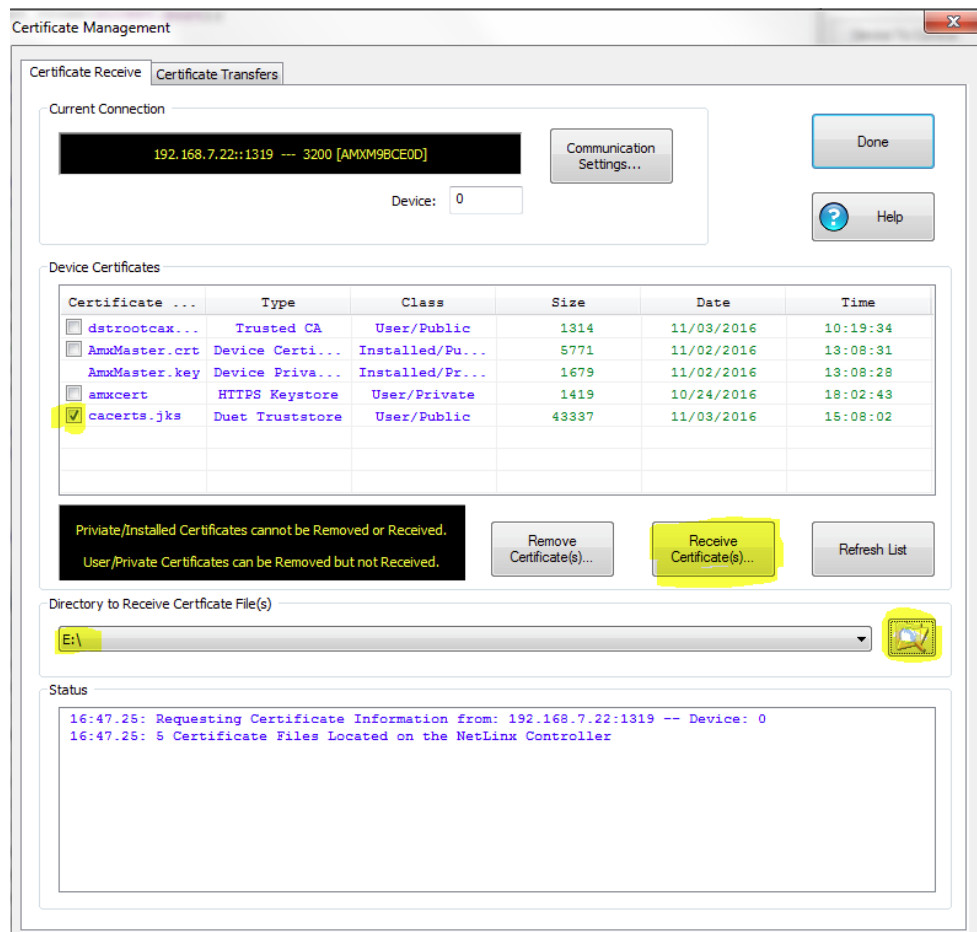

FIG. 474 Certificate Management - Receive tab

3. The status field should update to show when the file transfer is complete (FIG. 475):
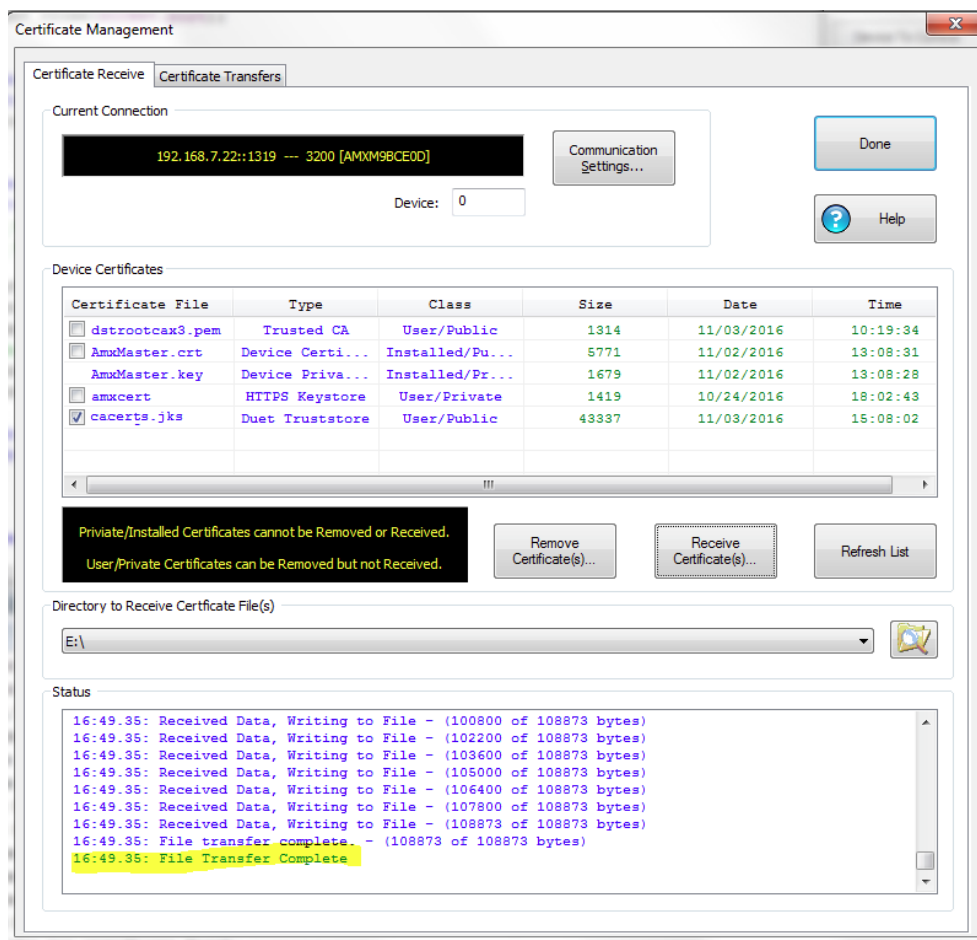
FIG. 475 Certificate Management - Receive tab - File Transfer Complete

4.   And you should now have a copy of the Duet Truststore from the master on the host machine (FIG. 476):
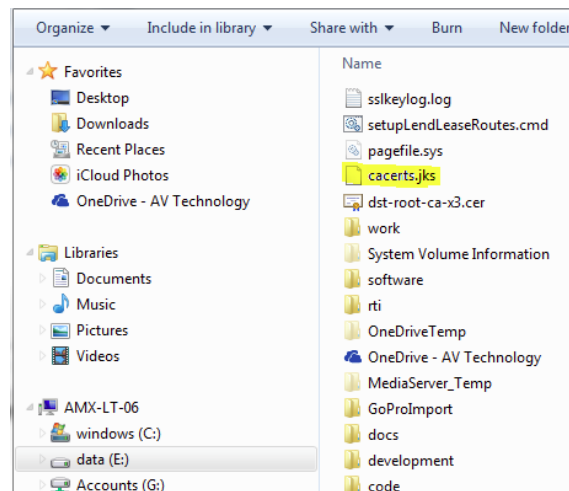

FIG. 476 Copy of the Duet Truststore on the host machine

Step 3: Import the Root CA SSL Certificate into the Duet Truststore

The following shows how to use the JRE/JDK keytool program to import the certificate into the Duet Truststore:

```
C:\Program Files\Java\jdk1.8.0_112\bin>keytool -list -alias rmssandbox -keystore
E:\duet.jks -storepass changeit

C:\Program Files\Java\jdk1.8.0_112\bin>keytool -importcert -v -alias rmssandbox -file
E:\dst-root-ca-x3.cer -keystore E:\duet.jks -storepass changeit -noprompt
Certificate was added to keystore
[Storing E:\duet.jks]

C:\Program Files\Java\jdk1.8.0_112\bin>keytool -list -alias rmssandbox -keystore
E:\duet.jks -storepass changeit
rmssandbox, 03/11/2016, trustedCertEntry,
Certificate fingerprint (SHA1): DA:C9:02:4F:54:D8:F6:DF:94:93:5F:B1:73:26:38:CA:6A:D7:7C:13
```

