Dell™ OpenManage™ Printer Manager v1.2

User Guide

www.dell.com | support.dell.com

Notes, Notices, and Cautions

NOTE: A NOTE indicates important information that helps you make better use of your computer.

NOTICE: A NOTICE indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

CAUTION: A CAUTION indicates a potential for property damage, personal injury, or death.

November 2008

Contents

Preface

This application can give you automated, consolidated configuration and control of network resources and Printers.

Consult this product's Release Notes for information about what is new in this release.

A Note About Performance

These applications are designed to help you manage your network with alacrity. Unfortunately, the devices they manage or the networks that communicate with those devices are not always as fast as this software. If discovery takes a long time (it can), often network and device latency is the culprit. You can also optimize installations to be faster and limit device queries with filters, but device and network latency limit how quickly your system can respond.

1

Starting The Application

Overview: Starting the Application

This application enforces security at the client level. You must have a valid user ID and password to log on to the application and use its features. You must also have an installed license.

Before you can run this application your system must have a running Application Server and Mediation Agent. Except in distributed installations, starting Application Server starts bothTypical installations implement Application Server so it runs in the background, even when you log out.

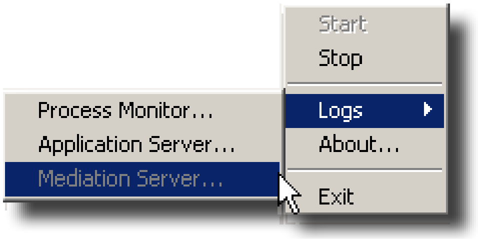
If you have not installed application server as a service, start one from the application's Windows® **Start** menu entry, or from a command line (`startappserver`).

The tray icons (in the lower right corner of the Windows start bar) indicate the current service condition.

Icon	Status
☒	Offline (no status available, or not controlled by server manager)
⚪	Idle
🟡	Running (initializing or shutting down)
🟢	Ready
🔴	Stopped

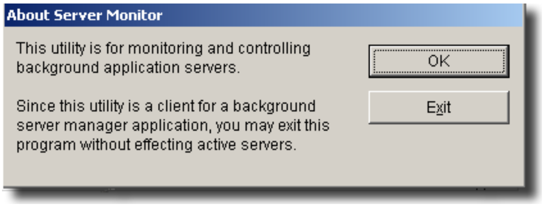
You can also right-click the icon to see the client menu.

Figure 1-1. Process Monitor Client Menu



The logs items let you see the recorded logs for Server Manager, Application, or Mediation Server. You can **Start** or **Stop** the service(s) running on your host and, with the **About** menu item, display the Server Manager about box (*Figure 1-2*).

Figure 1-2. About Process Monitor



This utility is for monitoring and controlling background application servers.

Since this utility is a client for a background server manager application, you may exit this program without effecting active servers.

NOTE: System changes can make the server manager system tray icon disappear in Windows while the process is still running. If you cannot make your icon reappear, try running `pmtray -r` from a command line, then restart the server manager with `pmtray`.

To start the application from Solaris do one of the following:

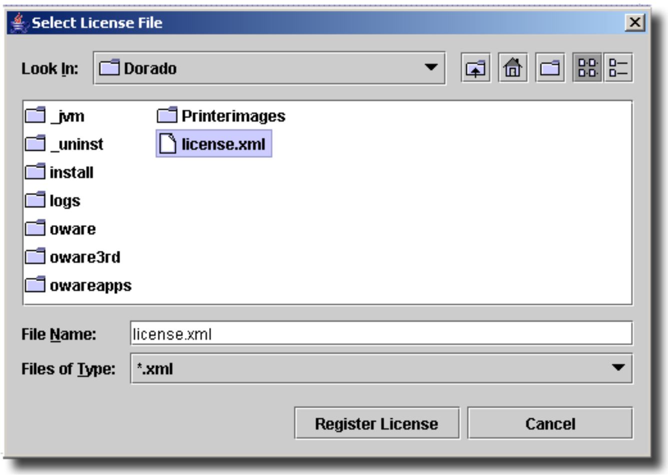
- Click on the icon on the front panel.
- Open a shell, set up the Oware environment by typing `. ./etc/dsienv,` then type `redcell`.

To start the application from Windows, select the application icon from the **Start** menu

Installing Licensing

You can install licenses for basic application server functionality, and for extended functionality for clients, drivers and applications. You can always install these from the **Settings**→ **Permissions**→ **Register License** menu item in the application client. Select the license file in that dialog on any client, and the application server will store the permissions to use that functionality on the database.

Figure 1-3. License File Selection



Select License File

Look In: Dorado

_jvm
_uninst
install
logs
oware
oware3rd
owareapps
Printerimages
license.xml

File Name: license.xml

Files of Type: *.xml

Application Server now requires a license. It should be installed by default, but if it has expired, or you have installed to a “headless” server (one without a monitor and keyboard), or if for any other reason the license is not available at startup the application server shuts down and will not start.

To install the license from a command line before you start application server, run the following commands in a command shell[1]:

```
>oware
>licenseimporter g:\path\license.xml
```

When it is finished, you should see:

```
importing.....done
```

The `g:\path` portion of this command line is an example. Correct it to wherever you have stored your license file—typically on the directory where you installed from.

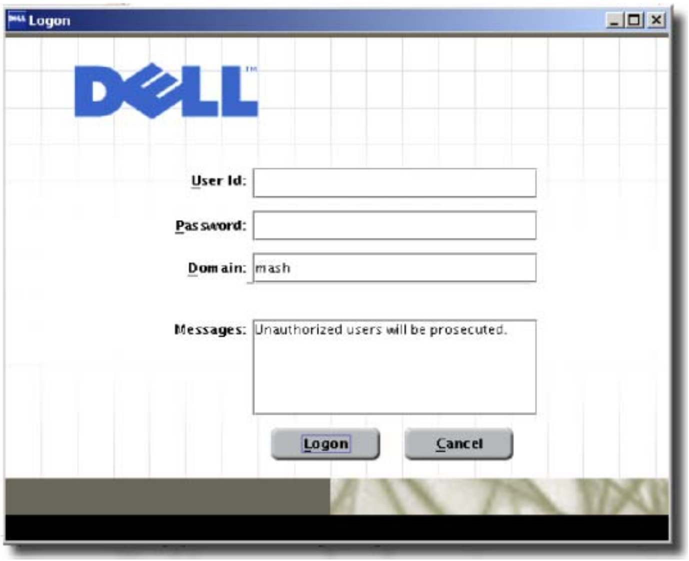
NOTE: If you import a license that, for example, changes the application’s capabilities, it does not immediately take effect. You must restart application server or wait at least 15 minutes.

[1] In Windows, open a command shell with *Start* > *Run* `cmd`.

Logging On

To log on, type a valid user name and password at the logon prompt. The default user name/password is *admin/[blank]*. The application prompts you to change the password the first time it starts

Figure 1-4. Login Prompt



Domain: mash

Messages: Unauthorized users will be prosecuted.

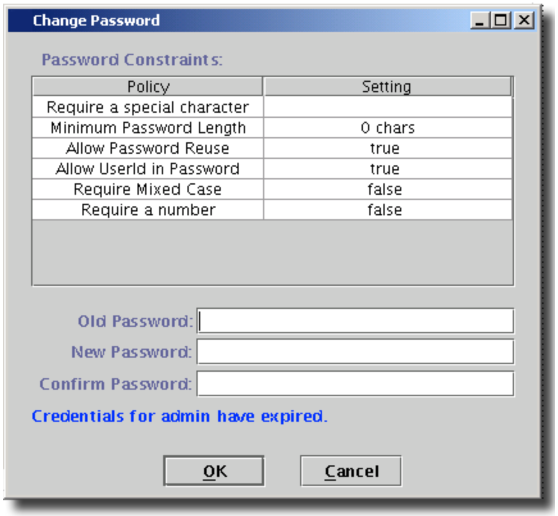
The *Domain* field is the application server partition (defaulting to the hostname of the application server in a single-server installation).

NOTE: Best practice for security in a production installation is to change admin / [blank].

Change Password

After your initial login, the application prompts you to change the password. By default, this does not restrict the password to having special character(s), or number(s). It also allows both upper and lower case letters for the new password.

Figure 1-5. Change Password Dialog



Change Password

Password Constraints:

Policy	Setting
Require a special character	
Minimum Password Length	0 chars
Allow Password Reuse	true
Allow UserId in Password	true
Require Mixed Case	false
Require a number	false

Old Password:

New Password:

Confirm Password:

Credentials for admin have expired.

You can set password constraints in the application (provided you have permissions to do so). The **Settings**→ **Change Password** menu item lets you change your password later.

Disabled Accounts

By default, you have three chances to enter the correct password before the system aborts the login. System administrators can change this number. The system does not let someone log on to an account disabled by too many log on retries. The administrator can also disable an account, in which case the lock-out period does not apply. A system administrator must re-enable the account before the user can access the application, or the login lockout period must have passed.

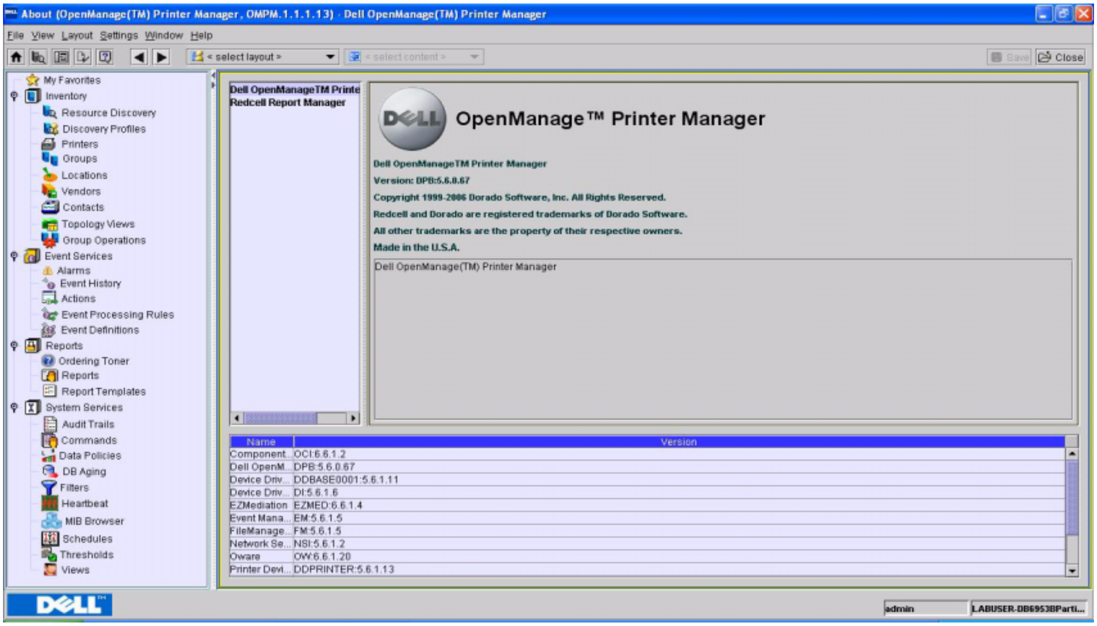
Application Server

The application server, which typically runs on a dedicated workstation, lets the system process incoming events and communicate with equipment and network devices. If the client application cannot connect to an application server, a warning message appears and the client does not launch.

The About Box

To see which products are installed, and what versions, click the **About** icon, or select the **Help**→ **About** menu item.

Figure 1-6. About Box



Dell OpenManageTM Printer Manager

Version: DPB:5.6.0.67

Copyright 1999-2006 Dorado Software, Inc. All Rights Reserved.

Redcell and Dorado are registered trademarks of Dorado Software.

All other trademarks are the property of their respective owners.

Made in the U.S.A.

Dell OpenManage(TM) Printer Manager

Name	Version
Component...	OCI:6.6.1.2
Dell OpenM...	DPB:5.6.0.67
Device Driv...	DDBASE0001:5.6.1.11
Device Driv...	DI:5.6.1.6
EZMediation	EZMED:6.6.1.4
Event Mana...	EM:5.6.1.5
FileManage...	FM:5.6.1.5
Network Se...	NSI:5.6.1.2
Oware	OW:6.6.1.20
Printer Devi...	DDPRINTER:5.6.1.13

The about box appears with the products listed on the left, and the version information for the selected product on the right. About boxes for device drivers list supported devices and their operating systems.

Logging Off

When you close the application, it asks if you want to *Show Editor* (with any pending edits), *Close*, *Close ALL*, *Close All & Exit*, or *Cancel* your request to log off. In any case, a confirmation dialog appears whenever you exit the client application

Web Client

This application now offers a portion of its functionality as a web client. To view the web client, open a browser (Internet Explorer® 6.0, Firefox ®1.5.0.3 or later) and open the following URL:

```
http://[appserver]:[port number]/
```

The "`[apppserver]`" text should be the name of the application server host.The `[port number]` can be either 80 or 8080, depending on your installation. Consult your installation guide for the correct one. If you have a popup blocker installed, you may have to click a link. When the web client opens, it presents a login screen. Once you log in, a subset of the application's services appear on the left navigation pane.

NOTE: When you first log in, you may have to restart the browser once you have reset your password.

For information about how to use the interface for web client capabilities, consult the relevant portion of this guide.

CAUTION: When you start a Web client, you must have a screen resolution of at least 1024x768. A warning message appears if you do not have this screen resolution, and while you can see the client, you can work with it only with difficulty.

In some cases the main title bar of the browser may not reflect which editor was just opened.

Online Help for Web Client

Online help does not work with the web client. On the other hand, the Acrobat version of the *User Guide* is the source of online help, and could offer the same kind of information if copied to the computer where the web client runs. You must have Acrobat installed on that client, but can refer to the *User Guide's* version of online help there.

Secure Web Client Connections

Web client connections enable HTTP and HTTPS by default on their respective ports. To make your client connection completely secure, you can disable HTTP and use HTTPS on port 8443 (rather than HTTP on 80—the unwritten default) or 8080 (as specified in the previous section's URL). The web server listens on the default HTTPS port 8443.

For a connection that is exclusively secure (HTTPS only, HTTP disabled), you must add a property to `owareapps/installprops/lib/installed.properties` with a text editor. Here is that property:

```
appserver.web.enable.https=true
```

This disables the HTTP connector thereby securing the server. To use HTTPS, then, use a URL like this:

```
https://MyAppserver:443
```

To force the client to use HTTPS (secure) for web connections to the server (such as opening the toner ordering pages) add the following line to `owareapps/installprops/lib/installed.properties` (this will be the same file as above when addressing this issue with the client when running locally on the server).

```
appserver.enable.https=true
```

Web vs. Java Clients

The following outlines the differences between web and Java clients:

Web Client	Java Client
Inventory	
Resource Discovery	Resource Discovery
Discovery Profiles	Discovery Profiles
Resources	Resources
Ports	Ports

Web Client	Java Client
Printers	Printers
Resource Roles	Resource Roles
Groups	Groups
Links	Links
Locations	Locations
Vendors	Vendors
Contacts	Contacts
	Topology Views
Group Operations	Group Operations
	Network Objects - nameSpaces
	Network Objects
Event Services	
Alarms	Alarms
Event History	Event History
Actions	Actions
Event Processing Rule	Event Processing Rule
Event Definitions	Event Definitions
Application Services	Application Services
OS Services	OS Services
Processes	Processes
File management	
	Configuration Files
OS/Firmware Deployment	OS/Firmware Deployment
Configuration Labels	Configuration Labels
	Configuration Generation
	Configlets
	Templates
	Schemas
	OS/Firmware Download and Save (on appserver)
Configlet (free-form) Editor	Configlet (free-form) Editor
File Servers	File Servers

Web Client	Java Client
Reports	
Reports	Reports
Report Templates	Report Templates
System Services	
Audit Trails	Audit Trails
Commands	Commands
Data Policies	Data Policies
DB Aging	DB Aging
Filters	Filters
Heartbeat	Heartbeat
MIB Browser	MIB Browser
Schedules	Schedules
Thresholds	Thresholds
Views	Views

You may also start the application server with a `-e` parameter, to initiate the secure connection. The command line is `startappserver -e.`

NOTE: You can reconfigure web client connections to different ports. Consult the *Installation Guide* for details.

Web Client and Clustered Servers

Currently, web clients must address only single servers, not clusters or partition names. Client failover is not possible, and if a clustered server fails, you must enter a new URL that includes one of the surviving hosts' name. Otherwise, the web client on clustered application servers behaves as the Java client would.

Licensing Web Client

To run the web client, you must have its license installed on the application server. See Installing Licensing for instructions.

2

Navigation

Overview

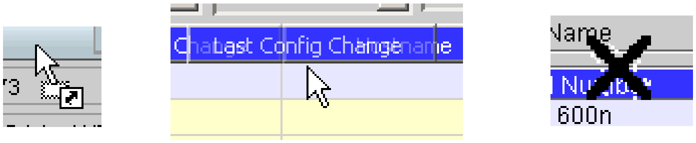
This section explains how to navigate the application. The application's Portal consists of the following sections:

- Toolbar
- Menu Bar
- Work Area

Drag and Drop

This software lets you drag and drop columns within screens that display information in tables. One caveat: since the screen has so much information, the "drop zone" can sometimes be small.

Figure 2-1. Drag and Drop Cursors



Java Client

Web Client

Column Deletion Cursor

NOTE: To drag a new column onscreen from the "+" menu, you must drop it over a column header or empty space.

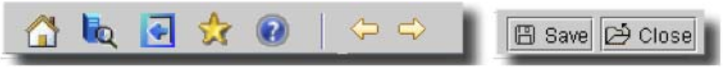
You can also drag and drop panels to relocate them within *Details* screens. The cursor appearance changes when you do this (Web and Java clients differ). To delete a column from the display, drag it *up* off the table, an "X" appears at the cursor when the column deletion is in progress. You can add columns with the *Available Attribute List* button (the plus sign) as explained in Title Bar.

NOTE: You must drag columns from the Available Columns list onto the columns already displayed. You cannot successfully drag and drop them elsewhere on the screen. Access the Available Columns list with the plus to the right of the Layout button.

Toolbar

The toolbar at the top of the initial screen is always visible.

Figure 2-2. Toolbar (two pieces of the same bar)



Hover the cursor over an icon for a text description. The following are in order, left-to-right.The following are buttons in this bar.These icons are active (not grayed out) only when relevant:

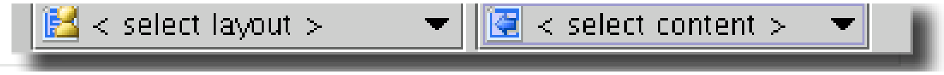
- **Home**—Opens the manager you have specified as your home page. See **SettingsÆ Options** on for how to set a home page.
- **Discovery Wizard**—Opens the discovery wizard.
- **Show / Hide Navigation Window**—This toggles the appearance / disappearance of the left panel of the screen. This has a tree of icons you can click to activate each of the application's features.
- **Options**—Opens the Portal Preferences in the work area.
- **Help**—Opens the Online Help. (See How to Get Help).
- **Prev/Next**—These cycle back and forth through the open screens (listed in the *Windows* menu).
- **Save**—Write the results of your changes in the screen open in the work area to the database. Ctrl+S is the keyboard shortcut.
- **Close**—Closes the active, selected layout in the work area. Ctrl+F4 is the equivalent keyboard shortcut.

NOTE: If you close individual sub-screens, in effect you are editing the layout (you can even close all content in a layout). The next time you open that layout, the deleted screens do not appear. If you want close the entire layout without editing it, use the close button on the toolbar.

Layout Bar

Between the toolbar icons and buttons, two pick lists let you quickly select layouts.

Figure 2-3. Layout Bar



This lets you alter the following:

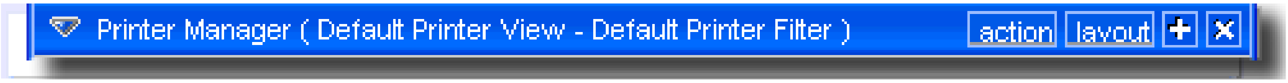
- **<Select Layout>**—This pick list lets you select from layouts configured in LayoutÆ New/Edit/Delete. Several layouts come with the application, and appear in this list by default.
- **<Select Content>**—This pick list lets you select available content for a selected layout. The content appears as an additional panel in the existing display. You can select among choices like *Contact Manager, Event History,* and so on. You can close existing content panels with the 'x' in their upper right corner. When you add content, the application preserves the altered layout, with additional content, later logins by the same user.

NOTE: The content added goes in the wide column only.

Title Bar

The title bar of sub-screens in newer managers also lets you act on the screens.

Figure 2-4. Title Bar



Printer Manager (Default Printer View - Default Printer Filter)
action
layout
+
X

In addition to the features on the Title Bar, the following are available there:

- Action Button / Right-Click Menu
- Layout Button
- Available Attribute List (+)

The title bar includes a *Triangle* at its left end that lets you click it to toggle whether the connected window appears below the title bar. It also includes a *Close Button*, the X at the top right of the panel's toolbar closes that panel. Closing a panel modifies the layout from the default. If you close a panel in a layout, then when you re-open it, your personal layout (with the closed panel) appears onscreen. If you close all the panels with these Xs, then the layout will be blank. Add panels to the screen as described in "*LayoutÆ New/Edit/Delete*" *on page* 38. To close a layout without deleting panels, use the Toolbar button. To re-open a layout (as you last modified or created it), use the Layout Bar.

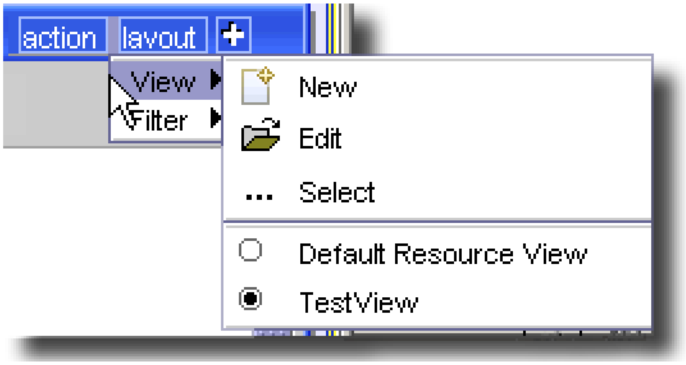
Action Button/Right-Click Menu

You can access the menu to manipulate items appearing on a screen either with the *action* button in the right end of the title bar, or by right-clicking a selected item. The menu items that appear when you do this depend on which application elements and device drivers you have installed.

Layout Button

In addition to the Layout Bar, a *layout* menu button appears when you click the *layout* button next to the action button at the top of most screens. This lets you create, edit and select from the available *View* and *Filter*.

Figure 2-5. Layout Menu



You can create a view, displaying a different arrangement of columns, or edit an existing view. At the bottom of this menu are available views, from which you can select. See "View Editor" on page 220 for a description of the screen that appears when you create or modify views.

Similarly, when you select Filter you can create, edit or select from available filters. See "Filter Editor" on page 213 for a description of the screen that appears when you create or modify filters. See "Filtering" on page 34 for a look at how filters appear and are immediately modifiable.

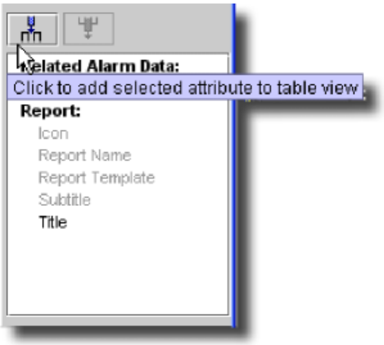
The list of the available views or filters that appears at the bottom of this menu is limited to 25. If you have more of either, click **Select** to open the appropriate manager view where you can select from more than 25.

NOTE: Some applications seed filters, so filters other than those you have created may appear listed. Some managers can display screens other than views and filters too. For example, the Topology screen's layout button displays other Topology Views in this list.

Move Up / Down / Left / Right—This relocates the selected panel in the screen. Other panels relocate to coexist with the moved panel.

Available Attribute List—The *Available Attribute List* button (a plus sign when the panel is closed, a minus sign when it is open) in the title bar toggles the appearance of a list of columns that appear in the selected screen.

Figure 2-6. Available Attribute List Toggle



Click to add selected attribute to table view

You can double-click a displayed attribute, or click the *Add Columns* button at the bottom of this panel, or right click and select *Add* to add it to the columns displayed. You can add more than one if you select multiple columns.

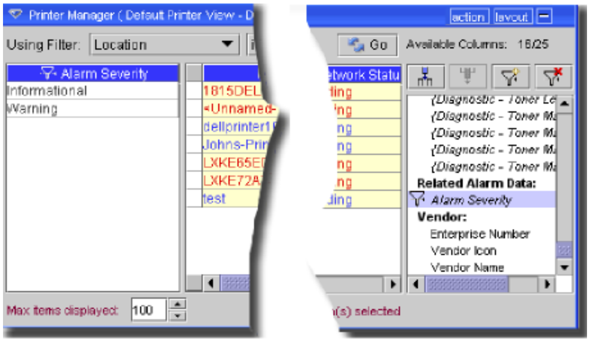
Displayed numbers like Available Detail Panels 2/25 mean that two of the available 25 slots for detail panels are in use. The first number is the count of detail panels open in the screen. The second number is the maximum allowed.

Click the *Layout*→ *Edit Layout* to edit layouts more broadly

Quick Group

One additional feature in some managers is the *Quick Group*. With this, you can display devices grouped by selected attributes. Click the plus (+) sign in the upper right corner of the list in the manager to display the available attributes on the right.

Figure 2-7. Quick Group



Using Filter: Location

Available Columns: 16/25

Max items displayed: 100

As described above, you can click the left two icons above the attribute panel to add or remove a selected attribute from the displayed columns in the list of equipment. You can also drag an attribute name to the list to display it there as a column.

The two icons on the right above the attribute panel group (or un-group) let you display groups of devices based on the attributes selected. When you select Quick Group attributes, those names appear in a panel to the left of the list of equipment. Click on an attribute value in that right panel to display the devices with this value. For example, devices whose last alarm is *Informational* appear when you click that attribute value in the left panel. If you select all values—or none— all devices appear, provided they conform to the filter selected at the top of this screen.

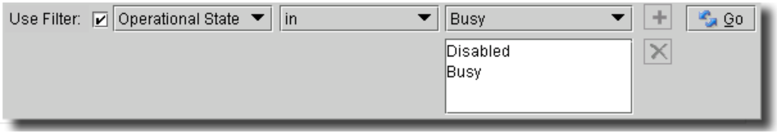
NOTE: The filtered view and Max Items number limit the devices you can Quick Group together. You must click Go after you revise either the filter or Max Items before applying a Quick Group to a revised list.

You do not need to leave the attribute panel open to use the Quick Group panel on the left. Click the minus (-) icon at the top right of this screen to close the attribute panel.

Filtering

Filters appear at the top of most managers. A filter like Name Like * displays all items (<unique ID> like / equals / begins with * is the typical default). Manipulate he pick lists to create more restrictive filters.

Figure 2-8. Filter



Use Filter: ☑ Operational State in Busy

Disabled
Busy

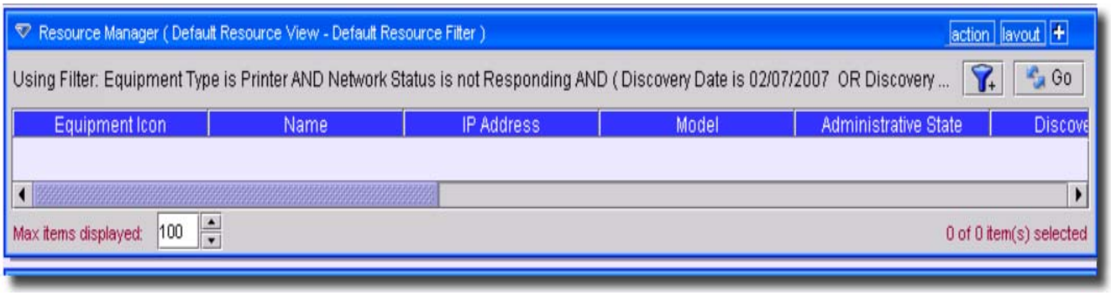
Filters consist of an attribute (equipment attributes like *Operational State*), an operator (like *in* / *not in*, *is* / *is not*) and a match term (like *Active*, *Busy*). Some operators like *in* / *not in* permit multiple match terms. To enter multiple match terms, select a term in the far right pick list, then click the plus sign (+). You can also select listed match terms and delete them (X). For other managers, you can create a different kind of filter .

Click *Go* to filter the display, or to refresh an existing filter's displayed list of items. For more about the capabilities available with filters.This describes creating new filters, and editing existing ones.

Multiple Criteria Filters

You can see filters with more than two criteria in a read only summary filter mode.

Figure 2-9. Multiple Filter Criteria - Summary



Resource Manager (Default Resource View - Default Resource Filter)

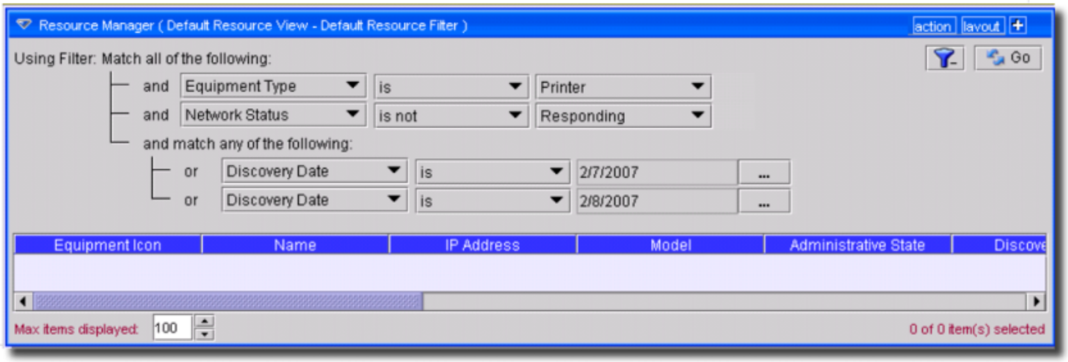
Using Filter: Equipment Type is Printer AND Network Status is not Responding AND (Discovery Date is 02/07/2007 OR Discovery ...

Max items displayed: 100

0 of 0 item(s) selected

While in this summary mode, click the funnel-and-plus button to see an expanded tree view where you can change the filter criteria parameters (attributes, operands and values). The changes to this tree's elements alter the multiple criteria filter itself. Click the funnel-and-minus on the expanded screen to display the summary screen.

Figure 2-10. Multiple Filter Criteria - Expanded



Resource Manager (Default Resource View - Default Resource Filter)

Using Filter: Match all of the following:

- and Equipment Type is Printer
- and Network Status is not Responding
- and match any of the following:
  - or Discovery Date is 2/7/2007
  - or Discovery Date is 2/8/2007

Max items displayed: 100

0 of 0 item(s) selected

You can click the Go button in either the summary and expanded filter to see the effect of the filter. The funnel-and-plus does not appear when a filter can appear in the available space (when it does not have enough criteria to require this summary/ expanded view pair)

You can click the Go button in either the summary and expanded filter to see the effect of the filter. The funnel-and-plus does not appear when a filter can appear

in the available space (when it does not have enough criteria to require this summary

/ expanded view pair).

Menu Bar

The application's menus mirror many of the functions those available in the Navigation Window. Here are a few commonly encountered menu items:

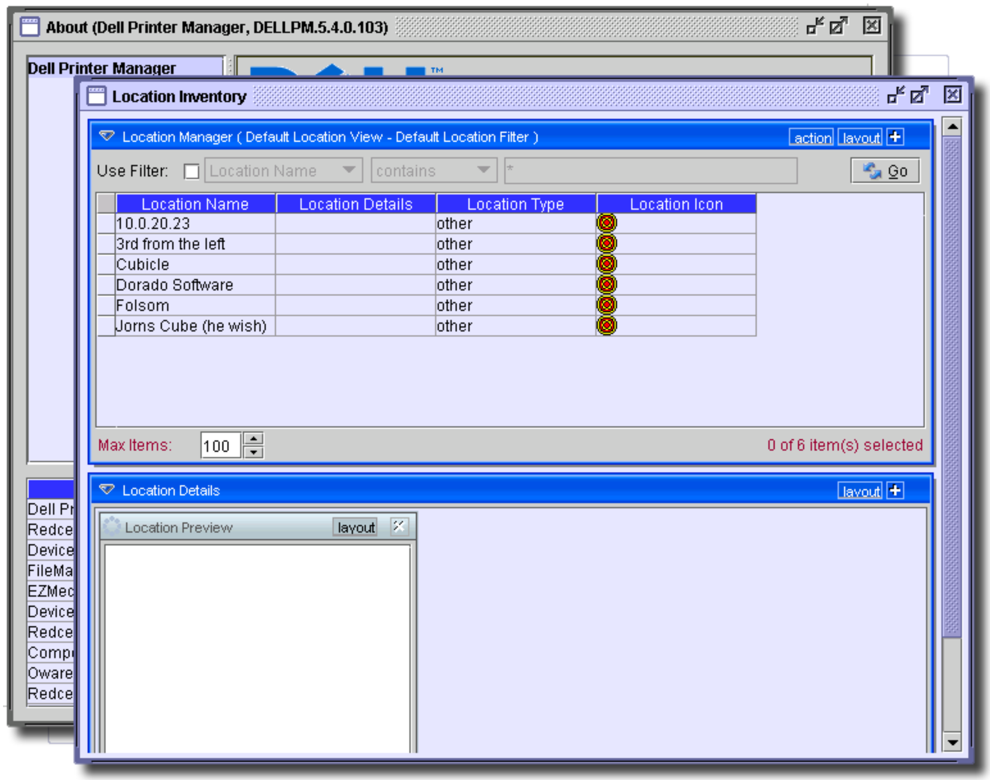
File

- **Open**—Opens submenus like *Inventory* , and other installed options. *File→ Open→ Inventory,* for example, has a menu item for each Inventory node in the navigation window. Menu node equivalents also appear under other application names (for example: Alarms). The subnodes and menu items both open screens in the work area.
- **Home**—Return to the selected home page.
- **Close**—Closes the top screen open in the work area. Ctrl+F4 is the keyboard shortcut.
- **Close All**—Closes all screens open in the work area.
- **Exit**—Close the client application. Ctrl+X is the keyboard shortcut. Ctrl+X, by itself will not close the client in its entirety if there are pending edits (a dialog appears requesting confirmation).

View

- **Launcher**—lets you pick between Multiple Document Interface (MDI) and Browser views. The MDI view lets you see several screens overlapping in the work area (Figure 2-11).

Figure 2-11. MDI View



Location Manager (Default Location View - Default Location Filter)

Use Filter: □ Location Name contains *

Location Name	Location Details	Location Type	Location Icon
10.0.20.23		other	●
3rd from the left		other	●
Cubicle		other	●
Dorado Software		other	●
Folsom		other	●
Jorns Cube (he wish)		other	●

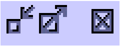
Max Items: 100

0 of 6 item(s) selected

NOTE: You can cascade and tile MDI windows from the *Window* menu.

When you have MDI windows open, the upper right corner has icons that let you (from left to right) minimize, maximize and close the window. Closing the window is equivalent to *Cancel*.
It abandons edits

Figure 2-12. Minimize, Maximize and Close MDI Window



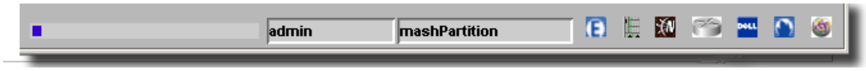
Browser view fills the work area with the selected screen(s). Use the *Windows* menu (or Ctrl+F6) to cycle between screens.

Navigation—To alter the appearance of the Navigation Pane, select By Feature or By Product. The first choice lets you see features grouped together, the last lets you see features grouped by installed product(s). The screens in this document may display or describe either.

Checkboxes let you enable (or uncheck and disable) the following:

- **Show Toolbar**—Displays/hides the toolbar
- **Status Bar** (the bottom of the portal screen)

Figure 2-13. Status Bar



admin

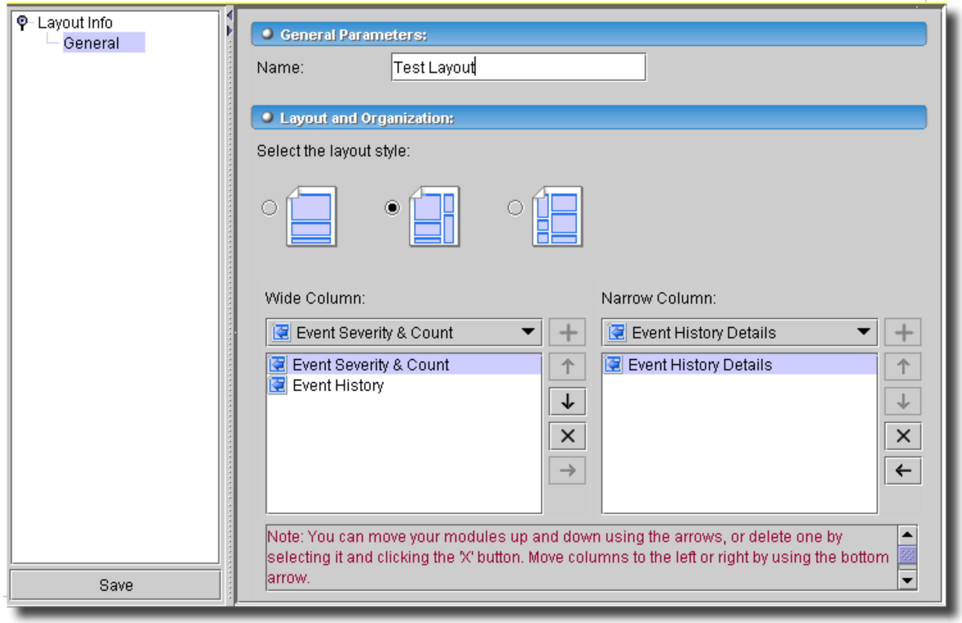
mashPartition

To the left of the status bar text, a progress bar appears that tracks current operations' progress. The left text displays the logged in user, and the right text displays the partition where application server is running.

Layout→ New/Edit/Delete

This menu appears when applicable. It lets you create (*New*), *Edit* or *Delete* a layout for the application. The first two menu options open the layout editor.

Figure 2-14. Layout Editor



Layout Info
General

General Parameters:

Name: Test Layout

Layout and Organization:

Select the layout style:

○ ● ○

Wide Column: Event Severity & Count
- Event Severity & Count
- Event History

Narrow Column: Event History Details
- Event History Details

Note: You can move your modules up and down using the arrows, or delete one by selecting it and clicking the 'X' button. Move columns to the left or right by using the bottom arrow.

Several default layouts appear for each user. If you modify one of these, the application saves it to the database, and it becomes uniquely yours (while retaining the same name as the default layout). Whenever you log on, this modified layout is available to you (or to the originating user). The layout editor lets you configure the following:

General Parameters

- **Name**—A unique identifier for this layout.

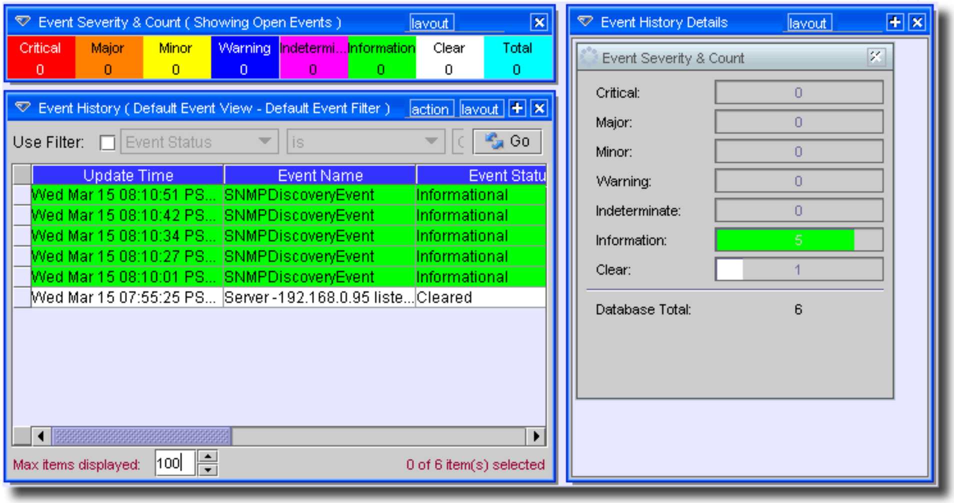
Layout and Organization

- **Select the layout style**—Select a radio button for the layout style you want. These include single column, two column with the narrow column on the right, and two column with the narrow column on the left. The appropriate column content selectors appear when you select a radio button.
- **Narrow / Wide Column**—Use the pick list(s) below these labels to select from available layout column contents. Once you find the item on the list, click the plus sign (+) to add it to the rows below the pick list. The up/down arrows next to these rows to re-order rows. The X removes selected content, and the right/left arrows move selected content between columns.

You can select related components with complementary displays. For example, *Alarm* and *Alarm Details*. When you select an Alarm in *Alarms*, the details of that port appear in the *Alarm Details* panel.

Click *Save* to make this layout available from the layout bar .The result of selecting a layout is that the screen appearance reflects your selections.

Figure 2-15. Layout Appearance



Event Severity & Count (Showing Open Events)

Critical	Major	Minor	Warning	Indetermi...	Information	Clear	Total
0	0	0	0	0	0	0	0

Event History (Default Event View - Default Event Filter)

Use Filter: □ Event Status is

Update Time	Event Name	Event Statu
Wed Mar 15 08:10:51 PS...	SNMPDiscoveryEvent	Informational
Wed Mar 15 08:10:42 PS...	SNMPDiscoveryEvent	Informational
Wed Mar 15 08:10:34 PS...	SNMPDiscoveryEvent	Informational
Wed Mar 15 08:10:27 PS...	SNMPDiscoveryEvent	Informational
Wed Mar 15 08:10:01 PS...	SNMPDiscoveryEvent	Informational
Wed Mar 15 07:55:25 PS...	Server-192.168.0.95 liste...	Cleared

Max items displayed: 100

0 of 6 item(s) selected

Event History Details

Event Severity & Count

Critical:	0
Major:	0
Minor:	0
Warning:	0
Indeterminate:	0
Information:	5
Clear:	1
Database Total:	6

Notice that screens listing items displayed have a *Max Items* field at their bottom. Limiting items displayed with a maximum number improves database search times. The default is typically 100.

Settings

This menu contains the following items:

Settings→ Permissions

This menu lets you open *User Manager*, *User Group Manager*, *Authentication Manager*, *Functional Permissions*, *Object Group Manager*, *Application Security Policy*, *Group Rights Summary*, and *Register License* items.

Settings→ Configuration

This menu lets you open *Control Settings*, *Filter Config* and *Inventory Config* editors. The application's *Administration* Section describes most of these items.

Settings→ Options

Lets you select the default page that appears when you open the application (the home page). You can also right-click nodes on the navigation pane to select one as a home page.

NOTE: You can also right-click a node on the navigation window and select Set as Home Page from the subsequent menu.

Settings→ Change Password

This opens a dialog that lets the logged in user change his password.

Window

The *Window* menu lets you select which screen appears in the work area if you have more than one open. *Next* and *Previous* arrows cycle through the open screens, while *Cascade* and *Tile* arrange them.

NOTE: If you open more than 20 windows, the Too Many Windows error message appears. To change the default of 20, set a property `redcell.open_window_warning_level=nn`, where `nn` is the number of windows. Best practice for good performance is to select fewer windows, or leave the default.

Help

This menu item lets you open *Help* for the open screen, or the entire online help text table of contents (*Help Topics*), or the *About* box . *Help→ Product Updates* opens a website where you can find additional updates and add-ons for this software.

Hiding and Displaying the Navigation Window

You can conceal the navigation window to increase the size of your work area. To hide the navigation window click on small arrows on the bar between it and the work area. This is a toggle; click those arrows again to redisplay the navigation window. Or, to resize it, drag the bar to a new location.

Work Area

The work area displays the application's managers, wizards, and editors. You can change the display of the items in this area between an HTML browser view and an MDI (Multiple Document Interface) view by selecting *View→ Launcher*, then selecting the desired view.

Column Titles

You can edit the column titles that appear in editors.

Color Conventions

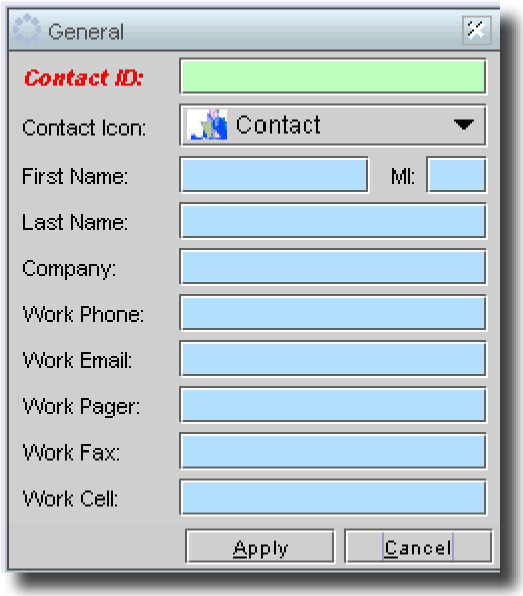
In many newer screens, blank fields have a blue background. These change to green when you change a field's contents, then click Apply. The green backgrounds persist until you save them to the database. If saving succeeds, background turns white, if it fails, then the green remains visible.

Mandatory fields have bold italic labels. If you do not enter a mandatory field when you edit a panel, a Validation error appears and the mandatory field label font turns red bold italic, and the background remains green. Labels with a violet background, and bold dark blue text indicate a warning is associated with the attribute value.

Detail Panels

When you select items at the top of a screen, frequently the details of those items appear in the Detail Panels at the bottom of the screen (though these do not appear in all screens).

Figure 2-16. Detail Panels



The Edit button appears at the bottom of detail panels if you can edit their contents.Cancel your edit if you want to return to the previous parameters.

NOTE: To refresh detail panels, select another item in the manager, then re-select the one for which you want details refreshed.

Closing and Saving

Many panels that appear in the Work Area have no *Close* or *Save* buttons—for example, the *Editing Authentication* screen you can access from *Authentication Manager* .To act in such panels, select menu items like *File* → *Close* (Ctrl+F4) or *File*→ *Save* (Ctrl+S). You can also use *Save* icon on the toolbar, or the X in the upper right corner of screens (closing screens typically prompt you to save work). For an account of the consequences of using the various X icons.

3

Conventions and Common Operations

Overview

This section discusses conventions used throughout these guides (online and print) and operations common to the application.

Conventions

The following conventions appear throughout this information:

Selecting Items From Menus

The phrase "select *Inventory* > *Locations* from the *File* > *Open* > menu or the Navigation Window" means you should do one of the following:

- click on the menu item listed. (*Inventory* is a subitem in the *Open* menu item in the *File* menu.)
- click on the *Inventory* node to expand it in the Navigation Window, then click on *Locations*.

NOTE: This can also indicate sub-nodes on a tree like the navigation window. For example: Inventory > Locations

The Command and Eraser Buttons

The command button has an ellipsis (...) on it [...] and appears whenever the command's completion may need additional steps.

Clicking on this button displays another dialog that typically lets you select an entry for an adjacent field.

The eraser button [✎] clears the adjacent field. Often it appears next to a field with a command button at the other end.

The GO Button

When you open a typical manager, you can then select a filter and click on *Go* to display all appropriate matches. Likewise, when you create a new record the manager may not automatically refresh. You must click on *Go* or *Refresh* to refresh the display.

Open / View and Import / Export

Users without write permission see *View* rather than *Edit* or *Open*. The application may gray out *Import* or *Export* menu items if permissions do not exist to use them.

Accelerators / Shortcuts

Whenever you see a letter underlined in the title of a menu or button, you can select that menu or button with Alt + [the letter]. Other shortcuts appear in the menus themselves.

Common Operations

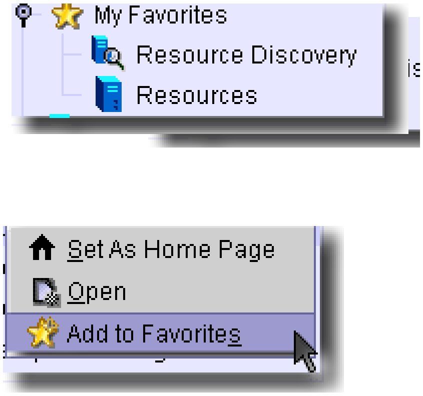
The following operations appear throughout the application:

Creating my Favourites

By default, two nodes of the navigation pane appear in **My Favorites** at its top:

Resource Discovery, and **Resources**

Figure 3-1. My Favorites, and Add to Favorites



Right-click any node in the navigation pane and select **Add to Favorites** to duplicate it in the **My Favorites** node.

Saving

Some dialogs have a *Save* button to save the results of your actions with that screen. If you do not see such a button, however, you can still use the toolbar *Save* icon and menu item *File* > *Save* with the same effect. You can also click the *Save* button whenever present within a screen itself to save your edits.

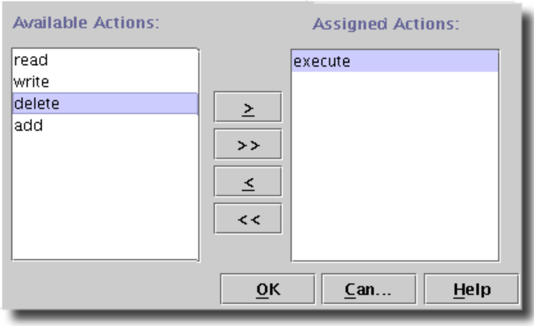
Previous

Some screens have a *Back* or *Previous* button. These are typically wizards, and the button allows you to return to the previous step. The larger screen also contains a pair of *Prev* / *Next* arrows in the toolbar (see Toolbar in the Navigation chapter). These let you cycle through the screens visible in the Windows menu (open screens)

Moving Items Between Lists

Many dialogs let you move items from one list to another.

Figure 3-2. Moving Between Lists



To move a single item from one list to another, select it and click on the > or < button. To move several items from one list to another, hold down the *Ctrl* key while clicking on the desired items. Click on the > or < buttons. To move all items from one list to another, click on the >> or << button, if it is available. You can see such lists in the Discovery Wizard when you select authentication objects .

Sorting Columns in Managers

You can sort lists of items in a column. To do so, click on the column header. Clicking on the heading again reverses the sort order. An arrow appears in the column to indicate it is the one sorted.

Setting Subnets

Many devices managed by this software set IP address and subnet combinations. Within the limitations of your network and devices, the following suggests some typical subnet calculations.

Consider this Class C subnet example:

192.168.10.33 with a subnet mask of 255.255.255.224

To calculate the subnet and broadcast address of that IP address:

256 - 224 = 32.

Subnets therefore repeat in increments of 32 (32, 64, 96...etc.) 192.168.10.33 must therefore be part of the 192.168.10.32 subnet. The next subnet is 64, so the broadcast address is 63 (the number just before the next subnet). The valid host range for this subnet is 10.33 - 10.62.

Another (class C) example:

192.168.10.33 with a subnet mask of 255.255.255.240.

To calculate the subnet and broadcast address of that IP address:

256 - 240 = 16.

Subnets therefore repeat in increments of 16 (16, 32, 48...etc.) This address must therefore be part of the 192.168.10.32 subnet, and the broadcast address is 47. The valid host range is 33 - 46.

Class B subnets are a little more complex. For example:

172.16.10.33 subnet mask: 255.255.255.224.

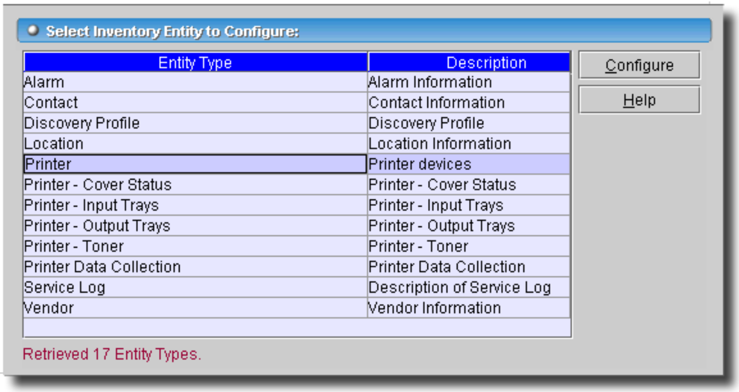
Subnets repeat in increments of 32 (256-224 = 32; 32, 64, 96...etc.). This is between 10.32 and 10.64, and the broadcast address is 10.63.

NOTE: A free subnet calculator is available at **www.dewassoc.com/support/useful/subnetcal.htm**

Inventory Config

You can configure custom fields that appear by default in the application's filters, managers and editors with the Inventory Config manager. Access this through *Settings > Configuration > Inventory Config*.

Figure 3-3. Inventory Config Manager



Entity Type	Description
Alarm	Alarm Information
Contact	Contact Information
Discovery Profile	Discovery Profile
Location	Location Information
Printer	Printer devices
Printer - Cover Status	Printer - Cover Status
Printer - Input Trays	Printer - Input Trays
Printer - Output Trays	Printer - Output Trays
Printer - Toner	Printer - Toner
Printer Data Collection	Printer Data Collection
Service Log	Description of Service Log
Vendor	Vendor Information

Retrieved 17 Entity Types.

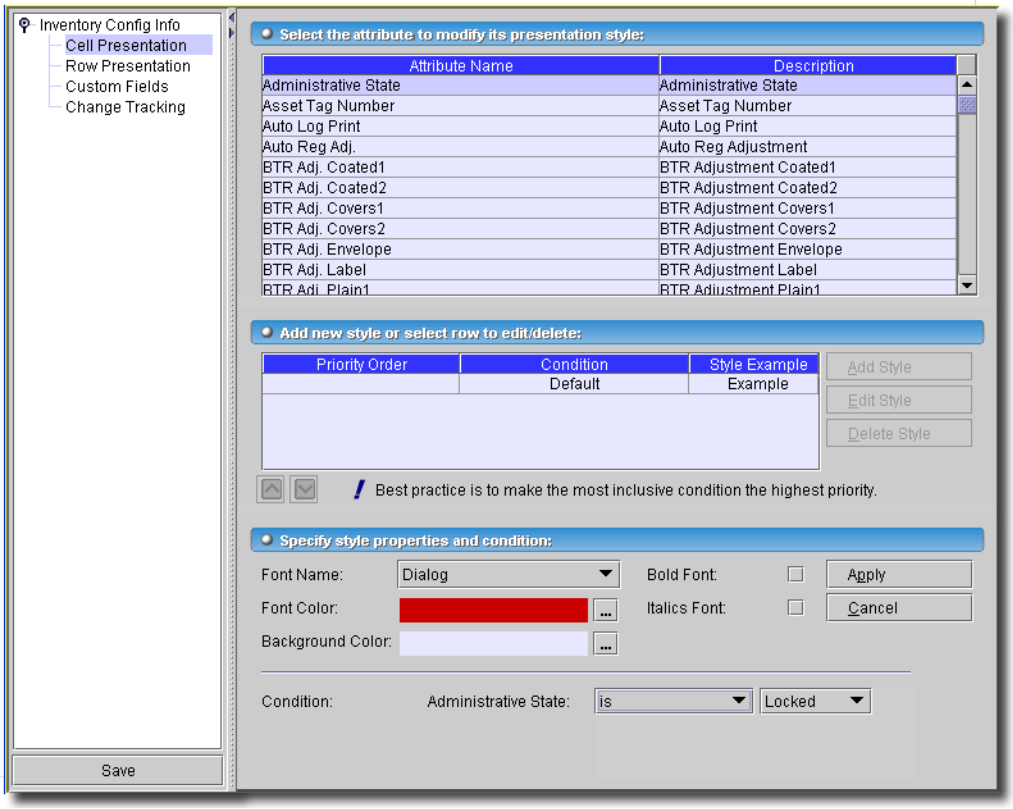
In the initial screen the *Entity Type* and *Descriptions* appear listed in rows. Select a row and click *Configure* to edit settings for this type. The Config Editor appears.