NOTE: *If you have previously installed AMX's Café Duet software application and have not added the JDK/JRE bin directory path to the PATH environment variable in Windows and are running the keytool program from outside the JRE/JDK /bin path you may inadvertently be running the keytool program that ships with Café Duet. If so, the options are slightly different and you may find that it doesn't work.*

This is the expected printout if you just type keytool at the command prompt:

```
>keytool
Key and Certificate Management Tool

Commands:

-certreq          Generates a certificate request
-changealias      Changes an entry's alias
-delete           Deletes an entry
-exportcert       Exports certificate
-genkeypair       Generates a key pair
-genseckey        Generates a secret key
-gencert          Generates certificate from a certificate request
-importcert       Imports a certificate or a certificate chain
-importpass       Imports a password
-importkeystore   Imports one or all entries from another keystore
-keypasswd        Changes the key password of an entry
-list             Lists entries in a keystore
-printcert        Prints the content of a certificate
-printcertreq     Prints the content of a certificate request
-printcrl         Prints the content of a CRL file
-storepasswd      Changes the store password of a keystore

Use "keytool -command_name -help" for usage of command_name
```

However, if you see this then you may be running the wrong keytool program:

```
>keytool
keytool usage:

-certreq    [-v] [-alias <alias>] [-sigalg <sigalg>]
            [-file <csr_file>] [-keypass <keypass>]
            [-keystore <keystore>] [-storepass <storepass>]
            [-storetype <storetype>] [-provider <provider_class_name>] ...

-delete     [-v] -alias <alias>
            [-keystore <keystore>] [-storepass <storepass>]
            [-storetype <storetype>] [-provider <provider_class_name>] ...

-export     [-v] [-rfc] [-alias <alias>] [-file <cert_file>]
            [-keystore <keystore>] [-storepass <storepass>]
            [-storetype <storetype>] [-provider <provider_class_name>] ...

-genkey     [-v] [-alias <alias>] [-keyalg <keyalg>]
            [-keysize <keysize>] [-sigalg <sigalg>]
            [-dname <dname>] [-validity <valDays>]
            [-keypass <keypass>] [-keystore <keystore>]
            [-storepass <storepass>] [-storetype <storetype>]
            [-provider <provider_class_name>] ...

-help
```

```
-identitydb  [-v] [-file <idb_file>] [-keystore <keystore>]
             [-storepass <storepass>] [-storetype <storetype>]
             [-provider <provider_class_name>] ...

-import      [-v] [-noprompt] [-trustcacerts] [-alias <alias>]
             [-file <cert_file>] [-keypass <keypass>]
             [-keystore <keystore>] [-storepass <storepass>]
             [-storetype <storetype>] [-provider <provider_class_name>] ...

-keyclone    [-v] [-alias <alias>] -dest <dest_alias>
             [-keypass <keypass>] [-new <new_keypass>]
             [-keystore <keystore>] [-storepass <storepass>]
             [-storetype <storetype>] [-provider <provider_class_name>] ...

-keypasswd   [-v] [-alias <alias>]
             [-keypass <old_keypass>] [-new <new_keypass>]
             [-keystore <keystore>] [-storepass <storepass>]
             [-storetype <storetype>] [-provider <provider_class_name>] ...

-list        [-v | -rfc] [-alias <alias>]
             [-keystore <keystore>] [-storepass <storepass>]
             [-storetype <storetype>] [-provider <provider_class_name>] ...

-printcert   [-v] [-file <cert_file>]

-selfcert    [-v] [-alias <alias>] [-sigalg <sigalg>]
             [-dname <dname>] [-validity <valDays>]
             [-keypass <keypass>] [-keystore <keystore>]
             [-storepass <storepass>] [-storetype <storetype>]
             [-provider <provider_class_name>] ...

-storepasswd [-v] [-new <new_storepass>]
             [-keystore <keystore>] [-storepass <storepass>]
             [-storetype <storetype>] [-provider <provider_class_name>] ...
```

Example of failure when accidentally using the keytool application that comes with Café Duet to either list the certificates within the Duet Truststore file or import a certificate:

```
>keytool -list -v -alias rmssandbox -keystore E:\duet.jks -storepass changeit
keytool error: java.security.cert.CertificateParsingException: java.io.IOException: subject key,
Unknown key spec: Invalid RSA modulus size.

>keytool -import -v -trustcacerts -alias rmssandbox -file E:\dst-root-ca-x3.cer -keystore E:\duet.jks
-storepass changeit
keytool error: java.security.cert.CertificateParsingException: java.io.IOException: subject key,
Unknown key spec: Invalid RSA modulus size.
```

You should add the JRE/JDK /bin folder to the front of the user PATH environment variable in Windows to guarantee that you are running the correct keytool program.

Step 4: Upload the Duet Truststore to the NX Master

1. Select **Certificate Manager** from the Tools menu in NetLinx Studio (FIG. 477):
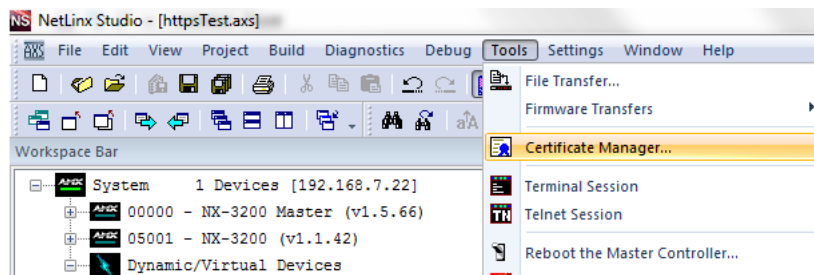

FIG. 477 NetLinx Studio

2. Go to the *Certificate Transfers* tab in the Certificate Management window, browse to the folder where you saved the duet.jks file and select it, and select **Duet Truststore** from the *Certificate Type* drop-down list (FIG. 478):
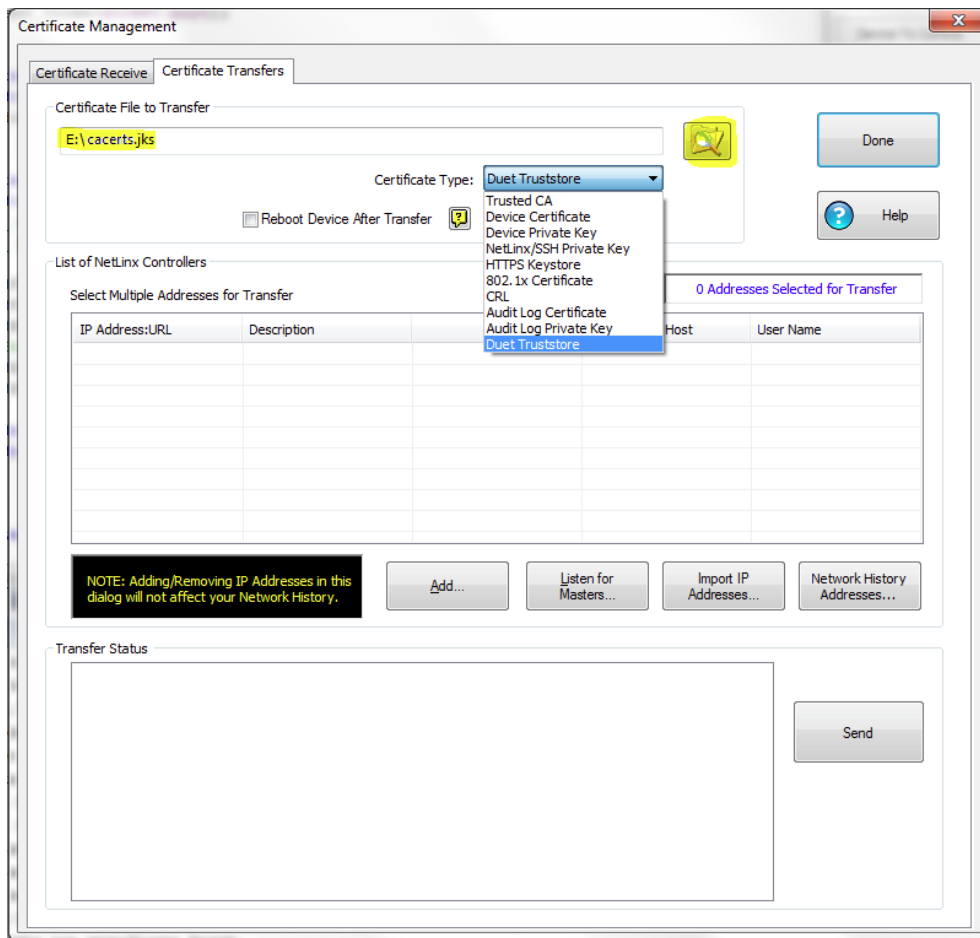
FIG. 478 Certificate Type - Duet Truststore