NOTE: You must restart the client and server to see the effect of some changes in this editor. Client restart is necessary to see the effects of presentation style changes, and application restart is necessary to see the effects of change tracking alterations.

Config Editor

The config editor lets you alter the presentation of information in screens and reports, it lets you configure custom fields, and change the type of tracking the application performs.

Figure 3-4. Config Editor - Cell Presentation


Inventory Config Info
Cell Presentation
Row Presentation
Custom Fields
Change Tracking
Save
Select the attribute to modify its presentation style:
Add new style or select row to edit/delete:
Add Style
Edit Style
Delete Style
Specify style properties and condition:
Apply
Cancel

Attribute Name	Description
Administrative State	Administrative State
Asset Tag Number	Asset Tag Number
Auto Log Print	Auto Log Print
Auto Reg Adj.	Auto Reg Adjustment
BTR Adj. Coated1	BTR Adjustment Coated1
BTR Adj. Coated2	BTR Adjustment Coated2
BTR Adj. Covers1	BTR Adjustment Covers1
BTR Adj. Covers2	BTR Adjustment Covers2
BTR Adj. Envelope	BTR Adjustment Envelope
BTR Adj. Label	BTR Adjustment Label
BTR Adj. Plain1	BTR Adjustment Plain1

Priority Order	Condition	Style Example
	Default	Example

Best practice is to make the most inclusive condition the highest priority.

Font Name: Dialog

Font Color: 🟥

Background Color:

Bold Font: □

Italics Font: □

Condition: Administrative State: is Locked

It has the following sub-panels

- Cell Presentation
- Row Presentation
- Custom Fields
- Change Tracking

NOTE: Not all types of data support all the example options that appear here.

The following sections describe these panels.

Cell Presentation

This panel configures the presentation of attributes in cells in managers. When you select a listed attribute in the upper panel its applicable presentation styles appear in the middle of the screen. The *default* style appears for all items. With the buttons to the right of the styles, you can *Add Style, Edit Style,* or *Delete Style.* You must select a listed style to do the last two.

When you add, or edit a style, the panel labelled *Specify style properties and conditions* appears in the lowest panel. This has the following fields and pick lists:

- **Font Name**—Select from a pick list of available fonts.
- **Font Color**—Select the font color picker that appears when you click the Command Button (...) to the right of the displayed color.
- **Background Color**—Select the background of the cell displaying the attribute information from the color picker that appears when you click the Command Button (...) to the right of the displayed color.
- **Bold Font**—Check to activate.
- **Italics Font**—Check to activate.
- **Condition**—This portion of the panel makes the display reflect an attribute condition. The attribute already appears, by default. Specify the condition by selecting an operator and value (some fields permit a range of values).

Click *Apply* to accept your edits, and list the condition in *Priority Order.* Click *Cancel* to abandon them.

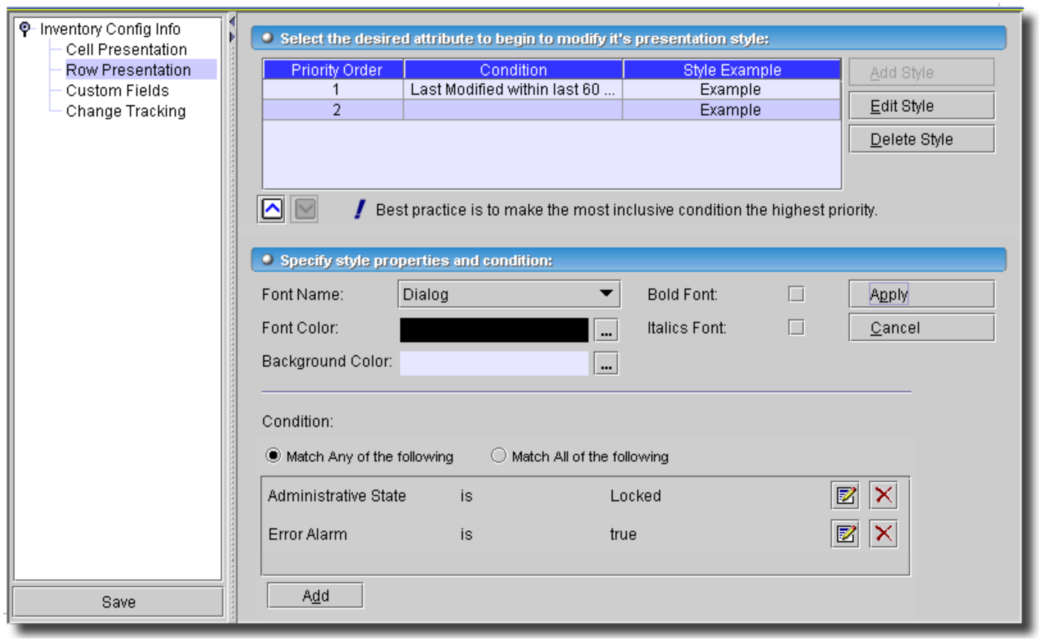
The condition then appears as a row in the middle of this screen. The first column of this table indicates its priority (the lower the number, the higher the priority). You can change priority order of selected rows with the up/down arrows below this list. The second column is a reminder of the *Condition* you set, and the third is an example of what text looks like when the attribute fits the condition.

NOTE: Best practice makes the most inclusive condition the highest priority.

Row Presentation

This panel configures the presentation of rows of attributes in managers.

Figure 3-5. Config Editor - Row Presentation



Priority Order	Condition	Style Example
1	Last Modified within last 60 ...	Example
2		Example

Best practice is to make the most inclusive condition the highest priority.

Font Name: Dialog

Font Color: ■ ...

Background Color: ...

Bold Font: □

Italics Font: □

Condition:

● Match Any of the following ○ Match All of the following

Administrative State	is	Locked
Error Alarm	is	true

With the buttons to the right of the styles, you can *Add Style*, *Edit Style*, or *Delete Style*. You must select a listed style to do the last two.

When you add, or edit a style, the panel labelled *Specify style properties and conditions* appears in the lowest panel. This has the following fields and pick lists:

- **Font Name**—Select from a pick list of available fonts.
- **Font Color**—Select the font color picker that appears when you click the Command Button (...) to the right of the displayed color.
- **Background Color**—Select the background of the cell displaying the attribute information from the color picker that appears when you click the Command Button (...) to the right of the displayed color.
- **Bold Font**—Check to activate.
- **Italic Font**—Check to activate.
- **Condition**—Select whether you want to *Match Any* or *Match All* of the conditions you add. The display then reflects an attribute condition. The attribute already appears, by default. Specify the condition by clicking *Add*, then selecting an attribute, operator and value (some fields permit a range of values). Click the green check mark to accept a single condition, or the click the blue

curved arrow to cancel editing and revert to whatever existed before you began editing. You can add more than one. You can also remove conditions by clicking the red "X," or edit an existing condition by clicking the notepad icon.

Apply to accept your edits, and list the condition in *Priority Order.* Click *Cancel* to abandon them.

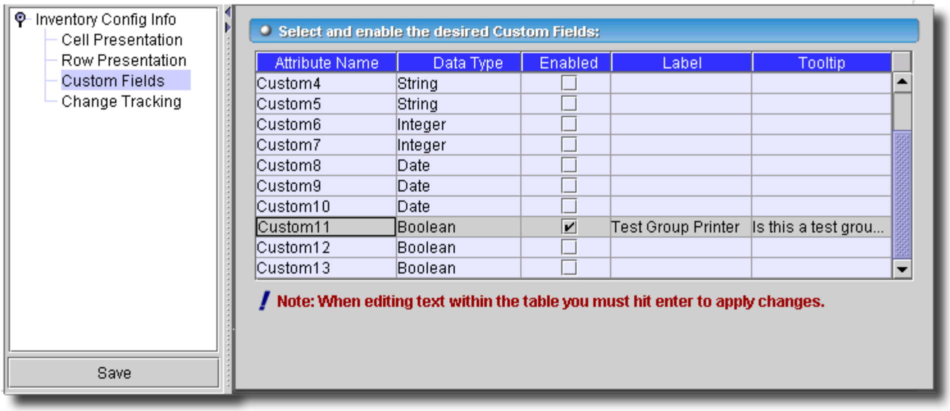
The condition then appears as a row at the top of this screen. The first column of this table indicates its priority (the lower the number, the higher the priority). You can change priority order of selected rows with the up/down arrows below this list. The second column is a reminder of the *Condition* you set, and the third is an example of what text looks like when the attribute fits the condition.

NOTE: Best practice makes the most inclusive condition the highest priority.

Custom Fields

You can create custom fields for the selected entity type in this screen. The fields here depend on the entity you select in Inventory Config.

Figure 3-6. Config Editor - Custom Fields



Select and enable the desired Custom Fields:

Attribute Name	Data Type	Enabled	Label	Tooltip
Custom4	String	□		
Custom5	String	□		
Custom6	Integer	□		
Custom7	Integer	□		
Custom8	Date	□		
Custom9	Date	□		
Custom10	Date	□		
Custom11	Boolean	☑	Test Group Printer	Is this a test grou...
Custom12	Boolean	□		
Custom13	Boolean	□		

Note: When editing text within the table you must hit enter to apply changes.

This screen lets you edit rows describing custom fields directly. Click in a column and start typing (some are read-only). The following are the columns:

- **Attribute Name**—This is a simple identifier, like *Custom1*, *Custom2*, and so on. (read only)
- **Data Type**—This describes the data type of the custom attribute (*String*, *Integer*, *Date*, *Boolean*–read only). When you select *Boolean* the field is a checkbox.
- **Enabled**—Check *Enabled* to activate the selected custom field.
- **Label**—The label that precedes the custom field(s) on the screen.
- **Tooltip**—The tip that appears when you hover the cursor over the custom field.

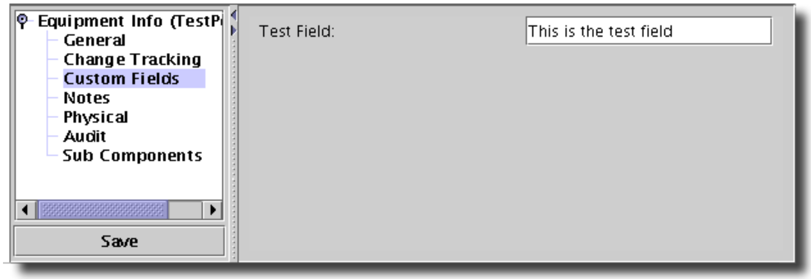
Add Custom Attribute Definition

Use the **Add New Attribute** button to create additional attributes you have configured in the lowest panel on this screen.

NOTE: Changes take effect only on screens you open after configuring the custom field.

Once you configure these labels, they appear in the editor appropriate to the Inventory Type selected.

Figure 3-7. Custom Field in Editor



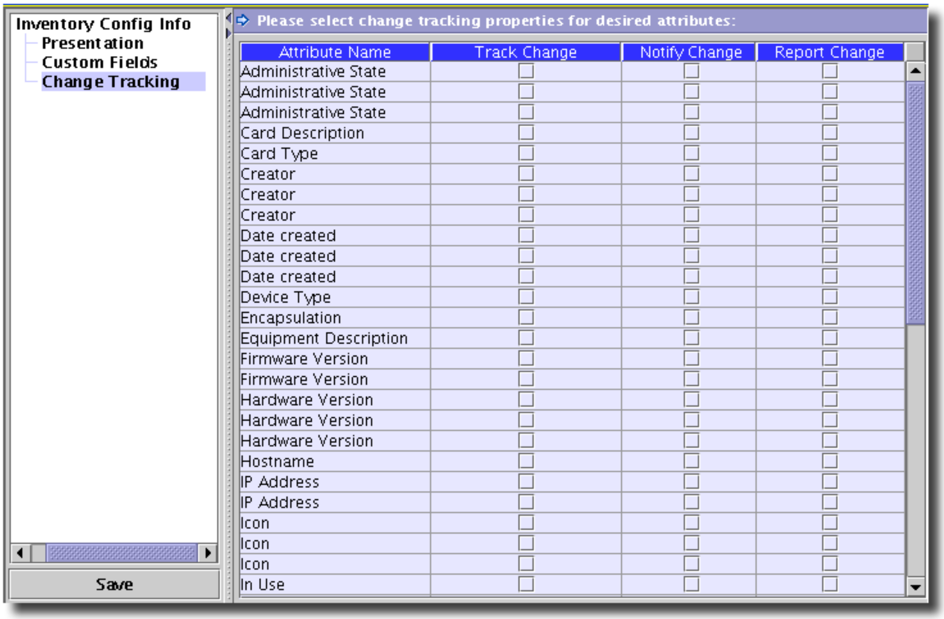
Test Field: This is the test field

Find an example of the equipment in the Resources Manager, select it, and click *Open* to see the custom field. You can also create filters to display equipment based on custom field contents.

Change Tracking

This panel lets you select types of notifications for the selected inventory type.

Figure 3-8. Config Editor -Change Trcking



Please select change tracking properties for desired attributes:

Attribute Name	Track Change	Notify Change	Report Change
Administrative State	□	□	□
Administrative State	□	□	□
Administrative State	□	□	□
Card Description	□	□	□
Card Type	□	□	□
Creator	□	□	□
Creator	□	□	□
Creator	□	□	□
Date created	□	□	□
Date created	□	□	□
Date created	□	□	□
Device Type	□	□	□
Encapsulation	□	□	□
Equipment Description	□	□	□
Firmware Version	□	□	□
Firmware Version	□	□	□
Hardware Version	□	□	□
Hardware Version	□	□	□
Hardware Version	□	□	□
Hostname	□	□	□
IP Address	□	□	□
IP Address	□	□	□
Icon	□	□	□
Icon	□	□	□
Icon	□	□	□
In Use	□	□	□

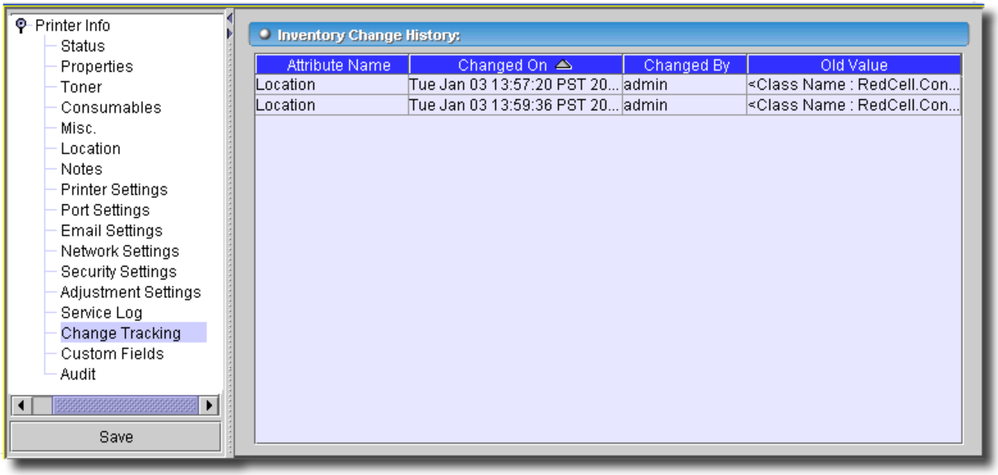
Setting up change tracking is an administrative task. You must first use the *Inventory Config* screen to select a type of inventory, then configure *Change Tracking* for that type. Select the attributes to track in the *Change Tracking* screen. You no longer must re-start the application server after having selected which attributes to track before any changes become visible.

If you do not have the correct authentication or permission to access the devices for which you want to perform change tracking, your system may be unable to retrieve attribute values and track changes may fail. The application server may display "unable to retrieve attribute" errors in such cases.

The listed attributes (the left column) vary, depending on the inventory type you selected in Inventory Config. Check one of the following three columns to change the tracking for the selected attribute:

- **Track Change**—Check to enable change tracking. This produces a log of changes for the selected inventory type and attribute. These typically appear in an Change Tracking editor panel.

Figure 3-9. **Change Tracking**



Attribute Name	Changed On	Changed By	Old Value
Location	Tue Jan 03 13:57:20 PST 20...	admin	<Class Name : RedCell.Con...
Location	Tue Jan 03 13:59:36 PST 20...	admin	<Class Name : RedCell.Con...

This history enumerates the changes *Attribute Name*, when it was *Changed on*, who it was *Changed by* and the *Old Value* in the rows of its display.

- **Notify Change**—Emit Change Notification which can trigger an action (see "Events, Rules and Actions" on page 187).
- **Report Change**—Save Changes for Reporting

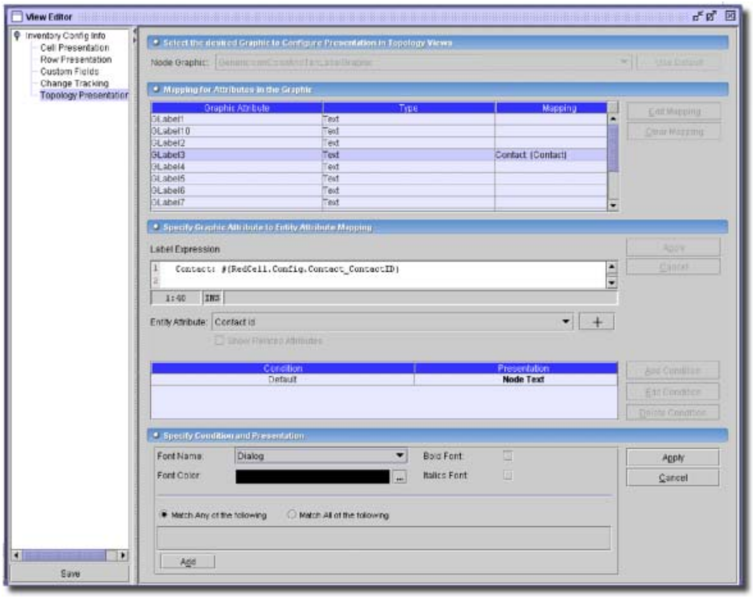
Click *Save*, and the changes in presentation, custom fields and tracking are preserved in the database for the selected inventory entity type.

NOTE: Setting up change tracking is an administrative task. You must first use the *Inventory Config* screen to select a type of inventory, then configure *Change Tracking* for that type. Select the attributes to track in the *Change Tracking* screen. Finally, you must re-start the application server after having selected which attributes to track before any changes become visible.

Topology Presentations

This screen configures the presentation of some entities you can display in Topology views (see "Topology Views" on page 153).

Figure 3-10. Topology Presentations



Graphic Attribute	Type	Mapping
GLabel1	Text	
GLabel10	Text	
GLabel2	Text	
GLabel3	Text	Contact (Contact)
GLabel4	Text	
GLabel5	Text	
GLabel6	Text	
GLabel7	Text	

Label Expression

```
Contact: #(RedCell.Config.Contact_ContactID)
```

1:40 INS

Entity Attribute: Contact id

Condition	Presentation
Default	**Node Text**

Font Name: Dialog

Font Color:

Bold Font: □

Italics Font: □

● Match Any of the following ○ Match All of the following

The screens vary, depending on the entity you are editing, the following describes a representative example. The *Contact*-related screen displays the following:

Select the Desired Graphic

Node Graphic—Select the desired graphic when this entity appears in Topology screens from the pick list. The contents of the next section (Mapping for Attributes in the Graphic) depends on the graphic you select here. Installation seeds the available graphics on the pick list. If you do not select a graphic, the application uses the default. You can click **Use Default** to return a selected graphic to the default.

If you select a *Link* as the entity type, no such selection is possible. Nevertheless, in general terms, you can configure the link's attributes (*Pattern*, *Width*, *Color*, *Label* and so on) as described below.

Mapping for Attributes in the Graphic

This portion of the screen displays the attributes associated with the selected graphic (or other entity). With the buttons to the right of this portion of the screen, you can *Clear Mapping* which removes any previous association for the attribute, or *Edit Mapping* which opens the editor below this screen.

Specify Graphic Attribute to Entity Mapping

This portion of the screen displays a text area (*Label Expression*) in which the selected *Entity Attribute* mappings appear. To enter such a mapping, select an *Entity Attribute* from the pick list next to that label and click the plus (+) to its right. The programmatic text designation for that attribute appears in the *Label Expression* text area. For example: `#{Redcell.Config.Contact_ID}`. You can also enter a combination of such designations and fixed, non-variable text you type in. For example:

```
Contact:#{Redcell.Config.Contact_Contact_ID}
```

This configures the Topology display for a contact as the word “Contact:” followed by the contact ID.

NOTE: If you select a graphic, like `#{Redcell.Config.Contact_Contact_Icon}`, then only the text label for that icon appears in text fields. This editor does not correct you if you select a graphic in a text field.

Click **Apply** to accept your edits and alter the list at the top of this screen, or **Cancel** to abandon them.

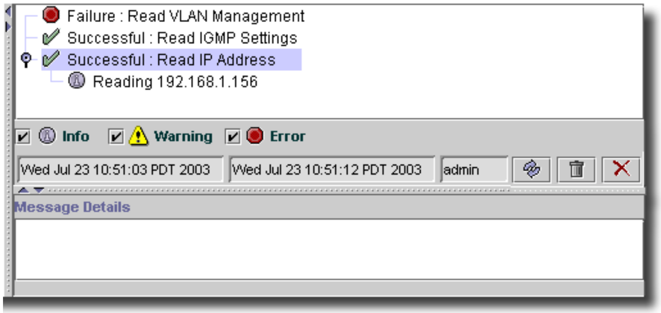
Specify Condition and Presentation

Finally, you can set the appearance of these configured attributes to alter based on filters. Click **Add Condition** to open an editor at the bottom of the screen to create such a condition (or *Edit Condition* to alter an existing, selected condition). Specifying conditions is like creating filters as described in "Filtering" on page 34. When the filter is satisfied, the appearance (presentation) configured applies within the Topology view. Click **Apply** to accept your edits, or **Cancel** to abandon them.

Results

The result of many application actions appears in a job status screen. These are preserved and catalogued in Audit Trail Manager.

Figure 3-11. Results Screen



Failure : Read VLAN Management
Successful : Read IGMP Settings
Successful : Read IP Address
Reading 192.168.1.156

☑ Info ☑ Warning ☑ Error

Wed Jul 23 10:51:03 PDT 2003 | Wed Jul 23 10:51:12 PDT 2003 | admin

Message Details

At its top, this screen displays a series of actions and sub-actions as a tree. When you select an individual action, *Message Details* (if available) appear in the lowest panel. The bar between these two panels lets you check the type of messages to display (*Info*, *Warning*, *Error*) and displays the time/date of the beginning and end of the selected message's action, and the user who initiated it. Icons to the right of the time/date information let you refresh the screen, let you refresh the view, remove the current job from the view, or cancel a selected running job, respectively.

How to Get Help

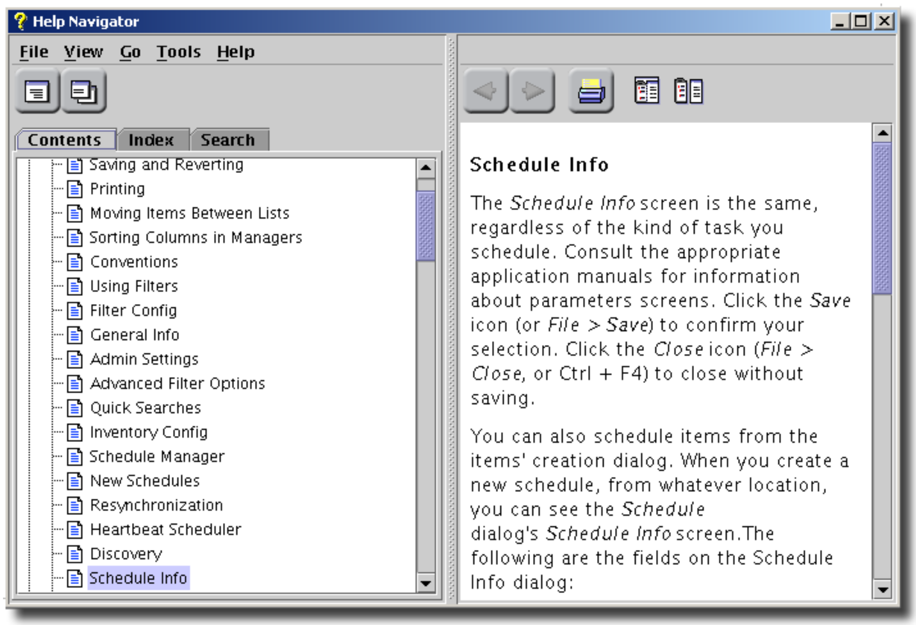
To access the electronic version of the manuals you must have Acrobat Reader installed. See the installation CD for information about viewing Acrobat files, and for an installation of that free reader.

The helpset may contain information about features your installation does not have. Typically you can license these features (or simply ignore the help, if it is not relevant).

Online Help

You can access the online help by opening the *Help* > *Help topics* menu item, clicking on the *Help* icon in the Toolbar, or by pressing the F1 key. This displays the Online Help Table of Contents, or a screen appropriate for the context.

Figure 3-12. Online Help System



Schedule Info

The *Schedule Info* screen is the same, regardless of the kind of task you schedule. Consult the appropriate application manuals for information about parameters screens. Click the *Save* icon (or *File > Save*) to confirm your selection. Click the *Close* icon (*File > Close*, or Ctrl + F4) to close without saving.

You can also schedule items from the items' creation dialog. When you create a new schedule, from whatever location, you can see the *Schedule* dialog's *Schedule Info* screen.The following are the fields on the Schedule Info dialog:

Pressing F1 typically displays help relevant to the screen that has focus in your application. Double-click a topic to open that topic in the right panel. You can also find relevant help topics by searching the *Index* tab, or with a full-text search from the *Search* tab. At its top, the panel displaying topics has (left-to-right) a button to restore focus to the *Navigator* (table of contents/index/search) panel, forward and back arrows to let you scroll though several topics, a print button, and dock/undock icons that let you combine/un-combine the *Navigator* and *Help Topic* windows.

⚠ **CAUTION: Because of the flexibility of this software, help and manuals may describe features unavailable for your system. This can be true either because you do not have permissions to access everything, or because you do not have some options installed.**

NOTE: Although index entries are frequent, they cannot comprehensively list every topic for which you may need help. When you cannot find the index entry you want, use the *Search* tab to perform a full-text search of the helpset. A similar feature exists for the Acrobat equivalent of the helpset, the manuals.

Troubleshooting

You can now use the `getlogs` script to package relevant logs if you need technical support. This script creates a logs.jar file in the root installation directory, and moves any existing copy of `logs.jar` to `oware\temp`. This jar compresses all logs necessary for troubleshooting. Read the jar yourself, or forward this jar to technical support to help troubleshoot.

Common Problems

The following are common problems you may want to check as part of your troubleshooting routine:

- Monitored devices must be configured to connect and send SNMP traps to the element management system.
- External FTP servers are preferable to internal, for performance reasons, and, if necessary, the network equipment using FTP to send/receive configuration files must have it enabled. If Backup / Restore fails, typically this means the FTP / TFTP server is offline or incorrectly configured. Check in the File Server Manager to correct this.

Troubleshooting Tips

The following are helpful tips when troubleshooting your application:

- **Connectivity to devices**—When devices are not discovered, ensure they are connected to the network with the `ping` command. Type the following:

  ```
  ping <device IP address>
  ```

  on a command line. If successful, several messages like the following appear:

  ```
  Reply from <device IP address>: bytes=32 time=1ms TTL=128
  ```

- **Correct community strings/passwords**—Verify SNMP community strings and command line passwords are accurate if you have difficulty connecting to a device that responds to `ping.` You can inspect these in the *Settings > Permissions > Authentication Manager*. You must re-enter passwords concealed by asterisks.
- **Firmware and Operating Systems**—Verify the equipment’s firmware and operating systems are among those supported. Supported firmware and operating systems appear listed in the application’s *About* screens.

For more troubleshooting tips, consult the *Installation Guide*.

4

Discovery

Overview

Discovery is how the application identifies and catalogs network elements. Once discovery identifies a network element, you can create equipment objects, so the application can communicate with the element. The type and depth of discovery depends on installed applications and device drivers.

Discovery based on installed drivers consists of physical discovery. Physical discovery represents the device

You can do discovery interactively, through the A*dvanced Discovery Wizard*, or you can set it up in advance and schedule it for automatic execution, as described in *Scheduling Discovery.*

Once discovery finds a device, it puts that device in the Discovered Entities section of the Resources Manager unless overridden by the installed device drivers.

Preventing Discovery Problems

The following describes some preventive practices to do when you discover a mixed vendor / mixed class network.

1. Manually telnet to a device to verify that you have the correct authentication information.
2. If you know the device, look at the config and verify that the SNMP community string is correct.
3. Discover the device.
4. If there are any problems with any devices, then telnet to any problem devices and verify that telnet works / authentication is good.
5. If there are SNMP problems, use this application's SNMP tool.

Here's how to use that SNMP tool:

1. With the application server running, open a shell (Start > Run cmd). In thatshell, type the following commands (followed by [Enter]):
2. oware.
3. snmpapitalk.
4. dest <IP address of device you want to talk to>
5. read <read community>
6. get <snmpoid>. For the snmpoid, you can use syslocation or sysname

A response should appear. If the device does not respond, then there is a problem with either the community string, a firewall or some other network problem.

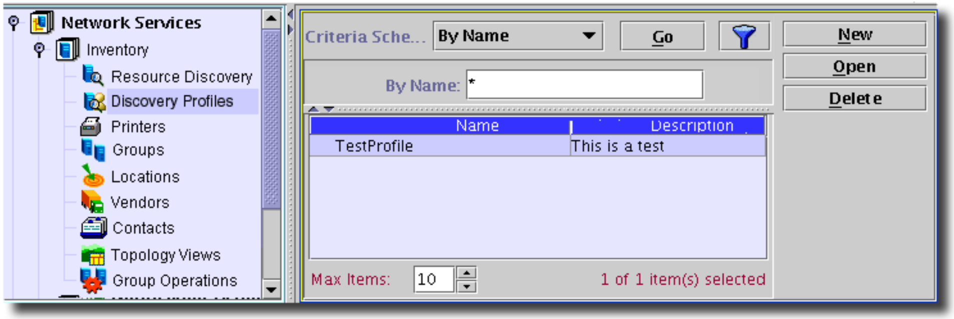
Resolve this before proceeding with discovery.

NOTE: This software comes with a default database aging policies to ensure your database does not overflow. You can modify this policy with the DAP editor.

Discovery Profiles

Profiles store the parameters for discovery, so you can easily execute (or schedule) repeated discoveries.

Figure 4-1. Discovery Profiles



Criteria Sche... By Name

By Name: *

Name	Description
TestProfile	This is a test

Max Items: 10

1 of 1 item(s) selected

This manager has the following buttons:

- **New**—Create a new profile. See Creating and Editing Discovery Profiles.
- **Open**—Edit an existing, selected profile. See *Creating and Editing Discovery Profiles*.
- **Delete**—Delete an existing, selected profile.

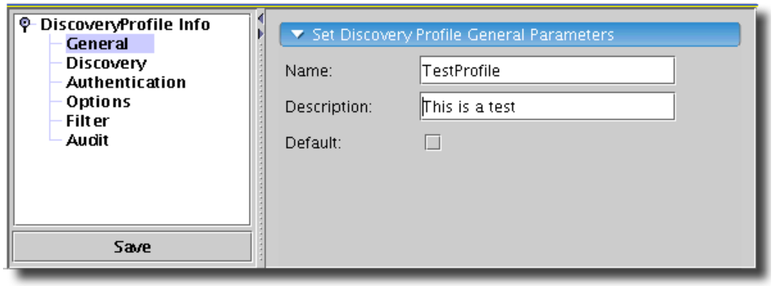
File > Import / Export—Import or export the listed profiles from/to an XML file.

NOTE: If the imported profiles refer to authentication credentials that do not exist on the system to which you have imported them, they do not work.

Creating and Editing Discovery Profiles

Open the *Discovery Profiles* manager, and click *New* to create a profile.

Figure 4-2. Discovery Profile Editor - General Tab



Name: TestProfile

Description: This is a test

Default: □

This editor has the following tabs:

- *General Tab*
- *Discovery Tab*
- *Authentication Tab*
- *Options Tab*
- *Filter*
- *Audit*

Click *Save* to preserve the profile you have edited. Click *Go* in the manager that appears in *Discovery Profiles* to see the profile listed.

General Tab

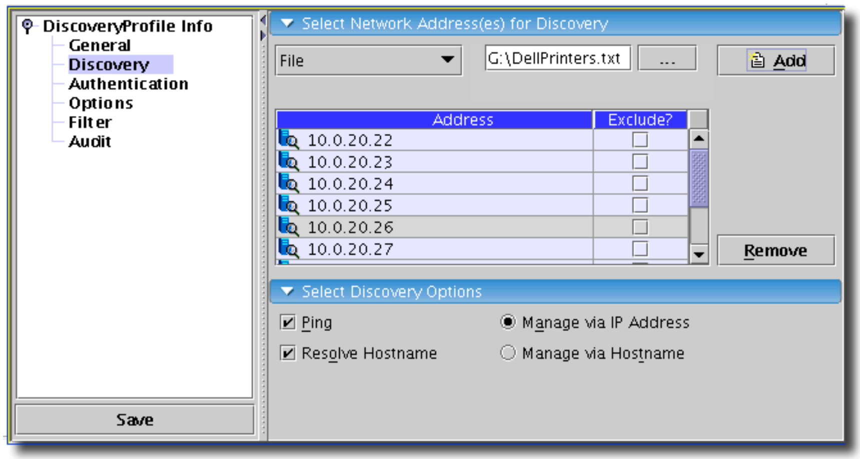
This tab labels and classifies the discovery profile. It has the following fields:

- **Name**—An identifier for the profile.
- **Description**—A text description of the profile.
- **Default**—Check to make this profile the default discovery profile.

Discovery Tab

Configure fields in this tab to specify the devices and methods of discovery.

Figure 4-3. Discovery Profile Editor - Discovery Tab



File: G:\DellPrinters.txt

Address	Exclude?
10.0.20.22	□
10.0.20.23	□
10.0.20.24	□
10.0.20.25	□
10.0.20.26	□
10.0.20.27	□

☑ Ping ● Manage via IP Address

☑ Resolve Hostname ○ Manage via Hostname

Use the pick list at the top of the screen to select the way you want to enter the network location of equipment you want to discover. Options include *IP Range*, *IP address*, *Hostname*, *Subnet*, *CIDR*, *File Name*, *Multicast SLP*, *SNMP Broadcast*. The field(s) to the right of this pick list alter to fit the selected type—for example, a command button (...) that leads to a file selection screen appears if you select *File* (a text file with IP addresses on individual lines). As you enter selections, click *Add* to list them. To exclude listed items, check the *Exclude?* column.

CAUTION: If you scan a broadcast address or range that include the broadcast address, the application discovers equipment ambiguously, because the response really is from multiple devices replying to the broadcast query. If you do a resync on the discovered item, the display becomes whatever information comes from the fastest responding printer. Generally, you the broadcast address comes from the bit complement of the subnet mask OR-ed bitwise with the IP address. For example, to broadcast a packet to an entire class B subnet using a private IP address space, the broadcast address would be 172.16.255.255.

This screen has the following selections in its lowest panel:

- **Ping**—Discover equipment with an ICMP ping. (Ping operations pass to the operating system and use its default settings, including TTL.)
- **Resolve Hostname**—Use the Directory Name Service (DNS) to resolve the hostname for equipment discovered.
- **Manage via IP Address / Hostname**—Manage the equipment with its IP address or hostname, depending on the radio button selected here.

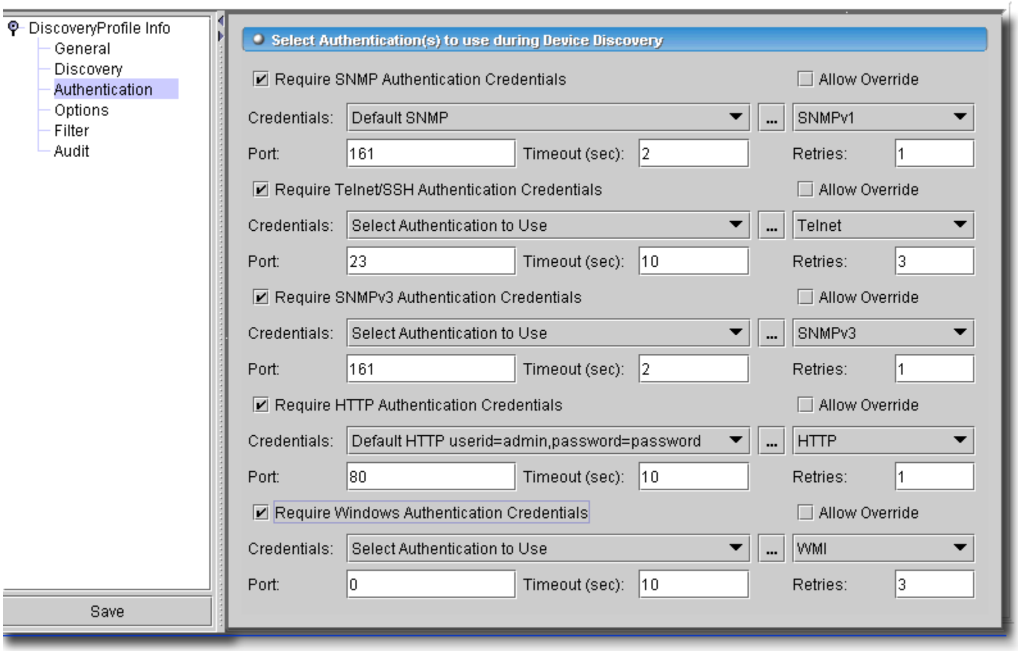
Refer to *IP Discovery Parameters* for more about the options available on this screen.

NOTE: This tab may appear during a profile-driven discovery, if you do not select equipment in the profile. Its appearance may also include the authentication information described in the *Authentication Tab* if those parameters are required but not specified.

Authentication Tab

This tab lets you select the authentication type and login/password to use for the selected discovery profile.

Figure 4-4. Discovery Profile Editor - Authentication Tab



☑ Require SNMP Authentication Credentials — □ Allow Override
Credentials: Default SNMP — SNMPv1
Port: 161 Timeout (sec): 2 Retries: 1

☑ Require Telnet/SSH Authentication Credentials — □ Allow Override
Credentials: Select Authentication to Use — Telnet
Port: 23 Timeout (sec): 10 Retries: 3

☑ Require SNMPv3 Authentication Credentials — □ Allow Override
Credentials: Select Authentication to Use — SNMPv3
Port: 161 Timeout (sec): 2 Retries: 1

☑ Require HTTP Authentication Credentials — □ Allow Override
Credentials: Default HTTP userid=admin,password=password — HTTP
Port: 80 Timeout (sec): 10 Retries: 1

☑ Require Windows Authentication Credentials — □ Allow Override
Credentials: Select Authentication to Use — WMI
Port: 0 Timeout (sec): 10 Retries: 3

Check the types of authentication to use with the discovery initiated with this profile. Potential types include *SNMP* (v1 and v2), *Telnet / SSH*, *SNMP v3*, *HTTP*, and *Windows*.

The SNMP Authentication type has two default SNMP objects (v1 and v2). You can select from these with the pick list to the right of the checkbox. To create new authentication objects (login/password combinations) click the command button (...) to the right of the pick list. See the Chapter 25, *Security* for more details about creating authentication objects.

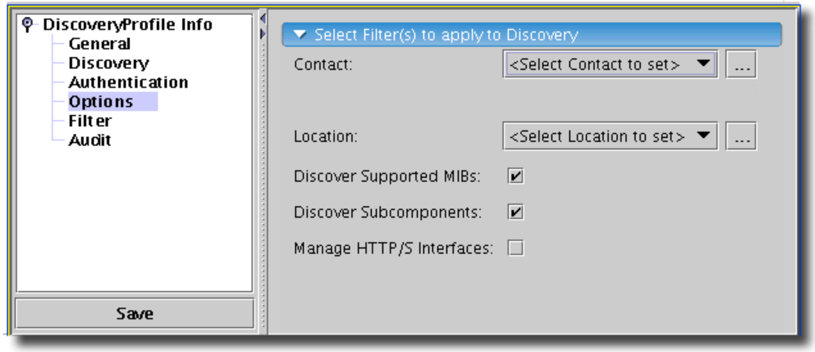
The *Allow Override* checkbox for each authentication type lets you override the default authentication by altering login credentials when you trigger discovery based on this profile.

NOTE: The screenshot above has all authentication types checked for clarity only. This is not required.

Options Tab

This tab lets you filter the equipment discovered, and choose whether you want to discover MIBs, Subcomponents, or manage HTTP or HTTPS interfaces on discovered equipment.

Figure 4-5. Discovery Profile Editor - Options Tab



Contact: <Select Contact to set>

Location: <Select Location to set>

Discover Supported MIBs: ☑

Discover Subcomponents: ☑

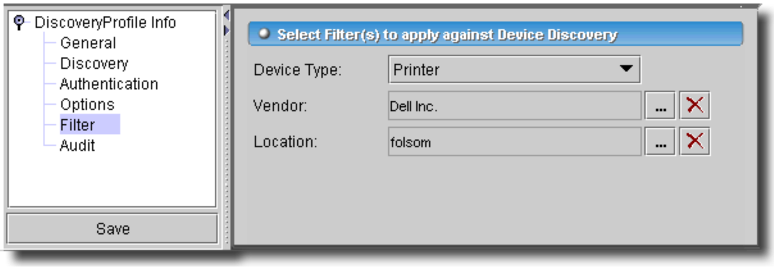
Manage HTTP/S Interfaces: ☐

You can also confine discovery to *Contact*, or *Locations* with the pick list to the right of those labels.

Filter

This tab lets you filter the discovery results.

Figure 4-6. Discovery Profile Editor - Filter Tab



Device Type: Printer

Vendor: Dell Inc.

Location: folsom

Confine the search by selecting a *Device Type*, *Vendor* and/or *Location* with the pick lists. To the right of *Vendor* and *Location* pick lists are command buttons (...) that let you create new vendors and locations.

Audit

This screen records the history of this profile’s use. See Chapter 13, *Audit Trails* for more information.

Advanced Discovery Wizard

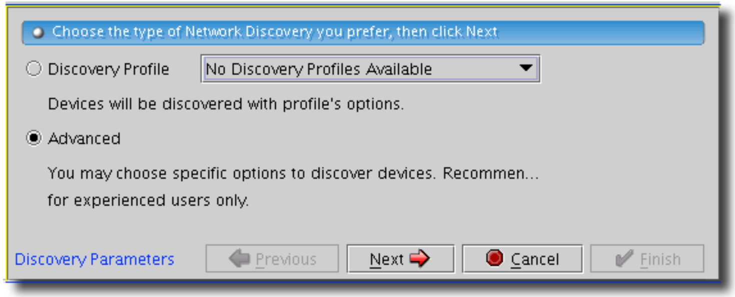
The Discovery Wizard simplifies the process of network element discovery, making it a step-by-step process. Select *Resource Discovery Wizard* from the *File > Open > Inventory* menu or from the Navigation Window to launch the Resource Discovery Wizard, to go through the following steps:

1. *Choose Resource Discovery Type* — This lets you select discovery with Discovery Profiles, or the Advanced discovery described in the following sections.
2. *IP Discovery Parameters* — Here, you can set IP addresses, ranges, and so on, as well as the preliminary discovery authentication like SNMP community names.
3. *Discovery Results* — Here, you can see the devices discovered with ICMP pings, SNMP, and so on, and select which devices you want to examine further in deep discovery.
4. *Set Properties/Authentication* — This screen lets you configure authentication for command-line interactions, or other types of device interactions, as appropriate.
5. *Network Inventory Update* — This displays an audit of the message traffic between this software and discovered devices. See Chapter 13, *Audit Trails* for more information about such audits and how the application saves them.

Choose Resource Discovery Type

This screen determines whether you will use a Discovery Profile, or do *Advanced* discovery. The following sections describe the latter.

Figure 4-7. Discovery Wizard—Choose Type



Choose the type of Network Discovery you prefer, then click Next

○ Discovery Profile — No Discovery Profiles Available

Devices will be discovered with profile's options.

● Advanced

You may choose specific options to discover devices. Recommen...
for experienced users only.

If you click the radio button next to *Discovery Profile*, you can select from among the available profiles on the pick list. See Discovery Profilesfor details about how to configure these.

If you click *Next* after having selected a profile, only the screens described in *IP Discovery Parameters* and *Network Inventory* screens appear.

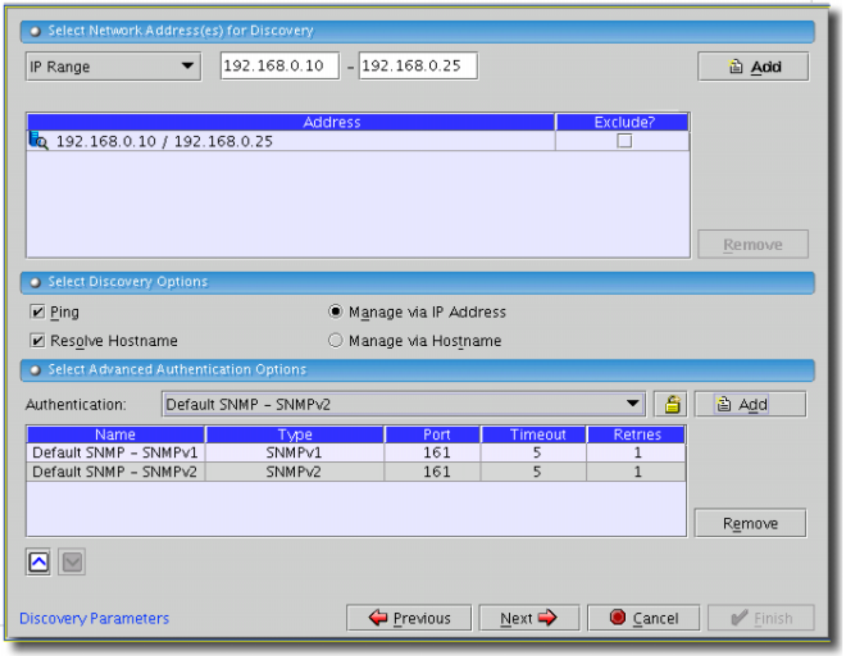
If you click *Advanced*, the following sections describe how to do this type of discovery.

Click *Next* to move to the next screen, or *Cancel* to abandon the discovery process. If you abandon discovery, a confirming dialog appears.

IP Discovery Parameters

In this step, specify addresses or address ranges to include or exclude, the authentication to use.

Figure 4-8. Discovery Wizard—Enter IP Address



Select Network Address(es) for Discovery

IP Range 192.168.0.10 - 192.168.0.25

Address	Exclude?
192.168.0.10 / 192.168.0.25	☐

Select Discovery Options

☑ Ping ● Manage via IP Address

☑ Resolve Hostname ○ Manage via Hostname

Select Advanced Authentication Options

Authentication: Default SNMP - SNMPv2

Name	Type	Port	Timeout	Retries
Default SNMP - SNMPv1	SNMPv1	161	5	1
Default SNMP - SNMPv2	SNMPv2	161	5	1

Discovery Parameters

Fill out the fields in this panel as follows:

Network Parameters

1 Select an address type from the drop-down list. The available types are:

- Single **IP Address** or **IP Range**—For example: a single IP address: 192.168.1.129 or a range: *From* 192.168.0.1 *To* 192.168.0.254
- **Hostname**—the name of the host you want to discover
- **Subnet**—*Net* 102.168.0.0 *Mask* 255.255.255.0
- **CIDR Address**—*Net* 192.168.0.0 / 24
- **File**—A text list of (carriage-return-separated) IP addresses. Use the command button (...) to open a file browser, or type in the fully qualified path and filename.

  NOTE: This field does not support wildcards like the asterisk (*).

- **SLP—**(Service Location Protocol) SLP dynamically locates services in the network. By default, some devices are SLP enabled which means they respond to SLP multicast packets with their service information. Management systems use this information to identify, locate and establish communication with them without any user inputs. This application's discovery supports SLP version 1.
- **Broadcast SNMP Discovery**—Every network comes with a broadcast address which can broadcast received packets to all the hosts in the network. For example, consider a network 192.168.0.1 - 192.168.0.254 with subnet mast 255.255.255.0 and broadcast address 192.168.0.255. If you send an SNMP packet to the broadcast address 192.168.0.255 from host 192.168.0.49, the packet gets broadcast to all the hosts from 192.168.0.1 to 192.168.0.254. All the SNMP enabled devices with respond to this request and send the response back to the host 192.168.0.49. This discovery option helps in locating new SNMP devices in the network without knowing the actual IP Address.

2 Click *Add* to add the address range and specifications to the processing queue. (or *Remove* to delete a previously created range you selected).

3 Decide whether you want to *Exclude* the added IP address(es) from your discovery. If so, check the *Exclude* checkbox.

The application sends each address in this range an Internet Control Message Protocol (ICMP) Echo command. If it receives a response, it lists the address as valid.

Select Discovery Options

4 Check *Ping* and *Resolve Hostname* if you want the application to do those things as it discovers equipment. Ping - checks ensure the application can reach the device with a ICMP Ping. If Ping is enabled and the device does not respond then it is removed from the discovered devices. If it is not enabled then it will not be removed.

Resolve Hostname does a hostname lookup with the network DNS server to determine whether the device has a hostname.

Both these options are global, not assignable to a single address / range, unless you separately discover such addresses / ranges.

5 Select whether you want to manage this device with its IP address or hostname. The latter is appropriate if the devices' IP addresses are dynamic (DHCP), the former if the devices IP address are static. When you manage *hostname*, DNS hostname entries are cached for 60 seconds.

Select Advanced Authentication Options

6 Select the SNMP credential(s) for this discovery from the pick list. You can also create a new credential with the *Add New Authentication* button (like a lock). Pressing this button presents the Authentication Editor and options for the kind of authentication to create. After saving this authentication, it appears in the list of available authentications and in the selected authentications in the table below.

Click *Add* to list the selected credential. The arrows below this list let you move selected credentials up or down so you can adjust the order in which the application tries them.

> **NOTE:** Discovery does not require SNMP. A Default SNMP Authentication appears here. If the discovered devices support the Default SNMP credentials then you do not even have to specify any authentication.

If your installed drivers support non-SNMP based discovery then they typically register these additional Authentication types. Discovery attempts to separate SNMPv1 and SNMPv2 discovery so we are sure that if a device supports SNMPv1 then they can specify this explicitly.

See *SNMP Authentication* below for more information about creating new credentials. You must have an SNMP credential to do discovery.

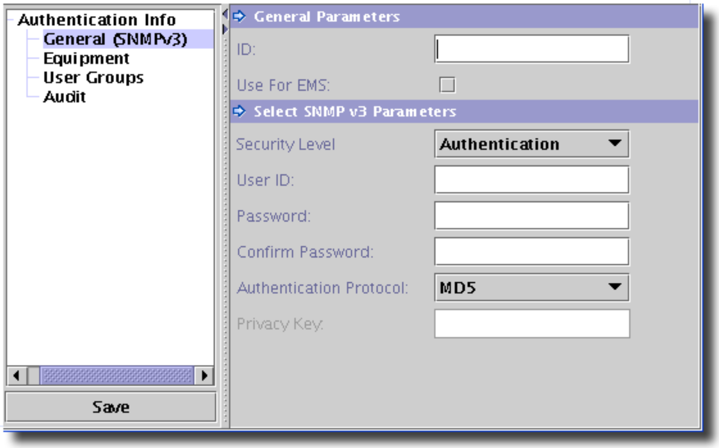
Click a cell and type to set the SNMP timeout, retries, and ports to query directly in the credentials table. Port 161 is the default. Click *Remove* to delete a selected, deleted credential.

7 When you are done, click *Next* to enter *Discovery Results*.

SNMP Authentication

If you want to use discovery and deeper discovery options offered by installed device drivers, you must add at least an SNMP authentication object. You can optionally add a WMI object for communications with Windows Management Interface. For SNMP discovery of the SysObjectID—the basis of device driver functionality—you must have an SNMP authentication object.

Figure 4-9. SNMP Authentication Object



ID:

Use For EMS: □

Security Level: Authentication

User ID:

Password:

Confirm Password:

Authentication Protocol: MD5

Privacy Key:

If you have the Authentication Manager open, first, click *Add*, then click *New*, and select *SNMP (v1, v2, or v3)*, or *WMI*. The subsequent screen specifies an object *ID*, SNMP *Version*, *Read*, *Write*, and *Trap Community*, (if you use SNMP v3) V3 *User Name*, V3 *Auth Protocol*, V3 *Auth Password*, and V3 *Priv Password* or (if you select WMI) the *Domain/Workspace*. Consult the Section for more information.

If you click the *Equipment* item in the navigation window, the application opens a dialog where you can select equipment related to the authentication, and the *User Groups* navigation item lets you specify those who can use this authentication.

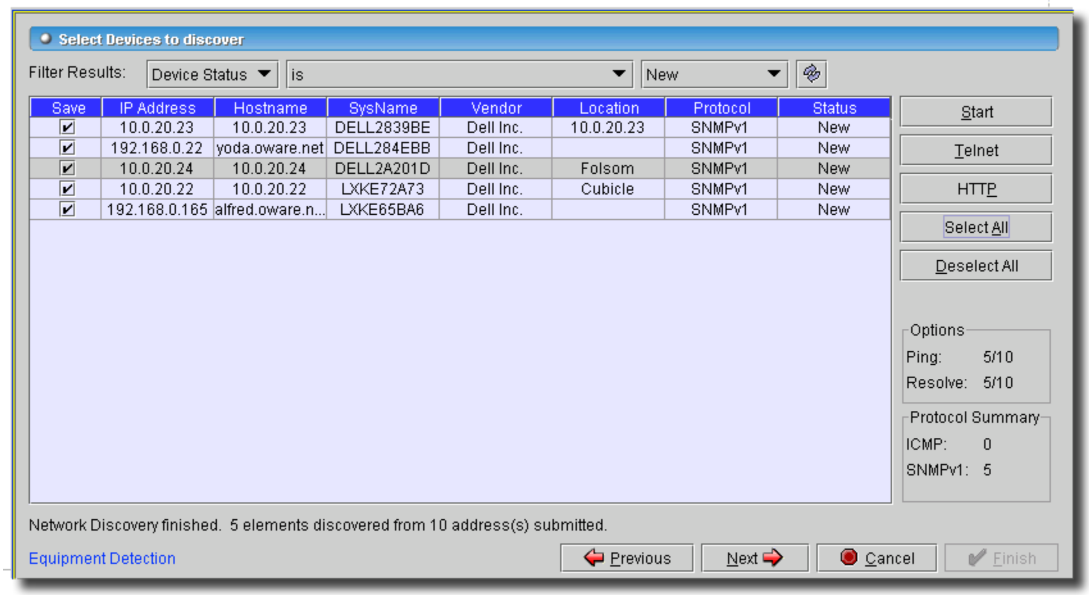
NOTE: You can also enter new and edit existing authentication objects in the Authentication Manager. Access this manager through Settings > Permissions > Authentication Manager.

If you do add an authentication object to this list, clicking the *Save* button, or the File > Save menu item stores it in the database.

Discovery Results

The Discovery Wizard displays a list of discovered equipment when discovery is complete.

Figure 4-10. Discovery Wizard—Discovery Results



Select Devices to discover

Filter Results: Device Status is New

Save	IP Address	Hostname	SysName	Vendor	Location	Protocol	Status
☑	10.0.20.23	10.0.20.23	DELL2839BE	Dell Inc.	10.0.20.23	SNMPv1	New
☑	192.168.0.22	yoda.oware.net	DELL284EBB	Dell Inc.		SNMPv1	New
☑	10.0.20.24	10.0.20.24	DELL2A201D	Dell Inc.	Folsom	SNMPv1	New
☑	10.0.20.22	10.0.20.22	LXKE72A73	Dell Inc.	Cubicle	SNMPv1	New
☑	192.168.0.165	alfred.oware.n...	LXKE65BA6	Dell Inc.		SNMPv1	New

Options
Ping: 5/10
Resolve: 5/10

Protocol Summary
ICMP: 0
SNMPv1: 5

Network Discovery finished. 5 elements discovered from 10 address(s) submitted.

You can elect to *Save* the results with the left-most checkbox, and can view the *IP Address*, *HostName*, *SysName*, *Protocol* (the one providing information for this screen), *Location*, and *Vendor* columns in the table of discovered entities. Only saved results appear in the next steps.

Filter Results

You can filter the discovered equipment that appears in this screen with its pick lists and text field. The default is *Device Status is New.* Here are the options:

- **Operators**—These connect the first and last filter terms. Options include *is*, *isn't*, *contains*, *doesn't contain*.

The following are the sets of first and last terms surrounding the operators in the middle column.

- **Device Status—**Selecting this lets you select the following in the far right of the filter: *Newly Discovered*, *No Response*, *Already Discovered*, and (if you checked *Skip Previously Discovered Networks*) *Previously Discovered*.
- **Protocol—**Selecting this lets you select the following in the far right of the filter: *ICMP*, *SNMPv1*, *SNMPv2*, and so on.
- **Status—**Selecting this lets you select the following in the far right of the filter: *New*, *Already Discovered*, *No Response*

Buttons

When you select a Result in the upper panel, the buttons on the right side of the dialog become active. These are the options:

- **Start**—Re-queries the network for the selected device's information.
- **Telnet**—Opens a Telnet session with the selected network element, if it supports Telnet. This application supports both a Telnet session and a Secure Shell session. The protocol used is specified in the management interface screen of the equipment editor. You can configure the equipment with multiple management interfaces so that the same device can use both telnet and SSH. If this is the case then the driver will determine which to use. If you choose *Direct Access* from a right-click menu, then the application presents this choice too.
- **HTTP**—Opens the default Web page of the HTTP server (if one exists) running on the specified network element.
- **Select All**—Selects all checkboxes in the active column. (This option has no effect unless the *Save* column is active.)
- **Deselect All**—Deselects all checkboxes in the active column.

During the Results phase of discovery, the following columns information appears in the table listing discovered entities:

- **Save**—Click the checkbox to add this device to the Resources Manager.
- **IP Address**—The IP address for this network element. This information is read-only.
- **Host Name**—The Host Name for this network element. This information is read-only.
- **SysName**—The SysName of this network element. This information is read-only.
- **Protocol—**Filter on: *ICMP*, *SNMPv1*, *SNMPv2*, and so on.

- **Location**—The Location for this network element. The application retrieves this information based on the device's SysObjectID. It is read-only.
- **Vendor**—The Vendor for this network element. This information is read-only.
- **Status—**Filter on: *New, Already Discovered, No Response*

Status

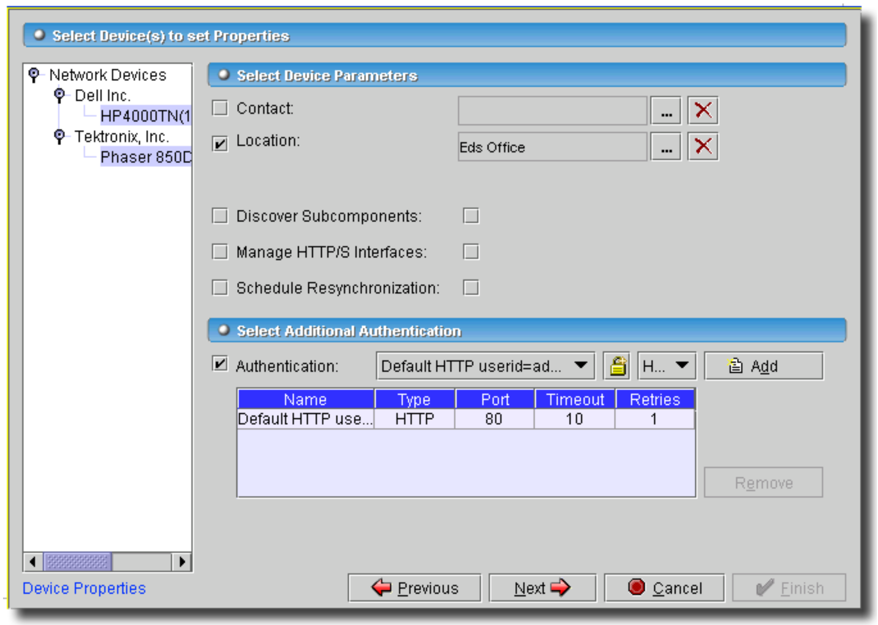
The *Options* and *Protocol Summary* boxes in the lower right corner of this screen lets you monitor discovery in progress, reporting ICMP ping and protocol-based responses.

Select the appropriate equipment to save then click *Next* to continue to the *Set Properties/Authentication* step. Click *back* to return to the *IP Discovery Parameters* step, or click *Cancel* to close the Wizard without discovering any network elements.

Set Properties/Authentication

You can manage further discovery results before saving your new equipment in this step.

Figure 4-11. Discovery Wizard—Edit Results



Select Device(s) to set Properties

Network Devices
- Dell Inc.
  - HP4000TN(1
- Tektronix, Inc.
  - Phaser 850D

Select Device Parameters

☐ Contact:

☑ Location: Eds Office

☐ Discover Subcomponents: ☐

☐ Manage HTTP/S Interfaces: ☐

☐ Schedule Resynchronization: ☐

Select Additional Authentication

☑ Authentication: Default HTTP userid=ad... H...

Name	Type	Port	Timeout	Retries
Default HTTP use...	HTTP	80	10	1

To apply command-line or HTTP authentication, changes in contacts, locations, and so on, to an item, select on the left, then select the item to apply on the right. You can also Ctrl+click to select multiple items on the left. If you select multiple items, you must also check the checkboxes to apply to all the selected items (*Contact*, *Location*, *Authentication* and so on). Once you click *Next* (or *Previous*), your selections are saved.

Fields like *Contact* and *Location* display any information discovered by SNMP, but if you multi-select, then these fields are cleared and any entry overrides previously discovered information.

Click a command button (...) that opens the appropriate manager to edit or add information. You can modify the following properties:

- **Contact**—The contact for the device. Click the command button (...) to open the appropriate manager to add or edit information. Type the name of the contact or use the Command button to open a browser through which you can specify the contact. See Chapter 9, *Contacts* for more information.
- **Location**—The location of the device. Click the command button (...) to open the appropriate manager to add or edit information. Type the name of a location or use the Command button to open a browser through which you can specify the location. See *Locations* on page 139 for more information.

  NOTE: Only the database (not the equipment itself) stores any editing done here.
- **Discover Subcomponents**—If the device supports the ENTITY MIB, selecting this option will discover cards, ports, backplanes, and so on.
- **Manage HTTP/S Interfaces**—Enables discovery of what is needed for management of these interfaces. You do not need to discover an interface to use it in a direct access (cut-thru) session.
- **Schedule Resynchronization**—Checkbox; select this option to automatically schedule this network element for resynchronization.

Select Additional Authentication

Click to select the object(s) on the left to assign their authentication credentials. When you click, any authentications already assigned appear in the table in this *Select Additional Authentication* portion of the screen. Select credentials from the pick list and click *Add* to list them in the table of assigned authentications. As long as an object on the left is selected, the table appears, and the listed authentications are tied to that object.

If necessary, you can assign more than one authentication to discovered equipment, but best practice is to assign only one for each protocol or communication method (for example, SSH is simply a more secure Telnet, so only one of these protocols would require authentication). If you assign multiple authentication objects to equipment, discovery may be correct, cycling through assigned authentications until it finds a successful match, but later queries initiated by the Equipment Editor (which remembers authentication assigned during discovery) may fail.

Click the *Add New Authentication* icon (the lock icon to the right of the pick list) to create new authentications for the pick list.

Once assigned, credentials appear as nodes under selected device objects on the left. The SNMP credentials already assigned in the *IP Discovery Parameters* step appear grayed out, but credentials assigned in this step are selectable. You can delete selected individual credentials assigned in this step by clicking the *Remove Authentication* button (looks like a trash can) at the bottom of the *Device Authentication* panel.

If you select credentials, but no object those credentials are assigned to all objects. You can also assign (sets of) credentials to multiple objects if you Ctrl+click to select several objects.

During the discovery process, the application tries each of the selected authentication profiles until one of the following is true:

- **a** It makes a successful connection.
- **b** It has tried all profiles unsuccessfully, in which case discovery assumes there is no SNMP management interface present at the current address.

When performing deep discovery, you must typically have the correct device driver installed and at least one authentication object (for example: an SNMP authentication object specifying a public read community). If you want this software to interact with a device using a command-line interface, you must add an authentication object here.

NOTE: Device discovery or resync can fail if network or device latency delays authentication beyond the time-outs specified here. You can increase time-outs if these fail, or simply take your network's latency into account when you set authentication time-outs in the first place.

NOTE: Note: When you set timeouts and retries for these authentications, some clients display the cursor only faintly. Backspace to delete any existing setting to confirm that the cursor is in the correct spot. Click [Enter] or somewhere else onscreen before proceeding to ensure the cursor is out of the cell where you are setting timeouts or retries.

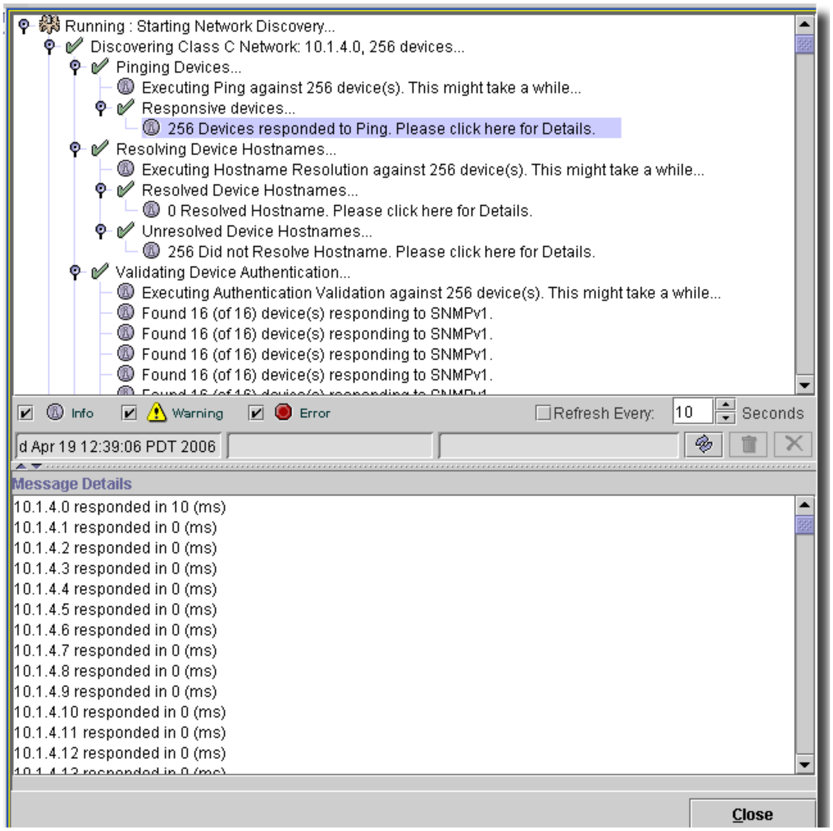
NOTICE: This screen is the only chance you have to set timeouts and retries for authentication. If you need to reset these values later, you must delete the discovered object and then re-discover it.

Click *Next* for *Discovery Wizard- Network Inventory Update*.

Network Inventory Update

The Discovery Wizard continues discovery of the selected options, and saves elements slated for a Save in the Resources manager.

Figure 4-12. Discovery Wizard - Network Inventory Update



```
Running : Starting Network Discovery...
  Discovering Class C Network: 10.1.4.0, 256 devices...
    Pinging Devices...
      Executing Ping against 256 device(s). This might take a while...
      Responsive devices...
        256 Devices responded to Ping. Please click here for Details.
    Resolving Device Hostnames...
      Executing Hostname Resolution against 256 device(s). This might take a while...
      Resolved Device Hostnames...
        0 Resolved Hostname. Please click here for Details.
      Unresolved Device Hostnames...
        256 Did not Resolve Hostname. Please click here for Details.
    Validating Device Authentication...
      Executing Authentication Validation against 256 device(s). This might take a while...
      Found 16 (of 16) device(s) responding to SNMPv1.
      Found 16 (of 16) device(s) responding to SNMPv1.
      Found 16 (of 16) device(s) responding to SNMPv1.
      Found 16 (of 16) device(s) responding to SNMPv1.
```

```
10.1.4.0 responded in 10 (ms)
10.1.4.1 responded in 0 (ms)
10.1.4.2 responded in 0 (ms)
10.1.4.3 responded in 0 (ms)
10.1.4.4 responded in 0 (ms)
10.1.4.5 responded in 0 (ms)
10.1.4.6 responded in 0 (ms)
10.1.4.7 responded in 0 (ms)
10.1.4.8 responded in 0 (ms)
10.1.4.9 responded in 0 (ms)
10.1.4.10 responded in 0 (ms)
10.1.4.11 responded in 0 (ms)
10.1.4.12 responded in 0 (ms)
```

This screen catalogs, step-by-step, the process of discovery. Additional information about the incremental messages appears in the lowest panel when you select the message in the upper panel. Ranges of discovered equipment appear (collapsed) on the job tree. (Discovery automatically organizes ranges into class C subnets.)

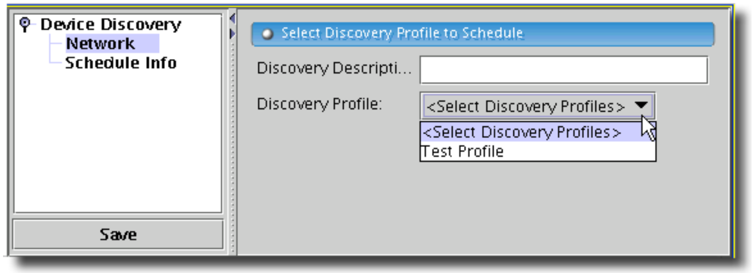
Click *Finish* to complete the discovery process and dismiss this dialog. You can click this button before the process finishes and review the result in the Audit Trail manager later.

NOTE: Some discovery processes occur even after Finish. If you want to edit a device’s routing protocol settings, for example, best practice is to wait a few minutes after the discovery wizard finishes otherwise these screens may be incorrect or not appear.

Scheduling Discovery

You can schedule and launch Discovery sessions for a specified Discovery profile. Access the Discovery Scheduler by selecting *File > Open > System Services > Schedules* from the menu or the Navigation Window. Create a new discovery schedule by clicking the *New* button, and select *Device Discovery* from the listed actions. Click *OK*, and the *Discovery Scheduler* opens.

Figure 4-13. Scheduling Discovery



Discovery Description provides a unique identifier for this scheduled event. Select the discovery profile from the pick list. See Discovery Profiles for more about creating profiles.

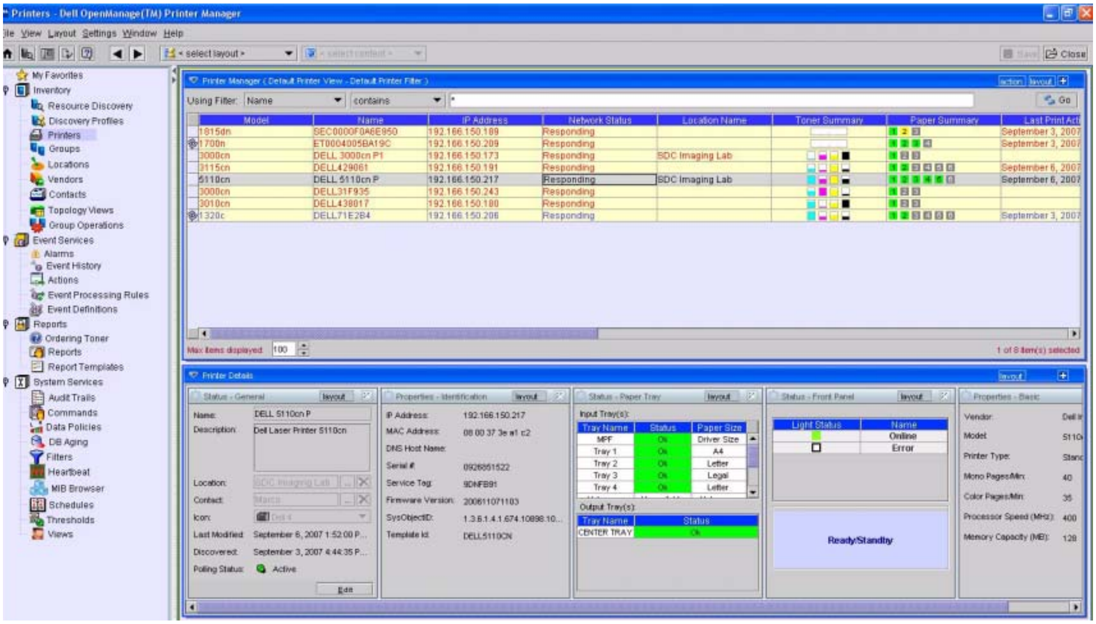
Scheduling discovery can add discovered devices automatically to the application. They appear in the Resources Manager as Discovered Entities. See Chapter 17, *Schedules* for details about managing (creating, deleting or modifying) scheduled events. Once you complete a schedule, use *File > Save* to save it to the database.

Printers

Printers

For some installations the first screen you see may be **Printers**. To make this screen appear, if it is not already visible, click its menu item in **File**→ **Open**→ **Inventory** or click the **Printers** node in the navigation window.

Figure 5-1. Printers Screen



Printer Manager (Default Printer View - Default Printer Filter)

Using Filter: Name contains *

Model	Name	IP Address	Network Status	Location Name	Toner Summary	Paper Summary	Last Print Acti
1815dn	SEC0000F0A6E950	192.166.150.189	Responding			1 2 3	September 3, 2007
1700n	ET0004005BA19C	192.166.150.209	Responding			1 2 3 4	September 3, 2007
3000cn	DELL 3000cn P1	192.166.150.173	Responding	SDC Imaging Lab		1 2 3	
3115cn	DELL429061	192.166.150.191	Responding			1 2 3 4 5 6	September 6, 2007
5110cn	DELL 5110cn P	192.166.150.217	Responding	SDC Imaging Lab		1 2 3 4 5 6	September 6, 2007
3000cn	DELL31F935	192.166.150.243	Responding			1 2 3	
3010cn	DELL438017	192.166.150.180	Responding			1 2 3	
1320c	DELL71E2B4	192.166.150.206	Responding			1 2 3 4 5 6	September 3, 2007

Max items displayed: 100

1 of 8 item(s) selected

Printer Details

Status - General

Name: DELL 5110cn P
Description: Dell Laser Printer 5110cn
Location: SDC Imaging Lab
Contact: Marco
Icon: Dell 4
Last Modified: September 6, 2007 1:52:00 P...
Discovered: September 3, 2007 4:44:35 P...
Polling Status: Active

Properties - Identification

IP Address: 192.166.150.217
MAC Address: 08 00 37 3e a1 c2
DNS Host Name:
Serial #: 0926851522
Service Tag: 9DNFB91
Firmware Version: 200611071103
SysObjectID: 1.3.6.1.4.1.674.10898.10...
Template Id: DELL5110CN

Status - Paper Tray

Input Tray(s):

Tray Name	Status	Paper Size
MPF	Ok	Driver Size
Tray 1	Ok	A4
Tray 2	Ok	Letter
Tray 3	Ok	Legal
Tray 4	Ok	Letter

Output Tray(s):

Tray Name	Status
CENTER TRAY	Ok

Status - Front Panel

Light Status	Name
🟩	Online
□	Error

Ready/Standby

Properties - Basic

Vendor: Dell I
Model: 5110
Printer Type: Stand
Mono Pages/Min: 40
Color Pages/Min: 35
Processor Speed (MHz): 400
Memory Capacity (MB): 128

In the default view, you can select equipment and see details about it in the lower panel (*Printer Details*). The *Printer Details* panels individually display information described in more detail in Printer Info, displaying that information without opening Equipment Editor. See also Column: Offline Time (Minutes) for a column available in the printers displayed.The X at the top right of the panel closes it.

NOTE: Some applications also display an Event History panel in the default layout.
Also: Scroll arrows let you scroll a pixel at a time, but clicking above or below the scrollbar block, or dragging the scrollbar block scrolls rapidly.

Click the **Go** button to refresh the list. If you revise the filter, this re-manages the equipment that appears listed. Columns in this list describe attributes of the discovered equipment. The left most column indicates whether the equipment has been resynchronized. Yellow rows have not been heard from for the last 60 minutes.

See Filters for more about filtering capabilities in general. See the Column: Offline Time (Minutes) on column for more specifics about filtering capabilities.

NOTE: Changing polling intervals does not have an impact on this 60-minute interval.

See Action / Context Menu for more about features on this screen.

NOTE: You can discover any printer with an IP address. The amount of information received from the printer by this application depends on the printers' support for SNMP and HTML interactions.

Column: Offline Time (Minutes)

Printer Manager can display a column called *Offline Time (Minutes)*—if you use the + button to select it. This shows the minutes since the application received a *down* response from a printer it is polling. The application resets this attribute when the response is not *down*.

You can also filter to find printers that are *down*. (For more, see Filtering) The filter finds the printer's status and the timestamp when the application observed this change with the filter attributes *HOST-MIB Device Status* and *HOST-MIB Change Timestamp*. The Date Filter also supports the *before last* operator—one that allows queries of the historical timestamps up to the value specified (for example before last 30 minutes would include all date values that are at least 30 minutes before the present time)

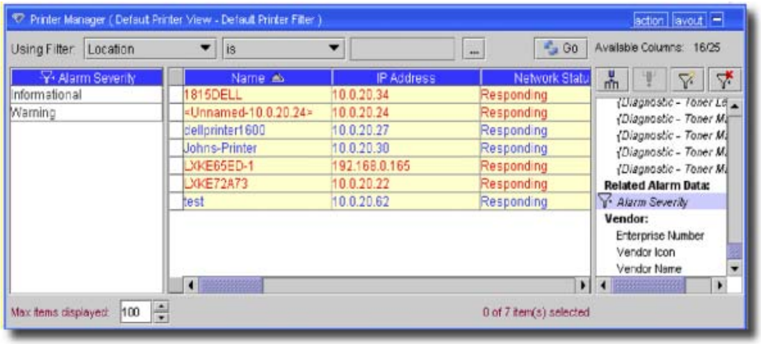
If a printer responds to the application, it is considered *up*. Forcing a resynchronization does not force reassessment of the network state. That status is assessed only when the heartbeat polling policy executes.

Related columns available for display are *Network Status (Responding / Not Responding*) that determines whether the printer is responding to the network, and *Printer Status* (*Online / Offline*) that determines whether it is available for printing.

Quick Group

One additional feature of this manager is the Quick Group. It can display printers grouped by a selected attribute. Click the plus (+) sign in the upper right corner of the list of printers to display the available attributes on the right.

Figure 5-2. Printer Quick Group


Printer Manager (Default Printer View - Default Printer Filter)

Using Filter: Location · is

Available Columns: 16/25

Alarm Severity
Informational
Warning

Name	IP Address	Network Statu
1815DELL	10.0.20.34	Responding
<Unnamed-10.0.20.24>	10.0.20.24	Responding
dellprinter1600	10.0.20.27	Responding
Johns-Printer	10.0.20.30	Responding
LXKE65ED-1	192.168.0.165	Responding
LXKE72A73	10.0.20.22	Responding
test	10.0.20.62	Responding

{Diagnostic - Toner Le
{Diagnostic - Toner M
{Diagnostic - Toner M
{Diagnostic - Toner M
{Diagnostic - Toner M
Related Alarm Data:
Alarm Severity
Vendor:
Enterprise Number
Vendor Icon
Vendor Name

Max items displayed: 100

0 of 7 item(s) selected

The two icons on the right above this panel group (or un-group) displayed data based on the selected attribute(s). When you select Quick Group attributes, a panel to the left of the list of equipment displays the selected attribute value(s). Click on an attribute value there to display the printers that have this value. For example, printers whose last alarm is *Informational* appear when you click that attribute value in the left panel. If you select all values—or none—all devices appear, provided they conform to the filter selected at the top of this screen.

NOTE: The filtered view and Max Items number limit the devices you can Quick Group together. You must click Go after you revise either the filter or Max Items before applying a Quick Group to a revised list.

You do not need to leave the attribute panel open to use the quick group panel on the left. Click the minus (-) icon at the top right of this screen to close the attribute panel.

Default Printer Template

Printer templates make messages from different types of printers intelligible to this software. Even if your network's printers are not part of those supported the templates included, a general, default printer template lets you discover and (in a limited way) manage printers which support standard SNMP communications.

Supported fields include the following:

- Name, contact and location
- Configuration: console localization, character set, country and language
- Identification: description, ID, serial number
- Display: number of characters and lines
- Hardware: hard drive, capacity, removability
- Network: IP address and mask
- SNMP: community names, uses.
- Trays (Status, capacity, name, paper type).

- Status: impressions count, page count, system uptime.
- Toners and toner levels.

The presence and accuracy of the information collected depends on the printer.

NOTE: You can see which printer types are supported by looking at the names of `.tpl` files in `owareapps\printer\lib.`

Limitations to Printer Messaging

Sometimes, you cannot poll the following attributes from a printer. The solution to this intermittent difficulty is to power cycle the printer (turn it on, then off):

- Asset Tag Number: Failed reading html doc URL:port_0/config/printer?br=8
- Blank Pages: Failed reading html doc URL:port_0/config/printer?br=4
- Collation: Failed reading html doc URL:port_0/config/printer?br=4
- Darkness: Failed reading html doc URL:port_0/config/printer?br=7
- Number of Copies: Failed reading html doc URL:port_0/config/printer?br=4
- PCL Orientation: Failed reading html doc URL:port_0/config/printer?br=9
- PS Error Report: Failed reading html doc URL:port_0/config/printer?br=10
- Panel Language: Failed reading html doc URL:port_0/config/printer?br=8
- Power Saver Time: Failed reading html doc URL:port_0/config/printer?br=8
- Resolution: Failed reading html doc URL:port_0/config/printer?br=7
- Resource Save: Failed reading html doc URL:port_0/config/printer?br=8
- Separator Sheets: Failed reading html doc URL:port_0/config/printer?br=4
- Separator Sources: Failed reading html doc URL:port_0/config/printer?br=4
- Service Tag Number: Failed reading html doc URL:port_0/config/printer?br=8
- Toner Alarm: Failed reading html doc URL:port_0/config/printer?br=8

The *Audit* screen lists unresponsive attributes in its messages during interactions like discovery. Select a message in the upper panel there to see details about which attributes did not respond.

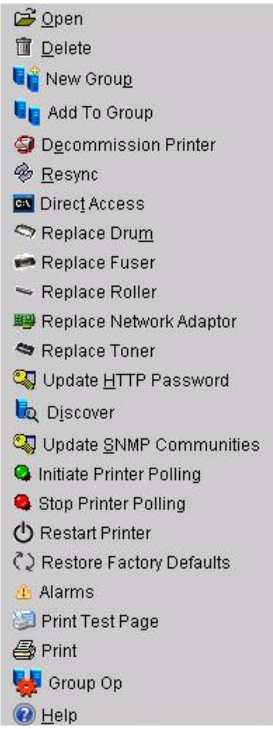
Printer Details

Printer Details panels appear (often several in a single screen) in the editor screens described following Printer Info. You can add these detail screens to the *Printer Details* portion of the screen by clicking the plus (+) in the upper right corner of that panel, and clicking **Add Detail Panel** when you have selected the one you want. To remove a detail panel, click on the X in its upper right corner. As always, layout edits are preserved for the next time you log in.

Action / Context Menu

Right-click a line in the listed printers, or click the **Action** button on top of that table to view a menu related to actions available for the selected equipment.

Figure 5-3. Printer Actions Menu



NOTE: Depending on whether you open this menu from the Action button or by right-clicking a printer, the order of menu items may change. The descriptions of what these items do, however, is the same.

Select more than one listed piece of equipment in the Printer Manager screen with Ctrl+click. The menu that appears once you have selected several printers may vary slightly, but will apply to all selected printers.

This action / right-click menu has the following items:

- **Open**—Open the equipment editor for the selected item. See Printer Info for more about this option.
- **Delete**—Delete the selected equipmentfrom the list.
- **New Group**—Create a new equipement group.
- **Add to Group**—Add the selected to an existing group. See the Chapter 7, *Groups* for more about groups.

- **Decommission Printer**—Decommission takes the printer out of service. It stops all polling, thresholds and heartbeats. It does not remove the printer from the database, however. You must confirm decommissioning in a subsequent popup that appears once you select this option. To recommission a printer, you must rediscover it. Decommissioning has a few more consequences:
  - It sets the IP address in the application's database to 0.0.0.0. Another printer can then be assigned to the existing IP address of the decommissioned printer; the discovery of this IP address on a new printer does not now cause its verification to fail.
  - You cannot resync a decommissioned printer without an error.
  - You cannot add a decommissioned printer to the heartbeat or threshold polling subscriptions (unless you re-commission it).
  - Unsupported features after decommissioning: initiate polling, print the test pages, restart printer.
  - The Front Panel and Toner levels panels no longer function in the *Printer Details* panels.
  - You can re-commission a decommissioned printer by using the discovery wizard and discovering the IP address of the printer. (The existing serial number in the database will match and the printer will get the new IP address).

  You should decommission a printer when you change printer hardware but leave the IP address for the older printer the same.

- **Resync**—Resynchronize the selected equipment's database description with its actual condition on the network.
- **Direct Access**—Open browser session to one selected printer.
- **Replace Drum / Fuser / Roller / Network Adaptor / Toner**—Record a service session for these replacements. Opens a service log screen where you can record these replacements and any accompanying comments. This softwarearchives such service occasions, as explained in Service Log.

NOTE: A Replace Toner service event occurs automatically any time the toner level increases more than 60%

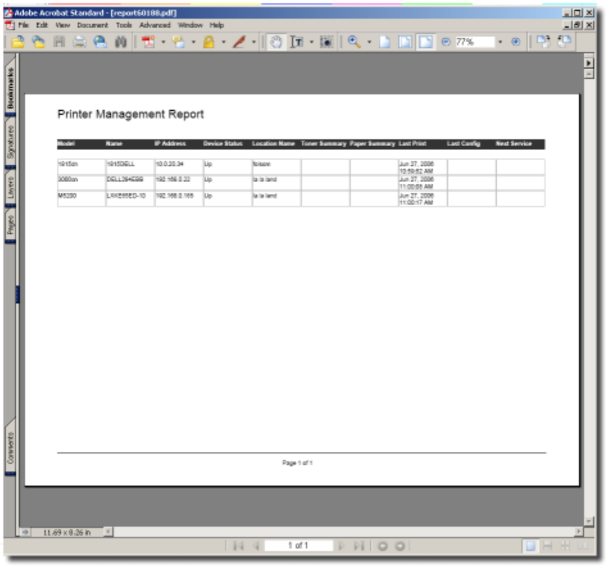
- **Update HTTP / SNMP Credentials**—Display a form where you can configure or select a new credential of the type selected. On the subsequent screen, you can select from a pick list of existing credentials, or click the command button(...) to create a new login / password credential for the appropriate protocol. Also on this next screen is the Update on Device checkbox. If that is checked, and the credentials you select or create are new for the device, the application will automatically update the device's credentials when you click OK on this screen.
- **Discover**—Open the Resource Discovery Wizard. (see Advanced Discovery Wizard)
  - **Initiate / Stop Printer Polling**— This starts or stops the data collection process for the selected printers. One or the other of these is disabled (grayed out). An accumulation of polling is required for most printer reports.

Stop Polling here only stops the opportunistic poll—general heartbeat and data collection still occur. Decommission stops printer thresholds and heartbeats too. You can also initiate or stop polling with an action triggered by a notification. (See Action Editor.)

Threshold reports require you to set thresholds. See Threshold Manager for more information.

- **Restart Printer**—Restart the selected printer.
- **Restore Factory Defaults**—Restore the selected printer to its original condition.
- **Alarms**—Display the alarms connected with the selected printer(s).
- **Print Test Page**—Print a test page on the selected printer.
- **Print**—Create an Acrobat report of the printers displayed in the inventory (change the filter and click *Go* to change this display).

Figure 5-4. Printer Management Report


Adobe Acrobat Standard - [report60188.pdf]
File Edit View Document Tools Advanced Window Help
77%
Bookmarks
Signatures
Layers
Pages
Comments
11.69 x 8.26 in
1 of 1

Printer Management Report

Model	Name	IP Address	Device Status	Location Name	Toner Summary	Paper Summary	Last Print	Last Config	Next Service
1815dn	1815DELL	10.0.20.34	Up	folsom			Jun 27, 2006 10:59:52 AM		
3000cn	DELL284E8B	192.168.0.22	Up	la la land			Jun 27, 2006 11:00:08 AM		
M5200	LXKE65ED-10	192.168.0.165	Up	la la land			Jun 27, 2006 11:00:17 AM		

Page 1 of 1

You must have the free Acrobat reader installed for this to function. See **www.adobe.com** to download and install this application.

NOTE: This report limits the number of columns to those that can fit on a single page width.

- **Group Op**—Select a group operation to perform on the selected printer(s).
- **Help**—Open the online help for this screen.

If you initiate polling on a selection including more than one device, only equipment not already polling begins to poll. Similarly, you can print test pages on all selected printers.

Printer Info

The following screens appear when you click **Open** after right-clicking a printer listed in the Printers screen. These describe details of the selected printer's operation and maintenance. The same information, slightly rearranged appears also in the *Printer Details* panels that can appear at the bottom of the screen. The editor includes the following screens (links to individual detail panel descriptions follow the node name link below):

- *Status*—General, Front Panel, Paper Tray Details, Toner Levels
- *Properties*—Identification, Image, Basic, Assets
- *Toner*
- *Consumables*—Paper Usage, Drum / Fuser / Roller
- *Misc*—Printer Queue, Toner Cartridge, Paper Tray Details
- *Location*
- *Notes*
- *Printer Settings*—Basic, PCL 1, Finishing, PCL 2
- *Port Settings*—HTTP, FTP, Port 9100, LDP
- *E-mail Settings*—E-mail Alert 1 / 2, E-mail Settings 1 / 2
- *Network Settings*—TCP / IP, DNS, Ethernet, Network
- *Object Groups*
- *Security Settings*—SNMP, IP Filter, Password
- *Adjustment Settings*—Auto Registration, Non-Dell Toner, Time Settings, Printer Interaction
- *Service Log*
- *Change Tracking*
- Custom Fields—See *Custom Fields*.
- *Audit*

NOTE: Slight variations may appear in the screens described here based on the selected printer.

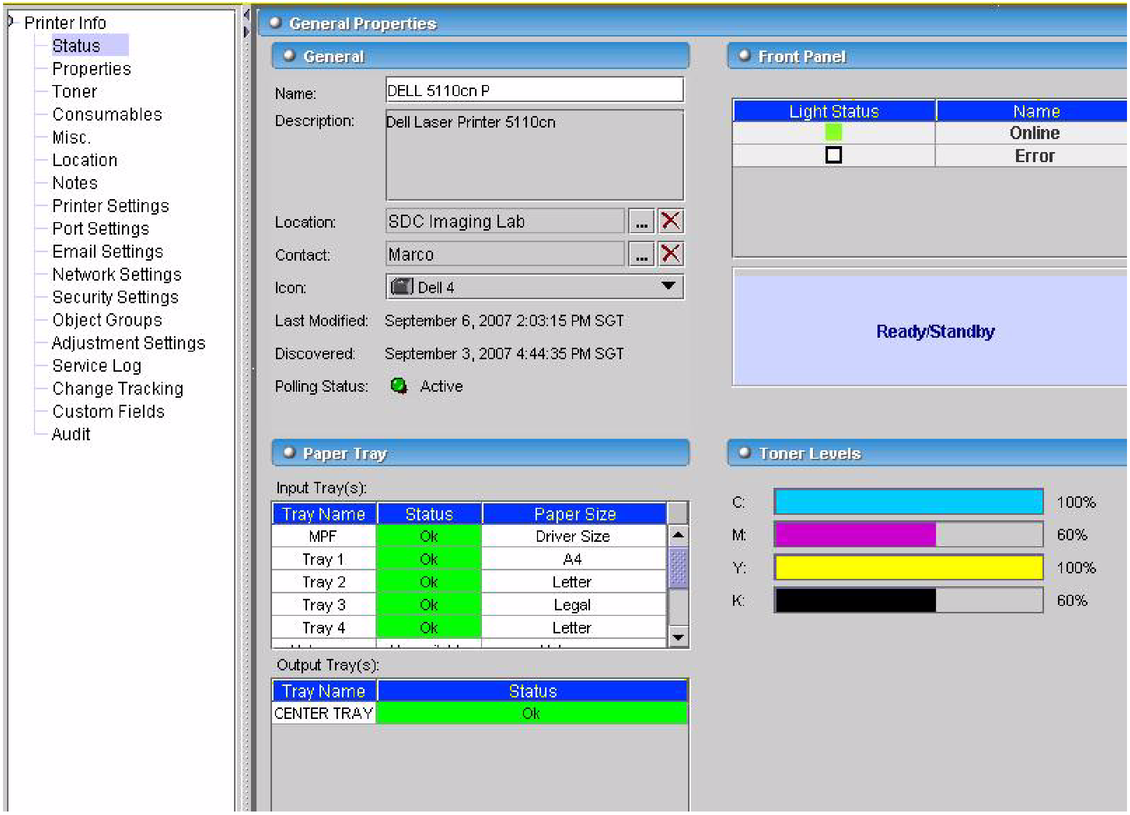
The following letters appear in descriptions:

- **P**—Setting is written/saved to the printer
- **PR—**A value read from the printer but not changeable.
- **PW**—A setting that can be saved to the printer but not read.
- **L**—Setting is written/saved to the local database.
- **M**—A static value for a given model
- **C**—Value is calculated from other fields on the device

Status

This screen exposes general status information about the selected printer.

Figure 5-5. Printer Info > Status



- Printer Info
  - Status
  - Properties
  - Toner
  - Consumables
  - Misc.
  - Location
  - Notes
  - Printer Settings
  - Port Settings
  - Email Settings
  - Network Settings
  - Security Settings
  - Object Groups
  - Adjustment Settings
  - Service Log
  - Change Tracking
  - Custom Fields
  - Audit

General Properties

General

Name: DELL 5110cn P

Description: Dell Laser Printer 5110cn

Location: SDC Imaging Lab

Contact: Marco

Icon: Dell 4

Last Modified: September 6, 2007 2:03:15 PM SGT

Discovered: September 3, 2007 4:44:35 PM SGT

Polling Status: ● Active

Front Panel

Light Status	Name
🟩	Online
□	Error

Ready/Standby

Paper Tray

Input Tray(s):

Tray Name	Status	Paper Size
MPF	Ok	Driver Size
Tray 1	Ok	A4
Tray 2	Ok	Letter
Tray 3	Ok	Legal
Tray 4	Ok	Letter

Output Tray(s):

Tray Name	Status
CENTER TRAY	Ok

Toner Levels

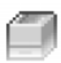
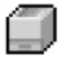
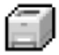
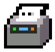
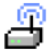
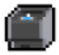
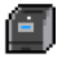
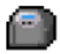
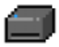
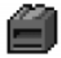
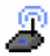
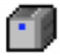
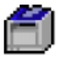
C:	100%
M:	60%
Y:	100%
K:	60%

It has the following fields:

General

- **Name**—The name of the device. For some printers this is strictly a descriptive name to assist in management. On some printers this value may be the Host Name of the printer, and may identify the printer on networks or for registration with a DNS or WINS server. (P, L)
- **Description**—The description of the device. (L)
- **Location**—The location of the device. A string describing the physical location of the printer. Note: When printers are discovered, new locations are automatically added to the list of locations in the Location Manager. (P, L)

- **Contact**—The Contact related to the device. Normally this is the person responsible for maintaining the operational state of the printer. (P, L)
- **Icon**—The icon displayed for this device. Many are automatically selected when you discover the device, some you must manually select in the *General* screen (noted below as *user selected*). Changing the icon selection has no real impact. Printers with template will automatically have an appropriate icon associated with them. Printers without a template will show the default printer icon. This is changeable, manually. (L)

Icon	Description
	A detected generic printer that conforms to no installed template or driver (user selected).
	A generic printer that conforms to an installed template or driver (user selected).
	A second generic printer that conforms to an installed template or driver (user selected).
	Laser Printer that conforms to an installed template or driver
	Wireless Bridge (user selected).
	Dell™ 5100cn
	Dell 3100, 3100cn
	Dell 5200
	Dell Printer
	Dell Multifunction (1600)
	Dell Wireless Bridge (user selected).
	Printer 1(user selected)
	Printer 2 Multi-Function Printer (user selected).

Icon	Description
🖨	Printer 3 Laser (user selected)
🖨	Printer 4 (type 1)
🖨	Printer 4 (type 2)

- **Last Modified**—This is the last time that the printer was modified, either because of a poll or because of user action (L)
- **Discovery Date**—The date the device was originally discovered (read-only), added to the printer inventory. (L)
- **Polling Status**—Green if polling is active, red if not. This value is the current status of Heartbeat polling for the device. When enabled the device will be monitored regularly to determine if it is still present on the network. (L)

Front Panel

This displays the following:

- [**Front Panel Light List**]—This list mimics the front panel lights of the device. Columns are:
- *Light Status*–A graphical representation of the light. This displays the color and the light's flash rate.
- *Name*–The name of the light as provided by the printer with SNMP. For printers without a template this name may not exactly match any text on the front panel of the printer.
- [**Front Panel Display**]—This field shows the current text from the front panel of the printer. Some newer printers use a graphical interface on the front panel. Many of these respond with text for the front panel that may not match the image visible on the physical front panel of the printer. This display's appearance is related to the printer's a functionality. Also, some printers that do not have a physical front panel visible may still provide the equivalent text display with this control.

Paper Tray Details

These values come from the individual printer and its currently state and are not editable here. This table provides a more detailed view of the printer paper tray summary in the main printer list. This displays the following:

- **Input Tray(s)**—Shows the status of the input trays of the printer. Columns include *Tray Name* (defined by the printer manufacturer), *Status* (OK, Low, Empty), and *Paper Size* (based on tray selection – on some printers this is soft set, and on others it may be automatically detected.) (PR)
- **Output Tray(s)**—Shows the status of the output trays of the printer. Columns are *Tray name* (defined by the printer manufacturer), and *Status* (OK, Warning, Full). (PR)

Toner Levels

This panel displays graphics that depict the CMYK levels (for cyan, magenta, yellow and black toner), and has an *Order Toner* link that opens the default browser to an order page for the selected printer. The web page that opens for this depends on the *Customer Settings* tab in the screen produced by **Settings→ Configuration→ Control Settings**. There, you can configure your company's premium account, if applicable, and see only supplies approved in your purchasing policies.

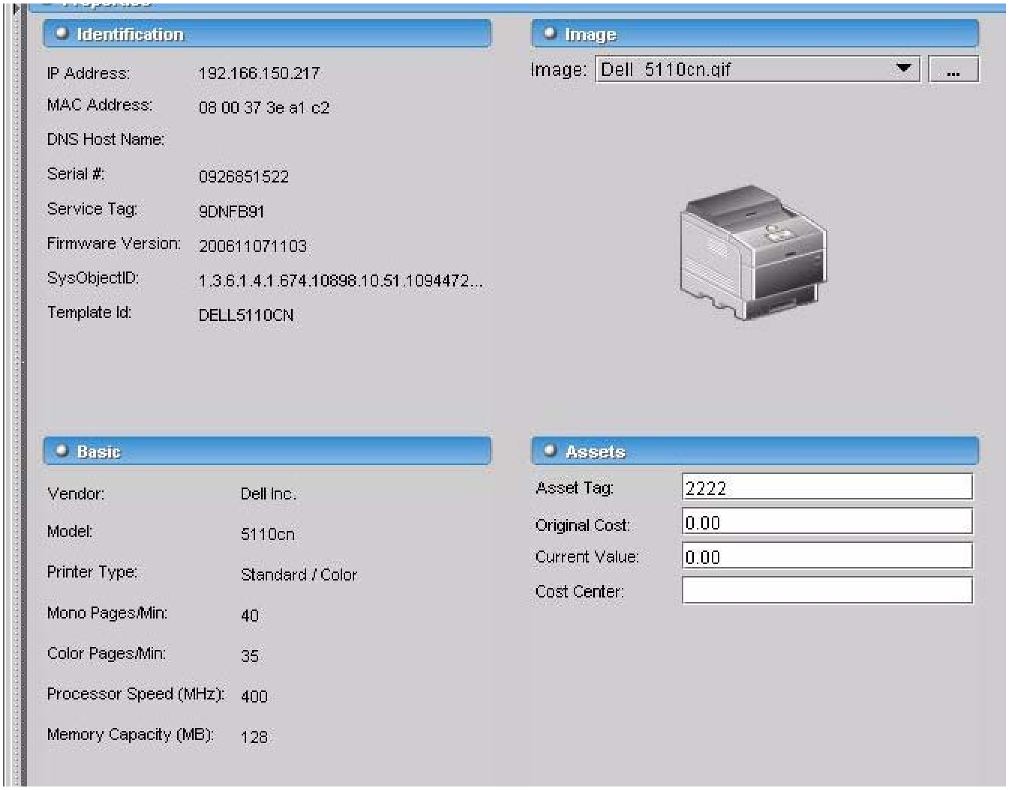
Toner also displays the following:

- **Estimated life (pages)**—This value provides an estimate of the pages remaining on the black toner cartridge. This value is a function of both the manufacturer's rating for the cartridge, based on an average of 5% coverage, and the real world usage of the printer. Printing with an average coverage higher or lower than 5% results in numbers that are different from the manufacturer's rating. (C)
- **Current pages on cartridge—**The number of pages that have been recorded as printed using the current cartridge. This value resets when a toner cartridge is replaced (via automatic detection or user action). (L)
- **Estimated pages remaining—**The estimated toner life based on actual usage, minus the pages that have been printed on the cartridges. The value represents an estimate only and varies subject to the result of the Estimate Life field. (C)
- **Estimated days remaining (per 2 week average)**—This value is an estimation of days remaining on the cartridge calculated by dividing the Estimated pages remaining by the average number of pages printed each day for the past 2 weeks. As print volumes increase (or average coverage increases) this number will be smaller. (C)
- **Estimated days remaining (per 6 months average)**—The same as Estimated days remaining based on the past 2 weeks usage, but based on the average pages printed each day for the past 6 months on this specific device. (C)

Properties

This screen displays additional printer properties.

Figure 5-6. Printer Info > Properties



Identification

IP Address: 192.166.150.217

MAC Address: 08 00 37 3e a1 c2

DNS Host Name:

Serial #: 0926851522

Service Tag: 9DNFB91

Firmware Version: 200611071103

SysObjectID: 1.3.6.1.4.1.674.10898.10.51.1094472...

Template Id: DELL5110CN

Image

Image: Dell 5110cn.gif

Basic

Vendor: Dell Inc.

Model: 5110cn

Printer Type: Standard / Color

Mono Pages/Min: 40

Color Pages/Min: 35

Processor Speed (MHz): 400

Memory Capacity (MB): 128

Assets

Asset Tag: 2222

Original Cost: 0.00

Current Value: 0.00

Cost Center:

This has the following fields:

Identification

This panel lists the following:

- **IP Address—**The IP address of the printer. (P,L)
- **MAC Address**—The Mac Address of the printer. (PR,L)
- **DNS Host Name**—This is the host name returned for the IP of the printer by the DNS server that is servicing this software’s application server. When a printer host name changes there may be a propagation delay before the name is updated in the DNS server queried by this software. This is normal.

- **Serial #**—This is the serial number reported by the printer and used for identification of the printer when reading configuration and status details. The serial number is the unique identifier used to track the history of a device. In some instances the hardware may not support reporting of a serial number. This limitation can be addressed in a printer template by mapping the serial to a different unique identifier like the MAC address of the printer. (PR,L)
- **Service Tag**—This is the Dell service Tag of the device. On many Dell printers the service tag is not pre-populated on the printer and must be entered by the user before this field will populate. You can update this field directly in the printer or printer management software. (P, PR)
- **Firmware Version**—The main firmware version of the printer. Many printers track several different subsections of the firmware, but provide an overall firmware version. On templated printers if an overall firmware version is not provided by the printer this displays the main engine version of the firmware, or the highest logical unit available. (PR)
- **SysObjectID**—This is the value returned by the printer by SNMP provided as a means to identify the type of hardware (the. model). This value directly affects the association of a template with a given model and is provided for diagnostic purposes. (PR)
- **Template Id**—The name of the template file being used to translate communications with the printer. For printers without an explicit template this will show as `Default.tpl`, the default template that maps this software's values to the standard locations defined in the industry standard printer MIBs, most notably RFC1759. (L)

Image

This field provides an image of the printer model. For printers with a template this will automatically be set to the correct image for that printer. This value can be changed at any time by the user, over-riding this value. Printers without a template will not have a default image, but one can be set by the user. If you want, you can select the image for the printer in the pick list. You can alter the available images themselves by putting .gif, .jpg, or .png files in the following directory: `[Installation Root]\owareapps\printer\images\printers`. (M, L)

Basic

This panel lists discovered properties. They are the following:

- **Vendor**—Determined by the enterprise ID of the device, or set by the template for a model when available.)
- **Model**—The model name of the device. For devices with a template this value is determined by the template automatically associated with the Device.
- **Printer Type**—The Printer Type (Color/Monochrome).
- **Mono Pages / Min**—The Manufacturer's reported speed of the printer in pages per minute for monochrome output.
- **Color Pages / Min**—The manufacturer's reported speed of the printer in pages per minute for color output.

- **Processor Speed—**The manufacturer's reported speed of the processor based on the model.
- **Memory Capacity**—The amount of memory currently installed in the printer.

These are fixed values from the manufacturer (M), except the *Memory Capacity*, which is read from the printer.

Assets

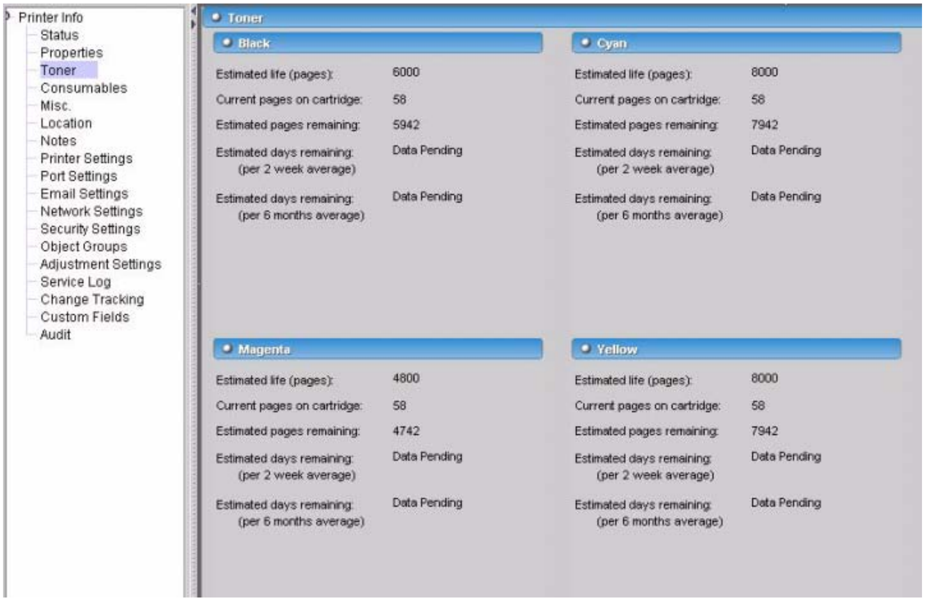
This panel lists the following properties:

- **Asset Tag—**The asset tag of the printer, normally used to hold an asset identifier value set by the owner for inventory and property tracking. (P)
- **Original Cost—**The original value of the asset, stored in the database. (L)
- **Current Value—**The current value of the asset, stored in the database. This value does not track historical changes; only the most recently entered value is available. (L)
- **Cost Center—**A value stored in the database tracking the cost center of the device. Historical changes are not tracked. Only the most recent value is available. (L)

Toner

This screen displays estimates about toner use and projections about the remaining life of toner cartridges.