3. Add your master (or masters) to the List of NetLinx Controllers. There are 4 x options to do this:
    - Add a single masters' IP address or URL
    - Listen for master controllers on the network and add the ones you want
    - Import a list of IP addresses from a file
    - Add one or more master IPs/URLs from the list stored in NetLinx Studios Master Connection Settings (FIG. 479):
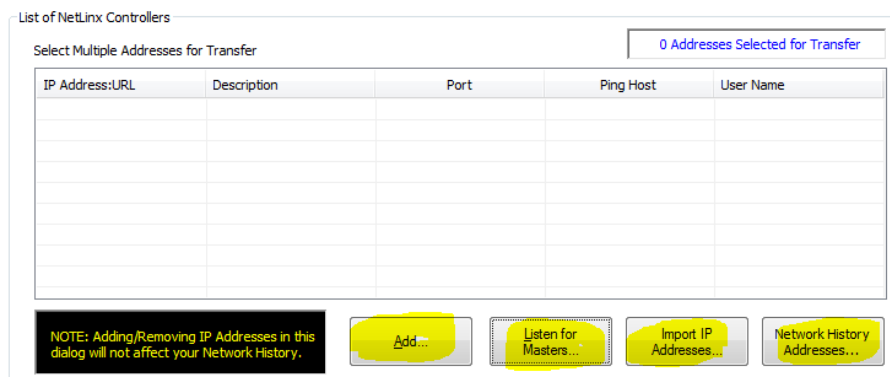