Figure 5-7. Printer Info > Toner



Black

Estimated life (pages): 6000
Current pages on cartridge: 58
Estimated pages remaining: 5942
Estimated days remaining: (per 2 week average) Data Pending
Estimated days remaining: (per 6 months average) Data Pending

Cyan

Estimated life (pages): 8000
Current pages on cartridge: 58
Estimated pages remaining: 7942
Estimated days remaining: (per 2 week average) Data Pending
Estimated days remaining: (per 6 months average) Data Pending

Magenta

Estimated life (pages): 4800
Current pages on cartridge: 58
Estimated pages remaining: 4742
Estimated days remaining: (per 2 week average) Data Pending
Estimated days remaining: (per 6 months average) Data Pending

Yellow

Estimated life (pages): 8000
Current pages on cartridge: 58
Estimated pages remaining: 7942
Estimated days remaining: (per 2 week average) Data Pending
Estimated days remaining: (per 6 months average) Data Pending

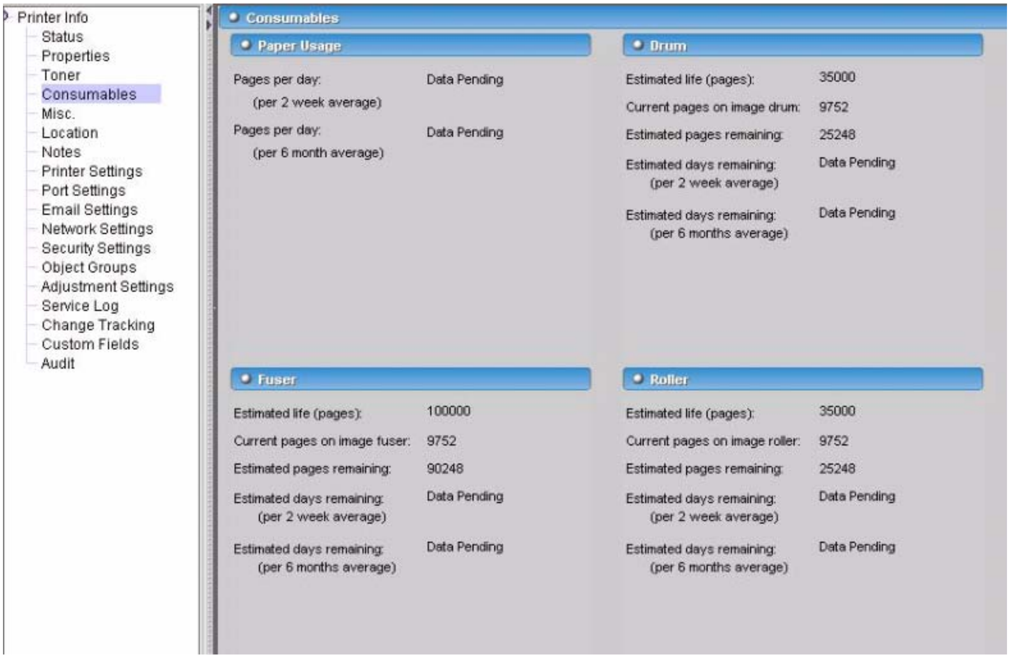
For estimates of remaining life to be meaningful, polling must have been active for the relevant period (two weeks or six months). This panel displays *Data Pending* when polling has not occurred for the required duration. You can consult the *Printer Age* column in This screen has the sub-panels for *Black*, *Cyan*, *Magenta* and *Yellow* toner. These have the following fields:

- **Est. toner life (total pages)**—The estimated total life of this toner, expressed in pages.
- **Current pages on toner cartridge**—The current count of pages printed on this cartridge.
- **Est. pages remaining**—The estimated remaining pages for the cartridge.
- **Est. days remaining (per 6 mths avg)**—The days of service remaining for the cartridge, based on the six month average daily consumption.
- **Est. days remaining (per 2 week avg)**—The days of service remaining for the cartridge, based on the two week average daily consumption.

Consumables

This screen displays the status of consumables like drum, fuser, roller, and paper.

Figure 5-8. Printer Info > Consumables



Printer Info
- Status
- Properties
- Toner
- Consumables
- Misc.
- Location
- Notes
- Printer Settings
- Port Settings
- Email Settings
- Network Settings
- Security Settings
- Object Groups
- Adjustment Settings
- Service Log
- Change Tracking
- Custom Fields
- Audit

Consumables

Paper Usage

Pages per day: (per 2 week average)	Data Pending
Pages per day: (per 6 month average)	Data Pending

Drum

Estimated life (pages):	35000
Current pages on image drum:	9752
Estimated pages remaining:	25248
Estimated days remaining: (per 2 week average)	Data Pending
Estimated days remaining: (per 6 months average)	Data Pending

Fuser

Estimated life (pages):	100000
Current pages on image fuser:	9752
Estimated pages remaining:	90248
Estimated days remaining: (per 2 week average)	Data Pending
Estimated days remaining: (per 6 months average)	Data Pending

Roller

Estimated life (pages):	35000
Current pages on image roller:	9752
Estimated pages remaining:	25248
Estimated days remaining: (per 2 week average)	Data Pending
Estimated days remaining: (per 6 months average)	Data Pending

This panel includes several fields with averages and projections about consumables' end of life. For these fields to be accurate, and in some cases to appear at all, the software must have collected enough data (*Data Pending* appears when not enough data has been collected yet for a meaningful conclusion). Typically these fields require two weeks' to six months' worth of data collected before the displayed conclusions are useful. Calculations are based on the default toner cartridge capacities. Set these to alternative capacities Misc.

The (read-only) fields displayed on this screen are the following:

Paper Usage

- **Avg Pages per day (over 6 months)** —The average daily use for the last six months.
- **Avg Pages per day (over 2 weeks)** —The average daily use for the last two weeks.

Drum / Fuser / Roller

These panels display the following information about their respective subjects:

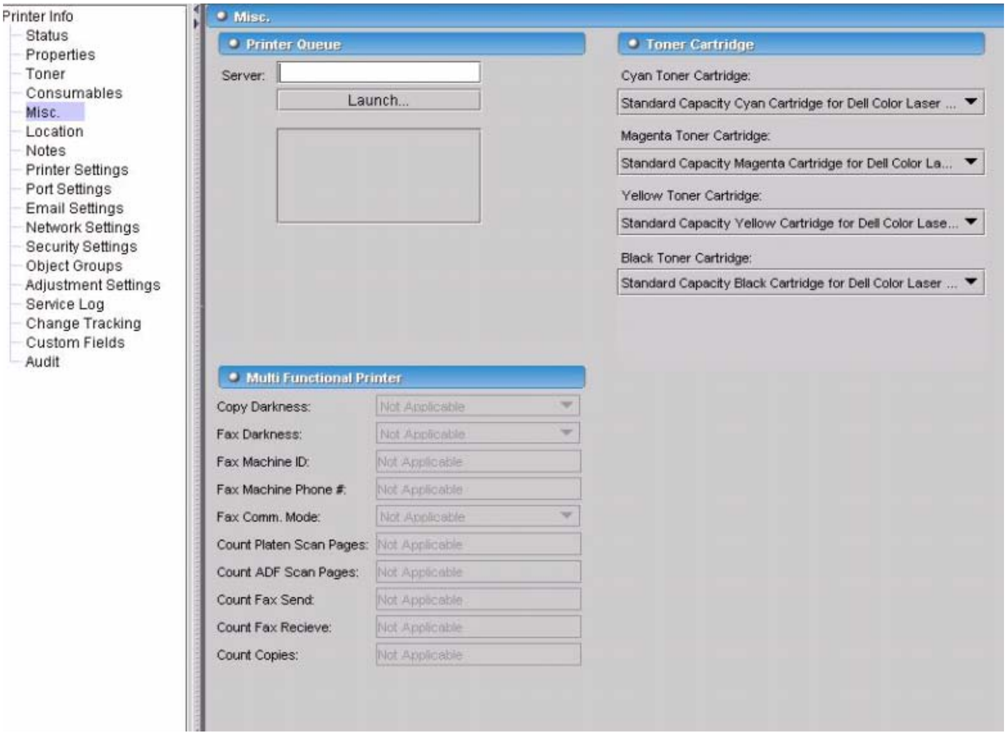
- **Est Life (total pages)**—The total printed pages over the life of this roller/drum/fuser. This comes from the manufacturer's estimate life for the component(M).
- **Current pages on image...**—The current count of pages printed on this roller/drum/fuser. Number of pages printed on the current drum. Reset by *Replace Drum*, for example, in the action menu. (C)

- **Est. pages remaining**—The estimated remaining pages for the roller/drum/fuser. This is calculated by subtracting the pages printed on the current drum / fuser / roller from the manufacturer's rated life for that part. (C)
- **Est. days remaining (per 6 mths avg)**—The days of service remaining for the roller/drum/fuser, based on the six month average daily consumption. Estimated days remaining on the current consumable, calculated using the average pages printer per day over this last 6 months on this specific printer.
- **Est. days remaining (per 2 week avg)**—The days of service remaining for the roller/drum/fuser, based on the two week average daily consumption. Estimated days remaining on the current consumable, calculated using the average pages printed per day over the last 2 weeks on this specific printer.

Misc

This screen displays miscellaneous printer attributes.

Figure 5-9. Printer Info > Misc



Server:

Cyan Toner Cartridge: Standard Capacity Cyan Cartridge for Dell Color Laser ...

Magenta Toner Cartridge: Standard Capacity Magenta Cartridge for Dell Color La...

Yellow Toner Cartridge: Standard Capacity Yellow Cartridge for Dell Color Lase...

Black Toner Cartridge: Standard Capacity Black Cartridge for Dell Color Laser ...

Copy Darkness: Not Applicable

Fax Darkness: Not Applicable

Fax Machine ID: Not Applicable

Fax Machine Phone #: Not Applicable

Fax Comm. Mode: Not Applicable

Count Platen Scan Pages: Not Applicable

Count ADF Scan Pages: Not Applicable

Count Fax Send: Not Applicable

Count Fax Recieve: Not Applicable

Count Copies: Not Applicable

This screen has the following panels and fields:

Printer Queue

Enter the IP address or hostname of the print server for the selected network printer in the *Server* field. Currently, only one queue is supported. When you click the *Launch* button after filling in the server, the operating system's print queue screen appears, displaying the pending print jobs for the selected printer. This value is provided for user convenience and does not imply tracking or management of the queue by this software. You can refer to the print server two ways:

- *Windows*–If the queue entered starts with a double backslash (\\), then clicking the launch button on a windows Java client will open a window printer queue window pointing to the printer. If the queue does not exist or the user does not have permissions this will be reported and handled by Windows. Access control is not part of this software.

- *HTTP*–If the queue entered starts with *http:* then a browser window opens with the location set to the queue string entered by the user. This is useful for web-based queue management tools, including CUPS.

Toner Cartridge

This panel lets you select a toner cartridge size from pick lists. Only one such pick list appears for a black printer, but four appear for the CMYK cartridges. Picking toner cartridges of different capacities impacts remaining life calculations (see Consumables) and toner replacement alerts. Toner cartridge capacities are *not* discovered. You must select them manually, from the part numbers appearing in the pick list, if the default selection does not apply.

Multi Functional Printer

These fields are relevant if the selected printer is also a copier, scanner and/or fax:

- **Copy Darkness**—Select from the pick list of available types. This sets the default darkness used when using the copy functionality of multi-function printers. (P)
- **Fax Darkness**—Select from the pick list of available types. (P)
- **Fax Machine ID**—Enter a text identifier that appears on faxes sent from this machine.(P)
- **Fax Machine Phone #**—The phone number for the service line connected to a multi-function printer for sending and receiving faxes. This number is often required on outgoing faxes. (P)
- **Fax Comm. Mode**—Select a communication mode from the pick list of available types. (P)
- **Count Platen Scan Pages**—Counts scans run on the scanner of a multi-function printer made by lifting the platen and physically placing the original. (P)
- **Count ADF Scan Pages**—Counts scans run on the scanner of a multi-function printer using the automatic document feeder (mechanical feeder). This typically includes copies, scans, and faxes. (P)
- **Count Fax Send**—Counts faxes sent on a multi-function printer. Note: Depending on the manufacturer this could be a count of faxes or count of fax pages sent. Consult your printer's user guide to determine which.. (P)
- **Count Fax Receive**—Number of Faxes received by a multi-function printer. (P)
- **Count Copies**—Number of copies (pages) made on a multi-function printer. (P)

Location

This screen displays a location for the selected printer, and a field where you can enter any notes about this printer or location.

Figure 5-10. Printer Info > Location

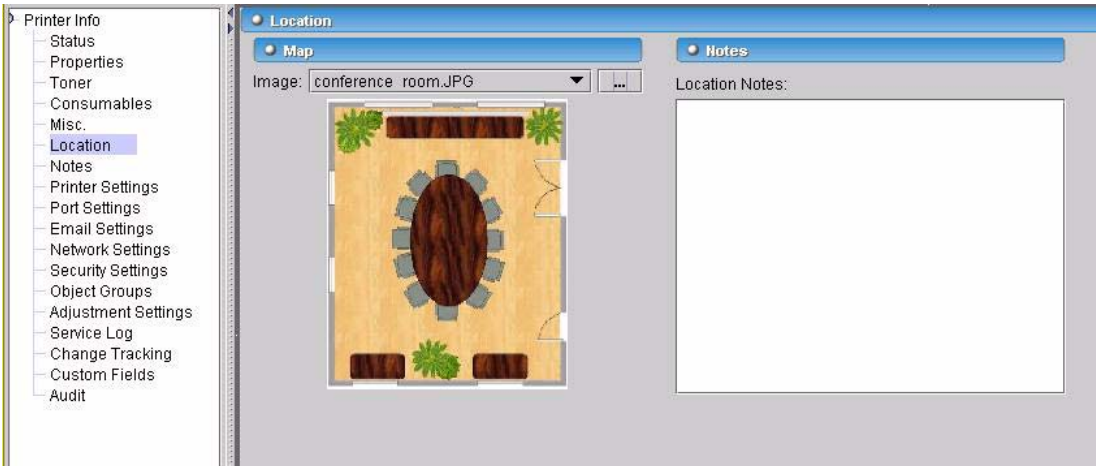


Image: conference room.JPG

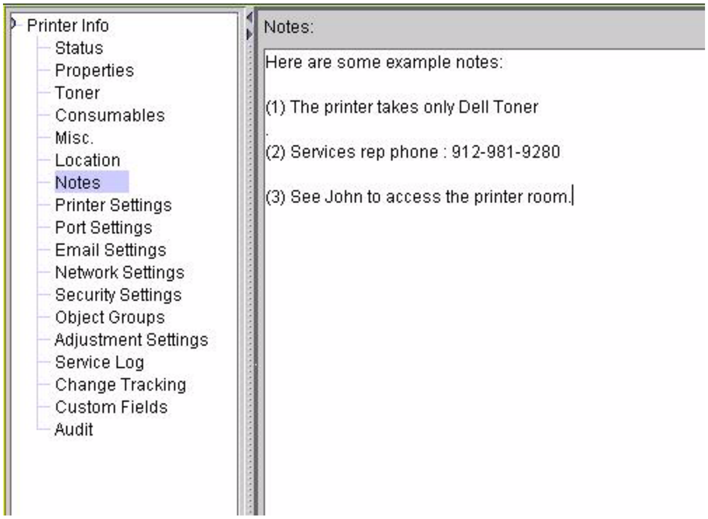
Location Notes:

Select images for the location in the pick list. Click the command button (...) to add .`jpg`, `.gif` or `.png` images to the pick list. Clicking the command button makes a file chooser appear; select the map file there. Once selected, these images are available to all clients. (L) Location *Notes* is a field provided to enter notes about the location of the printer, like a description of the location or instructions on getting to the (L)

Notes

This field provides a scratch pad area for notes on the printer, stored in the database.

Figure 5-11. Printer Info > Notes



Notes:

Here are some example notes:

(1) The printer takes only Dell Toner

(2) Services rep phone : 912-981-9280

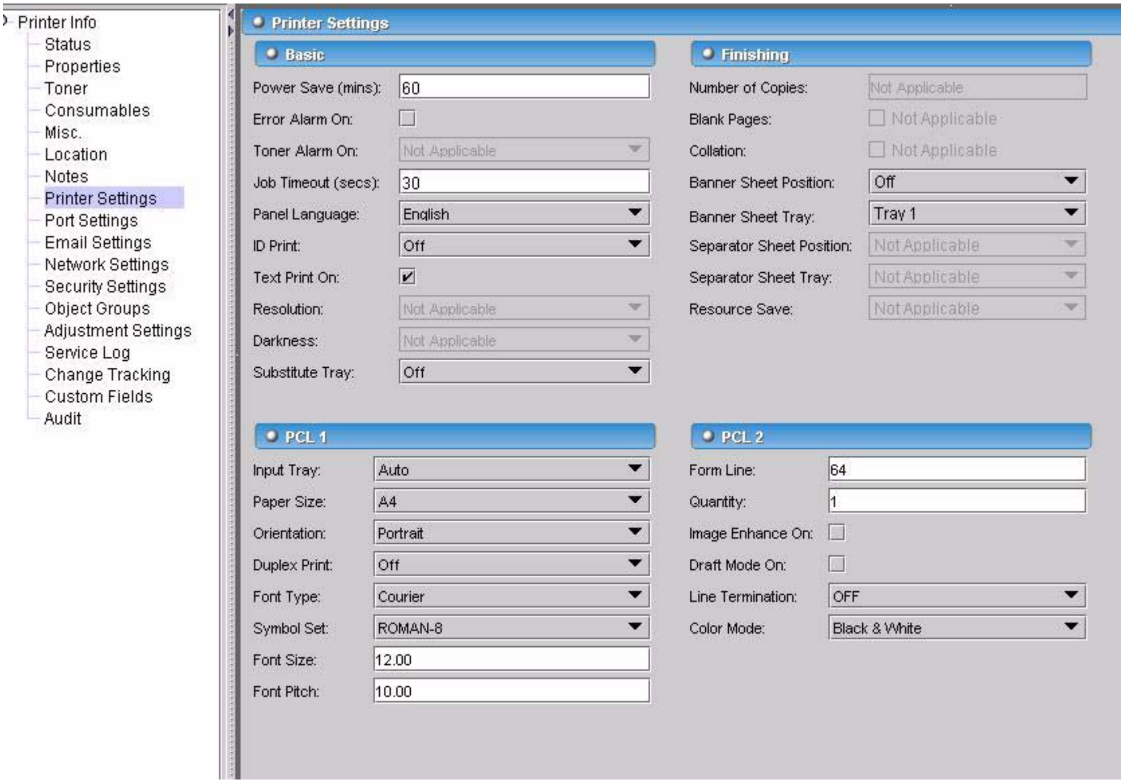
(3) See John to access the printer room.

It is stored the format you enter or revise, without any history of the revisions. Comments about the printer persist only as long as the printer exists in the database. Deleting and re-discovering the printer eliminates any notes. Notes might include temporary status notations like "John is on his way to replace the toner" to assist in managing the device. Enter notes, and click **Save** to preserve them.

Printer Settings

This screen displays settings for the selected printer.

Figure 5-12. Printer Info > Printer Settings



Printer Settings

Basic

Power Save (mins): 60
Error Alarm On: □
Toner Alarm On: Not Applicable
Job Timeout (secs): 30
Panel Language: English
ID Print: Off
Text Print On: ☑
Resolution: Not Applicable
Darkness: Not Applicable
Substitute Tray: Off

Finishing

Number of Copies: Not Applicable
Blank Pages: □ Not Applicable
Collation: □ Not Applicable
Banner Sheet Position: Off
Banner Sheet Tray: Tray 1
Separator Sheet Position: Not Applicable
Separator Sheet Tray: Not Applicable
Resource Save: Not Applicable

PCL 1

Input Tray: Auto
Paper Size: A4
Orientation: Portrait
Duplex Print: Off
Font Type: Courier
Symbol Set: ROMAN-8
Font Size: 12.00
Font Pitch: 10.00

PCL 2

Form Line: 64
Quantity: 1
Image Enhance On: □
Draft Mode On: □
Line Termination: OFF
Color Mode: Black & White

This screen has the following fields:

Basic

- **Power Save (mins)**—The time, in minutes the printer will wait to enter power save mode after the last activity. On most printers “activity” refers to a print job and is not affected by management activity, SNMP, and other network activity. (P)
- **Error Alarm On**—Check to activate an audible alarm in case of error. (P)
- **Toner Alarm On**—Check to activate an audible alarm in case of a toner alert. (P)
- **Job Timeout (secs)**—The time the printer will allow a job to process without printing before the job is terminated. This is a “watchdog” timer that prevents the printer from becoming permanently busy due to an invalid print job. (P)

- **Panel Language**—The language displayed on the LCD panel of the printer. On some printers there is only one universal language for all interfaces, including the front panel and web interface. On printers with templates if the Panel Language controls the printer's web page this option will be read-only, since changing it will prevent this software from performing status reads and updates to the printer via the web interface. (P)
- **ID Print**—On/Off status for a feature that prints the user name printing jobs in small font at the bottom of each page of those print jobs. (P)
- **Text Print On**—On/Off status that determines if the printer prints jobs that are purely text (not PCL, PS and so on). This is sometimes turned off when text printing is unused to prevent a corrupt PCL job from being interpreted as text. In that case the corrupt PCL job can print a large number of mostly blank pages. (P)

  NOTE: This option must be on for the *Print Test Page* feature of this software to work correctly.
- **Resolution**—Controls the default resolution of print jobs. Many printers largely ignore this setting since PCL and PS jobs normally specify a print resolution as part of the job and override this setting.
- **Darkness**—Controls the default darkness of print jobs. Many printers ignore this setting since PCL and PS jobs normally specify a print darkness as part of the job and override this setting.
- **Substitute Tray**—Select the input tray for printing when the input tray does not work from the pick list. Options can include *Nearest Size*, *Larger Size*, and so on.

PCL 1

Many PCL settings are simply default settings. Individual PCL jobs can specify different settings for the print job that override these settings. Consequently, changing these settings may not result in an obvious change in behavior of the device. On some printers this settings may also affect text printed in "text only" or *ASCII* mode.

- **Input Tray**—Select the input tray from the pick list. This selects the default tray for print jobs. (P)
- **Paper Size**—Select the paper size from the pick list. This specifies the default paper size used for print jobs. In general if Paper size is a value (like *Letter*) and the Input Tray is *auto* the printer selects a tray with that size paper for printer jobs that do not specify a tray. (P)
- **Orientation**—Set the default (*Landscape* / *Portrait*). (P)
- **Duplex Print**—Select the duplexing information from the pick list (*Long Edge*, *Short Edge*, *Off*). This determines the default duplex (two-sided) printing.
- **Font Type**—The default font for text print jobs sent this printer. (P)
- **Symbol Set**—The default font used for symbols in print jobs. (P)
- **Font Size**—The default point size of the font. (P)
- **Font Pitch**—The default pitch of the font. The pitch is the number of characters printed horizontally per inch. A smaller number results in larger gaps between the characters. This controls the space between characters only and does not change the drawing width of the characters. Setting it too high results in the letters actually overlapping. (P)

Finishing

- **Number of Copes**—Enter the default number of copies. This is largely ignored since most PCL and PS jobs contain a copy count as part of the job and will over-ride this setting. (P)
- **Blank Pages**—Check to print blank pages. If blank pages are disabled the printer will not print any page that has absolutely no content on it. This is useful for eliminating waste in print jobs. On print jobs where blank pages are desired, pages that contain a page number are not blank and will still print. Only pages with absolutely no content are skipped if this is checked. (P)
- **Collation**—Check to collate, if available. Enables the collation of output. When disabled (default on most printers) if you send a single job with a selection of four copies, the printer will optimize printing by printing the first page four times, then page two four times, and so on. When enabled it prints all of the pages of the job, then start over at the beginning resulting in four copies that have already been separated. Enabling this feature can slow printing and greatly increase memory use in the printer.
- **Banner Sheet Position**— Select from *Off*, *Top*, *Bottom*, or *Top & Bottom*. This enables the banner print function, as well as determining when it prints in relation to the print job. Banner pages contain printed text identifying the print job like the user, date and time, and so on.
- **Banner Sheet Tray**—Selects the paper tray used for banner pages. You could have banner pages print from a tray with lower cost paper, or paper that is easy to spot such as a bright color. (P)
- **Separator Sheet Position**—This selection identifies if and where a blank page should be placed between print jobs. Unlike *Banner print*, a separate sheet normally has no printed content. This uses less toner, and is slightly faster for printing on some printers. (P)
- **Separator Sheet Tray**—This selection lets you specify a tray for separator sheets, when they are enabled. For example you could put brightly colored paper in tray 4 and use that tray for separator sheets resulting in an easy to find divider between your print jobs. (P)
- **Resource Save**—On/Off status of functionality designed to lower the cost of printing. Sometimes called *Toner Save* or *Econo-mode*, this feature usually reduces the toner density globally for all print jobs, resulting in less toner per page and a slightly lower operating cost, with a slight reduction in quality. This is normally used on printers providing low importance output, like internal memos and drafts. This feature normally results in a very slight difference in quality and should not be confused with *Draft Mode* which may produce more drastic reduction in quality. (P)

PCL 2

Many PCL settings set defaults. Individual PCL jobs can specify different settings for the print job that override these settings. Consequently, changing these settings may not result in an obvious change in behavior of the device. On some printers this settings may also affect text printed in "text only" or *ASCII* mode.

- **Form Line**—Number of lines that should appear on a page when printing text-based print jobs. (P)
- **Quantity**—Default number of copies for a print job. Print jobs like PCL and PostScript normally contain a quantity that overrides this value so it is mostly ignored, except for text-based printing or jobs that do not specify a quantity. (P)

- **Image Enhance On**—Check to enable. For device that support special processing to enhance images. This may slow printing on some devices. (P)
- **Draft Mode On**—Check to enable. This turns on a lower quality mode that can result in faster printing and possibly lower toner usage, but at a very lower quality. Print Jobs like PCL and Postscript normally contain a quality setting that over-rides this value. (P)
- **Line Termination**—Specifies a line termination character. Select from the available options in the pick list (*Add-CR*, *CR-XX*, *OFF*, *Add-LF*). (P)
- **Color Mode**—Select from the pick list (*Color*, *Black-and-White*). The default value to determine if PCL jobs are printed in color or black and white (Monochrome). (P)

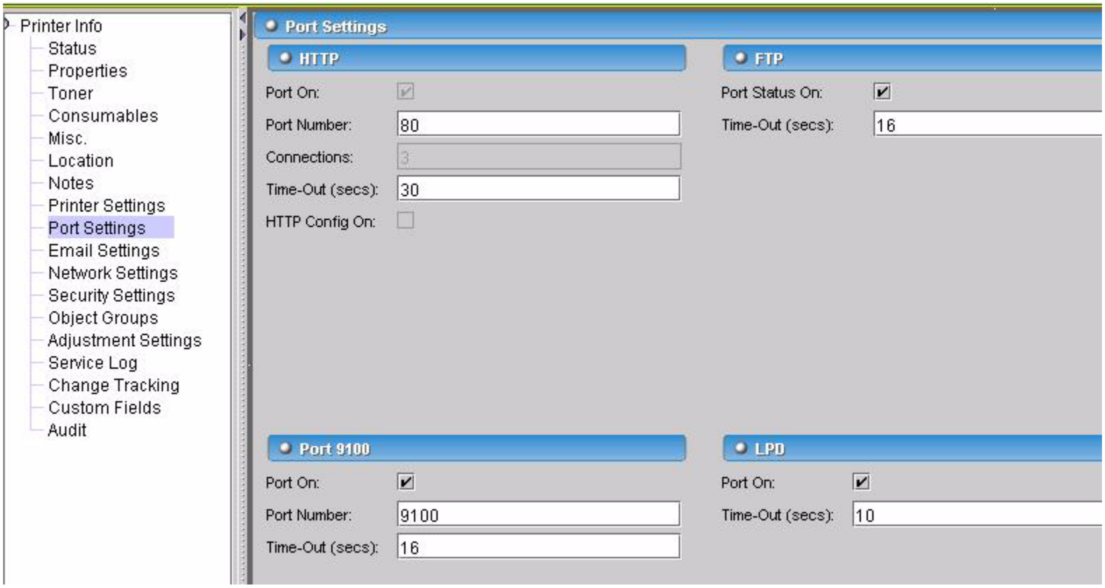
PS

- **Error Report On**—Enable the error report for PostScript print jobs. (P)
- **Time-Out (secs)**—Seconds for PostScript print job timeout. (P)
- **Paper Select Mode**—The method used to select paper sources when printing PostScript jobs. Select from the pick list. (P)

Port Settings

This panel displays the network settings for the selected printer.

Figure 5-13. Printer Info > Port Settings



Port Settings

HTTP

Port On: ☑
Port Number: 80
Connections: 3
Time-Out (secs): 30
HTTP Config On: □

FTP

Port Status On: ☑
Time-Out (secs): 16

Port 9100

Port On: ☑
Port Number: 9100
Time-Out (secs): 16

LPD

Port On: ☑
Time-Out (secs): 10

This screen has fields to configure the following:

HTTP

- **Port On**—Check to enable (when available). On/Off status of the HTTP port of the printer. In effect, this setting enables and disables the EWS (Embedded Web Server) of the printer. (P)
- **Port Number**—Enter a port number. This is the network port used to accept incoming EWS connections.(P)
- **Connections—** The Number of simultaneous connections allowed for the printer's EWS. This is read only on many printers. (P, PR)
- **Timeout (secs)**—The timeout value used by the EWS for handling connections. (P, PR)
- **HTTP Config On**—On/Off status controlling if configuration changes can be made by this software. Setting this value to *off* usually means you cannot turn it back on with this software, but instead must use the printer's front panel menu. (P)

FTP

- **Port Status On**—Check to enable. In effect, this setting enables and disables the FTP server of the printer.
- **Timeout (secs)**—This the timeout value used by the FTP server for handling connections.

Port 9100

- **Port On**—Check to enable (when available). This determines the status of port 9100 used for incoming print jobs. This normally includes PCL, PostScript and text jobs sent using the ethernet ports. The name of these settings does not change when the port 9100 functionality has been mapped to a new port number. (P)
- **Port Number**—An integer representing the port number used for network printing by most PCL and PostScript drivers, as well as network-based text print jobs. Changing this value results in the printer using a different port number but does not change the name from Port 9100. (P)
- **Timeout (secs)**—Time out for network connections on Port 9100 connections, regardless of the actual port number assigned. This is the network connection time out and independent from various timeouts associated with printing functionality. (P)

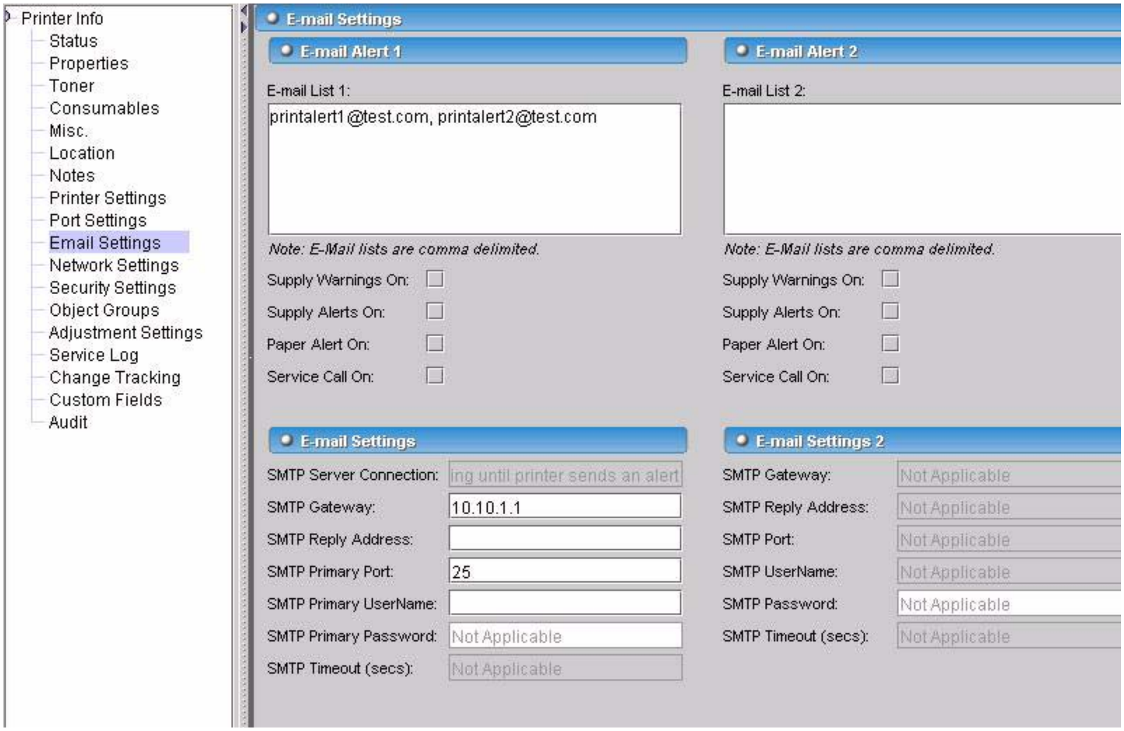
LDP

- **Port On**—Check to enable. This enabled/disables the ability to remotely print via LDP. Normally Port 515.
- **Time-Out (secs)**—Enter the number of seconds for timeout. This is the timeout value used by the LDP server for handling network connections.

E-mail Settings

This screen lets you configure e-mail alerts that originate with printers.

Figure 5-14. Printer Info > Email Settings



E-mail Settings

E-mail Alert 1

E-mail List 1: printalert1@test.com, printalert2@test.com

Note: E-Mail lists are comma delimited.

Supply Warnings On: □

Supply Alerts On: □

Paper Alert On: □

Service Call On: □

E-mail Alert 2

E-mail List 2:

Note: E-Mail lists are comma delimited.

Supply Warnings On: □

Supply Alerts On: □

Paper Alert On: □

Service Call On: □

E-mail Settings

SMTP Server Connection:	ing until printer sends an alert
SMTP Gateway:	10.10.1.1
SMTP Reply Address:	
SMTP Primary Port:	25
SMTP Primary UserName:	
SMTP Primary Password:	Not Applicable
SMTP Timeout (secs):	Not Applicable

E-mail Settings 2

SMTP Gateway:	Not Applicable
SMTP Reply Address:	Not Applicable
SMTP Port:	Not Applicable
SMTP UserName:	Not Applicable
SMTP Password:	Not Applicable
SMTP Timeout (secs):	Not Applicable

NOTE: These e-mails come from the printer, not this software. Best practice is to have the software not the printers emit the e-mails. See Chapter on Events, Rules and Actions. To set-up mail for this software, see SMTP / Email Settings.

This screen has the following fields:

E-mail Alert 1 / 2

These are the primary and secondary (backup) mail settings.

- **E-mail List 1/2**—Enter lists of e-mail addresses to send the alert. (P) This lists e-mail recipients for alerts generated by the printer. The format of this list varies by printer manufacturer and model. These addresses and alerts come directly from the printer and are not part of the event alert system of this software.

NOTE: When you enter multiple e-mail addresses, separate them with commas.

- **Supply Warnings On**—Check to enable an e-mail supply warning (for example, "you are *about* to run out of toner"). These mean supplies are nearly expended, and are pre-emptive, before an actual impact. (P)
- **Supply Alerts**—Check to enable a supply alert (for example, "you have run out of toner"). These occur when supplies run out or impact printing.(P)
- **Paper Alert**—Check to enable an alert, when paper runs out (P).
- **Service Call On**—Check this to generate an alert when the printer requires a service call for repair or a non-recoverable error state.

E-mail Settings 1 / 2

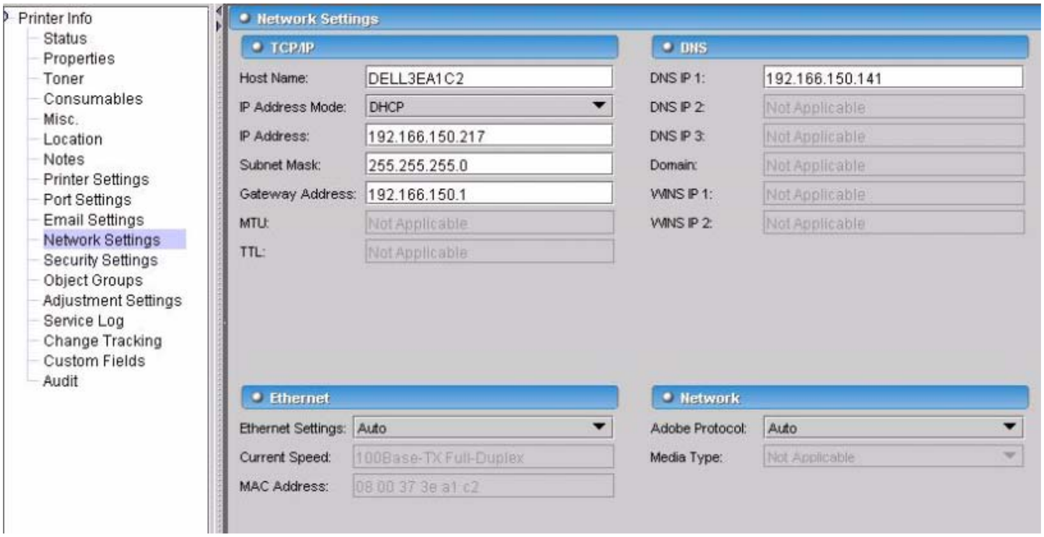
These are settings for the primary and secondary SMTP server for any e-mail notifications coming from the printers.

- **Email Settings**—Labels the e-mail settings for the printer.
- **SMTP Server Connection**—This read only attribute shows the status of the SMTP connection. On some printers the SMTP configuration is validated and will indicate the status based on the current configuration. (PR)
- **SMTP Gateway**—This is the destination address of the server that provides SMTP service (email) for outgoing messages. (P)
- **SMTP Reply Address**—The reply address included in outgoing messages from the printer. Normally it should reflect the name of the printer and/or IP address to facilitate knowing which printer generated the message. (P)
- **SMTP Primary Port**—The TCP/IP port on the server (SMTP Gateway) used for SMTP email services. This is normally port 25. (P)
- **SMTP Primary UserName**—For SMTP (mail) servers that require authentication, this is the user name used when submitting outgoing email. (P)
- **SMTP (Primary) Password**—For SMTP (mail) servers that require authentication, this is the password that will be used when submitting outgoing email. (P)
- **SMTP Timeout (secs)**—E-mail timeout for the selected printer to contact the SMTP server.

Network Settings

This screen displays TCP/IP, DNS, and Ethernet settings for the selected printer.

Figure 5-15. Printer Info > Network Settings



Host Name: DELL3EA1C2

IP Address Mode: DHCP

IP Address: 192.166.150.217

Subnet Mask: 255.255.255.0

Gateway Address: 192.166.150.1

MTU: Not Applicable

TTL: Not Applicable

DNS IP 1: 192.166.150.141

DNS IP 2: Not Applicable

DNS IP 3: Not Applicable

Domain: Not Applicable

WINS IP 1: Not Applicable

WINS IP 2: Not Applicable

Ethernet Settings: Auto

Current Speed: 100Base-TX Full-Duplex

MAC Address: 08 00 37 3e a1 c2

Adobe Protocol: Auto

Media Type: Not Applicable

This screen has the following fields:

TCP / IP

- **Host Name**—The network host name used by the printer. Changing this value changes both the printer and the local database, however updates to the DNS server by the device may not be immediate and may have to propagate in a complex network environment. (P)(L)
- **IP Address Mode**— Select from the available settings in the pick list. (P) The mode used by the printer to determine it's IP address.
- *Static*–Users set the printer IP explicitly.
- *Auto*–Enables all automatic IP assignment modes available.
- *DHCP*–Enable the DHCP protocol only.
- *ARP*–Enables ARP IP negotiation only.
- **IP Address**—This field is the IP address of the printer. Note: On some printers when an auto-IP mode is selected this field will not populate with the auto-negotiated IP, but instead reflects the last static IP of the printer or 0.0.0.0 if no IP has ever been set. (P)(PW)
- **Subnet Mask**— This field is the subnet mask for the printer. When you select an auto-IP mode on some printers this field does not populate with the auto-negotiated subnet mask, but instead reflect the last static subnet mask of the printer. (P)(PW)

- **Gateway Address**—This field is the IP of the gateway for the printer, which is the location where traffic should be sent that is not intended for the local subnet as determined by the subnet mask. When you select an auto-IP mode on some printers this field does not populate with the auto-negotiated subnet mask, but instead reflect the last static subnet mask of the printer. (P)(PW)
- **MTU**—This field is the MTU (Maximum Transmission Unit) used by the network drivers on the printer. This value sets the maximum packet size. (P)
- **TTL**—The TTL (time to live, specifying how long or how many more hops a packet can travel before being discarded or returned) for the selected printer. This field is the TTL value used by the network drivers on the printer. (P)

DNS

- **DNS IP 1/2/3**—Enter the first, second and third DNS server IP addresses on the printer. (P)
- **Domain**—The domain of which the printer is an intended member. (P)
- **WINS IP 1/2**—Enter the first and second WINS IP entries on the printer. (P)

Ethernet

- **Ethernet Settings**—The current ethernet settings. When this is selectable, you can select from the following settings: *SELECT, AUTO 10 BASETFULL, 10BASETHALF, 100BASETFULL*, or *100BASETHALF*. This is the current speed of the Ethernet interface. This reflects the actual speed/mode when the current setting is *Auto*. (PR)
- **MAC Address**—The MAC address of the ethernet interface on the selected printer. (PR)

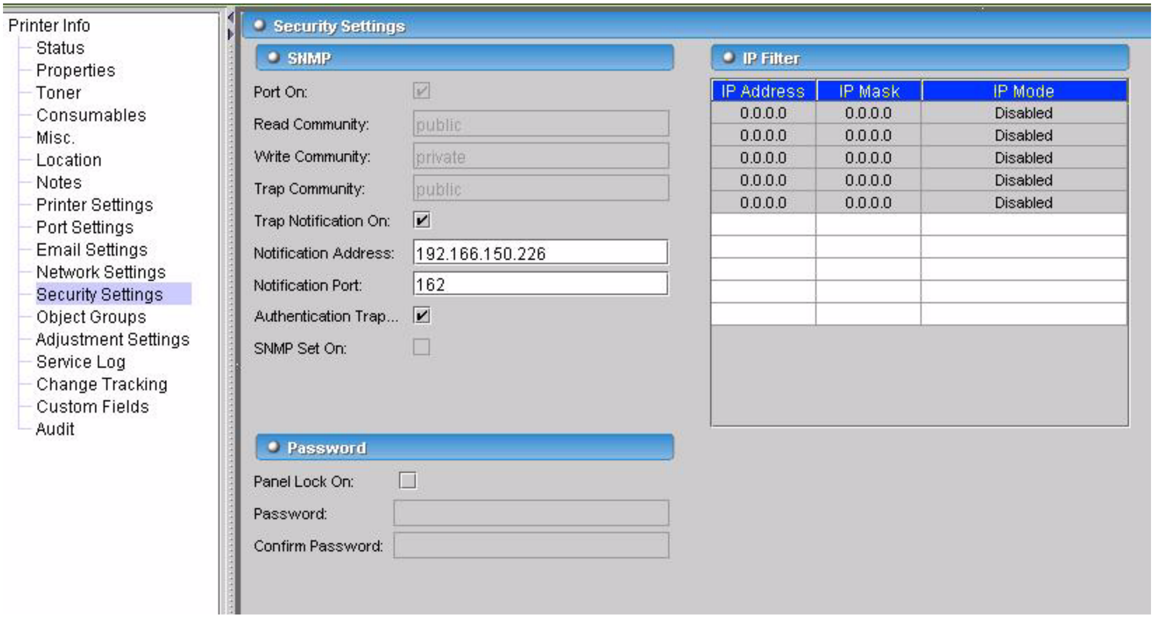
Network

- **Adobe Protocol**—When available, select from the alternatives in the pick list (*Auto, Standard, BCP, TBCP* or *Raw*). On some printers this value must be turned or set to Auto to print using the Adobe Protocol. (P)
- **Media Type**—The network connection media type, typically *Ethernet/RJ45* or *Coax/BNC/Thinnet*. (P)

Security Settings

This screen displays security settings for the selected printer.

Figure 5-16. Printer Info > Security Settings



Security Settings

SNMP

Port On: ☑

Read Community: public

Write Community: private

Trap Community: public

Trap Notification On: ☑

Notification Address: 192.166.150.226

Notification Port: 162

Authentication Trap... ☑

SNMP Set On: □

IP Filter

IP Address	IP Mask	IP Mode
0.0.0.0	0.0.0.0	Disabled
0.0.0.0	0.0.0.0	Disabled
0.0.0.0	0.0.0.0	Disabled
0.0.0.0	0.0.0.0	Disabled
0.0.0.0	0.0.0.0	Disabled

Password

Panel Lock On: □

Password:

Confirm Password:

This screen has the following fields:

SNMP

- **Port On**—On/Off status that enables and disables the SNMP port on the device, effectively turning this functionality on or off. This must be turned on for OMPM to manage the printer. (P)
- **Read Community**—The community name of the printer used for SNMP reads. (PW)
- **Write Community**—The community name of the printer used for SNMP writes. (PW)
- **Trap Community**—The community name of the printer used when sending traps. (PW)
- **Trap Notification**—On/Off status that enabled sending off traps by the printer. (PW)
- **Notification Address**—The address where the printer sends SNMP traps. Normally an IP or host name (determined by the printer) (P).

- **Notification Port**—The port (at the Notification Address) where the printer sends SNMP traps. (P)
- **Authentication Trap On**—Checking this controls sending of SNMP traps when there is a failed SNMP authentication. In effect it reports failed SNMP connections due to community name. Seeing several of these in a row for a device indicates someone is trying to guess at the community name to access the printer.
- **SNMP Set On**—On/off status that indicates if the printer should allow configuration changes via SNMP (SNMP Write enable). (P)

IP Filter

Use this panel to view the IP addresses that can communicate with your printer. Communication is either A*ccept*, *Reject*, or *Disabled* for the listed IP address and IP mask.

The IP security features of printers vary by manufacturer and model. Not all security models can be supported by a single interface. For devices with a security model that can be cross mapped these fields provide a method to edit those values. In some cases it may be best to directly access the device to configure these settings.

Security List—The security list provides a method of controlling access to the printer by IP address or range. The values available are:

- **IP Address**—A Network IP address
- **IP Mask**—A network IP mask value
- **IP Mode**—Selection mode determines whether the listed IP or mask values are to be excluded from access or added to the valid address group.

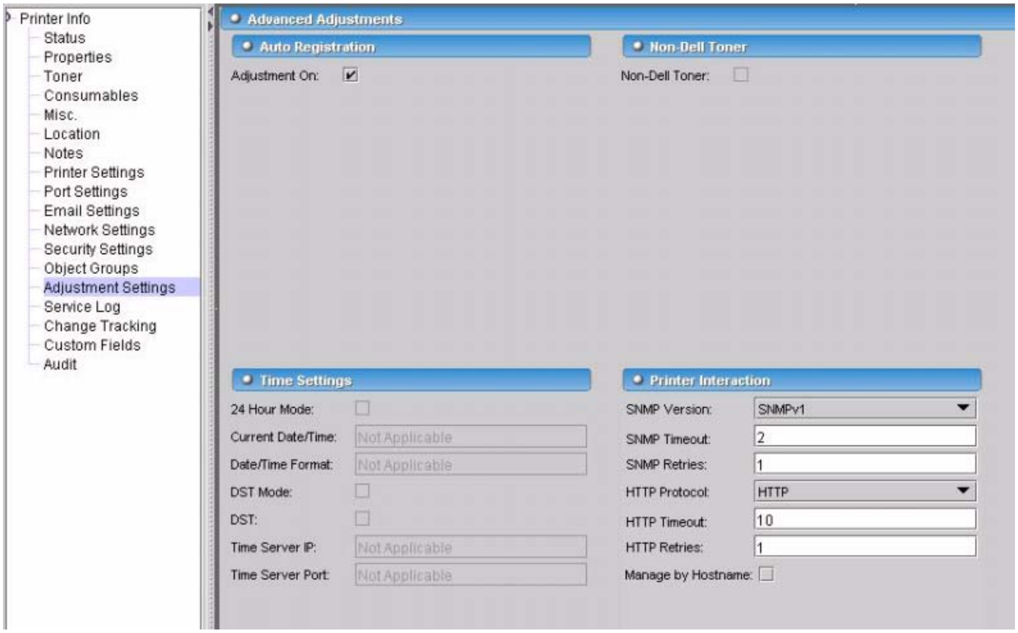
Password

- **Panel Lock On**—On/Off status that locks the front panel of the printer (the physical display and buttons on the front of the printer). On most printers this setting locks the ability to change the configuration of the device from the front panel (by passersby) but does not limit using the front panel to interact with the printer. The extent of features available from the front panel is determined by the individual printer. (P)
- **Password**—The password associate with the front panel of the printer. On printers where this is supported there may be a method for a user to enter a password at the front panel and change the configuration. This allows administrators to configure the device directly even with the front panel lock on. On many printers once a front panel password has been set it cannot be changed by this software because the previous password must be entered before a change. For this models you should directly access the printer to change this setting. (PW)
- **Confirm Password**—When changing the front panel password some printers require that the password be entered twice to prevent typographical errors. (PW)

Adjustment Settings

This screen displays Auto Adjustment Registration, Paper Density, and whether the toner is non-Dell.

Figure 5-17. Printer Info > Adjustment Settings 2



Advanced Adjustments

Auto Registration

Adjustment On: ☑

Non-Dell Toner

Non-Dell Toner: □

Time Settings

24 Hour Mode: □
Current Date/Time: Not Applicable
Date/Time Format: Not Applicable
DST Mode: □
DST: □
Time Server IP: Not Applicable
Time Server Port: Not Applicable

Printer Interaction

SNMP Version: SNMPv1
SNMP Timeout: 2
SNMP Retries: 1
HTTP Protocol: HTTP
HTTP Timeout: 10
HTTP Retries: 1
Manage by Hostname: □

This screen has the following fields:

Auto Registration

- **Adjustment On**—Check to enable. (P)

Non-Dell Toner

- **Non-Dell Toner**—Displays checked, if the toner on this printer is not from Dell. For Dell model printers this option enables use of toner cartridges purchased from vendors other than Dell. Note that using non-Dell toner often means the cartridge cannot report toner levels and you will be unable to track toner usage or receive notification when toner is low. (P)

Time Settings

- **24 Hour Mode**—Check to enable the 24 hour clock mode on the device. Some time modes are not supported on all devices. For example: 12 hour time without an integrated AM/PM indicator. On such devices only 24 hour mode is supported. (P)
- **Current Date/Time**—Enter the date / time. (P)

- **Date/Time Format**—Enter HH:MM:SS, MM/DD/YY, for example. This value sets printers that support multiple date time string format. This controls the order of the month, day, year, hour, minute, and seconds values to closer match formats used in different locales. (P)
- **DST Mode**—Check to enable Daylight Savings Time. You cannot modify DST on some printers if the DST Mode is on. This software may appear to allow setting this even though the printer does not accept the value because it is determining the Daylight Savings Time itself. (P)
- **DST**—Active only when DST is manual (the previous field is disabled). (P)
- **Time Server IP**—The IP address of a server providing network time services. If you do not know this value you should ask your network administrator. For printers set to an automatic IP mode such as DHCP this value will often by automatically set when the printer receives an IP address. (P)
- **Time Server Port**—The port for the network time service on the server set above. (P)

Printer Interaction

- **SNMP Version**—Selects the SNMP protocol version to communicate with this printer when requesting status or changing settings with that protocol. (P)
- **SNMP Timeout—**Selects the timeout period after which an SNMP request to this device is presumed to have failed. (P)
- **SNMP Retries**—Number of retries after a SNMP request fails. (P)
- **HTTP Protocol**—Selects whether the embedded web service (EWS) access to the printer is performed with HTTP (normal) or HTTPS (secure) when requesting status or changing setting via the printer's EWS.

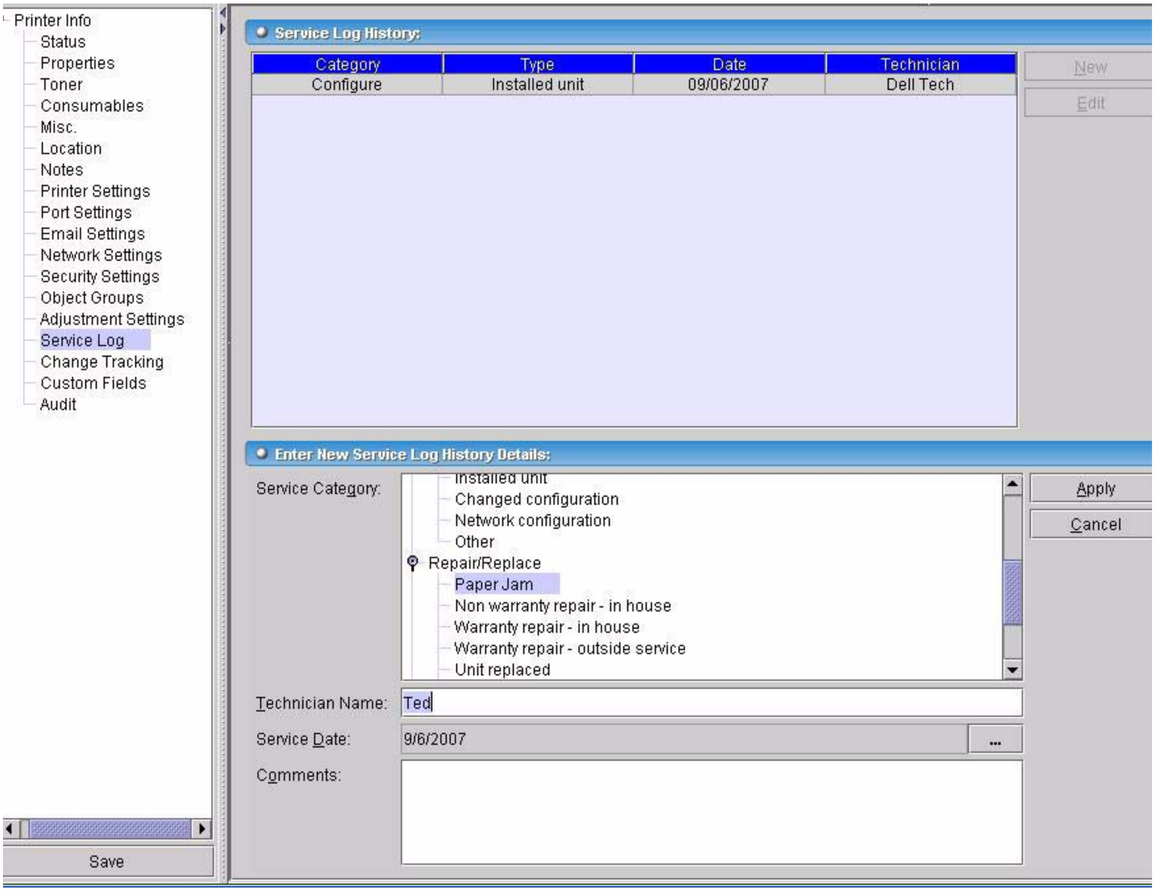
This applies to this software’s method of direct communication with the device and does not affect settings in the device or access to the printer outside of the software’s interaction. For example, enabling HTTPS makes this software communicate with the secure protocol but does make changes in the printer to enable HTTPS or disable HTTP. (P)

- **HTTP Timeout**—Amount of time to wait after a failed HTTP request before presuming the request has failed. (P)
- **HTTP Retries**—Number of retries after a HTTP (or HTTPS) request fails. (P)

Service Log

- This screen displays a record of service performed on the selected device.

Figure 5-18. Printer Info > Service Log



Category	Type	Date	Technician
Configure	Installed unit	09/06/2007	Dell Tech

Service Category:

Technician Name: Ted

Service Date: 9/6/2007

Comments:

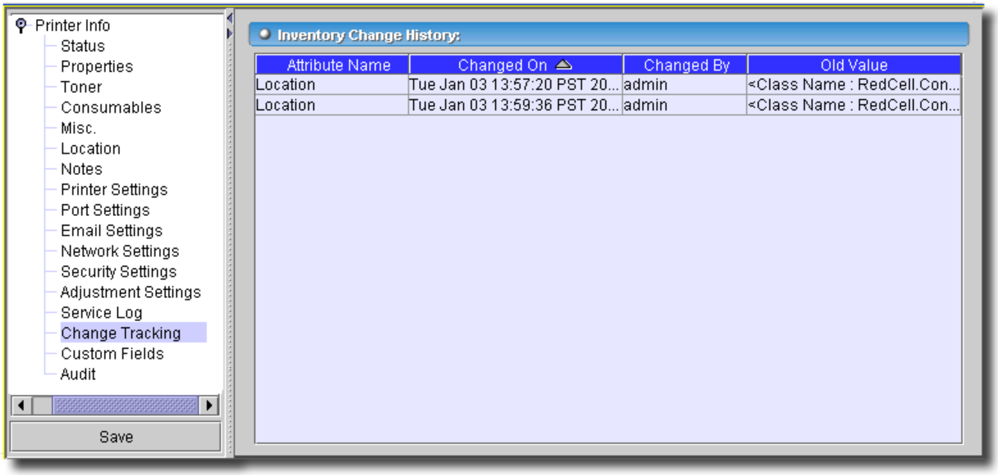
Click **Edit** to alter an existing, selected service item. To add a new service event, click **New** and the lower panel, **Enter New Service Log History Details** appears. Select a **Service Category**, enter a *Technician Name*, a *Service Date* (defaults to current date, but you can select from a calendar available when you press the control button [...] to the right of this field) and any *Comments*. This log consists of both automated events, like toner changes, and events entered by a user, like repairs or part replacements.

Click **Apply** to accept your edits, or **Cancel** to abandon them. When you click **Apply**, the item appears listed at the top of the screen.

Change Tracking

If you have configured attributes on your printers for change tracking, the results of that tracking appear on this screen.

Figure 5-19. Printer Info > Change Tracking



Inventory Change History:

Attribute Name	Changed On	Changed By	Old Value
Location	Tue Jan 03 13:57:20 PST 20...	admin	<Class Name : RedCell.Con...
Location	Tue Jan 03 13:59:36 PST 20...	admin	<Class Name : RedCell.Con...

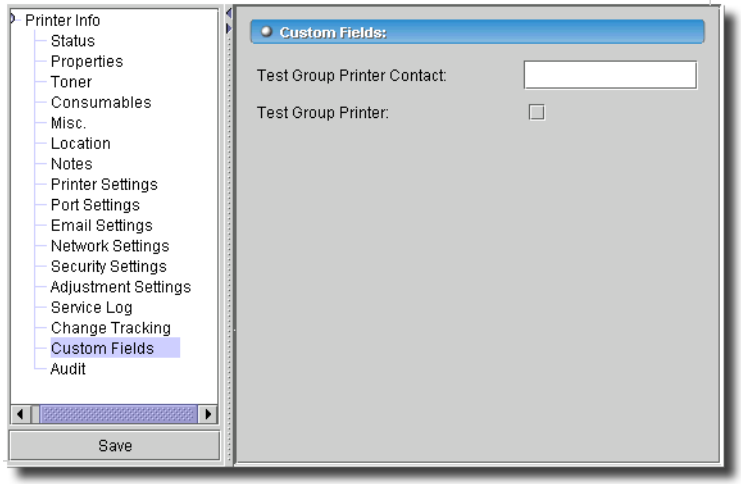
This screen displays columns outlining the *Attribute Name*, *Changed On* (date and time), *Changed By* (user login), and *Old Value* for each tracked change.

Setting up change tracking is an administrative task. You must first use the **Settings→ Configuration→ Inventory Config** manager to select a type of inventory (here, *Printer*), then configure **Change Tracking** for that type. Select the attributes to track in the **Change Tracking** screen. Finally, you must re-start the application server after having selected which attributes to track before any changes become visible.

Custom Fields

To add your own attributes to network's printers, you can configure **Custom Fields**. Configure custom fields that appear here with the Inventory Config manager. Access this through **Settings→ Configuration→ Inventory Config**. See Custom Fields for the details about how to do this.

Figure 5-20. Printer Info > Custom Fields



Test Group Printer Contact:

Test Group Printer: □

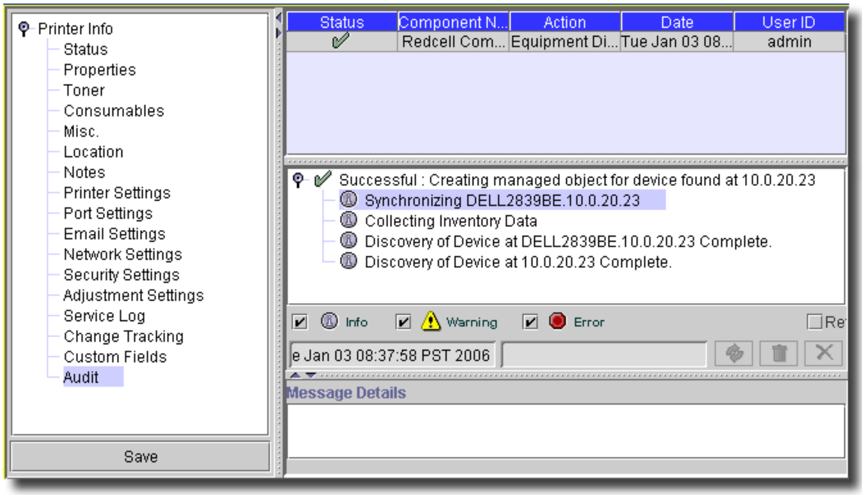
The fields that appear in Figure 5-20 are exemplary only. By default, the application contains no custom fields.

NOTE: You must restart the application server after configuring Custom Fields.

Audit

This screen displays the history of events involving the selected device.

Figure 5-21. Printer Info > Audit



Status	Component N...	Action	Date	User ID
✓	Redcell Com...	Equipment Di...	Tue Jan 03 08...	admin

- ✓ Successful : Creating managed object for device found at 10.0.20.23
  - Synchronizing DELL2839BE.10.0.20.23
  - Collecting Inventory Data
  - Discovery of Device at DELL2839BE.10.0.20.23 Complete.
  - Discovery of Device at 10.0.20.23 Complete.

☑ Info ☑ Warning ☑ Error □ Re

e Jan 03 08:37:58 PST 2006

Message Details

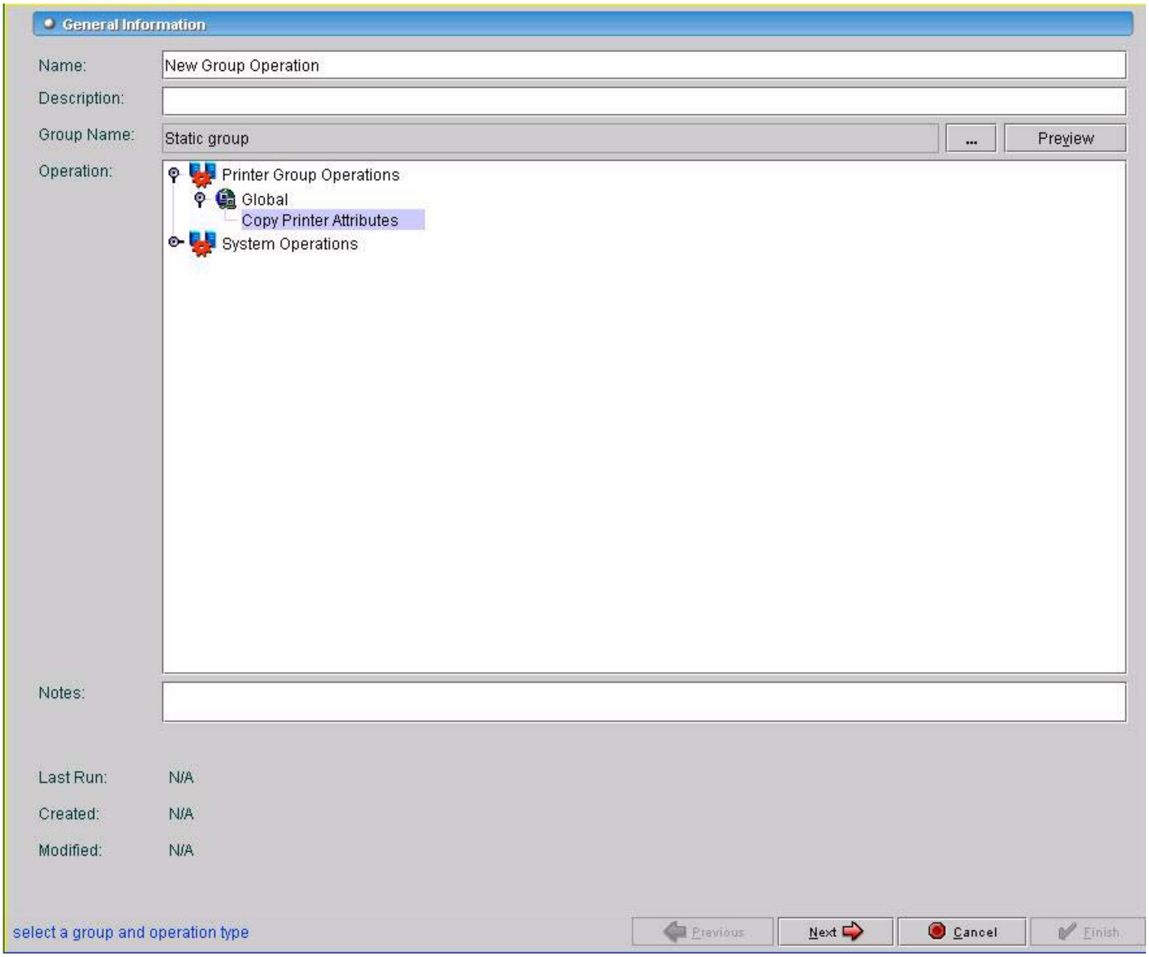
The history of events appears in the uppermost panel. Select one, and its details appear in the middle panel. You can further filter the middle panel display to conceal messages of type *Info*, *Warning* or *Error* by unchecking those below this panel. Below the check boxes is a time/date for the selected detail messages. The circular arrows to the right refresh the screen.

The lowest panel displays more information, if available, from any selected detail message.

Printer Group Operations

Group operations let you automate and schedule repetitive tasks performed on a group of printers. When you right-click a selected printer (or group of printers) and select *Group Op* from the menu, the following screen appears.

Figure 5-22. Printer Group Ops



General Information

Name: New Group Operation

Description:

Group Name: Static group

Operation:

- Printer Group Operations
  - Global
    - Copy Printer Attributes
- System Operations

Notes:

Last Run: N/A

Created: N/A

Modified: N/A

select a group and operation type

NOTE: Sometimes values sent to printers with group operations are not supported by one of them. As a result the value does not change for that printer, even if the group operation is successful.

The initial group operations screen lets you configure the following:

- **Name**—A unique identifier for this group operation.

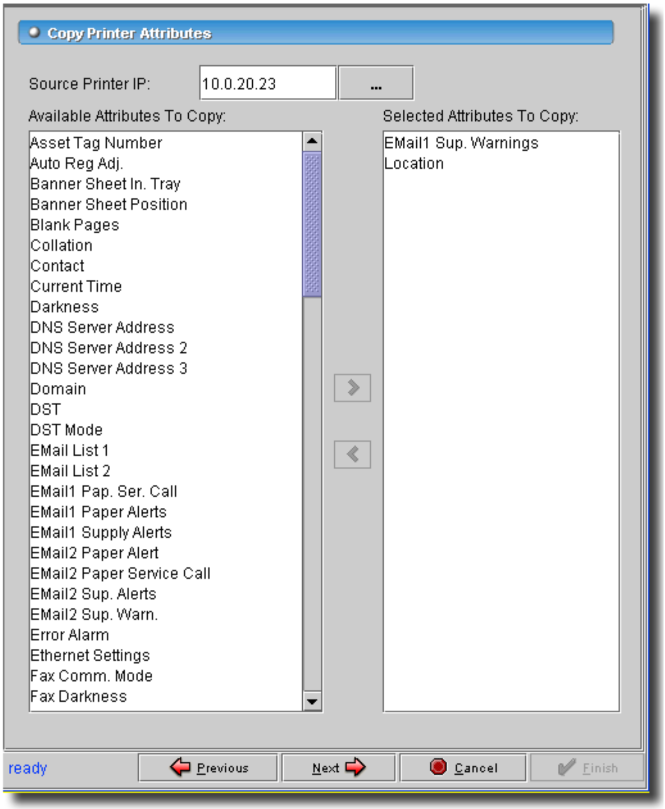
- **Description**—A text description for this group operation.
- **Group Name**—The group. When you select printers, it is a temporary group. When you start a group operation from the *Group Operations Manager*, you can select from the available groups with the command button (...).
- **Operation**—Select from the available operations that appear in the tree display. *Batch* operations address individual types of equipment, while *Global* operations. For Printers, the supported operation is *Copy Printer Attributes*. See *Printer Group Operations*, the next section, for details.
- **Last Run**—A read-only date when this operation was last run.
- **Created**—A read-only date when this operation was created.
- **Last Run**—A read-only date when this operation was last modified.

Click the *Next* button after you have selected *Copy Printer Attributes* (the only operation supported for printers) to continue configuring the group operation, or click *Cancel* to abandon this operation.

Copy Printer Attributes

This screen lets you select the printer attributes you want to change for the group of printers you selected in the previous screen. This group operation applies data from the template printer to each printer in the target group. This operation applies data opportunistically, so if a selected attribute is not writable on a target printer it skips that value and updates the target printer's other selected attributes (if there are any). A warning message appears in the group operation audit trail indicating this skip. If the selected attribute is not valid for one of the target printers then the target printer does not get updated. An error message appears in the group operation audit trail indicating this too.

Figure 5-23. Group Operation - Copy Printer Attributes



Copy Printer Attributes

Source Printer IP: 10.0.20.23

Available Attributes To Copy:

Asset Tag Number
Auto Reg Adj.
Banner Sheet In. Tray
Banner Sheet Position
Blank Pages
Collation
Contact
Current Time
Darkness
DNS Server Address
DNS Server Address 2
DNS Server Address 3
Domain
DST
DST Mode
EMail List 1
EMail List 2
EMail1 Pap. Ser. Call
EMail1 Paper Alerts
EMail1 Supply Alerts
EMail2 Paper Alert
EMail2 Paper Service Call
EMail2 Sup. Alerts
EMail2 Sup. Warn.
Error Alarm
Ethernet Settings
Fax Comm. Mode
Fax Darkness

Selected Attributes To Copy:

EMail1 Sup. Warnings
Location

ready

Use the *Source Printer IP* field to enter the IP address of the printer whose attributes are what this group operation configures on all other printers in the group. If, for example, the *Location* attribute is “Lab,” on this template printer, then the group operation here sets the location attribute of all printers to “Lab.”

You can also use the command button (...) to the right of this field to open a printer chooser screen. Make the selection there, and the IP address appears in the *Source Printer IP* field.

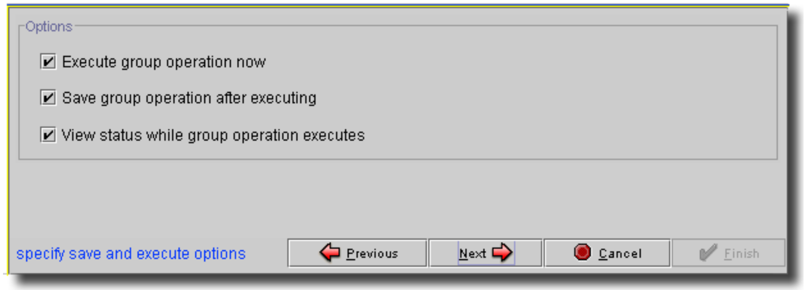
Use the arrows between **Available Attributes to Copy and Selected Attributes to Copy** to move the attributes you select between these panels. The **Selected Attributes to Copy** are those impacted by the group operation.

Click **Next** to move to the next screen, **Previous** to revisit the first screen or **Cancel** to exit this group operation configuration.

Options

The next screen lets you configure the type of execution for this group operation.

Figure 5-24. Group Operations - Execution



Options

☑ Execute group operation now

☑ Save group operation after executing

☑ View status while group operation executes

specify save and execute options

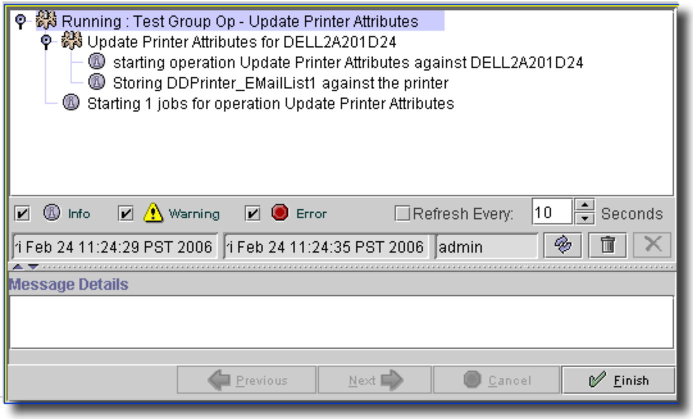
You can check the following, here:

- **Execute group operation now**—Rather than scheduling this for execution later, checking this executes the operation when you click *Next*.
- **Save group operation after executing**—This preserves the group operation after it is executed, so you can use it repeatedly.
- **View status while group operation executes**—This lets you view the status messages of the operation when you click *Next*. In any case, these messages are preserved in the application's Audit Trails. (See *Audit* for more about this.)

Audit

This screen displays the status of a group operation during its execution.

Figure 5-25. Group Operations - Audit



Running : Test Group Op - Update Printer Attributes
Update Printer Attributes for DELL2A201D24
starting operation Update Printer Attributes against DELL2A201D24
Storing DDPrinter_EMailList1 against the printer
Starting 1 jobs for operation Update Printer Attributes

☑ Info ☑ Warning ☑ Error □ Refresh Every: 10 Seconds

ri Feb 24 11:24:29 PST 2006 | ri Feb 24 11:24:35 PST 2006 | admin

Message Details

Status messages about the progress of the operation appear in the top of this screen. Some messages are in the tree structure, click the turners to see them all. When you select a message, the time and operator initiating the operation appear in the middle bar, while details about that message may appear in the *Message Details* panel at the bottom of the screen. See *Audit Trails* for more information about this screen and how the application preserves it.

Pre-Configured Dell Printer Reports

Templates for some existing reports come with your application. For these reports to contain useful data, if polling is not already running, you must right click the device and select *Initiate Printer Polling*.

Summaries

Whenever you have a daily, weekly, or quarterly summary report, these rely on "data roll-ups." For example, the daily roll up occurs at midnight. Partial days (weeks, quarters) are not included in reports where those periods are summarized.

NOTE: Because some reports need summaries that require enough data to make sense, you cannot produce these reports without first collecting the data. A weekly report, for example, may require at least an 8 day period to collect enough data.

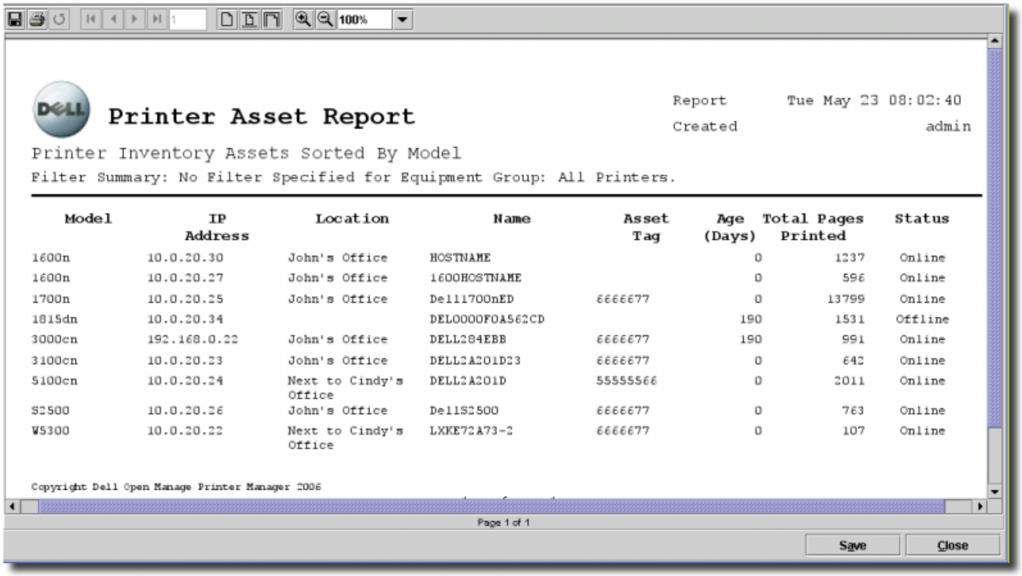
Reports include the following:

- *Printer Asset Report*
- *Printer Configuration Summary Report*
- *Printer Consumables Summary Reports*
- *Printer Page Volume Report*
- *Printer Consumables Calculated Life*
- *Printer Service Report Summary*

Printer Asset Report

This describes the *Model*, *IP Address*, *Name*, *Age*, *Print Volume* and *Status* for your existing, discovered inventory of printers.

Figure 5-26. Printer Asset Report



Printer Asset Report

Report Created Tue May 23 08:02:40 admin

Printer Inventory Assets Sorted By Model

Filter Summary: No Filter Specified for Equipment Group: All Printers.

Model	IP Address	Location	Name	Asset Tag	Age (Days)	Total Pages Printed	Status
1600n	10.0.20.30	John's Office	HOSTNAME		0	1237	Online
1600n	10.0.20.27	John's Office	1600HOSTNAME		0	596	Online
1700n	10.0.20.25	John's Office	Dell1700nED	6666677	0	13799	Online
1815dn	10.0.20.34		DEL0000F0A562CD		190	1531	Offline
3000cn	192.168.0.22	John's Office	DELL284EBB	6666677	190	991	Online
3100cn	10.0.20.23	John's Office	DELL2A201D23	6666677	0	642	Online
5100cn	10.0.20.24	Next to Cindy's Office	DELL2A201D	55555566	0	2011	Online
S2500	10.0.20.26	John's Office	DellS2500	6666677	0	763	Online
W5300	10.0.20.22	Next to Cindy's Office	LXKE72A73-2	6666677	0	107	Online

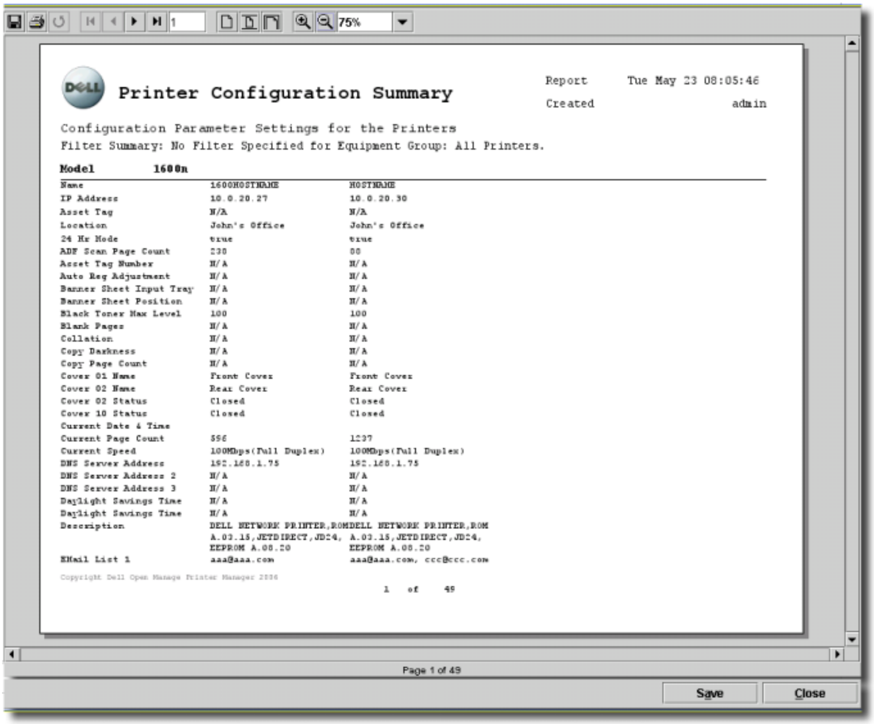
Copyright Dell Open Manage Printer Manager 2006

This comes in the following flavors: sorted by *age*, *location*, *model* and *print volume*.

Printer Configuration Summary Report

This report summarizes the configuration for your discovered printers.

Figure 5-27. Printer Configuration Summary Report



Printer Configuration Summary

Report Created Tue May 23 08:05:46 admin

Configuration Parameter Settings for the Printers

Filter Summary: No Filter Specified for Equipment Group: All Printers.

Model 1600n

Name	1600HOSTNAME	HOSTNAME
IP Address	10.0.20.27	10.0.20.30
Asset Tag	N/A	N/A
Location	John's Office	John's Office
24 Hr Mode	true	true
ADF Scan Page Count	230	80
Asset Tag Number	N/A	N/A
Auto Reg Adjustment	N/A	N/A
Banner Sheet Input Tray	N/A	N/A
Banner Sheet Position	N/A	N/A
Black Toner Max Level	100	100
Blank Pages	N/A	N/A
Collation	N/A	N/A
Copy Darkness	N/A	N/A
Copy Page Count	N/A	N/A
Cover 01 Name	Front Cover	Front Cover
Cover 02 Name	Rear Cover	Rear Cover
Cover 02 Status	Closed	Closed
Cover 10 Status	Closed	Closed
Current Date & Time		
Current Page Count	556	1237
Current Speed	100Mbps(Full Duplex)	100Mbps(Full Duplex)
DNS Server Address	192.168.1.75	192.168.1.75
DNS Server Address 2	N/A	N/A
DNS Server Address 3	N/A	N/A
Daylight Savings Time	N/A	N/A
Daylight Savings Time	N/A	N/A
Description	DELL NETWORK PRINTER,ROM A.03.15,JETDIRECT,JD24, EEPROM A.08.20	DELL NETWORK PRINTER,ROM A.03.15,JETDIRECT,JD24, EEPROM A.08.20
EMail List 1	aaa@aaa.com	aaa@aaa.com, ccc@ccc.com

Copyright Dell Open Manage Printer Manager 2006

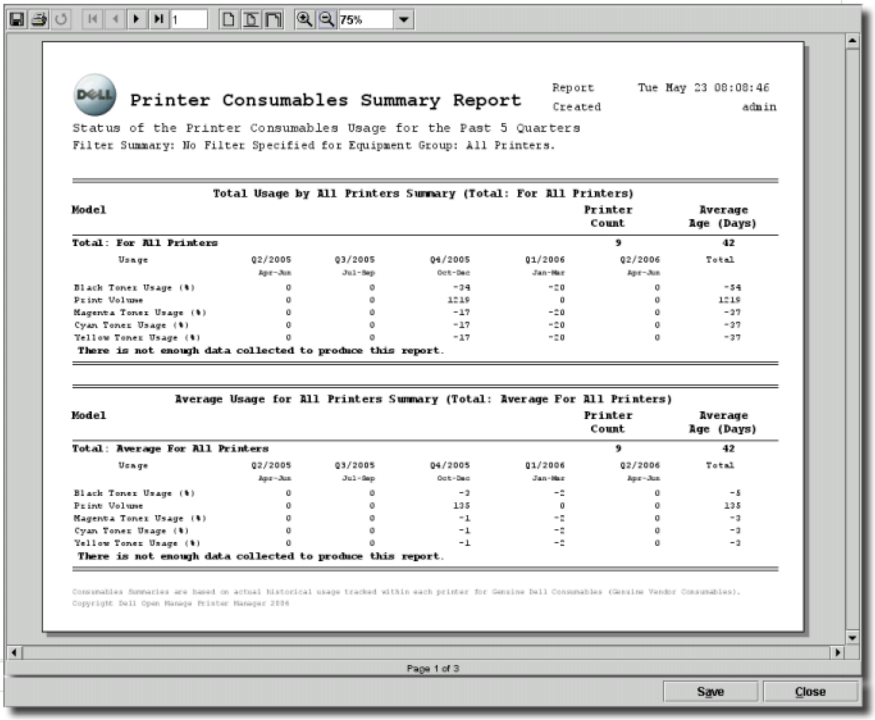
1 of 49

This lists the settings for the selected printers. These settings and values displayed depend on the capabilities of the printers.

Printer Consumables Summary Reports

These reports displays five quarters, six months and seven days of data about the selected printers.

Figure 5-28. Printer Consumables Five Quarter Summary Report



Printer Consumables Summary Report

Report Created Tue May 23 08:08:46 admin

Status of the Printer Consumables Usage for the Past 5 Quarters

Filter Summary: No Filter Specified for Equipment Group: All Printers.

Total Usage by All Printers Summary (Total: For All Printers)

Model					Printer Count	Average Age (Days)
Total: For All Printers					9	42
Usage	Q2/2005 Apr-Jun	Q3/2005 Jul-Sep	Q4/2005 Oct-Dec	Q1/2006 Jan-Mar	Q2/2006 Apr-Jun	Total
Black Toner Usage (%)	0	0	-34	-20	0	-54
Print Volume	0	0	1219	0	0	1219
Magenta Toner Usage (%)	0	0	-17	-20	0	-37
Cyan Toner Usage (%)	0	0	-17	-20	0	-37
Yellow Toner Usage (%)	0	0	-17	-20	0	-37

There is not enough data collected to produce this report.

Average Usage for All Printers Summary (Total: Average For All Printers)

Model					Printer Count	Average Age (Days)
Total: Average For All Printers					9	42
Usage	Q2/2005 Apr-Jun	Q3/2005 Jul-Sep	Q4/2005 Oct-Dec	Q1/2006 Jan-Mar	Q2/2006 Apr-Jun	Total
Black Toner Usage (%)	0	0	-3	-2	0	-5
Print Volume	0	0	135	0	0	135
Magenta Toner Usage (%)	0	0	-1	-2	0	-3
Cyan Toner Usage (%)	0	0	-1	-2	0	-3
Yellow Toner Usage (%)	0	0	-1	-2	0	-3

There is not enough data collected to produce this report.

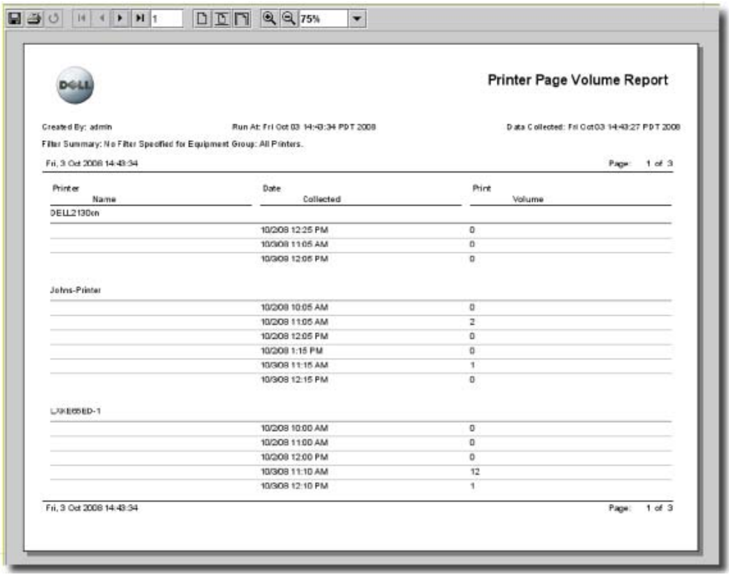
Consumables Summaries are based on actual historical usage tracked within each printer for Genuine Dell Consumables (Genuine Vendor Consumables).
Copyright Dell Open Manage Printer Manager 2006

This report must have at least a week's worth of data before it can display useful information. The Quarters' dates are based on calendar quarters. If you select a date range, the Quarter periods are based on the *End Date* if you filter on a date. The report then bases its appearance on the quarters that precede that date.

Printer Page Volume Report

This report monitors the page volume for the selected printers (and defaults to monitoring the group of all printers).

Figure 5-29. Printer Page Voulme Report



Printer Page Volume Report

Created By: admin   Run At: Fri Oct 03 14:43:34 PDT 2008   Data Collected: Fri Oct03 14:43:27 PDT 2008

Filter Summary: No Filter Specified for Equipment Group: All Printers.

Fri, 3 Oct 2008 14:43:34   Page: 1 of 3

Printer Name	Date Collected	Print Volume
DELL2130cn		
	10/2/08 12:25 PM	0
	10/3/08 11:05 AM	0
	10/3/08 12:05 PM	0
Johns-Printer		
	10/2/08 10:05 AM	0
	10/2/08 11:05 AM	2
	10/2/08 12:05 PM	0
	10/2/08 1:15 PM	0
	10/3/08 11:15 AM	1
	10/3/08 12:15 PM	0
LXKE65ED-1		
	10/2/08 10:00 AM	0
	10/2/08 11:00 AM	0
	10/2/08 12:00 PM	0
	10/3/08 11:10 AM	12
	10/3/08 12:10 PM	1

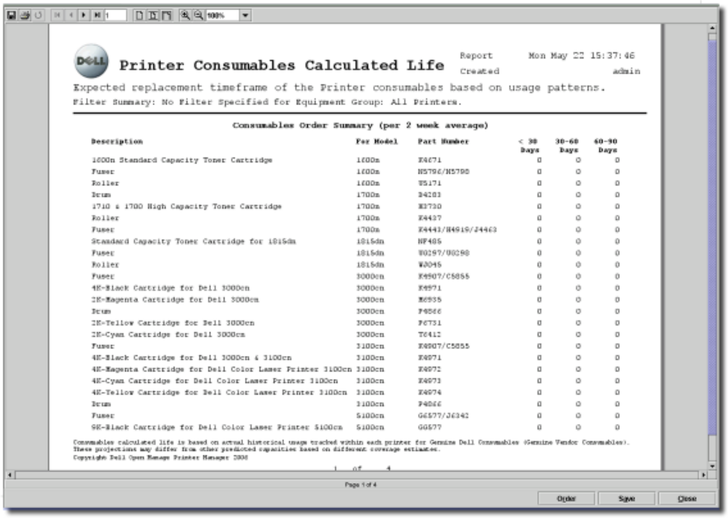
Fri, 3 Oct 2008 14:43:34   Page: 1 of 3

This catalogs the printer's name, the date, and the print volume for the date.

Printer Consumables Calculated Life

For a handy way to order consumables, select the *Consumables Calculated Life* report in the *Inventory Reports* manager, and click *Execute* to run it. (You may want to *Open* this report in *Inventory Reports* manager to select equipment, or otherwise alter its appearance). This report displays the calculated remaining life of printer consumables (toner, fuser, and so on).

Figure 5-30. Printer Consumables Calculated Life



Printer Consumables Calculated Life

Report Created Mon May 22 15:37:46 admin

Expected replacement timeframe of the Printer consumables based on usage patterns.

Filter Summary: No Filter Specified for Equipment Group: All Printers.

Consumables Order Summary (per 2 week average)

Description	For Model	Part Number	< 30 Days	30-60 Days	60-90 Days
1600n Standard Capacity Toner Cartridge	1600n	K4671	0	0	0
Fuser	1600n	H5796/H5798	0	0	0
Roller	1600n	T5171	0	0	0
Drum	1700n	D4283	0	0	0
1710 & 1700 High Capacity Toner Cartridge	1700n	K3730	0	0	0
Roller	1700n	K4437	0	0	0
Fuser	1700n	K4443/H4919/J4463	0	0	0
Standard Capacity Toner Cartridge for 1815dn	1815dn	NF485	0	0	0
Fuser	1815dn	U0297/U0298	0	0	0
Roller	1815dn	WJ045	0	0	0
Fuser	3000cn	K4907/C5855	0	0	0
4K-Black Cartridge for Dell 3000cn	3000cn	K4971	0	0	0
2K-Magenta Cartridge for Dell 3000cn	3000cn	M6935	0	0	0
Drum	3000cn	P4866	0	0	0
2K-Yellow Cartridge for Dell 3000cn	3000cn	P6731	0	0	0
2K-Cyan Cartridge for Dell 3000cn	3000cn	T6412	0	0	0
Fuser	3100cn	K4907/C5855	0	0	0
4K-Black Cartridge for Dell 3000cn & 3100cn	3100cn	K4971	0	0	0
4K-Magenta Cartridge for Dell Color Laser Printer 3100cn	3100cn	K4972	0	0	0
4K-Cyan Cartridge for Dell Color Laser Printer 3100cn	3100cn	K4973	0	0	0
4K-Yellow Cartridge for Dell Color Laser Printer 3100cn	3100cn	K4974	0	0	0
Drum	3100cn	P4866	0	0	0
Fuser	5100cn	G6577/J6342	0	0	0
9K-Black Cartridge for Dell Color Laser Printer 5100cn	5100cn	GG577	0	0	0

Consumables calculated life is based on actual historical usage tracked within each printer for Genuine Dell Consumables (Genuine Vendor Consumables). These projections may differ from other predicted capacities based on different coverage estimates.

Copyright Dell Open Manage Printer Manager 2006

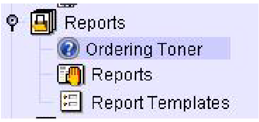
1 of 4

The report display includes printers, listing their consumables under the printer *Model*, *Name*, and so on. Individual consumables appear with the percentage used in printing the detected volume of printed pages and a calculated remaining replacement time frame.

Ordering Consumables from the Report

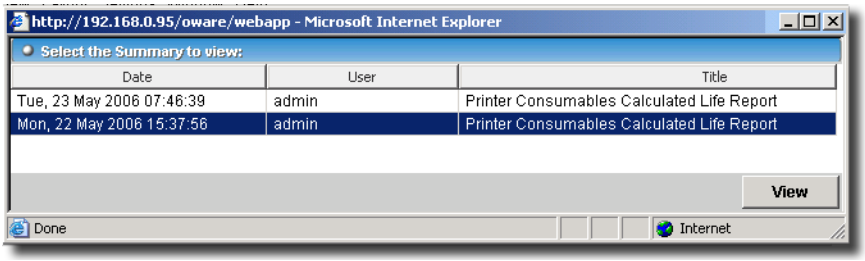
The bottom of the display for this report has an *Order* button. You can also click the link in the navigation pane to get these instructions.

Figure 5-31. Order Toner Link



Click the link on the report to open the Consumables Assistant in your default browser. This displays a link to the Consumables Assistant if you have a pop-up blocker. The first screen to appear lists the available consumables reports to view.

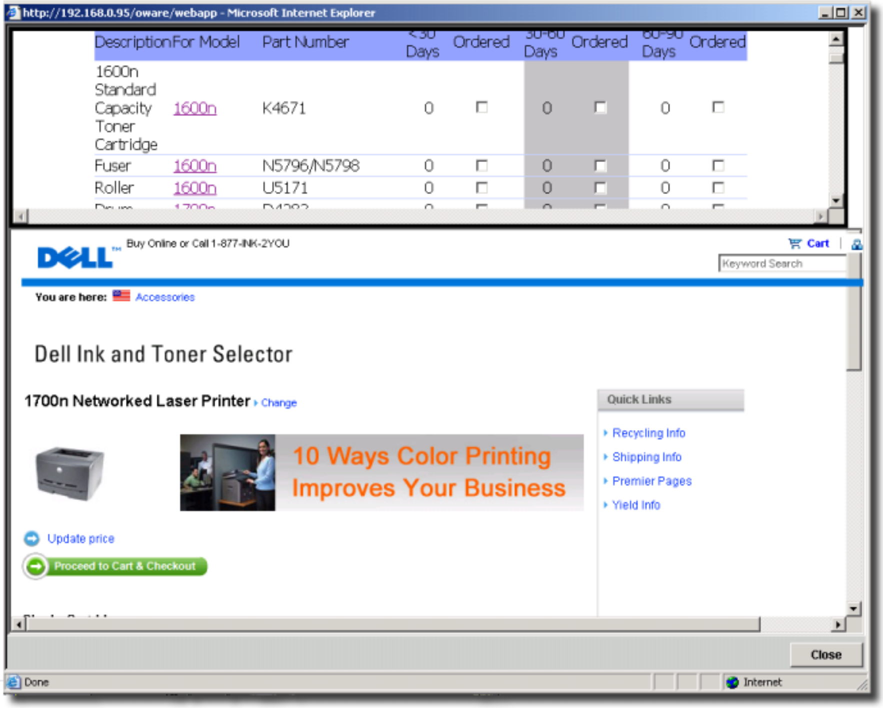
Figure 5-32. Consumables Assistant–First Screen


http://192.168.0.95/oware/webapp - Microsoft Internet Explorer
Select the Summary to view:
View
Done
Internet

Date	User	Title
Tue, 23 May 2006 07:46:39	admin	Printer Consumables Calculated Life Report
Mon, 22 May 2006 15:37:56	admin	Printer Consumables Calculated Life Report

Click *View* to get to the second screen. This screen lists all reported printers in a panel at its top.

Figure 5-33. Consumables Assistant–Second Screen


http://192.168.0.95/oware/webapp - Microsoft Internet Explorer

Description	For Model	Part Number	<30 Days	Ordered	30-60 Days	Ordered	60-90 Days	Ordered
1600n Standard Capacity Toner Cartridge	1600n	K4671	0	□	0	□	0	□
Fuser	1600n	N5796/N5798	0	□	0	□	0	□
Roller	1600n	U5171	0	□	0	□	0	□

DELL
Buy Online or Call 1-877-INK-2YOU
Cart
Keyword Search
You are here: Accessories

Dell Ink and Toner Selector

1700n Networked Laser Printer › Change

10 Ways Color Printing Improves Your Business
Quick Links
Recycling Info
Shipping Info
Premier Pages
Yield Info
Update price
Proceed to Cart & Checkout
Close
Done
Internet

When you click a printer name, the link opens the ordering page at the bottom of the screen.

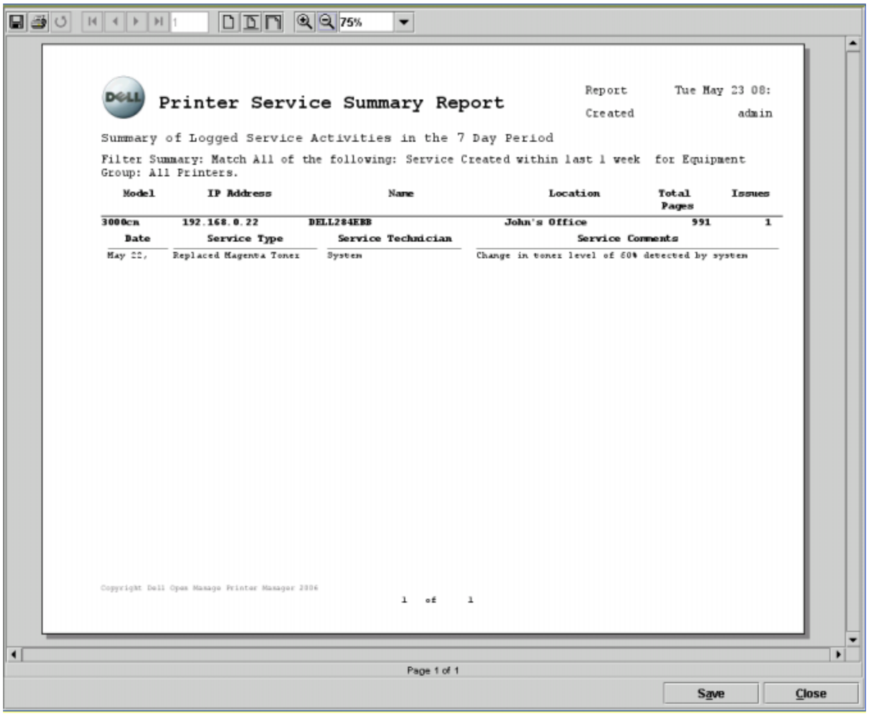
NOTE: If you are a premier customer (activated in **Settings**→ **Configuration**→ **Control Settings**→ **Customer Settings**), you may have to log in before you get to the consumables order page for the printer.

Notice that the top of this order screen displays the projected consumables needs for less than 30 days, 30-60 days, and 60-90 days. These columns also display a checkbox to remind you what printers you have ordered consumables for. The lower panel handles all ordering, shipping and payment. Follow the instructions there to order consumables.

Printer Service Report Summary

These reports display service events for the selected printer in the last seven days, month and quarter

Figure 5-34. Printer Service Report Summary



Printer Service Summary Report

Report Created Tue May 23 08:
admin

Summary of Logged Service Activities in the 7 Day Period

Filter Summary: Match All of the following: Service Created within last 1 week for Equipment Group: All Printers.

Model	IP Address	Name	Location	Total Pages	Issues
3000cn	192.168.0.22	DELL284EBB	John's Office	991	1

Date	Service Type	Service Technician	Service Comments
May 22,	Replaced Magenta Toner	System	Change in toner level of 60% detected by system

Copyright Dell Open Manage Printer Manager 2006

1 of 1

6

Thresholds

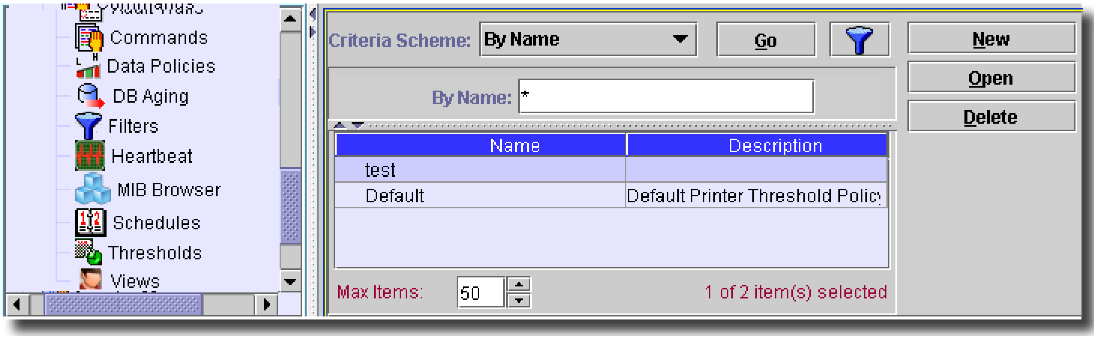
Introducing Thresholds

Threshold polling retrieves performance information about selected equipment.It is a prerequisite of some reports—for example, a trend report. The following sections describe how to manage polling policies.

Threshold Manager

This screen lets you manage the threshold policies that gather data from equipment.Open this with the Navigation Window, or **File > Open > System Services >Threshold Policies.** This manager displays listed policies according to the filter selected at the top of the screen. Click Go to refresh that screen.

Figure 6-1. Threshold Policies screen



Criteria Scheme: By Name

By Name: *

Name	Description
test	
Default	Default Printer Threshold Polic

Max Items: 50

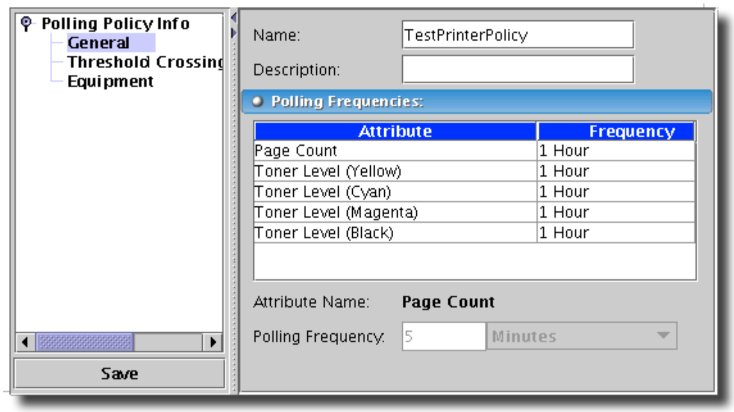
1 of 2 item(s) selected

Click New to create a new data threshold policy, or Open to edit a selected policy.Click **Delete** to remove a selected policy. When you click New or **Open**, the Threshold Policy Editor opens.

Threshold Policy Editor

This lets you edit the specifics of a new or existing threshold policy.

Figure 6-2. Threshold Policy Editor - General



Name: TestPrinterPolicy

Description:

Attribute	Frequency
Page Count	1 Hour
Toner Level (Yellow)	1 Hour
Toner Level (Cyan)	1 Hour
Toner Level (Magenta)	1 Hour
Toner Level (Black)	1 Hour

Attribute Name: **Page Count**

Polling Frequency: 5 Minutes

This screen has the following tabs:

- General
- Threshold Crossing Notifications
- Equipment

General

This screen lets you edit general information about the threshold policy. It has the following fields:

- Name — A unique identifier for the policy.
- Description —A text description of the policy.

Polling Frequencies

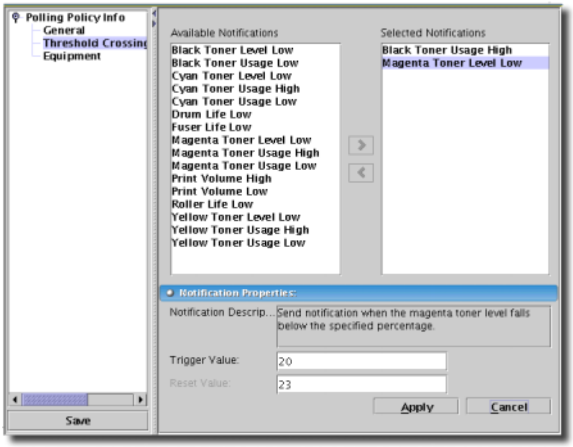
This lists the attributes whose data the application retrieves. Select an attribute by clicking it, and you can edit the frequency at the bottom of the screen.

- Attribute Name—A read-only identifier for the attribute.
- Frequency—Times per selected period when polling occurs.

Threshold Crossing Notifications

This screen lets you edit thresholds of notification for the threshold policy. Select a listed attribute in the Available Notifications panel, and click the arrow to move it to the Selected Notifications panel to activate a threshold.

Figure 6-3. Threshold Policy Editor - Threshold Crossing Notifications



Available Notifications

Black Toner Level Low
Black Toner Usage Low
Cyan Toner Level Low
Cyan Toner Usage High
Cyan Toner Usage Low
Drum Life Low
Fuser Life Low
Magenta Toner Level Low
Magenta Toner Usage High
Magenta Toner Usage Low
Print Volume High
Print Volume Low
Roller Life Low
Yellow Toner Level Low
Yellow Toner Usage High
Yellow Toner Usage Low

Selected Notifications

Black Toner Usage High
Magenta Toner Level Low

Notification Descrip... Send notification when the magenta toner level falls below the specified percentage.

Trigger Value: 20

Reset Value: 23

To edit the threshold, select the attribute in the **Selected Notifications** panel and click the **Edit** button in the Notification Properties panel. This activates the following:

Notification Description—A read-only description of the notification for this attribute.

Trigger Value—The value at which notification occurs.

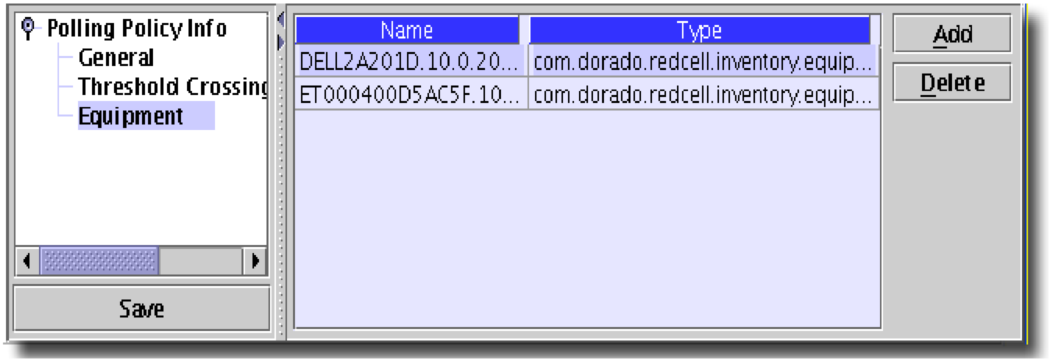
Reset Value —A value at which notification is reset.

Click **Apply** to accept your edits, or **Cancel** to abandon them.

Equipment

This screen lets you select equipment to poll.

Figure 6-4. Threshold Policy Editor - Equipment



Name	Type
DELL2A201D.10.0.20...	com.dorado.redcell.inventory.equip...
ET000400D5AC5F.10...	com.dorado.redcell.inventory.equip...

Click **Add** to select equipment, or select a listed piece of equipment and click **Delete** to remove it from the list.

Click **Save** to preserve this threshold policy in the database.

7

Groups

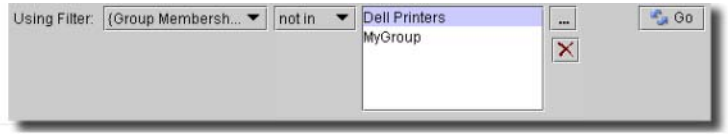
Introducing Groups

Groups manager provides functionality and screens that let you manage groups of equipment in your network. Group Operations let you select groups of equipment, then use *Group Operations Manager* to manage that equipment. See Group Operations Chapter 14, *Group Operations* for details of the next steps.

Certain dynamic groups are seeded by installing this software. For example *All Equipment* is a dynamic group containing all equipment. Similarly, discovery automatically produces vendor groups for all discovered equipment.

NOTE: You can now filter on group membership when groups are configured before the filtering operation.