FIG. 479 NetLinx Studio - List of NetLinx Controller

4.   Make sure that the checkbox besides the masters IP address/URL is ticked and click **Send** (FIG. 480):
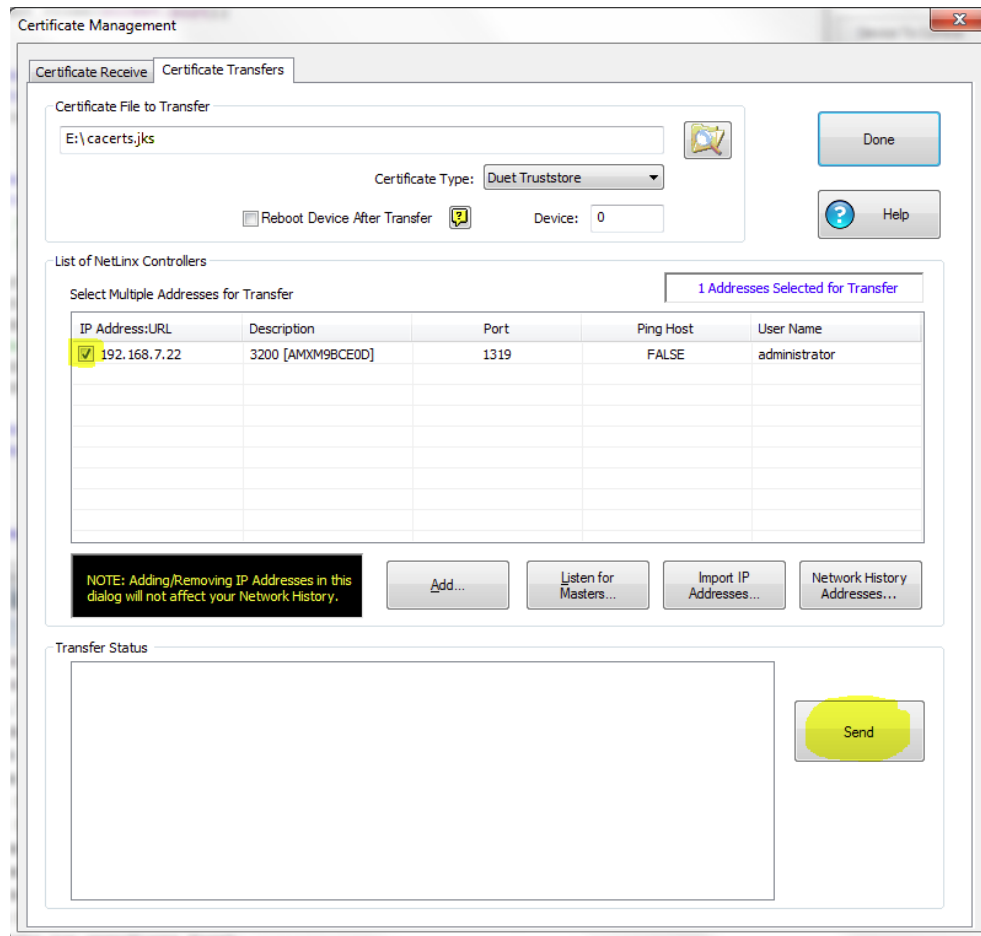
FIG. 480 Certificate Management - Transfer tab

NOTE: *The NX Master will have to be rebooted in order for the Duet Truststore on the master to be swapped out. You can either check the Reboot Device After Transfer checkbox prior to sending or reboot the master later.*

Step 5: Configure the NX Master to connect to the RMS Server via HTTPS

1.   Browse to the NX Masters' web page and log in. If the RmsNetLinxAdapter module is loaded you will see a button for **RMS** under *System Configuration*.

2.   Click on **RMS** (FIG. 481):
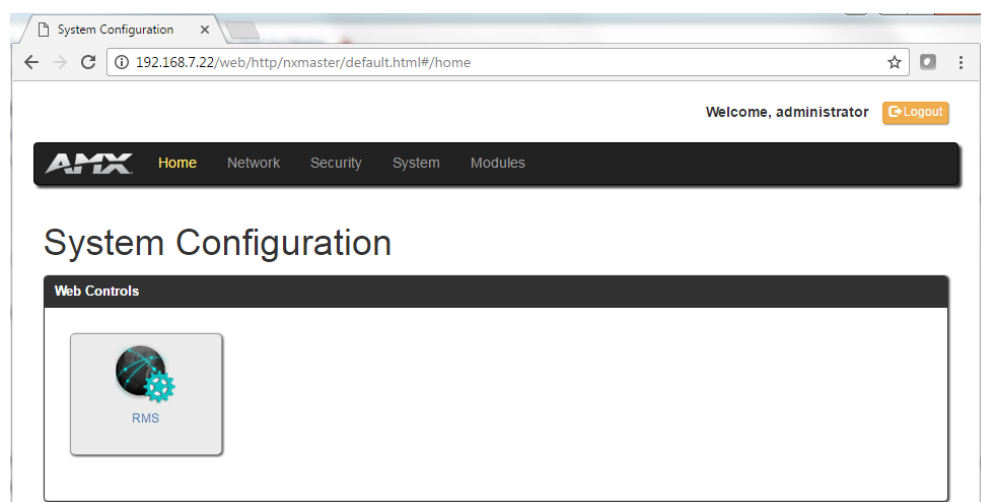
FIG. 481 NX Master –System Configuration

3.   Configure the NX Master to connect to the RMS server using HTTPS and click the **Test Connection** button (FIG. 482):