Figure 7-1. Filtering on Group Membership



Using Filter: {Group Membersh... not in

Dell Printers
MyGroup

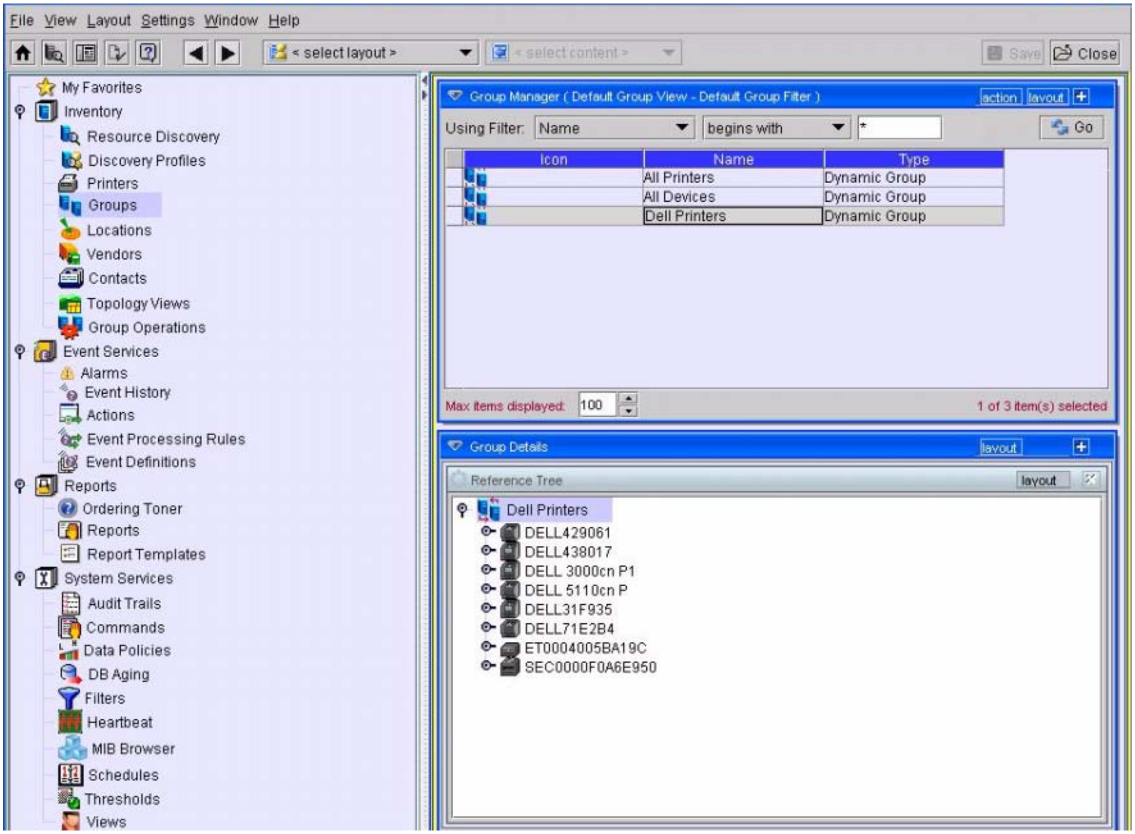
NOTE: When using such a filter, click the command button (...) to select one or more groups, and use the red "X" to delete a selected group. The operators are *in* and *not in*.

Groups Manager

This Manager lets you define equipment groups to perform operations that act on several pieces of equipment at once. Access it from the Navigation Window, or from **File→ Open→ Inventory→ Groups**.

Group Manager provides two types of groups, *static* and *dynamic*. A static group stores a static list of Equipment references. A dynamic group stores a filter definition that can dynamically query for Equipment.

Figure 7-2. Groups Manager



Using Filter: Name | begins with | *

Icon	Name	Type
	All Printers	Dynamic Group
	All Devices	Dynamic Group
	Dell Printers	Dynamic Group

Max items displayed: 100

1 of 3 item(s) selected

Dell Printers
- DELL429061
- DELL438017
- DELL 3000cn P1
- DELL 5110cn P
- DELL31F935
- DELL71E2B4
- ET0004005BA19C
- SEC0000F0A6E950

Filter the groups that appear by checking Filter, and selecting their Name (characters or wildcards) and click the Go button to populate the list of available groups.

With Action (or right-click) menu items, you can do the following:

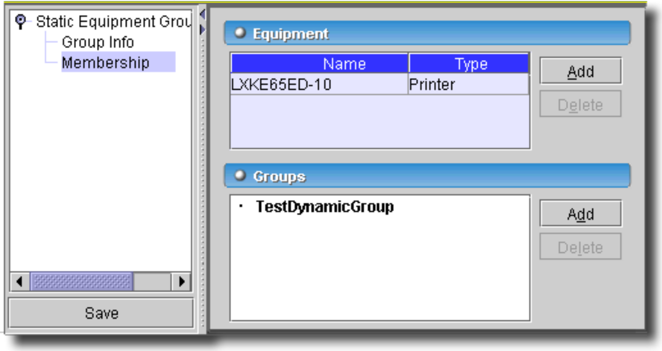
- New—Opens a screen where you can select whether you want to create groups as described in Static Groups on page 104 or Dynamic Groups on page 105. Whenever you open these editors, the Group Info tab lets you name the group. The other tab lets you select (or filter for) the resources in the group.
- Open—Opens the selected group for modification in the appropriate editor.
- Print—Prints the listed groups to an Acrobat file (you must have Acrobat reader installed). To change the list printed, use the filter at the top of this screen.
- Delete—Deletes the selected group. Select the group to remove and click Delete.The application prompts you for confirmation.
- Map—Opens the Topology Viewer, displaying the selected group’s equipment.See "Creating or Modifying Topology Views" on page 155 for more information.

- Import —Imports an XML file of groups.
- Export—Exports an XML file of the listed groups to a directory you select.Exported files can serve as backups or as seed files, and can be imported by clients running on other servers.
- Help—Opens the online help screen for this manager

When you select a group in the upper panel, the lower panel displays a tree, with the group's membership as sub-nodes. If you right-click a sub-node, an appropriate action menu appears.

Static Groups

a If you selected a static group, then you can click on the *Membership* node of the tree on the left. (See *Dynamic Groups* on page 136 for the alternative)



Name	Type
LXKE65ED-10	Printer

- TestDynamicGroup

Figure 7-3. Group Editor - Static Group Editor

This displays a table of entities with columns for Name and Type. Click the Add button to display a screen where you can select the equipment for this static group.You can also add sub-groups in the *Groups* panel below the *Equipment* panel. These appear as group nodes. You can add a dynamic group as a sub-group. Its contents are updated whenever the application runs the query that populates it.

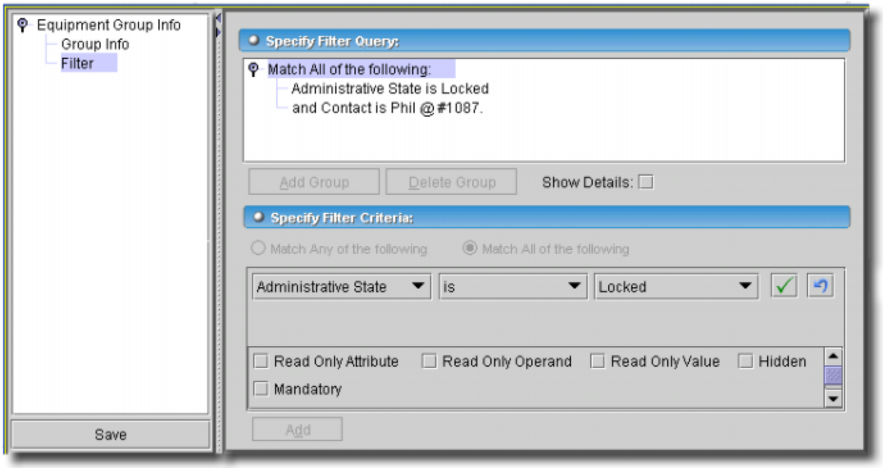
Click Save to confirm your selection. The equipment in the group appears in the groups details screen for this group, as described in Groups Manager on page 102.

NOTE: If equipment is in both the super- and sub-group, the application recognizes this and eliminates any conflict.

Dynamic Groups

If you selected a dynamic group, then you can click on the **Filter** node of the tree to see the filter criteria.

Figure 7-4. Group Editor - Dynamic Group Filter



Match All of the following:
Administrative State is Locked
and Contact is Phil @#1087.

Show Details: □

○ Match Any of the following ● Match All of the following

Administrative State | is | Locked

□ Read Only Attribute □ Read Only Operand □ Read Only Value □ Hidden
□ Mandatory

Click the radio button for Match Any of the following (“OR”), or Match All of the following (“AND”), then click the Add button at the bottom of the screen, and selectan item to match, an operator, and the match criteria. For more information (about the Show Details checkbox and the checkboxes for Read Only, Hidden and Mandatory attributes, see "Filter Editor" on page 213.

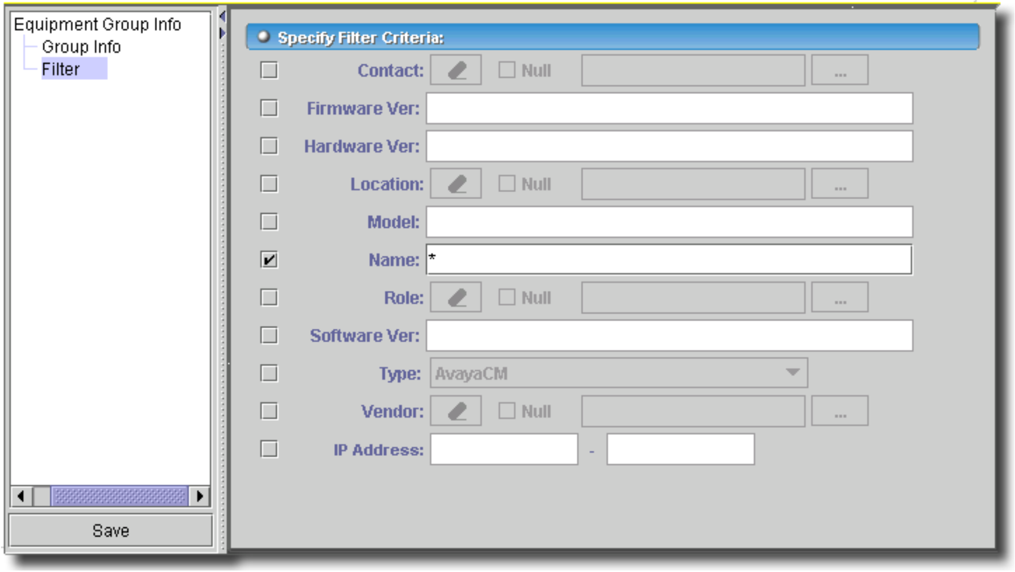
Click Save to confirm your filter selection. The filtered equipment appears in the groups details screen for this group, as described in Groups Manager.

Legacy Dynamic Groups

Some groups from previous versions of this software may have a different filter screen.

Check the criteria you want, and fill in the fields next to the checkbox with specifics, or with wildcard characters.

Figure 7-5. Group Editor – Legacy Dynamic Groups



○ Specify Filter Criteria:

☐ Contact: ☐ Null ...

☐ Firmware Ver:

☐ Hardware Ver:

☐ Location: ☐ Null ...

☐ Model:

☑ Name: *

☐ Role: ☐ Null ...

☐ Software Ver:

☐ Type: AvayaCM

☐ Vendor: ☐ Null ...

☐ IP Address: -

8

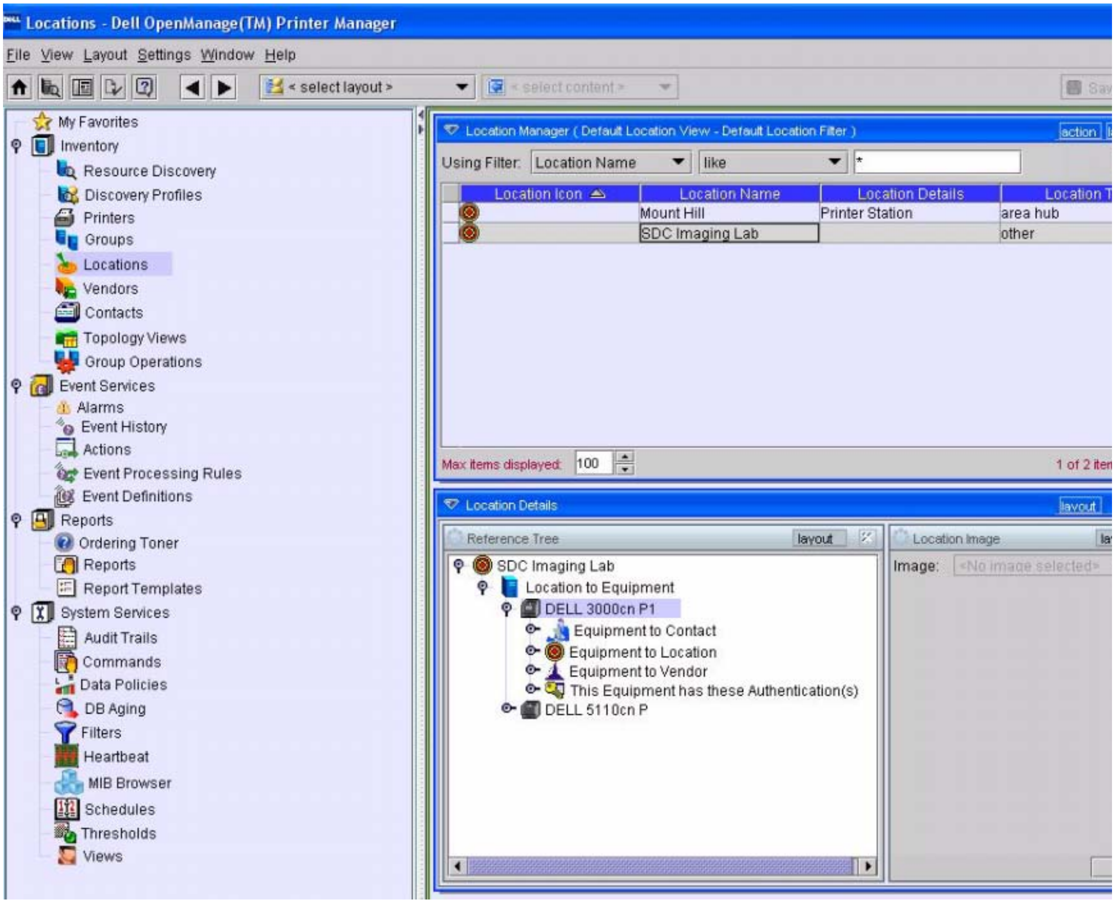
Locations

Overview

You can specify equipment locations within the Locations screen. Note that locations can have "Parent" Locations, they can be subsets of another location. For example, if network objects are on the third floor of a facility, you can designate both the building and the specific floor as locations; the building would be the parent of the floor.

To access the Locations screen, select **Inventory**→ **Locations** from the **File**→ **Open**→ menu or the Navigation Window. The Locations screen appears.

Figure 8-1. Locations Screen



Using Filter: Location Name | like | *

Location Icon	Location Name	Location Details	Location T
●	Mount Hill	Printer Station	area hub
●	SDC Imaging Lab		other

Max items displayed: 100

1 of 2 iten

Image: <No image selected>

The drop-down menu at the top of the window lets you apply a top-level location filter to restrict the display. Click *Go* when the Locations screen opens to display all defined locations.

The following are the *Action* menu and right-click menu controls on the Locations screen (not all appear, necessarily):

- **New**—Opens the Location Editor, through which you can define a new location. See *Location Editor* on page 141 for more information
- **Open**—Opens a Location Editor for the selected location. You must select a location before this option appears in the context (right-click) menu. See *Location Editor* on page 141 for more information.
- **Delete**—Deletes the selected location. Select the location to remove and click Delete. The application prompts you for confirmation.

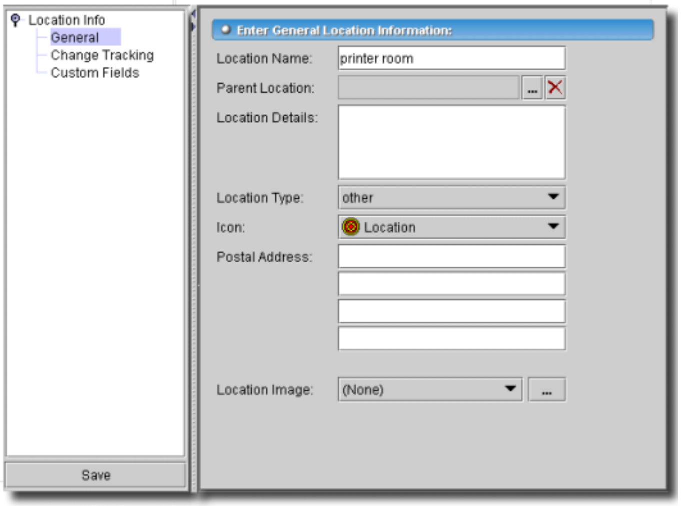
When deleting a parent location, the application prompts you before deleting its associated child locations.

- **Print**—Create an Acrobat report of the items displayed in the inventory (change the filter and click Go to change this display). You must have the free Acrobat reader installed for this to function. See **www.adobe.com** to download and install this application.
- **Map**—Opens the Topology Viewer, displaying the selected location. If you select more than one location clicking *Map* opens a new map with the world map as the default background. If you select only one location, then that location appears using the background *Location image* specified. See *Creating or Modifying Topology Views* on page 155 for more information.
- **Import / Export**—This appears in the menu accessible in the *Action* button, and imports / exports information about all locations as a text file. Exported files can serve as backups or as seed files, and can be imported by clients running on other servers.
- **Alarms**—View the alarms in the selected location.
- **Help**—Opens the help for this screen.

Location Editor

When you click **New** or **Edit** in the Locations screen the Location Editor appears. Enter or modify information about the Location; you can specify name, parent location, address, and details, among other things.

Figure 8-2. Location Editor - General



Location Name: printer room

Location Type: other

Icon: Location

Location Image: (None)

If you click *New* with an existing location selected, the application prompts you to see whether this is a sub-location of the selected item. This editor has the following tabs:

- General
- Change Tracking
- Custom Fields

The following sections describe these.

General

The following are the fields in the Location Editor:

- **Location Name**—A unique name for the Location.

  NOTE: If you alter the name of an existing location already in use by existing equipment, the editor creates a new location. To change a location name, you must delete the original location and the equipment using it then re-make it. You can change the name of an unused location without deleting anything.

- **Parent Location**—The "parent" of this location (the location to which this location is subordinate). Click the Command button (...) to open a Browser through which you can select a Parent Location. Click the Eraser icon to clear the Parent Location field.
- **Location Details**—Type of location, as selected from the drop-down menu. Available types are: Customer, Provider, and Other.
- **Location Type**—Specifies the way coordinates are designated; see Coordinate Types for more information. Valid types are: v-h coordinates, lat-long, NPA-NXX, country-city, ST-Country, CITY-ST.
- **Coordinates**—Coordinates of location, using the Coordinate Type specified above.

  NOTE: Coordinates do not relocate icons in geographic topology; dragging icons does.

- **Icon**—Select an icon from the drop-down list to associate it with the location.
- **Postal Address**—The address of location.
- **Location Image**—Select an image for the location. Once you select a file, it appears on the pick list, and is available from whatever client you chose (its location is on the application server). Typically these load from `\owareapps\redcell\backgrounds`. Any `.jpg, .gif`, or `.png` file can be an image. Once you load a file, it is available to all clients.

Click the *Save* icon to save the Location.

Coordinate Types

You can define locations using a variety of coordinate types, enabling accurate definition of locations. The following are the default coordinate types:

v-h coordinates—Vertical/horizontal coordinates, developed by Bell Systems.

lat-long—Latitude and longitude.

Example: 38.57N, 121.47W

NPA-NXX—Area code and prefix.

Example: 916-939

country-city—Country and city access codes.

Example: 049-071

Co-ordinates type and co-ordinates values are not used for displaying the location in geographic topology.

Change Tracking

This field is blank unless you have set it up in *Change Tracking* on page 51 (selecting a Vendor in *Inventory Config* on page 46. If you have done so, a log of changes to the selected inventory type and attributes appear in this screen.

Custom Fields

This panel is empty unless you have configured *Custom Fields* previously. See *Inventory Config* on page 46 for instructions about how to configure custom fields, and *Custom Fields* on page 50 for examples.

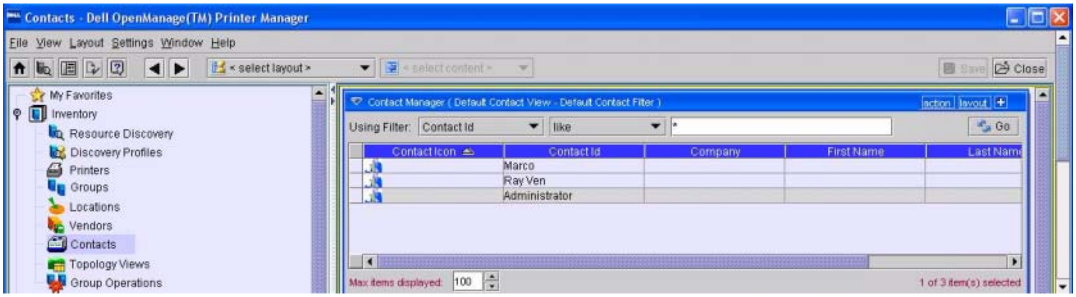
Contacts

Overview

The Contacts screen lets you organize and manage your contacts. To access the *Contacts* screen, select it from the **File→ Open→ Inventory** menu, click its icon in the Navigation pane.

Click **Go** when the Contacts screen dialog initially opens to display all defined contacts. You can filter the display by configuring a search term, operator and match term, then clicking **Go**. For more information about Filters, see "Filter Wildcards" on page 215.

Figure 9-1. Contacts screen



Contacts - Dell OpenManage(TM) Printer Manager

Contact Manager (Default Contact View - Default Contact Filter)

Using Filter: Contact Id like *

Contact Icon	Contact Id	Company	First Name	Last Name
	Marco			
	Ray Ven			
	Administrator			

Max items displayed: 100

1 of 3 item(s) selected

When you select a contact, the Details panels at the bottom of this screen display specifics about the contact. See Creating or Modifying a Contact: General Tab for details of what can appear here. You can edit information in individual panels by clicking Edit. Click Apply after editing to save this information to the database.

To work with listed contacts or create new ones in this inventory, right click a listed item. The following context menu items appear:

- **New**—Creates a new contact. See *Creating or Modifying a Contact* on page 146 for more information.
- **Open**—Opens the selected contact for modification. See *Creating or Modifying a Contact* on page 146 for more information.
- **Delete**—Deletes the selected contact. The application prompts you for confirmation before removing the contact from the system.

- **Print**—Create an Acrobat report of the items displayed in the inventory (change the filter and click Go to change this display). You must have the free Acrobat reader installed for this to function. See **www.adobe.com** to download and install this application.
- **Map**—Displays the contact in the Topology Viewer. See *Creating or Modifying topology Views* for more information.
- **Import / Export**—This appears in the *Action* button menu, and imports / exports information about all contacts as a text file. Exported files can serve as backups or as seed files, and can be imported by clients running on other servers.

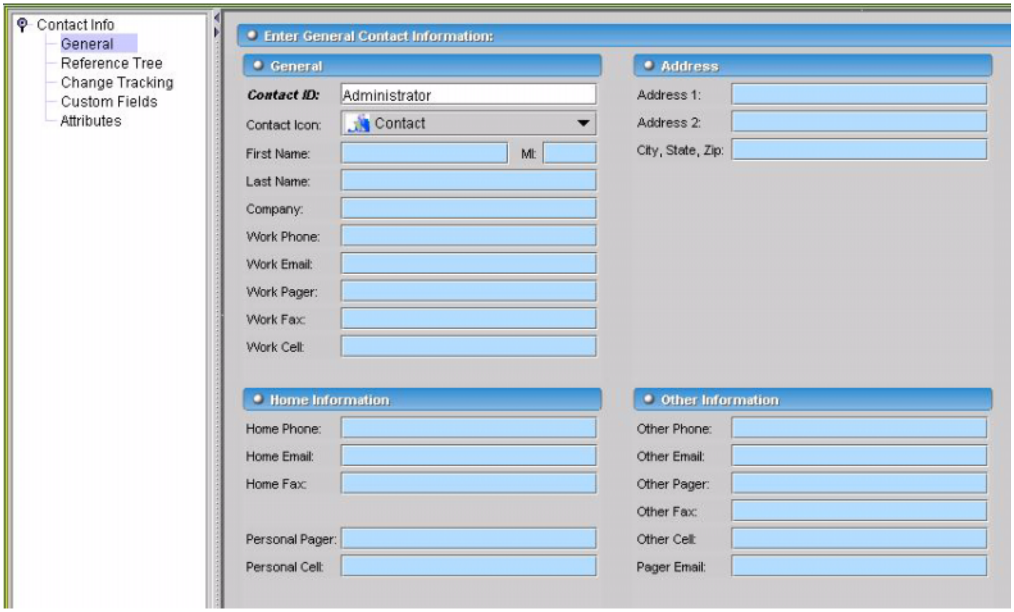
NOTE: This report limits the number of columns to those that can fit on a single page width.

- **Help**—Opens the help for this screen.

Creating or Modifying a Contact

When you create or modify a contact the Contact Editor appears

Figure 9-2. Contact Editor



Contact ID: Administrator

Contact Icon: Contact

Close or save this screen with the icons on the toolbar, or items in the *File* menu.

General

The following are the fields in this screen:

Contact ID—A unique identifier for this contact.

Contact Icon— The icon associated with this contact.Select an icon from the drop-down list..

- **First Name**—First Name
- **Middle Initial**—Middle Initial
- **Last Name**—Last Name
- **Company**—Company
- **Address**—Three lines for the address of this contact.
- Work Phone—
- Work Email—
- Work Pager—
- Work Fax—
- Work Cell—
- Address
- Address1 / 2 —Enter up to two lines of address information.
- City, State, Zip—Enter the city, state and postal code for the contact.
- Home Information
- Home Phone—
- Home Email—
- Home Fax—
- Personal Pager—
- Personal Cell—
- Other Information
- Other Phone—
- Other Email—
- Other Pager—
- Other Fax—
- Other Cell—
- Pager Email—

Click the **Save** icon (or **File→ Save**) to save and close the contact, or click the **Close** icon to close it without saving changes.

Reference Tree

This panel displays icons reflecting relationships with a selected contact.

Change Tracking

This field is blank unless you have set it up in Change Tracking (selecting a Vendor in Inventory Config. If you have done so, a log of changes to the selected inventory type and attributes appear in this screen.

Custom Fields

This panel is empty unless you have configured *Custom Fields* previously. See *Inventory Config* for instructions about how to configure custom fields.

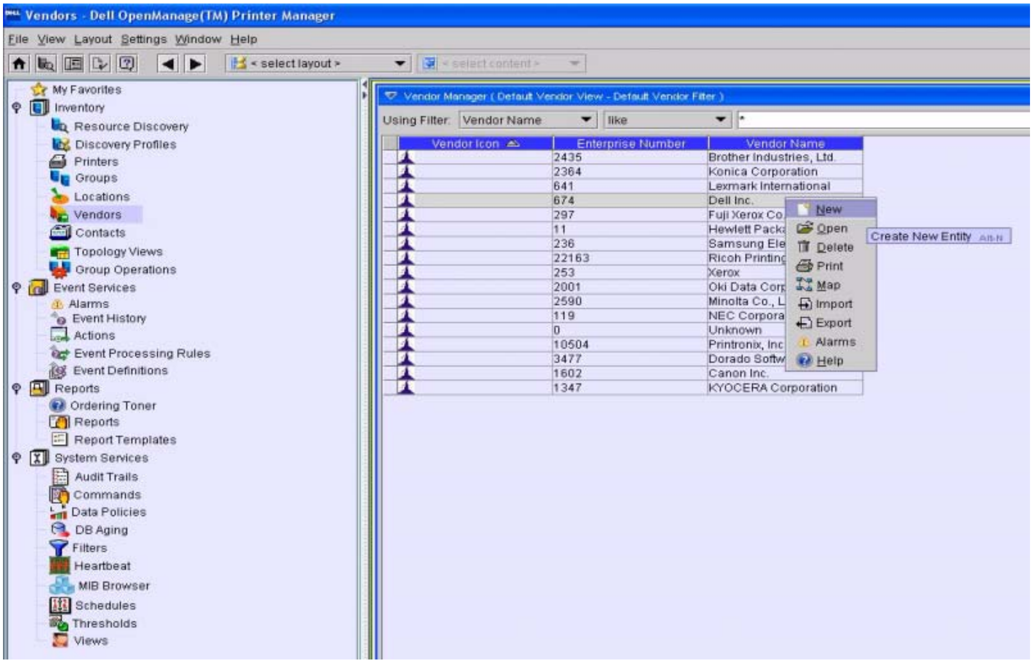
10

Vendors

Overview

You can create and modify contact information for vendors who supply equipment through the Vendors screen. To access the *Vendors* screen, select this from the **File→ Open→ Inventory** menu or the Navigation Window.

Figure 10-1. Vendors screen



Using Filter: Vendor Name like *

Vendor Icon	Enterprise Number	Vendor Name
	2435	Brother Industries, Ltd.
	2364	Konica Corporation
	641	Lexmark International
	674	Dell Inc.
	297	Fuji Xerox Co.
	11	Hewlett Packa
	236	Samsung Ele
	22163	Ricoh Printing
	253	Xerox
	2001	Oki Data Corp
	2590	Minolta Co., L
	119	NEC Corpora
	0	Unknown
	10504	Printronix, Inc
	3477	Dorado Softw
	1602	Canon Inc.
	1347	KYOCERA Corporation

The Vendors screen provides predefined filters to let you restrict the display, and also incorporates a search feature. Check the **Match All** box and configure the search term, operator and match term differently to restrict the list of filters displayed. Click column titles to sort on that column (repeated clicking toggles ascending/descending sort).

Right click a listed item to view the context menu providing controls for the Vendors screen. It has the following menu items:

- **New**—Creates a new vendor. See Creating Vendors for more information.
- **Open**—Edit an existing Vendor. See Creating Vendors for more information.
- **Delete**—Deletes the selected vendor. The application prompts you for confirmation before removing the vendor from the system.

  NOTE: When you delete a vendor through the Vendors screen it does not delete the relevant contacts. You must delete them through the Contacts screen.

- **Print**—Create an Acrobat report of the items displayed in the inventory (change the filter and click Go to change this display). You must have the free Acrobat reader installed for this to function. See **www.adobe.com** to download and install this application.
- **Map**—Displays the instances of managed objects from this vendor in a Topology Viewer. See Creating or Modifying Topology Views for more information.
- **Import / Export**—This appears in the *Action* button menu and imports / exports information about all vendors as a text file. Exported files can serve as backups or as seed files, and can be imported by clients running on other servers.
- **Help**—Open the help for this screen.

Creating Vendors

Creating or modifying a vendor displays the Vendor Editor, which contains the following panels:

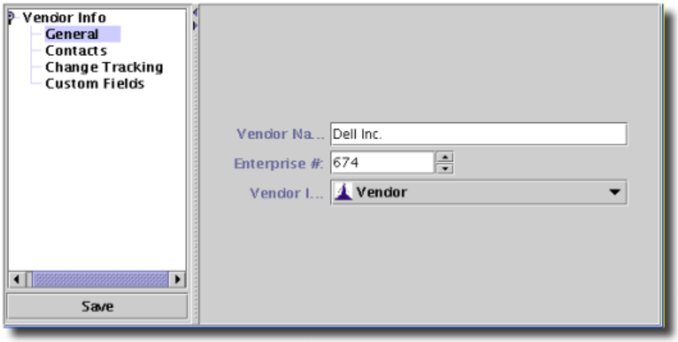
- General Panel
- Contacts Panel

Make changes as needed, then click *Save* to save the data or *Cancel* to close the editor without saving any changes.

General Panel

- This panel displays general information about the vendor.

Figure 10-2. Vendors screen—Information Panel



Vendor Na... Dell Inc.

Enterprise #: 674

Vendor I... Vendor

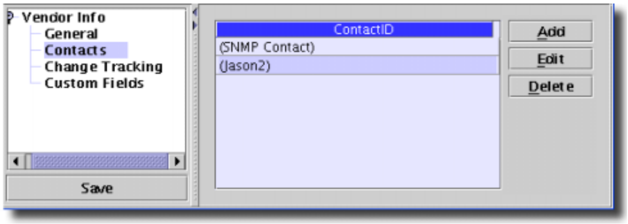
The following are the fields on this panel:

- **Vendor Name**—The name of the vendor. This entry must be unique.
- **Enterprise #**—The unique number assigned this vendor. Best practice is *not* to change this.
- **Vendor Icon**—The icon associated with the vendor, selected from the drop-down list.

Contacts Panel

This panel displays contacts associated with a vendor. See Contacts for more information on contacts.

Figure 10-3. Vendors screen—Contacts Panel



ContactID
(SNMP Contact)
(Jason2)

Click any of the following buttons:

- **Add**—Opens the Contacts screen. Select the contact to add and click *OK* to add it to the list.
- **Edit**—Opens the selected contact in the Contact Editor.
- **Delete**—Removes the selected contact from the list.

Change Tracking

This field is blank unless you have set it up in Change Tracking (selecting a Vendor in Inventory Config. If you have done so, a log of changes to the selected inventory type and attributes appear in this screen.

Custom Fields

This panel is empty unless you have configured *Custom Fields* previously. See *Inventory Config* for instructions about how to configure custom fields.

11

Topology

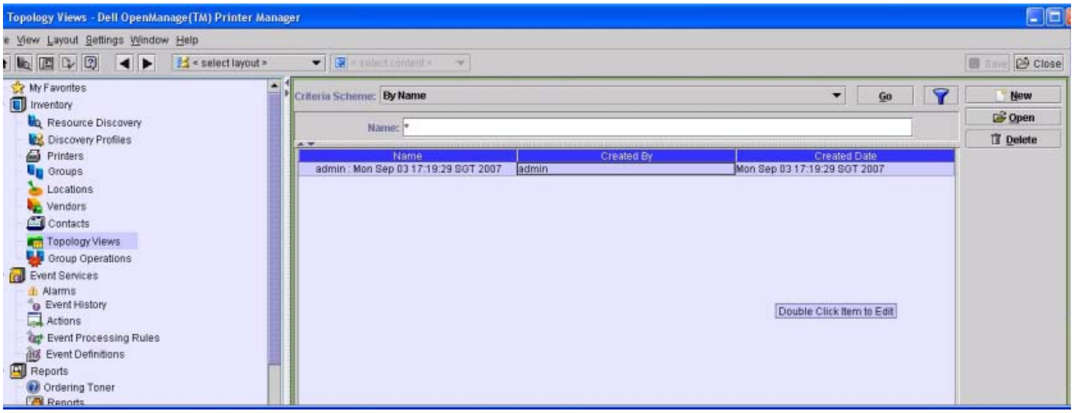
Overview

Topologies can model equipment locations, both logically and geographically, and can display their hierarchical relationships. The Topology viewers let you view and monitor network devices, and respond to network alarms.

Topology Views

You can access topology views through the *Map* button in various screens, or by opening or creating a topology view from the Topology Views screen (available in the navigation window, or from **File→ Open→ Inventory→ Topology Views**).

Figure 11-1. Topology Views



Topology Views - Dell OpenManage(TM) Printer Manager

Criteria Scheme: By Name

Name: *

Name	Created By	Created Date
admin : Mon Sep 03 17:19:29 SGT 2007	admin	Mon Sep 03 17:19:29 SGT 2007

Double Click Item to Edit

Once you have arranged the view as you would like it, click the **Save** button (or press Ctrl+S), and the View Manager preserves that view, named for the creating user and date.

You can filter multiple views as described in *Filter Wildcards*. If you want to create a view, click the *New* button. Select a view and click **Open** to see or edit a view, or click **Delete** to remove it from those listed.

NOTE: Unless you create a filter and save it as described in Chapter 18, Filters, any filters you create here are not preserved.

Use the *Action* button to open the menus, or right-click the list of views. The following are the available items in this menu:

New—Create a new, blank topology view.

Open—Open an existing topology view to edit.

Delete—Delete an existing, selected topology view.

Copy—Copy an existing topology view as the basis for a new view.

Print—Print a list of views. To alter the list, use the filter at the top of this screen.

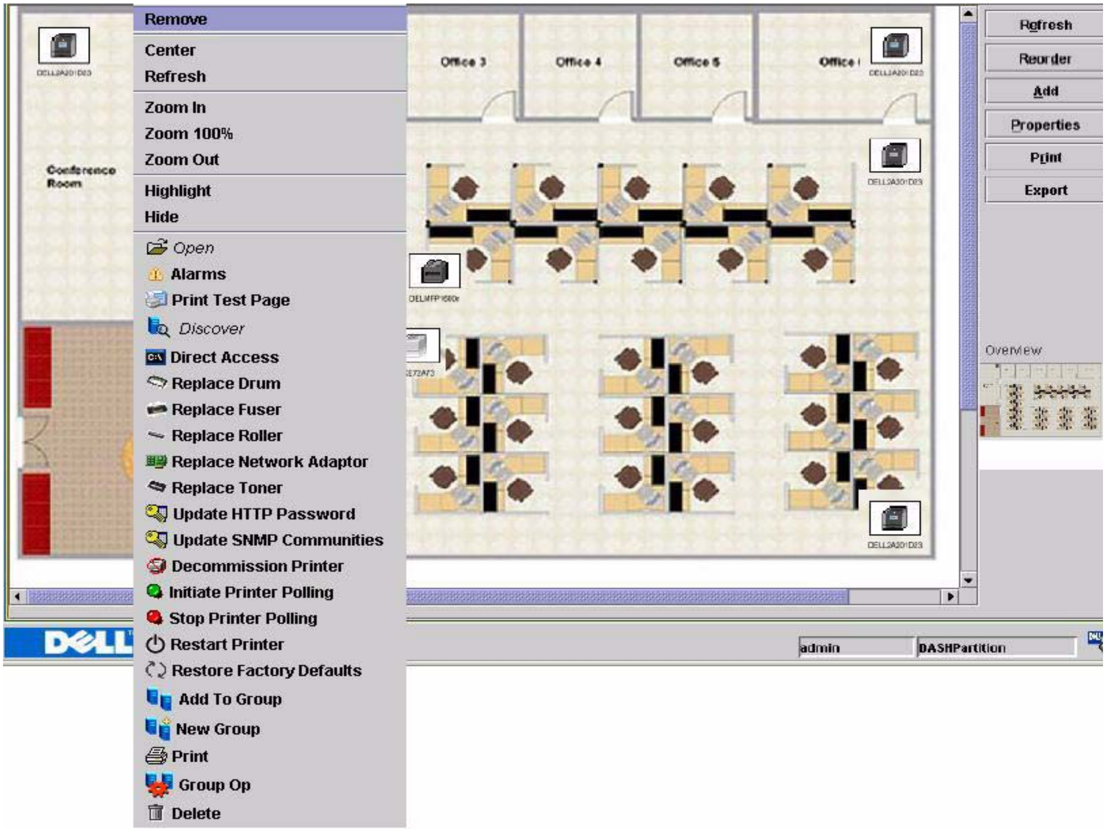
The printout appears as an Acrobat file, from which you can send the list to a printer, or save it as a file. You must have the free Acrobat reader installed for this to work correctly.

Help—Create a new topology view.

Creating or Modifying Topology Views

When you *Open* or create a *New* view, the screen that appears displays the equipment with the arrangement and background you select.

Figure 11-2. Viewing Topology



The view that appears on the left is typically a detail of a larger layout. To move your point of view through the larger layout, click and drag the *Overview* rectangle in the middle of the right panel.

NOTE: In addition to panning the view, you can click and drag the mini-icons in the *Overview* rectangle. The larger icons in the topology view move to reflect their movements in *Overview*.

This panel includes the following buttons:

- **Add a Content** — This opens a pair of component chooser screens. First, you must select the type of component you want to add. For example: *Authentication*, *Contact*, *Equipment Subcomponents*, *Link*, *Location*, *Printer*, *Vendor*. Notice that if you add a *Contact* connected with a subcomponent, a dotted line connects them when they appear together in the view.

See "Creating or Modifying a Contact" on page 146, "Location Editor" on page 141, or "Creating Vendors" on page 150 for more about the screen that appears once you select the type of object you want to add to the view.

NOTE: Until you select a link from the subsequent screen, no links appear in a view, even if you select linked equipment. If you Add a link, the equipment endpoints of the link will appear, even if you do not initially see them in your view.

- **New Link** — Select (at least) two components within the view, then click this item. You are prompted for the type of link you will create. For example: *ATMLink*, *BGPPeerLink*, *EthernetLink*, *FibreChannelLink*, *IPNextHopLink*, *ISIS1PeerLink*, *ISIS2PeerLink*, *ISISPeerLink*, *LogicalLink*, *OSPFNeighborLink*, *PhysicalLink*, *RIPPeerLink*, *SONETLink*. When you discover links between devices and entire network, an out-of-domain indicator appears if the end point of a link is not yet discovered. If you discover that missing end point, the topology does not change unless you perform link discovery again.
- **Open View** — Returns you to the manager described in "Topology Views" on page 153.
- **Refresh**—Update the display.
- **Reorder**—Update the display, calculating the new order based on any changes you have made to the configuration in *Properties*.
- **Properties**—Alter the properties of this view. See "Topology View Properties" on page 158.
- **Save**—Save the view. By default its name concatenates the creating login ID, date, and time. You can change this in the screen described in "Topology View Properties" on page 158.
- **Print**—Print the display. See "Printing Topology Views" on page 160 for details.
- **Hide Overview & Legend**—This conceals the right-hand portion of the screen
- **Help**—Opens online help for this topic.

You can also configure the display with Context Menus.

Context Menus

If you right-click an icon, the context menu appears. Exact content depends on the selection, but can include the following items:

- **Remove**—Deletes the selected icon from the view. If you click *Remove* on a primary object (one not present because of filtering), it deletes the object from the Topology view. If you remove a secondary object (one present because of filtering), it's hidden.
- **Center**—Move the selected icon to the center of the view. This does not center icons on the edge of the view, but makes its best effort to move the selected icon toward the center. Best practice is to zoom first, then center.
- **Refresh**—Update the display.
- **Zoom In / Out / 100%**—These manipulate the magnification of the selected view. Saving does not preserve magnification, but it will preserve the placement of icons onscreen.
- **Highlight / Unhighlight**—Paints the selected icon a different color, or toggles the highlight off.

- **Hide**—Conceal the selected object in this view.
- **Alarms** — View the alarms of the selected item.
- **Open**—Opens the appropriate editor for the selected object; for example, the equipment editor.
- **Print Test Page**—Appears if the selected object is a printer.
- **Discover**—Open the Resource Discovery Wizard.
- **Resync**—Query the selected device to update its attributes.
- **Direct Access**—Opens a browser session with the selected object.
- **Replace Drum / Fuser / Roller / Network Adaptor**—Opens the service log for the selected printer to log these replacements.
- **Update HTTP Password / SNMP Communities** —Lets you update the authentication for the selected printer.
- **Decommission Printer**—Stops polling and thresholding on the selected printer.
- **Initiate / Stop Printer Polling**—Starts or stops polling for reports and consumables estimates.
- **Restart Printer**—Restarts the selected printer
- **Restore Factory Default** — If the selected item is a printer, you can restore the printer to factory default.
- **Add to Group**—Lets you add the selected object to a group.
- **New Group**—Lets you make a new group. See Chapter 14, *Group Operations* for more about groups.
- **Group Op**— Initiate a group operation on the selected equipment. This opens the Group Operations screen.
- **Delete**—Lets you delete the selected object, after confirming that is what you want to do.

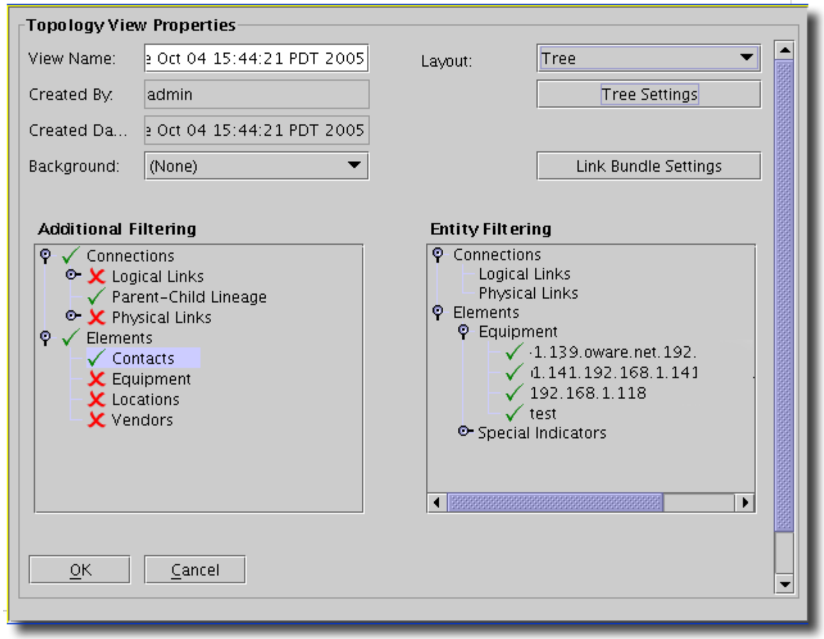
  In addition to the zoom menu items mentioned previously, the following items appear if you click a non-icon area on the view:

- **Refresh**—Update the display.
- **Reorder**—Update the display, calculating the new order based on any changes you have made to the configuration in *Properties*.
- **Add**—The same as the A*dd* button described previously.
- **Properties**—The same as the *Properties* button described previously.
- **Print**—Print the display. See Printing Topology Views for details.

Topology View Properties

This dialog lets you alter properties in your topology views.

Figure 11-3. Topology View Properties



Topology View Properties

View Name: ᵉ Oct 04 15:44:21 PDT 2005

Created By: admin

Created Da... ᵉ Oct 04 15:44:21 PDT 2005

Background: (None)

Layout: Tree

Additional Filtering

- ✓ Connections
  - ✗ Logical Links
  - ✓ Parent-Child Lineage
  - ✗ Physical Links
- ✓ Elements
  - ✓ Contacts
  - ✗ Equipment
  - ✗ Locations
  - ✗ Vendors

Entity Filtering

- Connections
  - Logical Links
  - Physical Links
- Elements
  - Equipment
    - ✓ 1.139.oware.net.192.
    - ✓ 1.141.192.168.1.141
    - ✓ 192.168.1.118
    - ✓ test
  - Special Indicators

You can access it with the **Properties** button in the topology view, or by right clicking an object in a view and selecting properties.

In this screen you can view or configure the following:

- **View Name**—A text field where you can enter, or alter an identifier for this view. If you change the name, you can select **File→ Save**, and the view name is altered in the **Topology Views** screen. You can also **File→ Save As...** a copy of the view once you have changed the name (but only after you change the name).
- **Created By**—A read-only reminder of the username who created the view.
- **Created Date**—The view's creation date (read-only).
- **Background**—Use this pick list to select a background for the view. The backgrounds must be `.png, .gif` or `jpg` files. Load a background by selecting the image file after you click the command button (...) to the right of the pick list. Once you load the background image this way, it appears in the pick list. Using these backgrounds, you can display your equipment topology on a map.

The default resolution for backgrounds is 1600 X 1200 pixels. You can change the height and width globally by overriding two properties:

```
com.dorado.redcell.topology.view.width=[pixels]
```

and

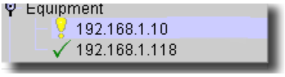
```
com.dorado.redcell.topology.view.height=[pixels]
```

The application maintains the original image's aspect ratio between width and height to avoid stretching images, widening or lengthening the image until it reaches the smallest dimension, regardless of what you enter in the properties.

> **NOTE:** Best practice is to override property files in `owareapps\installprops\lib.` Create a text file there with the `.properties` extension, and enter the above properties. The advantage of overriding properties like this is that installations of updates or patches do not overwrite your property tunings. In any case, you must restart application server before the application recognizes the changes.

- **Additional Filtering**—This tree displays possibilities for global topology filtering. Click the turners to expand the tree. Elements next to a green check appear in the display; elements with a red "X" do not. Click the element to toggle between check and X.
- **Entity Filtering**—This panel lets you configure the appearance of topology connections or equipment by specific entity (rather than global type). It also lets you configure the appearance of special indicators. Click the turners to expand the tree. Elements next to a green check appear in the display; elements with a red "X" do not. Click the element to toggle between check, X or the yellow exclamation point. This third category highlights the selected icon, surrounding it with a colored rectangle.

Figure 11-4. Topology Highlight Filtering

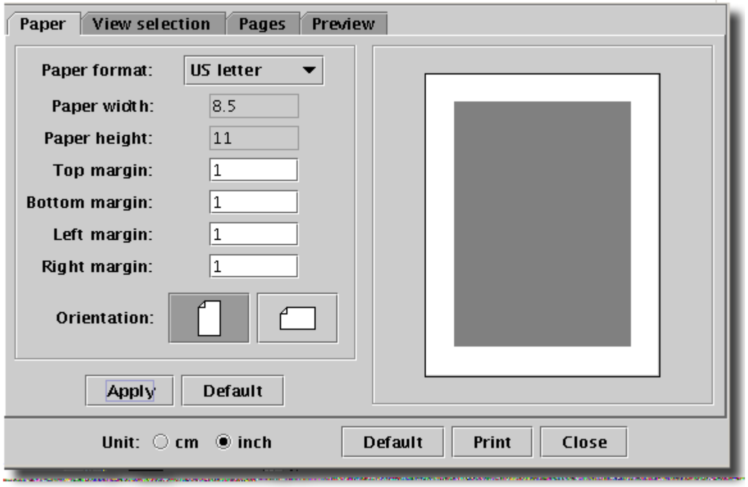


- **Layout**—The pick list to the right of this label lets you select from several layout possibilities. You can further configure these layouts by selecting one, then clicking the *<Layout Type> Settings* button. When you select *Settings*, you can *Apply* your settings, or *Reorder* (recalculated the layout using available data) the display with the buttons at the bottom of this screen. *Close* abandons your edits.

Printing Topology Views

- If you print a topology, a configuration dialog appears with four tabs.

Figure 11-5. Print Dialog–Paper Tab



Paper format: US letter
Paper width: 8.5
Paper height: 11
Top margin: 1
Bottom margin: 1
Left margin: 1
Right margin: 1
Orientation:
Unit: ○ cm ● inch

Paper

The *Paper* tab has the following fields:

- **Paper Format**—Select from the pick list (*A3*, *A4*, *A5*, *US Executive*, *US Letter*, *US Legal*, and *Custom*). The current default is *A4* (and measurements default to *cm*).
- **Paper width / height**—A pair of read-only fields, unless you select *Custom* in the pick list above them.

NOTE: Set the units for this display at the bottom of the Print dialog.

Bottom / Top / Left / Right Margin—Set the margins in these fields.

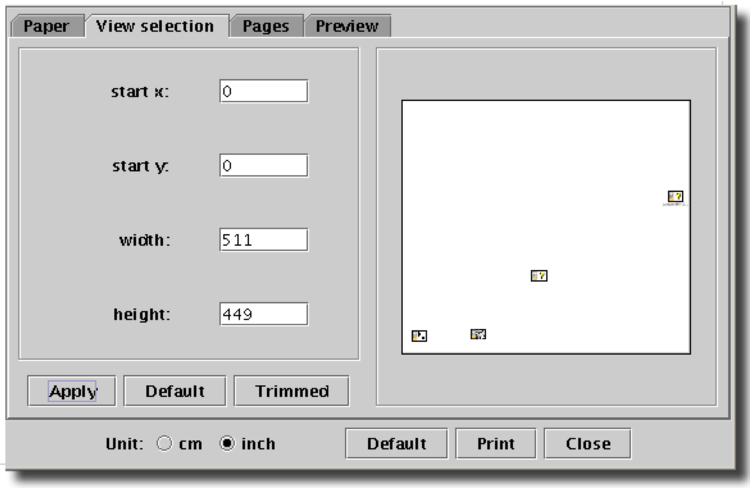
Orientation—Click on the icons to select

Click *Apply* to execute any edits on this print job, click *Default* on this tab to return to the tab's defaults. Click *Default* at the bottom of the screen to reset all tabs' defaults. Click *Print* to print the screen, or *Close* to abandon the print job and close this screen.

View selection

This screen previews the print job on the right, and lets you select what portion of the screen you want to print.

Figure 11-6. Topology Print–View Selection



start x: 0

start y: 0

width: 511

height: 449

Unit: ○ cm ● inch

You can configure the printed screen with the following fields:

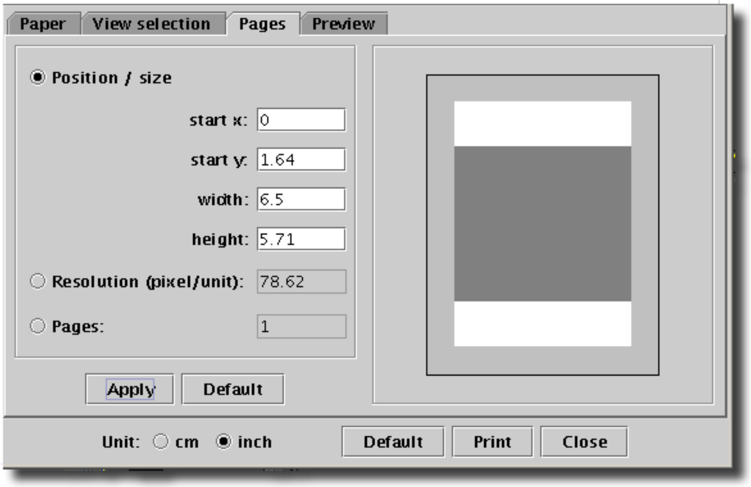
- **start x / y** —Number of pixels to move the printed area (horizontal / vertical). Minus numbers move to the left/down, positive numbers move to the right/up.
- **start y**—The vertical pixel to start printing (from zero at the bottom).
- **width / height**—Measured in pixels.

Click **Apply** to execute any edits on this print job, click **Default** on this tab to return to the tab's defaults. Click **Trimmed** to crop the printed area so it does not display white space in the preview the right. Click **Default** at the bottom of the screen to reset all tabs' defaults. Click **Print** to print the screen, or **Close** to abandon the print job and close this screen.

Pages

You can select the way your view appears on paper (preview on the right) three different ways.

Figure 11-7. Topology Print–Pages



● Position / size

start x: 0

start y: 1.64

width: 6.5

height: 5.71

○ Resolution (pixel/unit): 78.62

○ Pages: 1

Unit: ○ cm ● inch

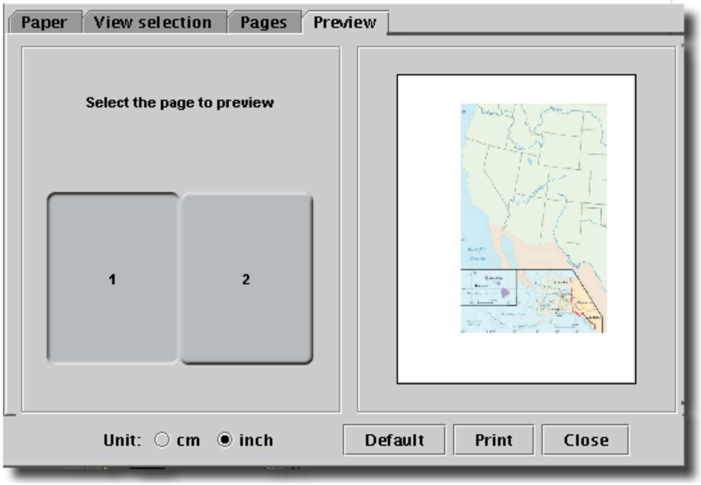
Select the way with the radio buttons.

- **Position / Size**—Enter the *start x/y*, *width / height* in the appropriate fields and the preview rearranges the appearance (resolution, pages) to match.
- **Resolution (pixel/unit)**—Select a resolution, and the preview will display how Position/size and pages change.
- **Pages**—Select the number of pages to cover with your print job. The other elements of this display change too.

Preview

If you want to preview multiple pages, you can see them by clicking on the page icons to the left of the preview panel.

Figure 11-8. Topology Print–Preview



Unit: ○ cm ● inch

Click *Default* to return all tabs to their defaults, *Print* to execute the print job you have configured, or *Close* to abandon the print job and close this window.