FIG. 482 NX Master -Server Connection Configuration

- You should get the following message indicating that the HTTPS connection is successful (FIG. 483):
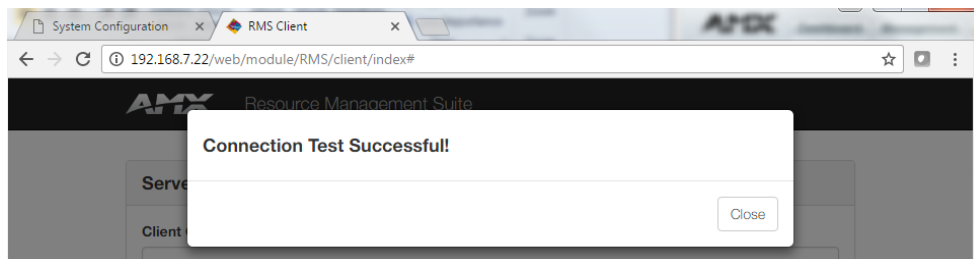

FIG. 483 NX Master -Connection Test Successful

- If you got an error when testing the connection on the NX Master then something went wrong. Possibly the wrong certificate was loaded into the Duet Truststore or maybe the master was not rebooted after uploading the Duet Truststore (FIG. 484):
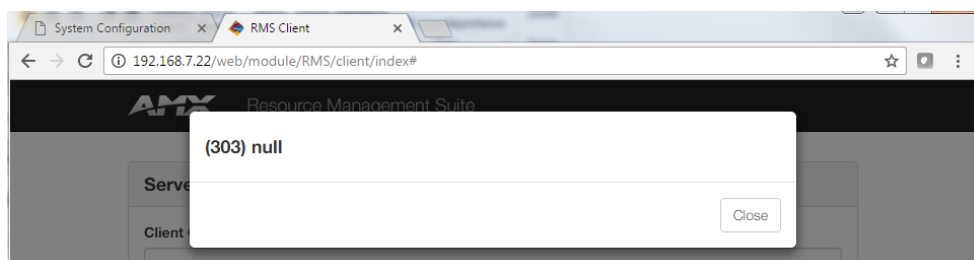

FIG. 484 NX Master -Connection Test Fail

4. To verify the connection on the RMS server browse to the RMS servers' web page and select **Unassigned Client Gateways** under *Client Gateway Management* (FIG. 485):
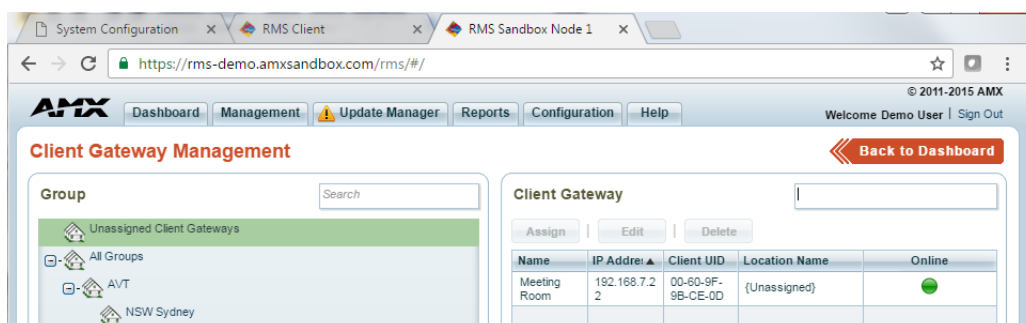
FIG. 485 RMS Enterprise - Client Gateway Management