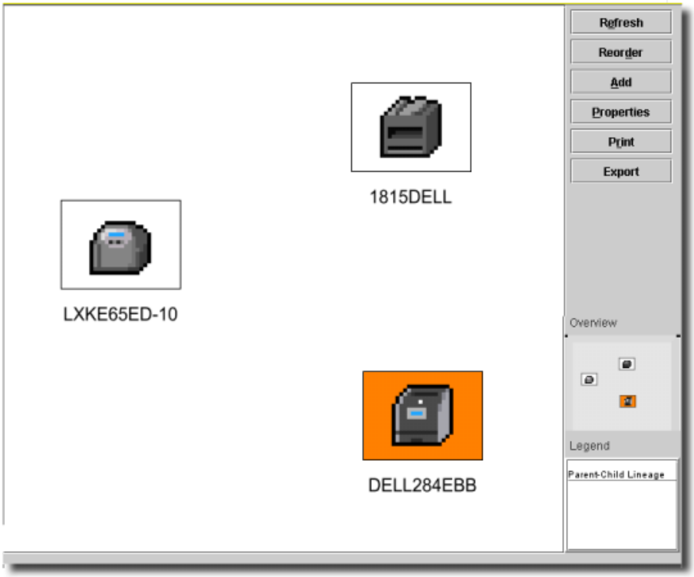
NOTE: Also: This does not resync alarms or communicate with the device or any northbound system, andis completely different from device resync.

This resyncs alarm state for topology. For example, if a device receives a critical open alarm, the topology view for the equipment should go red. If for some reason if the topology view does not reflect the alarm state properly, you can select the equipment and click alarm resync which will force the application to resync between alarms and topology.

Alarms in Topology

If you have the Event Services application installed, Topology views also display the color of the highest priority alarm on device icons.

Figure 11-9. Alarms in Topology



12

Heartbeat Policies

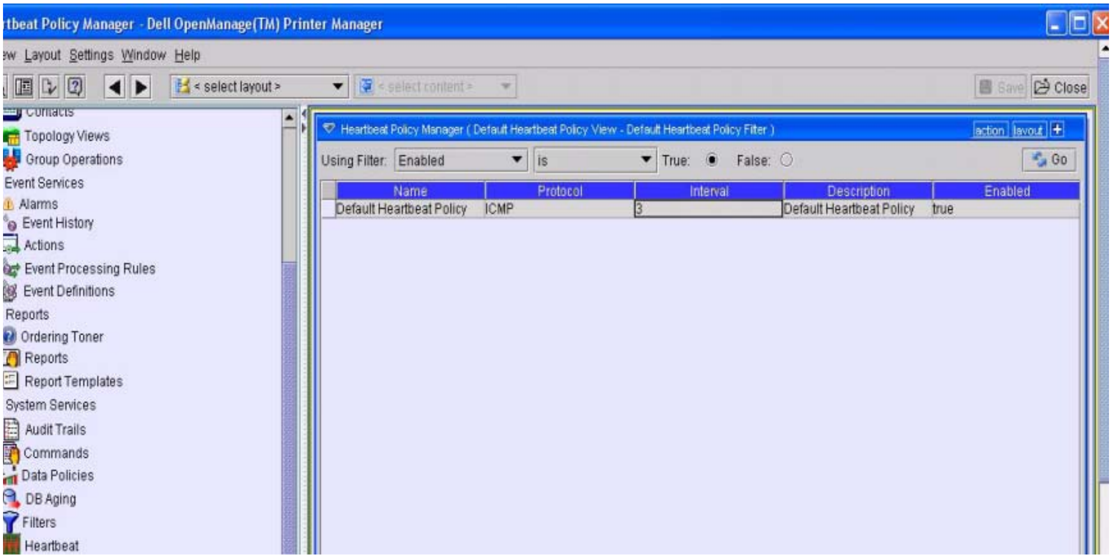
Introducing Heartbeats

Heartbeats are ICMP, SNMP, or HTTP pings to devices. These ensure the device is “alive and well” to respond to network events. (Ping operations pass to the operating system and use its default settings, including TTL.)

Heartbeat Policies

To manage equipment heartbeats more elaborate than ICMP ping, you must create items in the Heartbeat Policy Manager. Open this with the Navigation Window, or **File→ Open→ System Services→ Heartbeat**

Figure 12-1. Heartbeat Policies



Using Filter: Enabled is True: ● False: ○

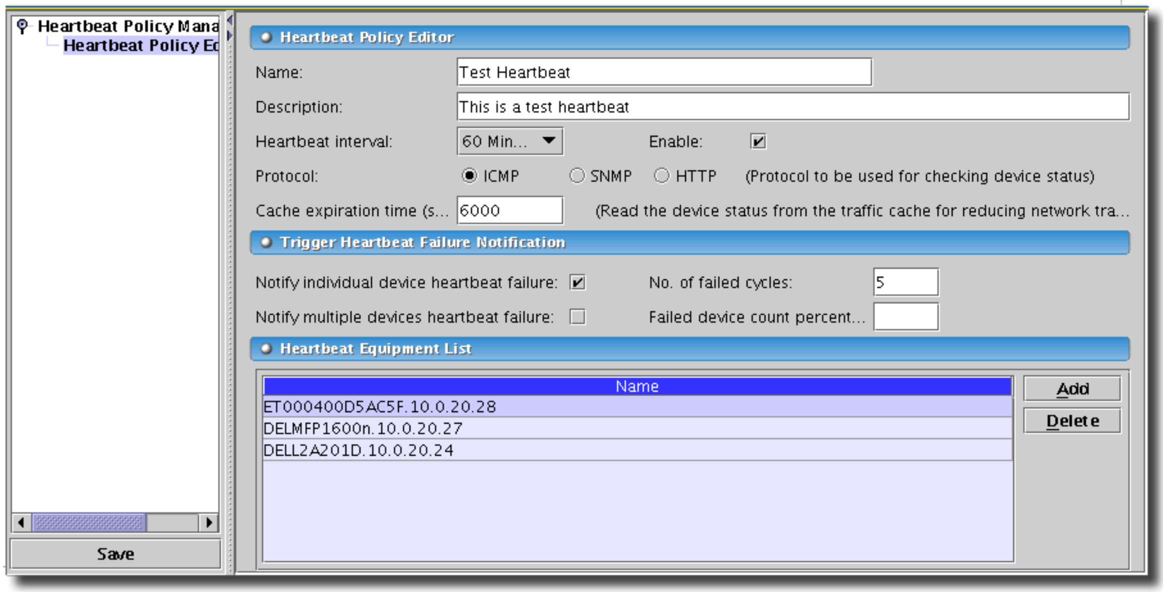
Name	Protocol	Interval	Description	Enabled
Default Heartbeat Policy	ICMP	3	Default Heartbeat Policy	true

This manager displays listed heartbeat policies according to the filter selected at the top of the screen. Click **Go** to refresh that screen. Click **New** to create a new heartbeat policy, or **Open** to edit a selected policy. Click **Delete** to remove a selected policy. When you click **New** or **Open**, the Heartbeat Policy Editor opens.

Heartbeat Policy Editor

This editor lets you configure heartbeats.

Figure 12-2. Heartbeat Policy Editor



Heartbeat Policy Mana
Heartbeat Policy Ed

Heartbeat Policy Editor

Name: Test Heartbeat

Description: This is a test heartbeat

Heartbeat interval: 60 Min... Enable: ☑

Protocol: ● ICMP ○ SNMP ○ HTTP (Protocol to be used for checking device status)

Cache expiration time (s... 6000 (Read the device status from the traffic cache for reducing network tra...

Trigger Heartbeat Failure Notification

Notify individual device heartbeat failure: ☑ No. of failed cycles: 5

Notify multiple devices heartbeat failure: □ Failed device count percent...

Heartbeat Equipment List

Name
ET000400D5AC5F.10.0.20.28
DELMFP1600n.10.0.20.27
DELL2A201D.10.0.20.24

This screen has the following fields:

Heartbeat Policy Editor

- **Name**—A unique identifier for the heartbeat policy.
- **Description**—A text description for the heartbeat policy.
- **Heartbeat interval**—Select from 3 - 60 minutes with the pick list.
- **Enable**—Check to enable this heartbeat policy.
- **Protocol**—Select the protocol to use when checking device’s status with the radio buttons. Select from among the available protocols: *ICMP, SNMP,* or *HTTP.*
- **Cache expiration time**—Enter how many seconds to cache the last notification of traffic to the device that can serve as a heartbeat. This feature reduces network traffic since the application does not send heartbeats if an appropriate traffic notification exists in the cache. To be effective, the cache should exceed the heartbeat interval.

  The server maintains a last-accessed cache for each device—basically retaining the last time it was accessed. The heartbeat policy can refer to that cache instead of sending its own query, and thereby can reduce network traffic.

Setting cache expiration to 0 in the heartbeat policy indicates that the application should not use the cache. A non-zero value indicates a time span in seconds—for example: 30 seconds. If we have accessed the printer within that time span—within the last 30 seconds—then the application will not ping the device, assuming that the printer is still responding since we recently accessed it for some other reason. So the cache time should be actually be less then heartbeat interval, since it would make much sense to poll the printer every 3 minutes if access to the printer within the last hour suffices as a heartbeat.

Trigger Heartbeat Failure Notification

The following parameters configure the kinds of notifications that can occur for this policy.

- **Notify individual device heartbeat failure**—Checking this sends a trap notifying users of an individual device's failure to respond to a heartbeat.
- **Notify multiple devices heartbeat failure**—Checking this sends a trap notifying users of the listed group of devices' failure to respond to a heartbeat.
- **No. of failed cycles**—The failure must exceed this threshold before the application produces a notification.
- **Failed Device percent**—The percentage of devices that must fail before the application issues a heartbeat failed notification.

Heartbeat Equipment List

Click **Add** to select equipment for this heartbeat policy. Select listed equipment and click **Delete** to remove them.

Click **Save** to preserve this policy.

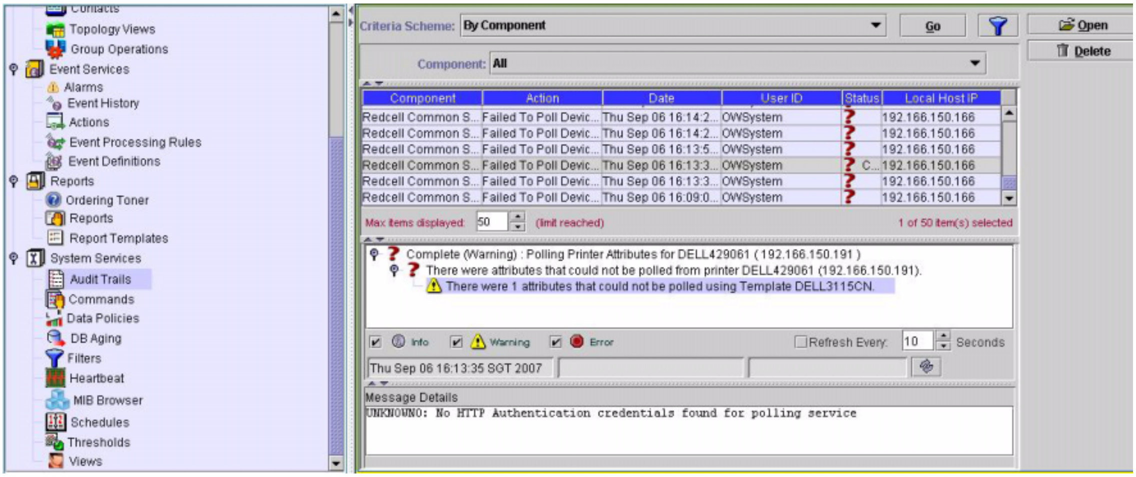
13

Audit Trails

Introducing Audit Trails

You can see the same messages described in Audit History in the Audit Trails screen. Open this screen from **File→ Open→ System Services→ Audit Trails**, or from the node on the navigation window.

Figure 13-1. Audit Trails screen



Criteria Scheme: By Component

Component: All

Component	Action	Date	User ID	Status	Local Host IP
Redcell Common S...	Failed To Poll Devic...	Thu Sep 06 16:14:2...	OWSystem	?	192.166.150.166
Redcell Common S...	Failed To Poll Devic...	Thu Sep 06 16:14:2...	OWSystem	?	192.166.150.166
Redcell Common S...	Failed To Poll Devic...	Thu Sep 06 16:13:5...	OWSystem	?	192.166.150.166
Redcell Common S...	Failed To Poll Devic...	Thu Sep 06 16:13:3...	OWSystem	? C...	192.166.150.166
Redcell Common S...	Failed To Poll Devic...	Thu Sep 06 16:13:3...	OWSystem	?	192.166.150.166
Redcell Common S...	Failed To Poll Devic...	Thu Sep 06 16:09:0...	OWSystem	?	192.166.150.166

Max items displayed: 50 (limit reached) 1 of 50 item(s) selected

```
? Complete (Warning) : Polling Printer Attributes for DELL429061 ( 192.166.150.191 )
  ? There were attributes that could not be polled from printer DELL429061 (192.166.150.191).
    ⚠ There were 1 attributes that could not be polled using Template DELL3115CN.
```

☑ Info ☑ Warning ☑ Error □ Refresh Every: 10 Seconds

Thu Sep 06 16:13:35 SGT 2007

Message Details

```
UNKNOWN0: No HTTP Authentication credentials found for polling service
```

The following are components of this screen:

- **Criteria Scheme**—At the top of this manager, you can elect to filter what audit messages appear here with the pick box labelled *Criteria Scheme*. You can use any existing filter, or create a new one with the *Create/Edit a Filter* button (the key).
- **By Component**—Select from the list of available components to further narrow the list of audit messages that appears.

Components from which you can select appear in a table with columns for *Status*, *Date*, *Component*, *Action*, and *User*. Selected messages appear in the middle screen area, which is like Audit History. The messages (*Type*, *Time* and *Message* appear in the lowest table. Checking the checkboxes next to the various icons further filters what messages appear.

Audit Trails Editor Panel

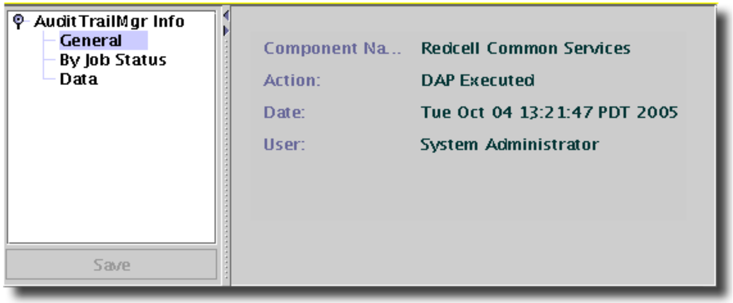
When you open a history item, the Audit Trails Editor panel appears. It has the following panels (described in subsequent sections):

- General
- By Job Status
- Data

General

When you select a component, then click the **Open** button, a multi-panel editor appears.

Figure 13-2. Audit Trails Editor - General



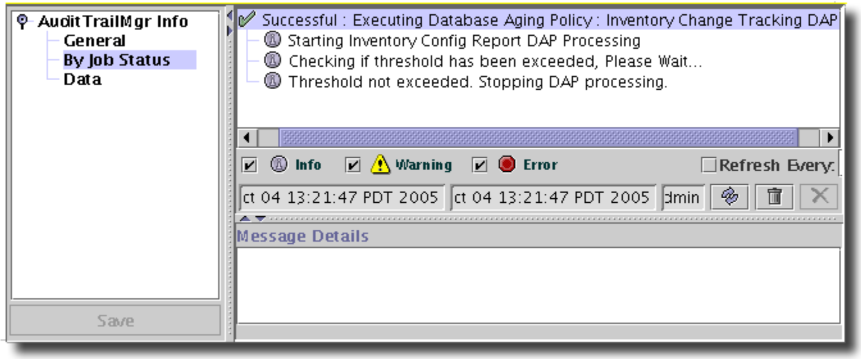
Component Na... Redcell Common Services
Action: DAP Executed
Date: Tue Oct 04 13:21:47 PDT 2005
User: System Administrator

The first panel (*General*), reiterates the *Component Name*, *Action*, *Date*, and *User* for the selected item.

By Job Status

This screen outlines the status message information for the selected component(s).

Figure 13-3. Audit Trail Editor - By Job Status



✓ Successful : Executing Database Aging Policy : Inventory Change Tracking DAP

- Starting Inventory Config Report DAP Processing
- Checking if threshold has been exceeded, Please Wait...
- Threshold not exceeded. Stopping DAP processing.

☑ Info ☑ Warning ☑ Error □ Refresh Every:

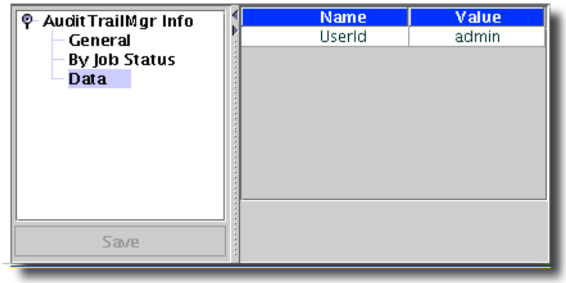
ct 04 13:21:47 PDT 2005 | ct 04 13:21:47 PDT 2005 | dmin

This is a standard audit screen. Messages appear at the top. The date and time of the selected message appear in the middle, and any details about that message appear in the lowest panel.

Data

This screen lets you view and edit the selected trail's data.

Figure 13-4. Audit Trail Editor - Data



Name	Value
UserId	admin

The exact appearance of the screen depends on the audit action selected before you click **Open**. For some jobs, it does not appear at all.

In some screens, you can also click **View...** buttons, where they appear, to see existing data.

14

Group Operations

Overview

The application’s (optional) Group operations let you act on groups of devices—even heterogeneous groups. You must make the groups before you can operate on them. You can make groups of interfaces too, not just entire devices.

NOTE: This feature is an option that can be standard in some versions. You must also have drivers installed that support group operations before you can use them. Consult the section of this guide that discusses the product or addon for more information about specific Group Operations.

Open the Group Operations Manager from from **File→ Open→ Inventory→ Group Operations**, or from its node in the Navigation Pane. A typical manager appears. See Group Operations Manager for details.

Group operations are asynchronous. You can monitor them as they occur, and have occurred, with the features explained in Audit History.

NOTE: Use Group Ops to schedule operations on more than one device at the same time instead of scheduling multiple individual operations at the same time.

Group Operations Wizard

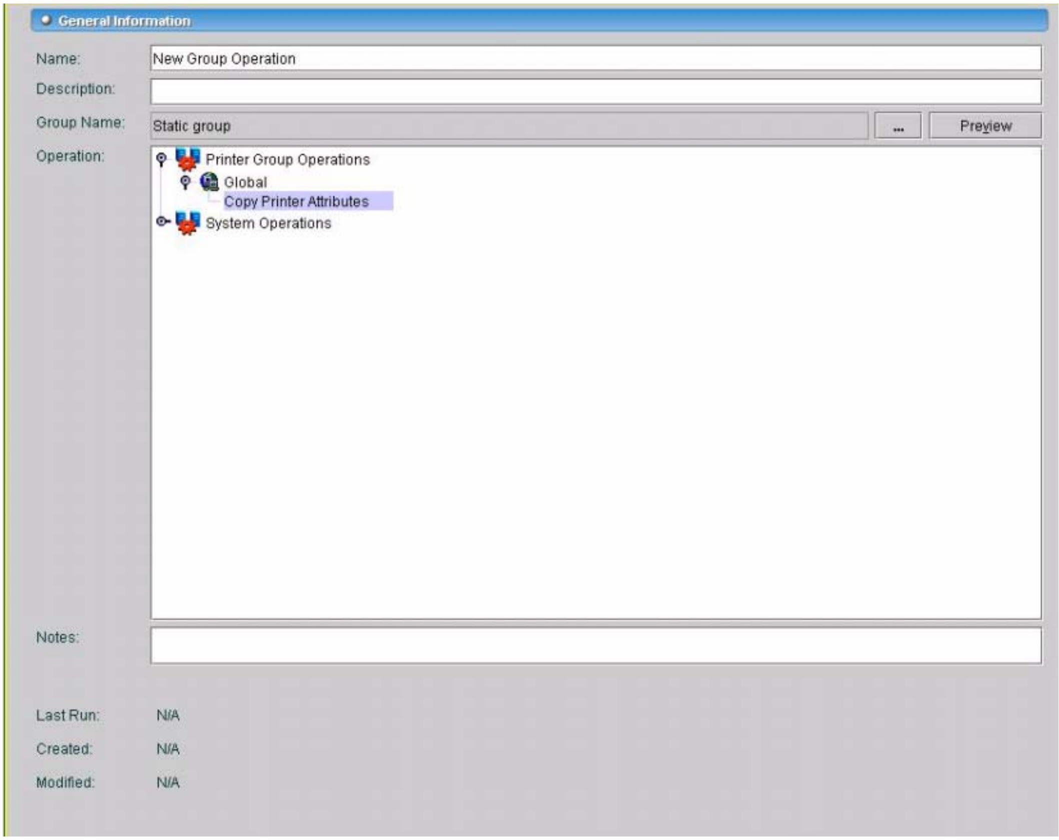
Clicking **New** opens the **Group Operations Wizard**. This walks you through creating a group operation with the following steps :

- Group and Type
- Action Screen
- Save and Execute Options
- Status

Group and Type

The first screen in this Wizard lets you select a group and type of operation.

Figure 14-1. Select a Group and Operation Type



General Information

Name: New Group Operation

Description:

Group Name: Static group

Operation:

- Printer Group Operations
  - Global
    - Copy Printer Attributes
- System Operations

Notes:

Last Run: N/A

Created: N/A

Modified: N/A

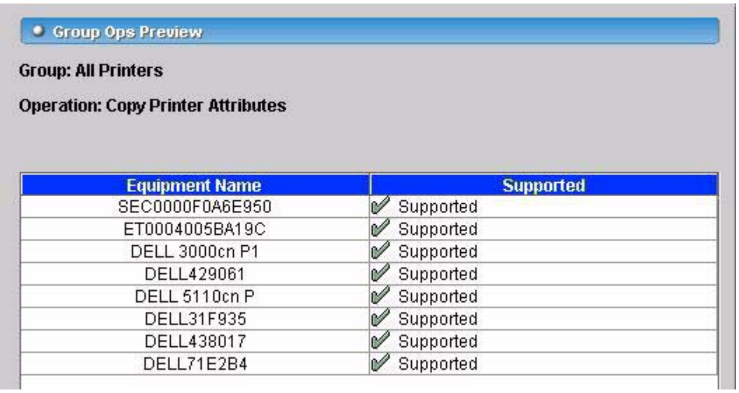
The exact contents of this panel depend on the applications and device drivers you have installed. It has the following information:

- **Name**—The unique identifier for the group operation you are creating.
- **Description**—A text description of the group operation.
- **Group**—The (previously created) equipment group on which this operation acts. Use the command button (...) to change the selection.
- **Operation**—Consists of nodes for drivers and applications, in addition to the standard *System Operations* node. Under these nodes, *Global* operations essentially do the same thing to the entire group. *Batch* operations do grouped, device- or instance-specific actions.

System Information actions work for any device that supports SNMP MIB 2 (and those that do not if you are only updating the database). Other devices require that a Device Driver be installed and support the given type.

- **Notes**—A text field where you can enter notes about the group operation you are creating.
- **Last Run**—(Read only) The time this operation last ran.
- **Created**—(Read only) The time you created this operation.
- **Modified**—(Read only) The time you last modified this operation.
- **Preview**—Click this button so the application can test the group operation against the equipment in the selected group. The subsequent screen tells whether the devices support the action

Figure 14-2. Group Operations Preview Screen



Group: All Printers

Operation: Copy Printer Attributes

Equipment Name	Supported
SEC0000F0A6E950	✓ Supported
ET0004005BA19C	✓ Supported
DELL 3000cn P1	✓ Supported
DELL429061	✓ Supported
DELL 5110cn P	✓ Supported
DELL31F935	✓ Supported
DELL438017	✓ Supported
DELL71E2B4	✓ Supported

You can proceed with the group operation, or abandon it, as appropriate, based on this screen.

Action Screen

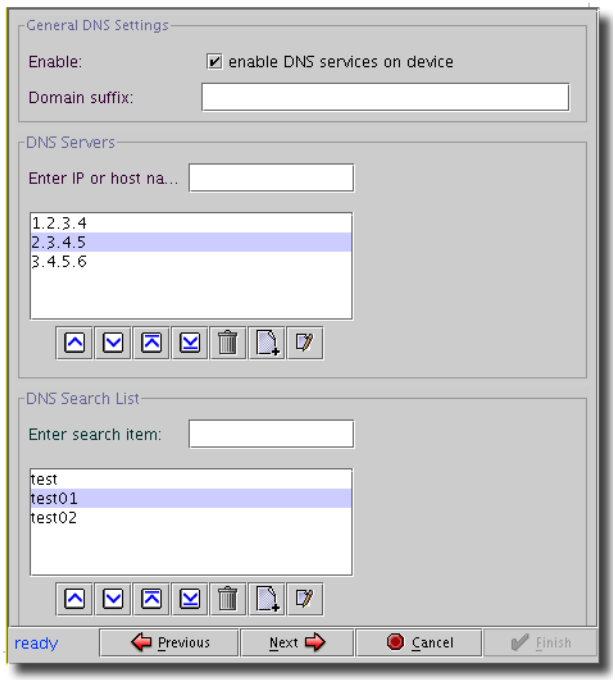
The next screen (click **Next** to get there) lets you specify the parameters for the action you selected in the first screen. Here are some action screens that can appear:

- DNS Servers
- Gateway
- Time Servers
- Network Services
- Port Speed and Duplex
- System Information

DNS Servers

You can set the DNS Server attributes in this screen.

Figure 14-3. Group Operations DNS Servers



General DNS Settings

Enable: ☑ enable DNS services on device

Domain suffix:

DNS Servers

Enter IP or host na...

1.2.3.4
2.3.4.5
3.4.5.6

DNS Search List

Enter search item:

test
test01
test02

It has the following fields, checkboxes and tables (defined when not self-evident):

- **Enable**—A checkbox you must select before any fields are writable below it.
- **Domain Suffix**—DNS domain suffix.

Enter devices in this screen in fields above the lists of devices, then click the *Add New Item* icon to insert the text you type into these lists. You can manage the priority of items with the arrow buttons, and delete or edit selected items with the buttons for those functions once you select an item displayed in the table.

DNS Servers

- **Enter IP or Hostname**—Enter the DNS server hostname you want to add to the servers in the table here.

DNS Search List

- **Enter Search Item**—Enter the DNS server hostname you want search for (and that you want to appear in the table) here.

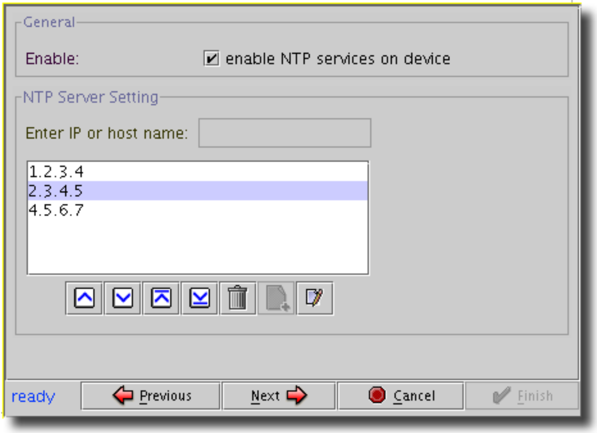
Gateway

Selecting this in the previous screen means you must type the (default) *Gateway IP Address* for the selected group in the subsequent screen.

Time Servers

Assign time servers to the selected group.

Figure 14-4. Group Operations: Time Servers



General

Enable: ☑ enable NTP services on device

NTP Server Setting

Enter IP or host name:

```
1.2.3.4
2.3.4.5
4.5.6.7
```

ready

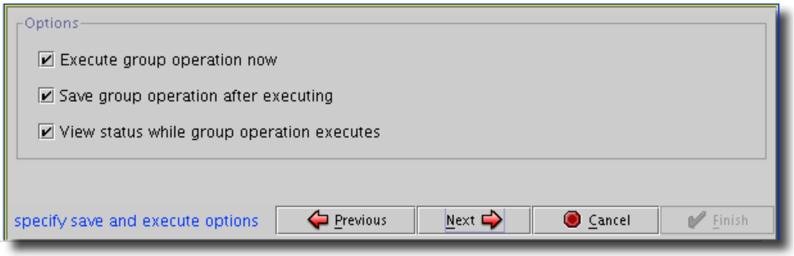
Click the checkbox to enable NTP services for the group.

Enter server names in the *Enter IP or host name* field, and use the *Add New Item* button to add the name to the list displayed. You can also delete and edit selected items on this list with the buttons below it. The arrow buttons manage the order of the list.

Save and Execute Options

The next screen lets you select options for saving, executing, and viewing operations you have specified.

Figure 14-5. Group Operations: Save and Execute Options



Options

☑ Execute group operation now

☑ Save group operation after executing

☑ View status while group operation executes

specify save and execute options

By clicking the checkboxes, you enable the following:

- Execute Group Operation Now
- Save Group Operation after Executing
- View status while group operation executes.

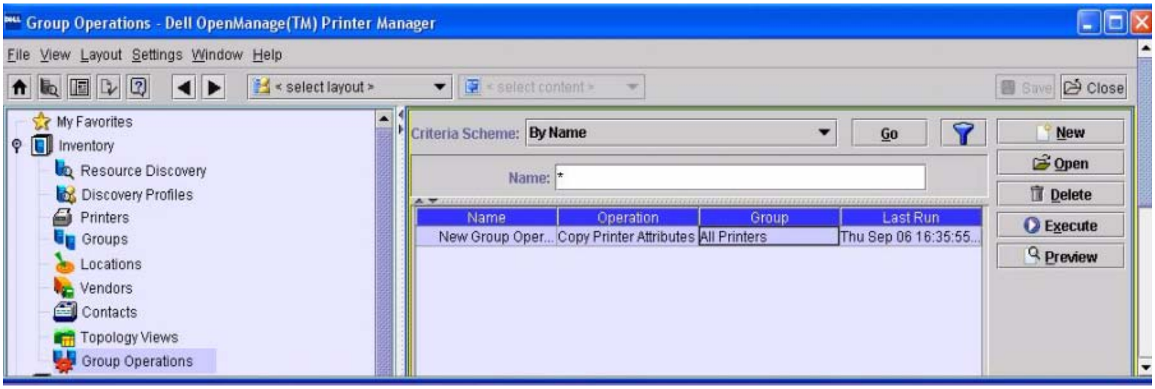
Status

The final screen that appears displays the status of the group operation (provided you elected to view that status).

Group Operations Manager

Once you have created a group operation, you can view and alter portions of it in the Group Operations Manager.

Figure 14-6. Group Operations Manager



Criteria Scheme: By Name

Name: *

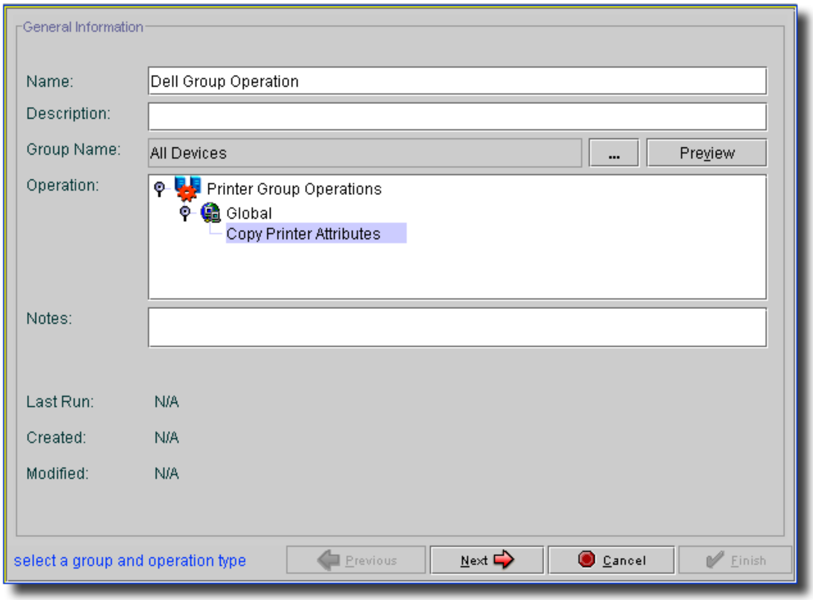
Name	Operation	Group	Last Run
New Group Oper...	Copy Printer Attributes	All Printers	Thu Sep 06 16:35:55...

When you select an existing group operation, you can *Open*, *Delete*, or *Execute* it with the buttons on the right of this manager. If you *Open* it, the Group Operations Editor appears. When you select *New*, the *Group Operations Wizard* appears.

Group Operations Editor

This editor has several panels that let you manage existing groups.

Figure 14-7. Group Operations: Editor, General



General Information

Name: Dell Group Operation

Description:

Group Name: All Devices

Operation:
- Printer Group Operations
  - Global
    - Copy Printer Attributes

Notes:

Last Run: N/A

Created: N/A

Modified: N/A

select a group and operation type

The panels are:

- General
- Settings
- Audit History

General

The General panel reiterates the screen you saw first in Group and Type. You can alter the description and notes, but the other fields are read-only.

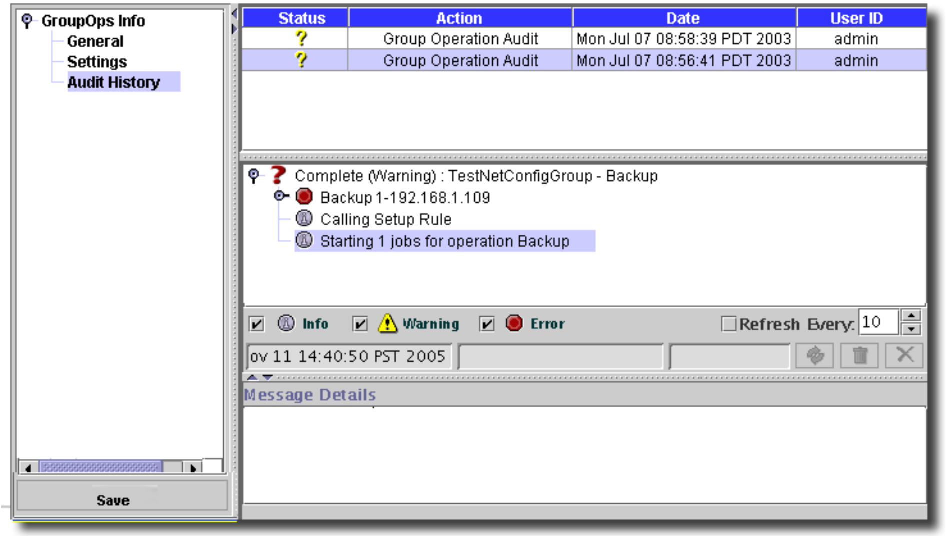
Settings

This panel depends on the operation selected. In our example, we made a batch operation setting the IP address on the selected devices. The *Settings* panel is therefore one like *Action Screen*.

Audit History

This panel displays the history of group operations in some detail.

Figure 14-8. Group Operations: Audit History



Status	Action	Date	User ID
?	Group Operation Audit	Mon Jul 07 08:58:39 PDT 2003	admin
?	Group Operation Audit	Mon Jul 07 08:56:41 PDT 2003	admin

- ? Complete (Warning) : TestNetConfigGroup - Backup
  - ● Backup 1-192.168.1.109
  - Calling Setup Rule
  - Starting 1 jobs for operation Backup

☑ Info ☑ Warning ☑ Error □ Refresh Every: 10

ov 11 14:40:50 PST 2005

Message Details

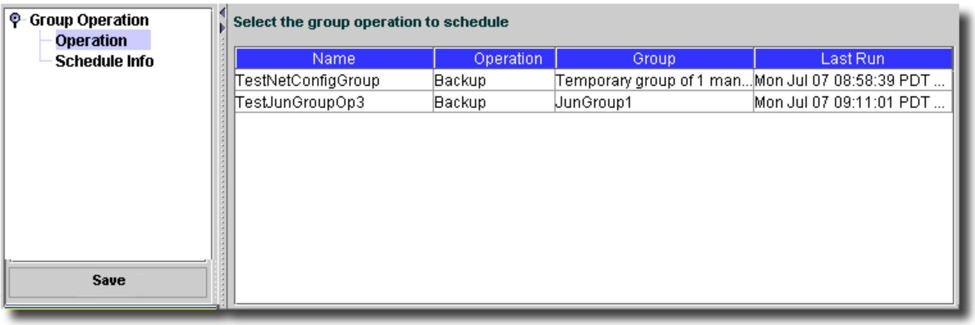
Notice that the top panel lists group operations runs, while the middle panel displays the details of the selected run, and the lowest panel shows the contents of a selected node in the middle panel.

The bar between the lowest and middle panels displays the details concerning a specific message: its start and end time, and the user requesting the operation. You can also use the buttons on the right of this bar to *Refresh*, or *Delete* the currently selected job or *Cancel* a running job.

Scheduling Group Operations

You can schedule group operations from the **File→ Open→ System Services→ Schedules** menu item. If you create a new entry and select Group Operations you open a Group Operation screen where you select which group operation to schedule. Use the *Schedule Info* tab to enter the specifics of how it is to be scheduled. See Schedules for more about that tab.

Figure 14-9. Scheduling a New Group Operation



Select the group operation to schedule

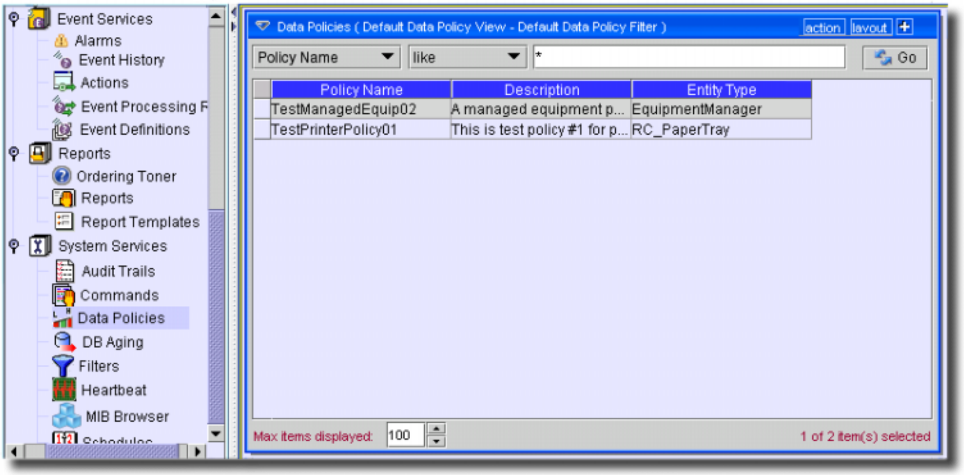
Name	Operation	Group	Last Run
TestNetConfigGroup	Backup	Temporary group of 1 man...	Mon Jul 07 08:58:39 PDT ...
TestJunGroupOp3	Backup	JunGroup1	Mon Jul 07 09:11:01 PDT ...

After you have created a scheduled item you can edit it by clicking **Open** in the Schedules screen. Editing an item displays the Group Operation that is being scheduled in a similar list.

Data Policies

This screen lets you manage data policies. These policies let you scan equipment for compliance with them, and emit notifications (see Events, Rules and Actions) that describe them when you save or poll equipment.

Figure 15-1. Data Policies



Policy Name	Description	Entity Type
TestManagedEquip02	A managed equipment p...	EquipmentManager
TestPrinterPolicy01	This is test policy #1 for p...	RC_PaperTray

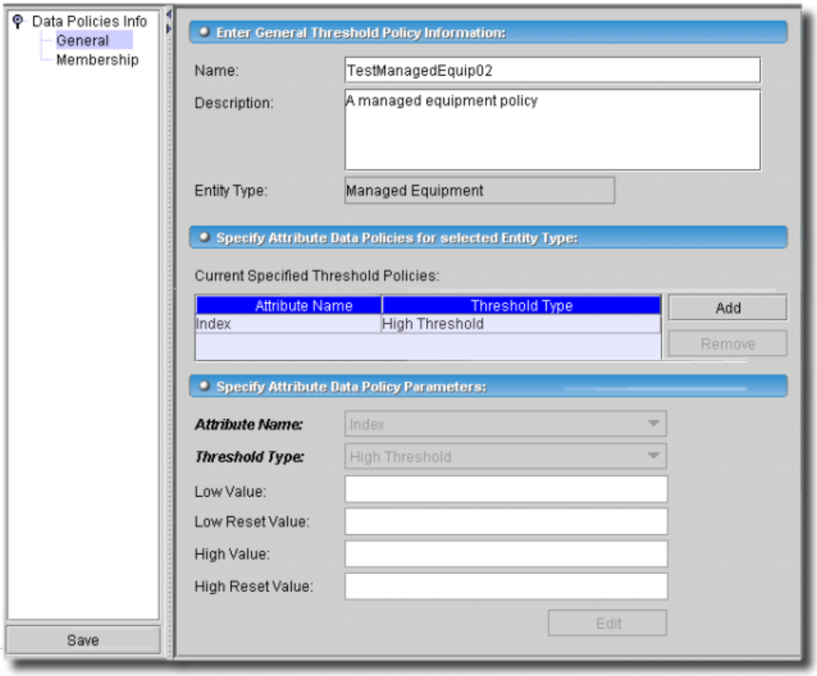
The policies appear listed at the top of this screen. You can filter the items displayed when you check the Use Filter checkbox. The details panel at the bottom of this screen display details of the selected policy. The Action button (or right click) menu contains the following items:

- New—Opens the Data Policy Editor, through which you can define a new mapping.See Data Policy Editor - General for more information about the Mapping Editor.
- Open—Opens the selected Data Policy for modification. See Data Policy Editor -General for more information.
- Delete—Deletes the selected policy. Select the policy to remove and click Delete.The application prompts you for confirmation.
- Print—Print the listed items to an Acrobat file. (You must have Acrobat reader installed for this to work properly.) Change the filter and click Go to change this printed report’s appearance.
- Export/Import—Export or import the listed items as/from XML.
- Help—Open the context-sensitive help for this screen.

Data Policy Editor - General

This screen creates or alters data policies.

Figure 15-2. Data Policy Editor



Enter General Threshold Policy Information:

Name: TestManagedEquip02

Description: A managed equipment policy

Entity Type: Managed Equipment

Specify Attribute Data Policies for selected Entity Type:

Current Specified Threshold Policies:

Attribute Name	Threshold Type
Index	High Threshold

Specify Attribute Data Policy Parameters:

Attribute Name: Index

Threshold Type: High Threshold

Low Value:

Low Reset Value:

High Value:

High Reset Value:

This screen has the following fields:

Name—A text identifier for the policy.

Description—A text description for the policy.

Entity Type—Select from the entities available in the pick list. These can include Correlation, Interface, Link, Printer, Printer - Input Trays, Printer - Output Trays,Printer - Toner, Process, and Vendor.

Threshold Policies

This table contains the specified threshold policies. Click Add to activate the lowest panel's editor, where you can specify the policy's parameters, or select a policy and click Remove to delete it.

Policy Editor

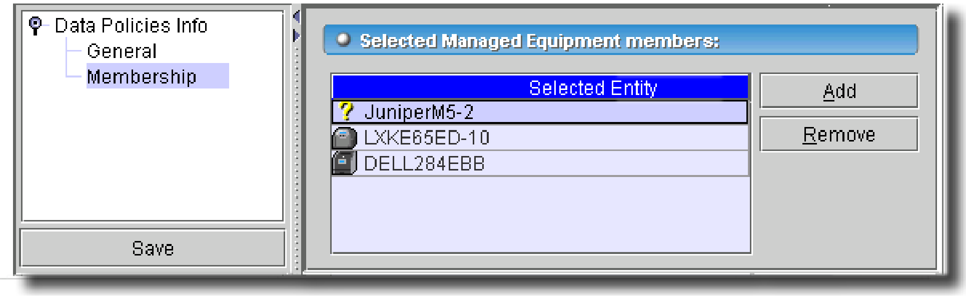
- Attribute Name—Select from the pick list. Options vary, depending on the Entity Type selected at the top panel of this screen.
- Threshold Type—Select from High Threshold, or Low Threshold, and enter the High / Low Value and High / Low Reset Value. Reset values reset the data notification for the selected parameter. If equipment exceeds the Low Threshold at 10, and something makes that parameter 40 when the Low Reset value is only 30, then the application clears the Low Threshold event.

Click Save to preserve your edits.

Data Policy Editor - Membership

This screen lets you manage the equipment membership monitored by your data policies.

Figure 15-3. Data Policy Editor - Membership



Selected Entity
JuniperM5-2
LXKE65ED-10
DELL284EBB

Click Add to select equipment where you want to apply the policy configured in the Data Policy Editor - General screen. Select a piece of equipment and click **Remove** to delete it.

Click **Save** to preserve your edits.

16

Events, Rules and Actions

Overview of Events, Rules and Actions

The following screens let you configure this application to react, according to rules, to internal events, and implement configured actions. For example, you can configure the application to act when a backup occurs (and, say, send an e-mail). You can also configure reactions to certain failures. For example, if pushing a configuration file to a device fails, an event can trigger a rule with an action to restore the last known good configuration. This provides powerful capabilities.

NOTICE: Configuring circular or self-referred actions can severely impact this system’s performance.

The following sections describe correlating and configuring events, and their mapped actions.

Terms

The following terms appear throughout the explanations that follow:

- **Action**—The outcome of the event, after processed by any Event Processing Rules.
- **Alarm**—Some, but not all, events appear as alarms, notifying users in the *Alarm* display.
- **Correlation**—A general term describing the interaction of events. A redundant event that is also an Alarm can simply increase the Alarm count, for example, rather than creating a new Alarm.
- **Event**—A message within the Element Management System (EMS). See Event Definitions for a description of configuring these.
- **Event Processing Rules**—Rules that specify the interaction between events, and any *Action* outcome. See Event Processing Rules, and Actions Manager.
- **Reject**—When you configure an event to be *Reject*ed, it goes no further in the EMS.
- **Suppress**—When you configure an event to be *Suppress*ed, it appears in the screen described in *Event History*, but nowhere else.
- **Message Template**—Part of Event Definitions. These are messages to be matched when you correlate events. See Message Template.

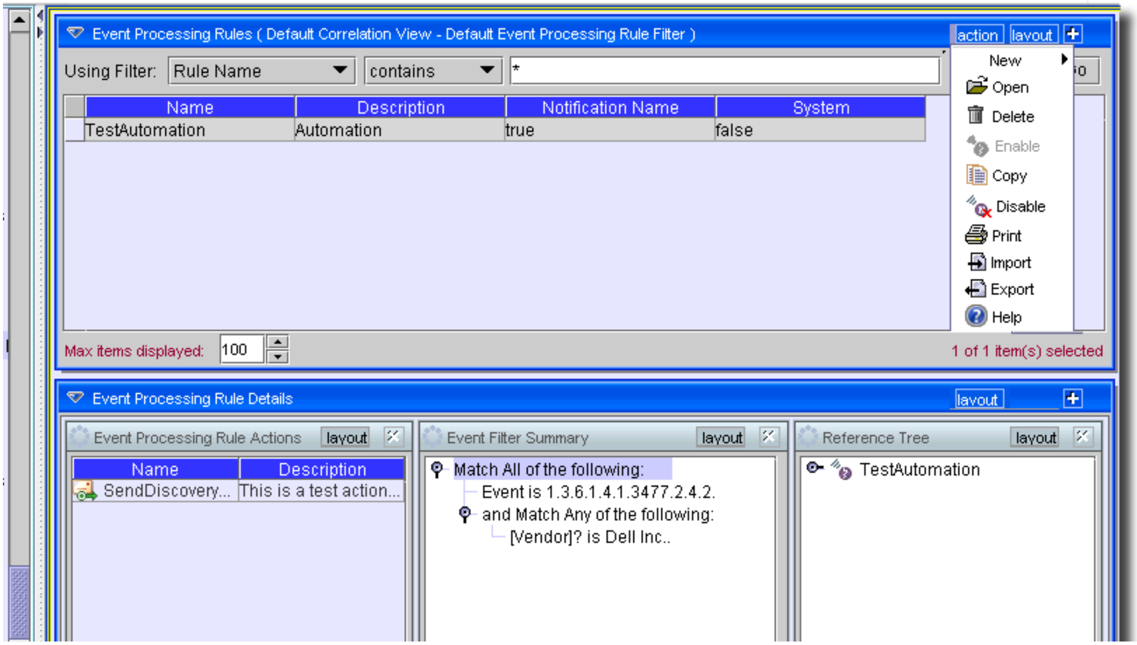
Some Example Use Cases

- Without any special configurations, when Alarms arrive at the same severity, they increment the alarm count on the first one that arrives.
- If you configure correlation, then when a correlated incoming alarm's key bindings match the initial alarm, that same count increment occurs. If they do not match, the system generates a new alarm
- If you configure correlation, and the Message Template or Severity do not match for otherwise matching alarms, then the EMS closes the existing alarm and opens a new alarm.

Event Processing Rules

This manager lets you configure rules for event processing.

Figure 16-1. Event Processing Rules



Event Processing Rules (Default Correlation View - Default Event Processing Rule Filter)

Using Filter: Rule Name contains *

Name	Description	Notification Name	System
TestAutomation	Automation	true	false

Max items displayed: 100

1 of 1 item(s) selected

Event Processing Rule Details

Event Processing Rule Actions

Name	Description
SendDiscovery...	This is a test action...

Event Filter Summary

Match All of the following:
Event is 1.3.6.1.4.1.3477.2.4.2.
and Match Any of the following:
[Vendor]? is Dell Inc..

Reference Tree

TestAutomation

This screen lets you filter a list of processing rules based on *Description*, *Enabled*, *Event Name*, *Owner*, *Rule Name*, *Rule Type*, *Valid*. Some of these (and *icon*) are columns in the table of rules.

As in a typical manager, the filter is at the top of the screen. With this manager you can configure rules that respond to internal events in the EMS. The manager has the following *Action* menu items (accessed with the *Action* button, or a right-click):

- **New**—Lets you select among the different types of editor for the rule you are configuring. Available types include the following:
  - *Automation*—Opens the Automation Event Processing Rule Editor through which you can define a new Action.
  - *Correlation*—Opens the Correlation Event Processing Rule Editor where you can create or modify this type of rule.
- **Open**—Opens the selected Action for modification. See Action Editor for more information.
- **Enable**—Enables the selected rule(s).
- **Copy**—This copies the selected rule and opens the editor. You must rename it to begin with something other than "CopyOf [Original Name]" (its default name) before you can save the rule.

  NOTE: If you want to change the behavior of a system rule, copy it, then disable it. Then configure the copy do the desired behavior.
- **Disable**—Disables the selected rule(s).
- **Delete**—Deletes the selected action. Select the action to remove and click *Delete*. The application prompts you for confirmation.
- **Print**—Print the listed correlations to an Acrobat file. (You must have Acrobat reader installed for this to work properly.) Change the filter and click *Go* to change this printed report's appearance.
- **Export/Import**—Export or import the action as/from XML.
- **Help**—Open the context-sensitive help for this screen.

Event Processing Rule Details

The lowest portion of this layout contains detail panels that display *Event Processing Rule Actions* for the selected rule. These describe the actions connected to a rule. When rules are not part of the *System*, you can right click an action and edit it in Action Editor.

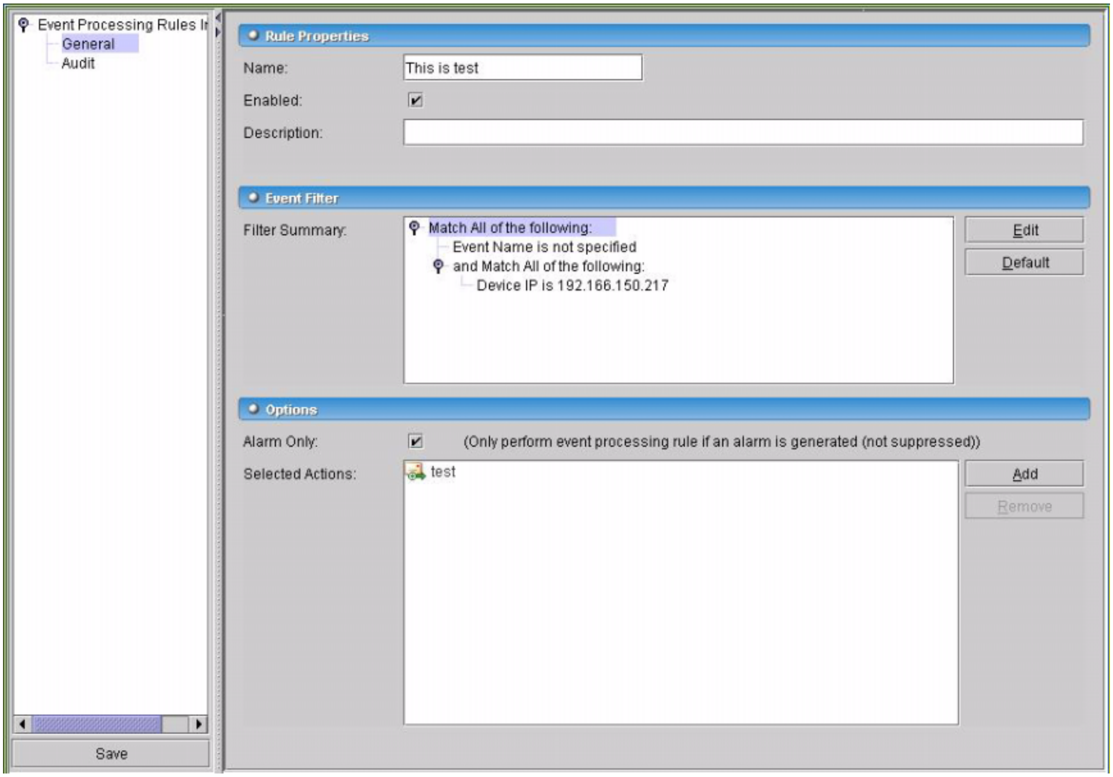
The *Event Filter Summary* displays the filter information for the selected rule in a tree format.

Finally, the *Reference Tree* for the selected rule displays any related actions and event processing rules in a tree.

Automation Event Processing Rule Editor

This editor lets you create new or modify existing event processing automation rules. Among other things, these correlate events with actions that they trigger.

Figure 16-2. Automation Event Processing Rule Editor



Name: This is test

Enabled: ☑

Description:

Filter Summary:
- Match All of the following:
  - Event Name is not specified
  - and Match All of the following:
    - Device IP is 192.166.150.217

Alarm Only: ☑ (Only perform event processing rule if an alarm is generated (not suppressed))

Selected Actions: test

This editor has the following fields and selection options:

Rule Properties

- **Name**—A text identifier for the rule.
- **Enabled**—Check to enable this rule's action.
- **Alarm Only**—Check to enable this rule's action only when the system first generates an alarm without suppressing it. Subsequent alarms do not trigger the rule.
- **Description**—A text description of the rule.

Event Filter

Click *Add* to create an event filter criterion for this rule (or *Edit* to configure an existing set of criteria), so the rule only appears for certain events, equipment, vendors, and so on. This opens the Event Filter Criteria editor. Click *Default* to revert to the event filter's unaltered default criteria. A prompt appears confirming this selection.

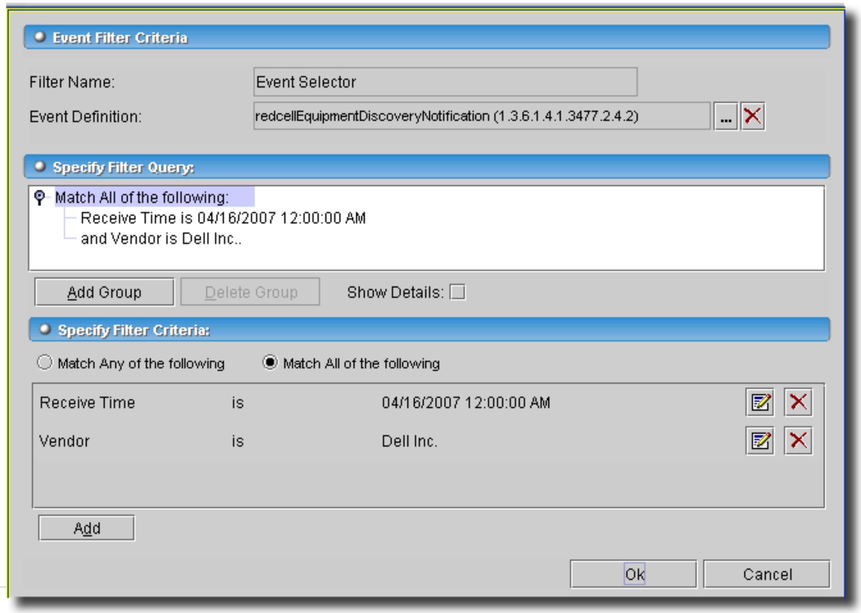
Options

Click *Add* to select an action created in *Actions Manager*. You can also click *New* in the subsequent selector screen to create a new action as described in that section. You can create a rule as you would in Actions Manager in the selector too. Notice that you can elect to have multiple actions occur for a single event.

Event Filter Criteria

This screen configures what must match for the processing rule to run.

Figure 16-3. Event Filter Criteria



Event Filter Criteria

Filter Name: Event Selector

Event Definition: redcellEquipmentDiscoveryNotification (1.3.6.1.4.1.3477.2.4.2)

Specify Filter Query:

Match All of the following:
Receive Time is 04/16/2007 12:00:00 AM
and Vendor is Dell Inc..

Show Details: □

Specify Filter Criteria:

○ Match Any of the following ● Match All of the following

Receive Time	is	04/16/2007 12:00:00 AM
Vendor	is	Dell Inc.

It has the following sections, fields and selectors:

Event Filter Criteria

- **Filter Name**—A text identifier for the filter.
- **Event Definition**—You can optionally select an event with the command button (...), or delete it with the red “X” button. Selecting an event is not necessary, but if you do select one, the available filter criteria below are limited to those appropriate to the event selected. If you select no event, then only generic filter criteria appear in the next section of the screen.

  NOTE: If you want to filter on event varbind data, then select the event. The varbind attributes appear in the lowest panel.

Specify Filter Query

Click *Add Group* to create a group of matching criteria. The *Match Any of the following* and *Match All of the following* radio buttons determine whether the selected group of criteria is configured with a logical *OR* or a logical *AND* for its components.

Click *Add* to create criteria. Edit these as described in "*Filter Editor*" *on page* 213.

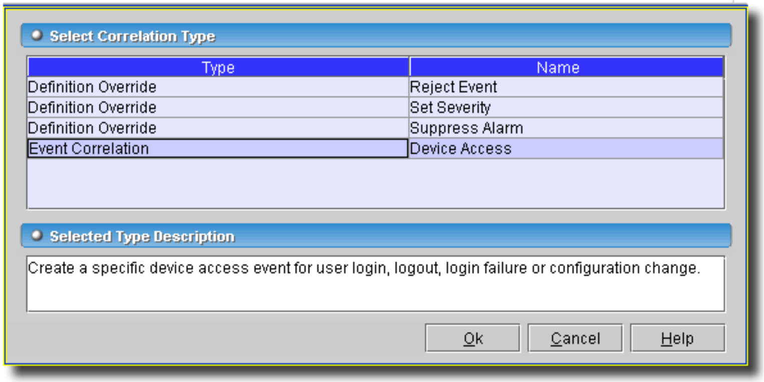
Audit

The *Audit* tab displays a history of the rule's use.

Correlation Event Processing Rule Editor

When you select *Correlation* as the type of new rule you want to create, or edit, this editor appears. When you are creating a new rule, you must select which type from an intervening screen.

Figure 16-4. Correlation Rule Type Selector



Select Correlation Type

Type	Name
Definition Override	Reject Event
Definition Override	Set Severity
Definition Override	Suppress Alarm
Event Correlation	Device Access

Selected Type Description

Create a specific device access event for user login, logout, login failure or configuration change.

For new rules, you must select from the following for this screen

- Set Severity
- Reject Event
- Suppress Alarm
- Event Correlation

If you are editing an existing rule, clicking *Open* selects the correct type automatically. On these panels, the *Audit* tab displays a history of the rule's use. Event History in all screens, the *Audit* tab displays a history of the rule's use.

Set Severity

This screen lets you set the severity of the correlated event as you would in Automation Event Processing Rule Editor. The difference here is that the *Options* panel provides a pick list for selecting the severity of the event propagated when the event you correlate appears. "*Event Filter Criteria*" *on page 191* describes you can select the correlated event(s) where you set the severity in the event(s) propagated.

Reject Event

This screen lets you configure how to reject correlated events, discarding them. It is like the one in Automation Event Processing Rule Editor. The difference here is that no *Options* panel appears since the filtered events are to be rejected. "*Event Filter Criteria*" *on page 191* describes how to select the event(s) to reject.

Suppress Alarm

Use this as you would the Automation Event Processing Rule Editor screen. N *Options* panel appears since this describes the events to be suppressed. Suppressed events / alarms do not appear in the Alarm display, but, unlike rejected events, the Event History screen can display a record of them. Use "*Event Filter Criteria*" *on page 191* to select the event(s) / alarm(s) to suppress.

Event Correlation

This screen is like Automation Event Processing Rule Editor's. Here, however, the *Options* panel lets you select from among several classifications for the correlated (and propagated) events. Selection from the *Access Type* pick list for *User Login*, *User Logout*, *Login Failure* and *Config Change*. This selection determines the type of correlated access event to produce.

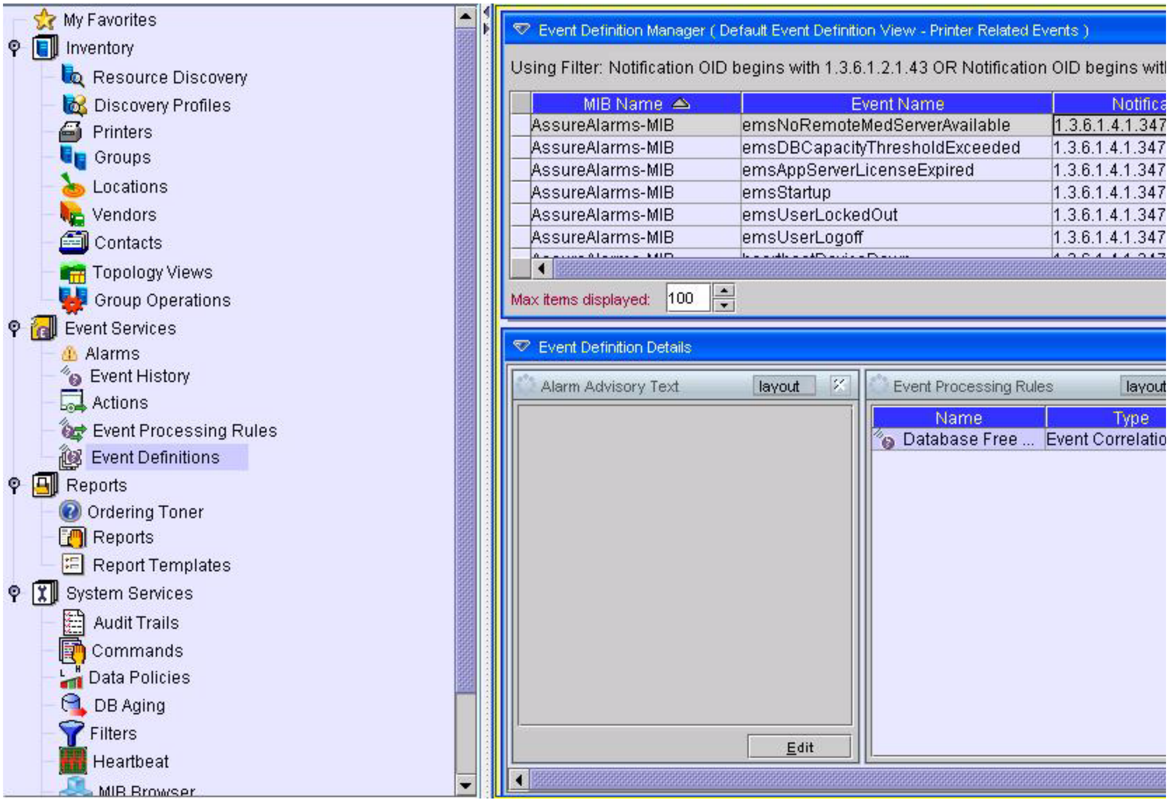
All access events have a variable for device user. Choosing the access event with which to correlate is the filter's function (see *Event Filter Criteria*). Once you select an event, you can choose a username variable in the *UserName Variable* pick list. Sometimes such variables contain more than just the user name (for example in a syslog message). In such cases, specify a regular expression in *UserName RegEx* to extract the exact username portion.

NOTE: If your filter returns more than a single event, then the UserName Variable and UserName RegEx fields are disabled.

Event Definitions

This screen manages the event definitions for your system.

Figure 16-5. Event Definitions



Event Definition Manager (Default Event Definition View - Printer Related Events)

Using Filter: Notification OID begins with 1.3.6.1.2.1.43 OR Notification OID begins wit

MIB Name	Event Name	Notifica
AssureAlarms-MIB	emsNoRemoteMedServerAvailable	1.3.6.1.4.1.347
AssureAlarms-MIB	emsDBCapacityThresholdExceeded	1.3.6.1.4.1.347
AssureAlarms-MIB	emsAppServerLicenseExpired	1.3.6.1.4.1.347
AssureAlarms-MIB	emsStartup	1.3.6.1.4.1.347
AssureAlarms-MIB	emsUserLockedOut	1.3.6.1.4.1.347
AssureAlarms-MIB	emsUserLogoff	1.3.6.1.4.1.347

Max items displayed: 100

Event Definition Details

Name	Type
Database Free ...	Event Correlatio

This screen displays a filtered list of actions. As in a typical manager, the filter is at the top of the screen. You can filter on the following behavior: *Default Behavior (Alarm*, *Reject*, or *Suppress)*, *Event Name*, *MIB Name*, *Message*, *Notification OID*, *Severity* and *Valid* (*True/False* radio buttons) criteria. In this screen, you can configure events that, when correlated as described in "Event Processing Rules" on page 188, trigger actions. The manager has the following menu items (accessed with the *Action* button, or a right-click):

- **Open**—Opens the selected Event for modification. See Event Definition Editor for more information.
- **Set Severity**—The severity of the event. You can alter the default with the pick list.
- **Set Behavior**—Use the pick list to select *Alarm*, *Reject*, or *Suppress*.

- **Load MIB**—You can load a MIB, if you have one available as a file.
- **Print**— Prints the events to a pdf file.
- **Unload MIB**—You can unload the MIB for the selected event if you have another to load that better describes the event. When you unload a MIB the events in it disappear from the Event Definitions manager unless they have previously been altered and saved. In this case such MIB events remain with the *valid* field set to *false*. After you reload the MIB the valid field is set back to *true*.
- **Import**—Import an XML event definition.
- **Export**—Export an XML event definition for the selected rule.
- **Help**—Open the online help for this screen.

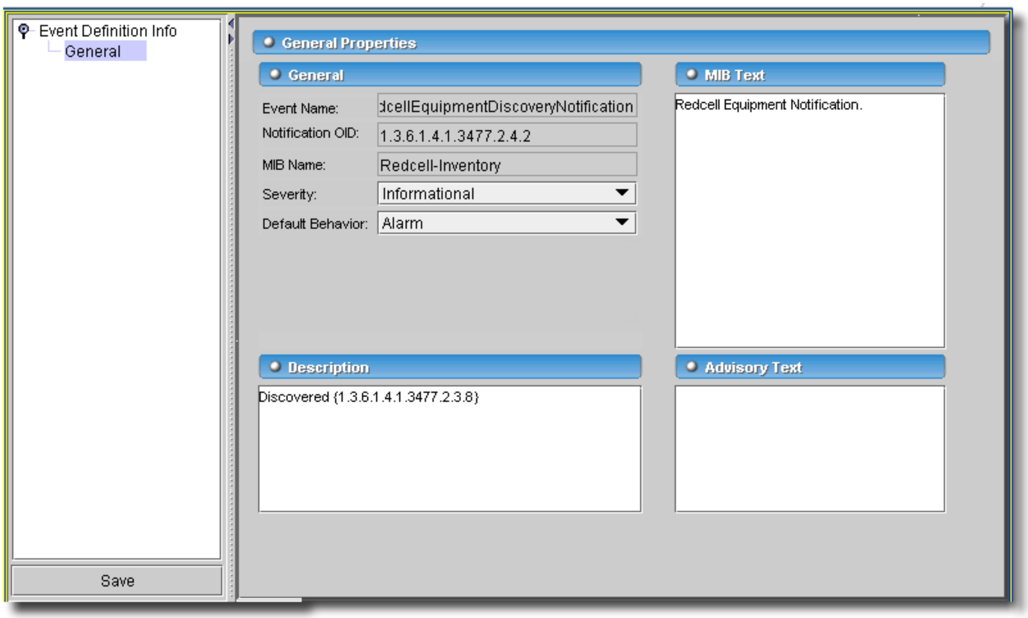
Detail Panels

Detail panels exist for editable text MIB Text and Advisory Text. You can also see listed *Event Processing Rules* that use this event, and their type. Select a rule and double-click or right-click and select *Open* to edit this rule as described in *Automation Event Processing Rule Editor or Correlation Event Processing Rule Editor*. Finally, you can configure a message to accompany this event with the *Event Message Template* detail panel. Click *Edit* to enter text, then *Apply* to accept it.

Event Definition Editor

This screen lets you edit the selected event.

Figure 16-6. Event Definition Editor - General



Event Name: dcellEquipmentDiscoveryNotification

Notification OID: 1.3.6.1.4.1.3477.2.4.2

MIB Name: Redcell-Inventory

Severity: Informational

Default Behavior: Alarm

Redcell Equipment Notification.

Discovered {1.3.6.1.4.1.3477.2.3.8}

This has the following panels:

- General
- Correlation

Event or Alarm correlation means locating existing alarms relevant to a new alarm and making the appropriate updates. If an event is suppressed, then the application performs no alarm correlation.

Alarms only correlate if they are for the same entity. By default, a new alarm correlate only against existing alarms for the same event type. You can augment the scope of existing alarms affected by a new alarm by adding correlated events in these screens. To further refine the alarms affected, you can correlate based on key bindings to an event definition. All event data indicated as a key binding must match for alarms to correlate.

NOTE: This means you can arrange for alarms from a device to only correlate if they come from, for example, a specified port.

Once a new alarm correlates to an existing alarm, the existing alarm is either closed or its count increases incrementally. Several factors have an impact on this behavior. Generally, the count of an existing alarm only increments for a new alarm of the same type, same message, and same key variable bindings.

The following describes the details in these panels

General

- **Event Name**—A read-only reminder of which event this is.
- **Notification OID**—The object identifier for the event.
- **MIB Name**—The name of the MIB in which this event's information appears.
- **Severity**—If the new alarm is a clearing severity, then any existing alarm to which it correlates is closed. Otherwise, if the new alarm severity does not match the existing severity then the existing alarm is closed and a new alarm opened for the new severity.
- **Default Behavior**—The default that occurs with this event. You can alter the default with the pick list (*Alarm*, *Suppress*, *Reject*).

MIB Text

This is a text field for a description of the event. You can override any default MIB description here.

Advisory Text

Editable Text to be sent with this event.

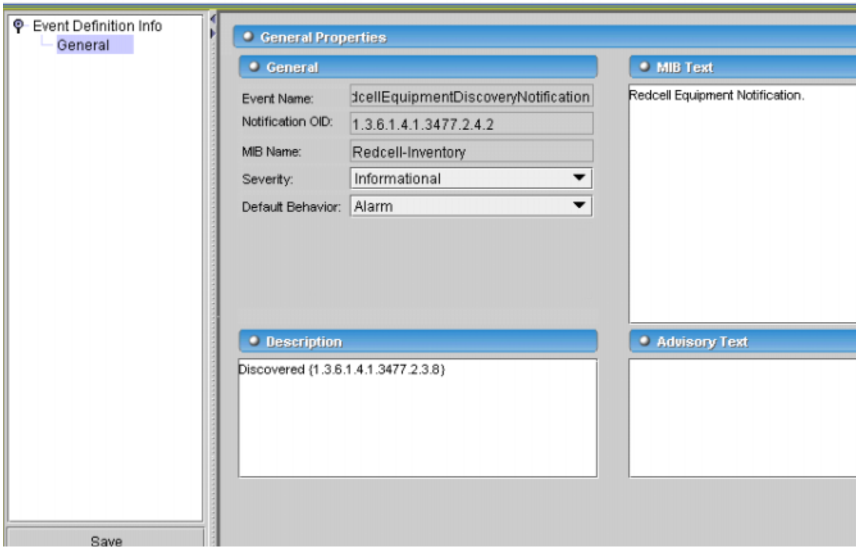
Message Template

This is a template for messages that accompany this event. If a message template exists for an existing, correlated alarm and the generated text does not match the original alarm, then the EMS closes the existing alarm, and generates a new one.

Correlation

This panel configures the events correlated with the definition you are configuring.

Figure 16-7. Event Definition Editor - Correlation



Event Name: dcellEquipmentDiscoveryNotification

Notification OID: 1.3.6.1.4.1.3477.2.4.2

MIB Name: Redcell-Inventory

Severity: Informational

Default Behavior: Alarm

Redcell Equipment Notification.

Discovered (1.3.6.1.4.1.3477.2.3.8)

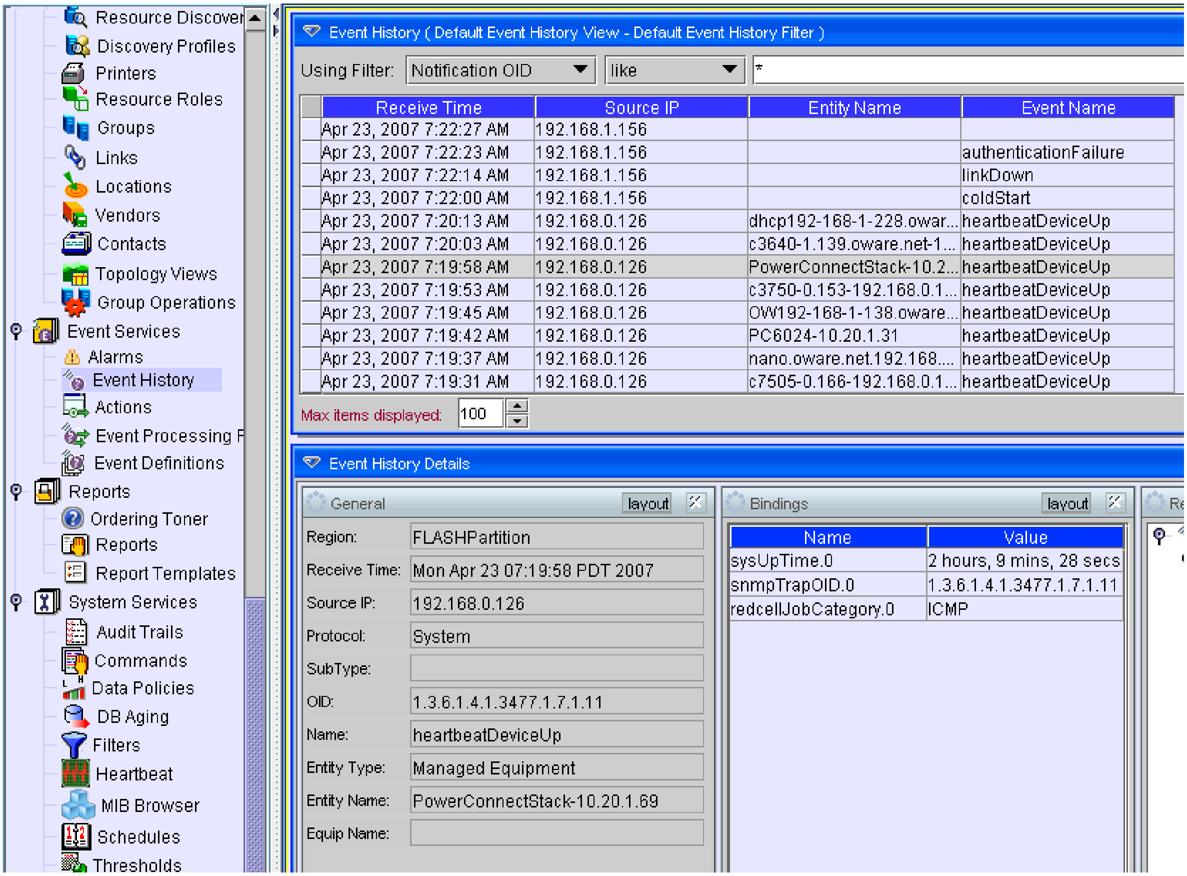
This screen lets you configure the following:

- **Correlated Events**—The list of events correlated with this one. Click *Add* to select events from those available, or *Remove* to delete a selected event.
- **Key Bindings**—This lists the varbinds correlated with this event. Move *Available Variables* (on the left) to *Key Variables* with the arrows between these two panels. The variables considered keys for correlation are the key bindings for the target alarm in the correlation process. This means that if event A is defined to include event B as a correlated event, comparison of the key bindings defined for event B is also considered when comparing a new alarm for event A to an existing alarm for event B.

Event History

The Event History manager, accessible from the navigation pane or *File* > *Open* > *System Services* menu, lets you see a comprehensive (or filtered) list of events within this application.

Figure 16-8. Event History



Event History (Default Event History View - Default Event History Filter)

Using Filter: Notification OID | like | *

Receive Time	Source IP	Entity Name	Event Name
Apr 23, 2007 7:22:27 AM	192.168.1.156		
Apr 23, 2007 7:22:23 AM	192.168.1.156		authenticationFailure
Apr 23, 2007 7:22:14 AM	192.168.1.156		linkDown
Apr 23, 2007 7:22:00 AM	192.168.1.156		coldStart
Apr 23, 2007 7:20:13 AM	192.168.0.126	dhcp192-168-1-228.owar...	heartbeatDeviceUp
Apr 23, 2007 7:20:03 AM	192.168.0.126	c3640-1.139.oware.net-1...	heartbeatDeviceUp
Apr 23, 2007 7:19:58 AM	192.168.0.126	PowerConnectStack-10.2...	heartbeatDeviceUp
Apr 23, 2007 7:19:53 AM	192.168.0.126	c3750-0.153-192.168.0.1...	heartbeatDeviceUp
Apr 23, 2007 7:19:45 AM	192.168.0.126	OW192-168-1-138.oware...	heartbeatDeviceUp
Apr 23, 2007 7:19:42 AM	192.168.0.126	PC6024-10.20.1.31	heartbeatDeviceUp
Apr 23, 2007 7:19:37 AM	192.168.0.126	nano.oware.net.192.168....	heartbeatDeviceUp
Apr 23, 2007 7:19:31 AM	192.168.0.126	c7505-0.166-192.168.0.1...	heartbeatDeviceUp

Max items displayed: 100

Event History Details

General

Region:	FLASHPartition
Receive Time:	Mon Apr 23 07:19:58 PDT 2007
Source IP:	192.168.0.126
Protocol:	System
SubType:	
OID:	1.3.6.1.4.1.3477.1.7.1.11
Name:	heartbeatDeviceUp
Entity Type:	Managed Equipment
Entity Name:	PowerConnectStack-10.20.1.69
Equip Name:	

Bindings

Name	Value
sysUpTime.0	2 hours, 9 mins, 28 secs
snmpTrapOID.0	1.3.6.1.4.1.3477.1.7.1.11
redcellJobCategory.0	ICMP

The top of this screen displays a list of events.By default it displays all events but you can use filters to limit the list that appears. As is typical for these displays, you can also sort by the column name by clicking on the heading of columns (clicking repeatedly toggles the sort order between descending and ascending).

Columns that appear in this table are described in General and Alarm Table Columns.General

Right-click an event, or click the *Action* menu for the following options:

- **Open > Event Detail—**This opens an alarm viewer (see Editing Event History Entity).
- **Open > Entity—**This opens an editor where you can configure the entity from which this alarm came.
- **Open > Equipment—**This opens an editor where you can configure the device (where the Entity may be a subcomponent) from which this alarm came.
- **Open > Event Definition—**This opens an editor where you can configure the device from which this alarm came. See Event Definitions.
- **Open > Processing Rules**—This opens rule manager filtered to display only the rules associated with the selected Event. See "Event Processing Rules" on page 188 for more about what additional action you can take.
- **Map**—Open a topology view displaying the equipment selected alarm(s) came from.See Topology. on page 153
- **Print**—This lets you print the listed events to a pdf file. For this to work correctly, you must have Acrobat installed. To change the contents of this report, change the filter.
- **Help**—Opens the online help for this screen.

When you select an event, its details appear in the detail panels below.

- General
- Bindings
- Reference Tree
- Description

The following sections describe these panels.

General

The first panel displays general information. this includes the following fields:

- **Region**—The partition the notification came from.
- **Receive Time**—The time the event was received and its time zone
- **Source IP**—Its source's IP address.
- **Entity Name**—The name of the entity referred to in the event. Its identity depends on the event configured.
- **Type**—The event's type. (*Subtype* describes SNMPv2 *inform/traps*)
- **Name**—The event's instance identifier.
- **Entity Type**—The event's entity type.
- **Entity OID**—The event's entity object identifier. The entity can differ from the source, for example, if this software wraps a northbound trap.

Bindings

This panel displays the variable binding name and value pairs that accompany the event. The contents of this panel depend the event's configuration. Bindings have appended an identifying number that displays the instance of the event for this binding.

Reference Tree

This panel displays any connections between this event and correlated rules and/or actions in tree form. Click the turner to the left of any node to display the tree. below that node. Double-click or right-click a node and select *Open* and you can edit that component .

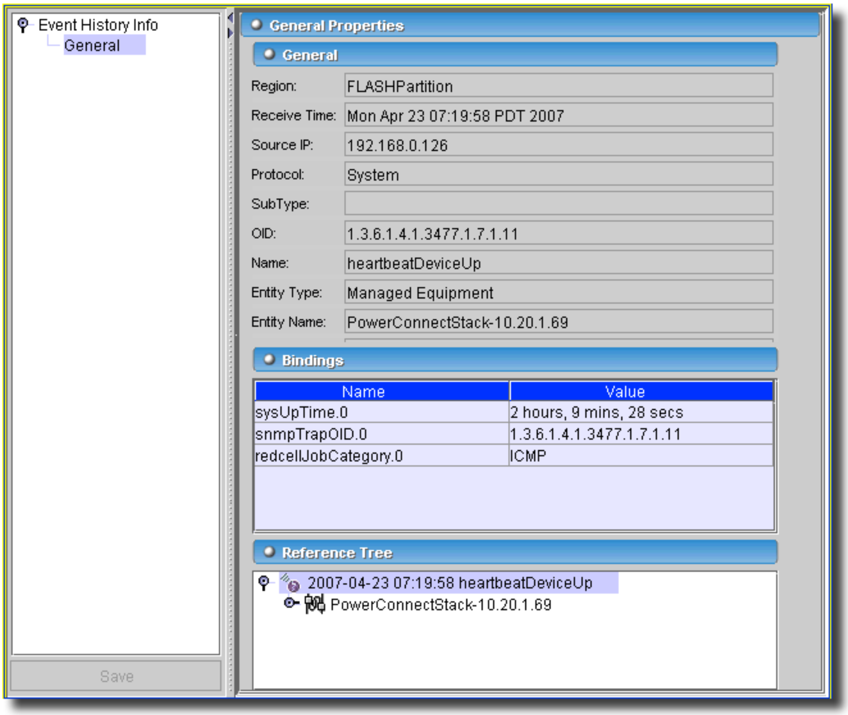
Description

This panel contains a description of the selected event.

Editing Event History Entity

This screen displays the information about a selected event when you click *Open*.

Figure 16-9. Editing Event History Entity



Region: FLASHPartition
Receive Time: Mon Apr 23 07:19:58 PDT 2007
Source IP: 192.168.0.126
Protocol: System
SubType:
OID: 1.3.6.1.4.1.3477.1.7.1.11
Name: heartbeatDeviceUp
Entity Type: Managed Equipment
Entity Name: PowerConnectStack-10.20.1.69

Name	Value
sysUpTime.0	2 hours, 9 mins, 28 secs
snmpTrapOID.0	1.3.6.1.4.1.3477.1.7.1.11
redcellJobCategory.0	ICMP

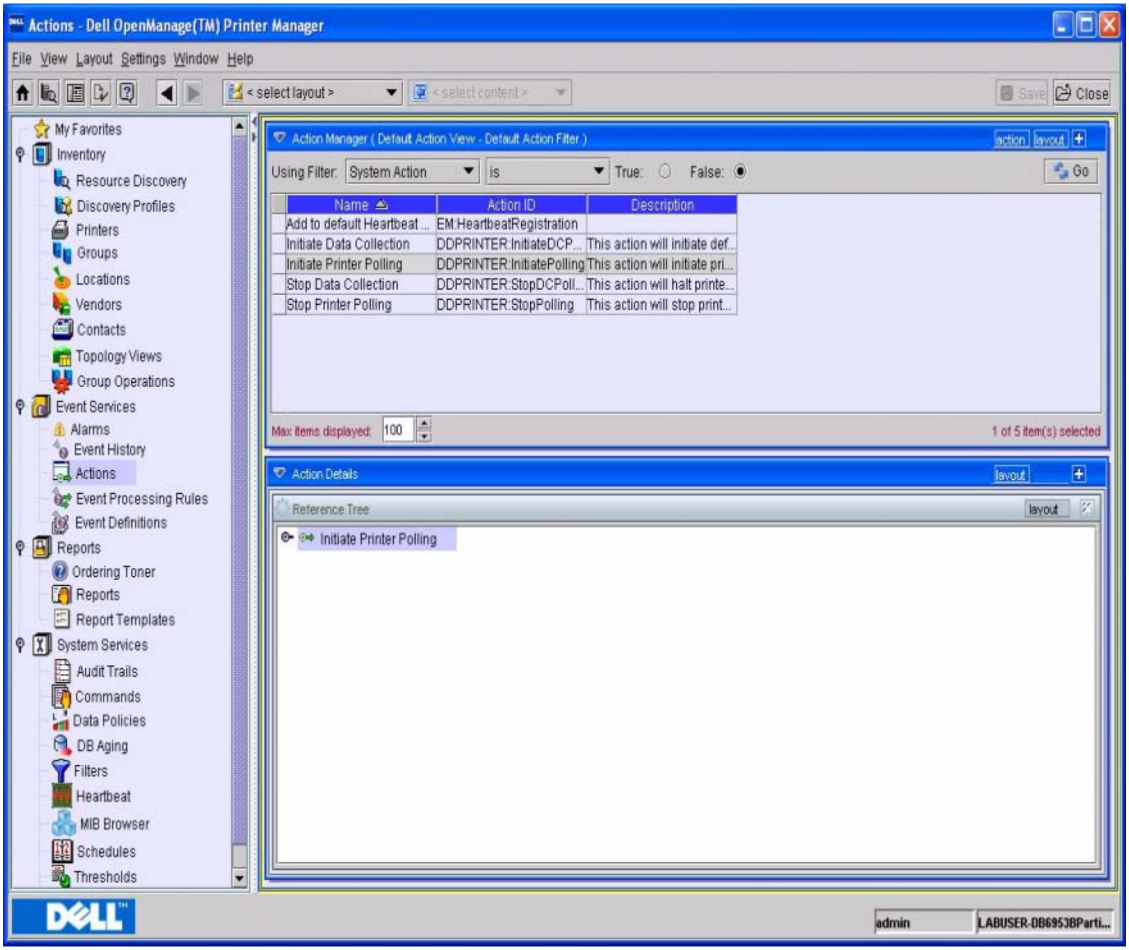
2007-04-23 07:19:58 heartbeatDeviceUp
PowerConnectStack-10.20.1.69

This screen displays the information visible in the General, Bindings and Reference Tree details panels.

Actions Manager

Open Actions Manager by clicking it in the navigation window.

Figure 16-10. Actions Manager



Using Filter: System Action is True: ○ False: ●

Name	Action ID	Description
Add to default Heartbeat ...	EM:HeartbeatRegistration	
Initiate Data Collection	DDPRINTER:InitiateDCP...	This action will initiate def...
Initiate Printer Polling	DDPRINTER:InitiatePolling	This action will initiate pri...
Stop Data Collection	DDPRINTER:StopDCPoll...	This action will halt printe...
Stop Printer Polling	DDPRINTER:StopPolling	This action will stop print...

Max items displayed: 100

1 of 5 item(s) selected

Initiate Printer Polling

This screen displays a filtered list of actions. As in a typical manager, the filter is at the top of the screen, in this case in conjunction with *Name*, *Action ID*, *Description* and *System Action* (*True/False* radio buttons) criteria. System actions are unalterable actions available throughout this software's system.

In this screen, you can configure actions that will respond to events. The manager has the following menu items (accessed with the *Action* button, or a right-click):

- New—Opens the Action Editor, through which you can define a new Action. See Action Editor for more information.

- **Open**—Opens the selected Action for modification. See Action Editor for more information.
- **Delete**—Deletes the selected action. Select the action to remove and click *Delete*. The application prompts you for confirmation.
- **Copy**—This copies the selected action and opens the editor. You must rename it to begin with something other than "CopyOf [Original Name]" (its default name) before you can save the action.
- **Print**—Print the listed correlations to an Acrobat file. (You must have Acrobat reader installed for this to work properly.) Change the filter and click *Go* to change this printed report's appearance.
- **Export/Import**—Export or import the action as/from XML.
- **Help**—Open the context-sensitive help for this screen.

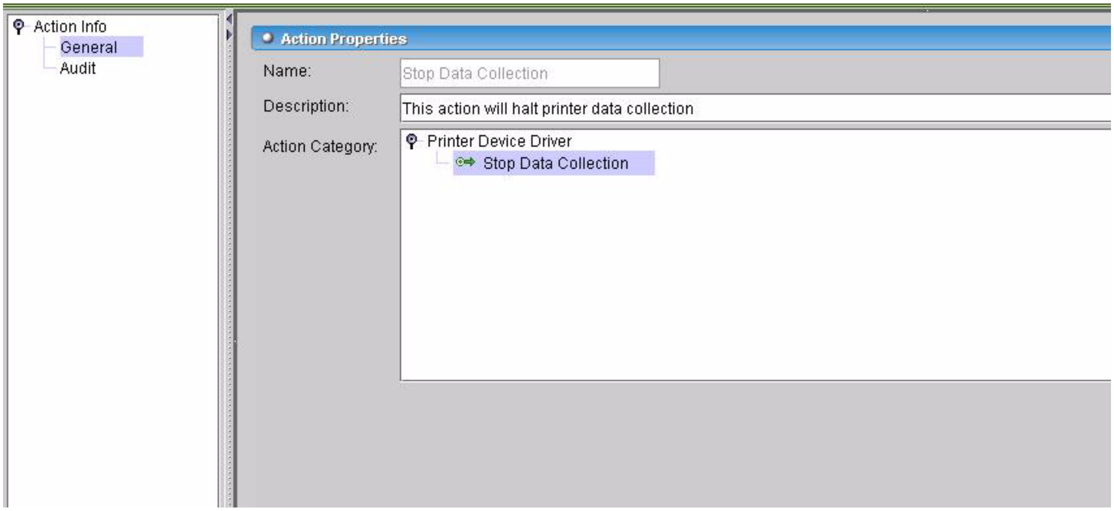
Action Details

The lowest portion of this layout contains a detail panel with a reference tree for the selected action that displays any related events and event processing rules.

Action Editor

When you click *New* or *Open* in Action Manager, you open the Action Editor. Here, you can configure the kind of action you want to respond to internal actions within this EMS.

Figure 16-11. Action



Name: Stop Data Collection

Description: This action will halt printer data collection

Action Category: Printer Device Driver > Stop Data Collection

Actions are, in effect, global group operations for the devices in question. The screen where you configure them has the following fields:

Action Properties

- **Name**—A unique identifier for the action.
- **Action Category**—Select from the tree. This selection determines the fields that appear in the lower portion of the screen (many selections make no fields appear). Examples of categories available includes options that vary depending on what options you have installed. The lowest panel in this screen changes, depending on the selection you make. Those selections are like the following:

  Event Management

  - *Equipment Heartbeat Registration*—Specify the heartbeat policy with the command button (...). It opens a selection screen.
  - *Execute Command*—Specify the command executable with the command button (...). It opens a selection screen.
  - *Forward Northbound as SNMP v2*—Specify the destination address, port and SNMP community string.

  Printer Device Driver

  - *Initiate Data Collection*—This starts data collection for the printer.
  - *Initiate Printer Polling*—This starts polling the printer.
  - *Stop Data Collection*—This stops data collection on the printer.
  - *Stop Printer Polling*—This stops polling the printer.

  Redcell Common Services

  - *Email*—Specify a destination address, then click *Add*. You can specify more than one, and specify a header/footer and e-mail message to be triggered by correlation.

Click *Save* once you have configured the action as you would like, or click *Close* (in the toolbar) to abandon your edits.

The *Audit* tab displays a history of the action related to this link.

17

Schedules

Introducing Scheduling

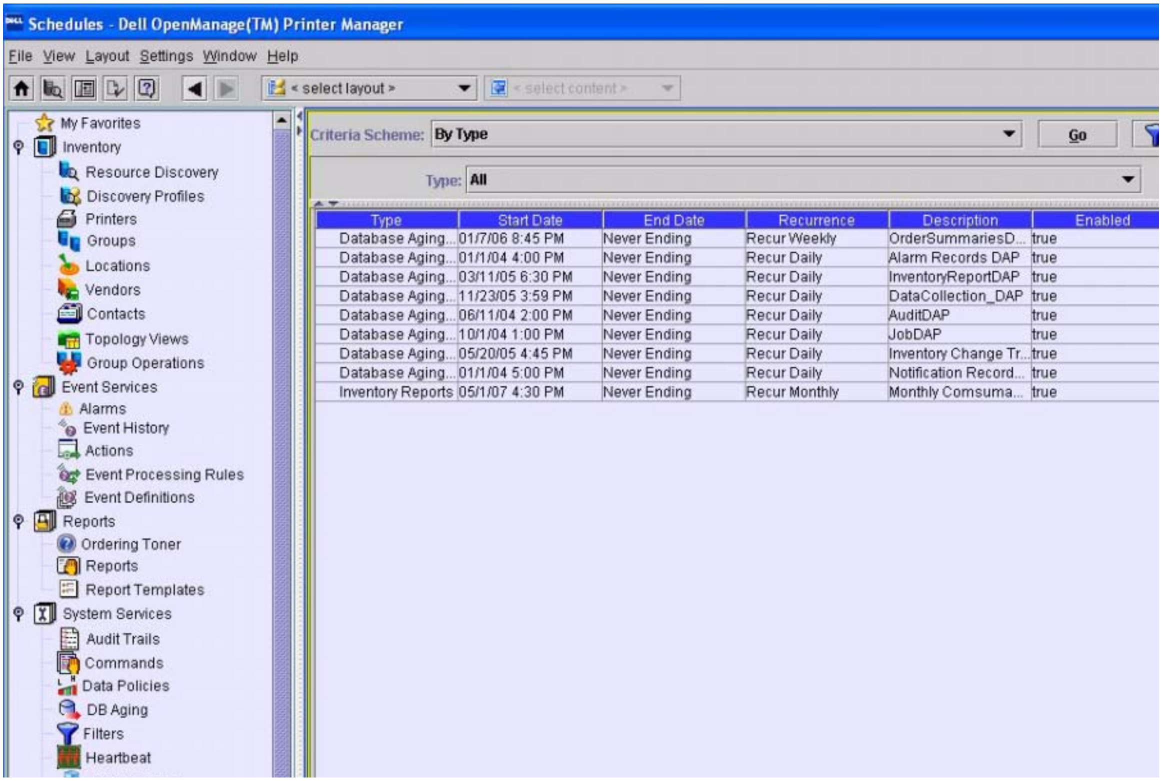
You can schedule a variety of actions with this application. The following sections describe how to do this.

NOTE: Use Group Ops to schedule operations on more than one device at the same time instead of scheduling multiple individual operations at the same time.

Schedules

Use the Schedules screen to set the start and stop time, as well as any recurrence pattern for processes that support this feature. You can *Edit*, *Execute* and *Delete* scheduled items in the Schedules screen (under the *System Services* node of the navigation window or from **File**→ **Open**→ **System Services**→ **Schedules**).

Figure 17-1. Schedules screen



Criteria Scheme: By Type

Type: All

Type	Start Date	End Date	Recurrence	Description	Enabled
Database Aging...	01/7/06 8:45 PM	Never Ending	Recur Weekly	OrderSummariesD...	true
Database Aging...	01/1/04 4:00 PM	Never Ending	Recur Daily	Alarm Records DAP	true
Database Aging...	03/11/05 6:30 PM	Never Ending	Recur Daily	InventoryReportDAP	true
Database Aging...	11/23/05 3:59 PM	Never Ending	Recur Daily	DataCollection_DAP	true
Database Aging...	06/11/04 2:00 PM	Never Ending	Recur Daily	AuditDAP	true
Database Aging...	10/1/04 1:00 PM	Never Ending	Recur Daily	JobDAP	true
Database Aging...	05/20/05 4:45 PM	Never Ending	Recur Daily	Inventory Change Tr...	true
Database Aging...	01/1/04 5:00 PM	Never Ending	Recur Daily	Notification Record...	true
Inventory Reports	05/1/07 4:30 PM	Never Ending	Recur Monthly	Monthly Comsuma...	true

This manager uses typical filtering . You can also select **File→ Import and Export** back up schedules or configure other systems.

⚠ **CAUTION: Best practice is to spread out jobs occurrences rather than concentrating them in a narrow period. This conserves computing resources and avoids bottlenecks. You can schedule a large number of devices within a small recurring time. Operations (like pinging all the devices) may take longer than the allotted time. If that is the case, the system will continue to work on the jobs sequentially and will create a backlog of devices. The system will continue to process the data; if this is combined with a network slowdown, it is possible that this may cause resource issues within the application server itself.**

New Schedules

When you click *New*, the application prompts you for the type of schedule to create (available types depend on your installation). Depending on the type you select, the next screen changes. *Device Resync* and *Device Discovery* are the default scheduled task types available. The Schedule Info is common to all schedules.You can schedule several things, including the following tasks:

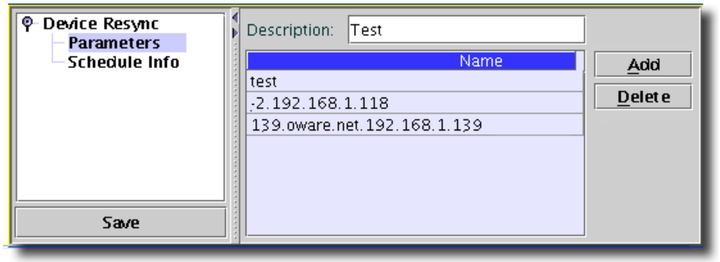
- **Database Aging Policy—**Policy implementation.
- **Device Discovery**—Device discovery.

- **Device Resync**—See Resynchronization, below.
- **Firmware Download**—Schedules updates from supported Firmware suppliers.
- **Group Operation**—Schedule a group operation.

Resynchronization

If you select *Device Resync* when creating a new schedule, you can select devices to re-query (resync) so the database contains the latest device configuration.

Figure 17-2. Resynchronization Scheduler



Description: Test

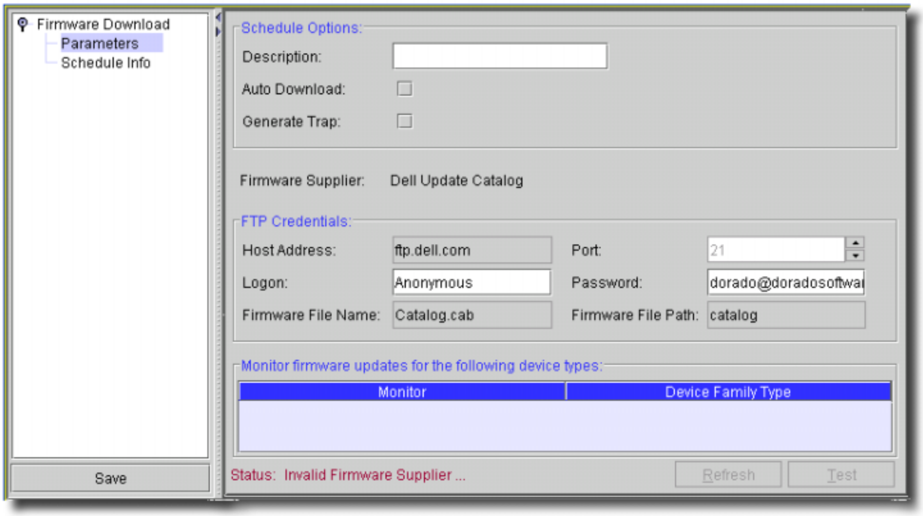
Name
test
-2.192.168.1.118
139.oware.net.192.168.1.139

Type the *Name* of the schedule, then click *Add* to select devices for this resynchronization. The *Schedule Info* tab is where you set the schedule times.

Firmware Download

If you select this scheduling firmware download, and have a supplier who supports automated downloads of firmware, you can configure that download with this screen.

Figure 17-3. Schedule Firmware Download Parameters



Schedule Options:

Description:

Auto Download: □

Generate Trap: □

Firmware Supplier: Dell Update Catalog

FTP Credentials:

Host Address:	ftp.dell.com	Port:	21
Logon:	Anonymous	Password:	dorado@doradosoftwa
Firmware File Name:	Catalog.cab	Firmware File Path:	catalog

Monitor firmware updates for the following device types:

Monitor	Device Family Type

Status: Invalid Firmware Supplier ...

You can configure the following with this screen:

Schedule Options

Description—A text identifier for the scheduled download.

Auto Download—Check to activate automated download.

Generate Trap—Check to activate trap generation on download.

Firmware Supplier—The vendors known to support this feature (currently: none support scheduled downloads).

FTP Credentials

Host Address / Port—The address and port for FTP connection. The default port is 21.

Logon / Password—The FTP logon / password combination.

Firmware File Name / Path—The name of the firmware file and path.

Monitor firmware updates for the following device types

Select (or multi-select with Ctrl+Click) devices for which you want firmware updates. Click Refresh to update the list, and Test to test the download.

Discovery

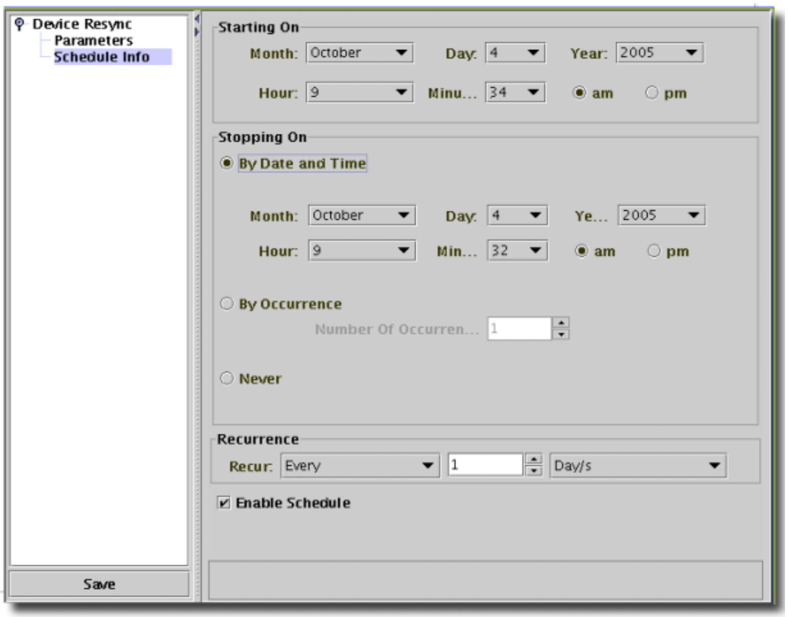
If you schedule *Discovery*, then you can select a discovery profile (see *Discovery Profiles* on page 60).

Schedule Info

The *Schedule Info* screen is the same, regardless of the kind of task you schedule. Consult the appropriate application manuals for information about parameters screens. Click the *Save* icon (or **File**→ **Save**) to confirm your selection. Click the **Close** icon (**File**→ **Close**, or Ctrl + F4) to close without saving.

You can also schedule items from the items' creation dialog. When you create a new schedule, from whatever location, you can see the *Schedule* dialog's *Schedule Info* screen.

Figure 17-4. Schedule Info Screen



Starting On

Month: October Day: 4 Year: 2005

Hour: 9 Minu... 34 ● am ○ pm

Stopping On

● By Date and Time

Month: October Day: 4 Ye... 2005

Hour: 9 Min... 32 ● am ○ pm

○ By Occurrence

Number Of Occurren... 1

○ Never

Recurrence

Recur: Every 1 Day/s

☑ Enable Schedule

The following are the fields on the Schedule Info dialog:

- **Starting On**—This section defines the date and time when the schedule becomes active. Select values for Month, Day, Year, Hour, and Minute from the appropriate drop-down lists.
- **Stopping On**—This section defines when the schedule stops being active. Select one of the following options:
    - **By Date and Time**—Select this option, then select the Month, Day, Year, Hour, and Minute from the appropriate drop-down lists.
    - **By Occurrence**—Select this option, then specify the number of occurrences of the scheduled process after which it becomes inactive.
    - **Never**—Select this option to specify that the scheduled process never stop.
- **Recurrence**—The Recurrence section determines how often the schedule recurs in relation to the settings in the Stopping On section.

  - **Recur**—Select a recurrence option. Available options are *Every*, *Only Once*, *Increment* (by minute), *Only at Startup*. If you select *Every*, specify an interval. The following are interval options: *Minute/s*, *Weekend Day/s*, *Hour/s*, *Week/s*, *Day/s*, *Month/s*, *Weekday/s*, *Year/s*

- **Enable Schedule**—Uncheck this to disable the schedule. By default it is enabled.

Click the **Save** button (or toolbar icon) to save this schedule to the database.

18

Filters

.

Table 18-1. Wildcard Characters

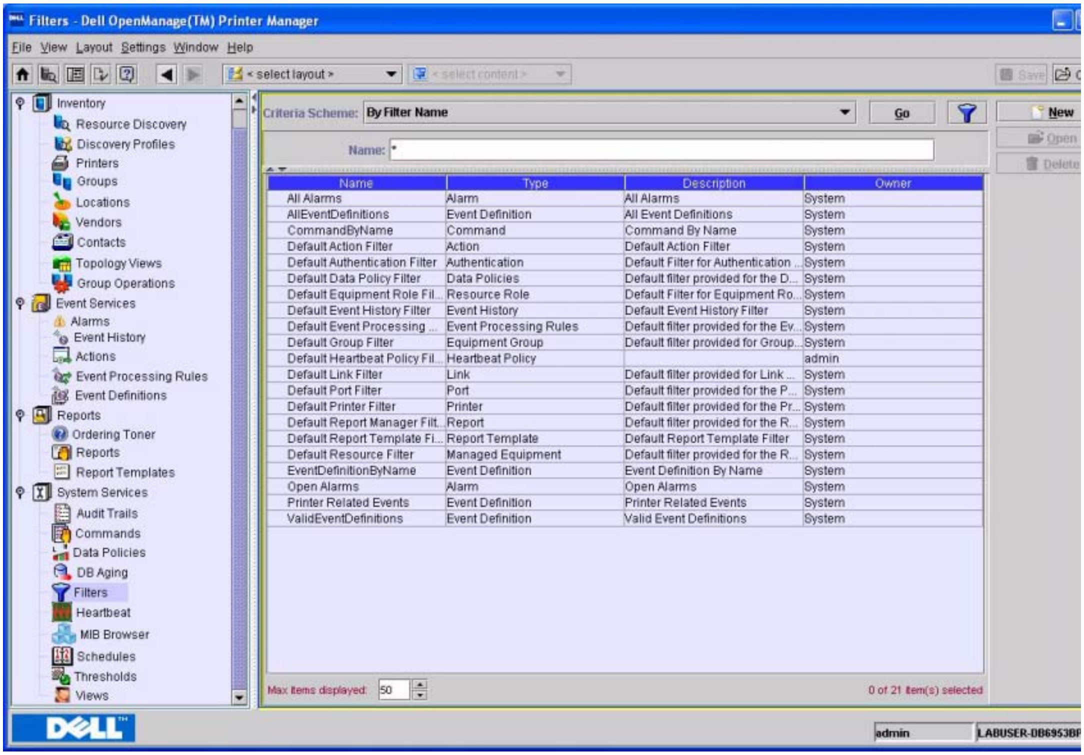
Character	Usage
*	Matches any sequence of characters in a string, including an empty sequence.
?	Matches any single character in a string.
\x	Matches the single special character “x.” This provides a way of avoiding the special interpretation of the asterisk (*), **question mark (?) or bracket characters** ([ ]) in a pattern.

Filters

Managers typically use filters to reduce the number of records shown.You can configure the filters that appear by default in the application’s managers with the Filters screen, and through the key icon at the top of many managers.

Access Filters screen through the navigation window or through **Settings→ Configuration→ Filter Config**.

Figure 18-1. Filters screen



Criteria Scheme: By Filter Name

Name: *

Name	Type	Description	Owner
All Alarms	Alarm	All Alarms	System
AllEventDefinitions	Event Definition	All Event Definitions	System
CommandByName	Command	Command By Name	System
Default Action Filter	Action	Default Action Filter	System
Default Authentication Filter	Authentication	Default Filter for Authentication ...	System
Default Data Policy Filter	Data Policies	Default filter provided for the D...	System
Default Equipment Role Fil...	Resource Role	Default Filter for Equipment Ro...	System
Default Event History Filter	Event History	Default Event History Filter	System
Default Event Processing ...	Event Processing Rules	Default filter provided for the Ev...	System
Default Group Filter	Equipment Group	Default filter provided for Group...	System
Default Heartbeat Policy Fil...	Heartbeat Policy		admin
Default Link Filter	Link	Default filter provided for Link ...	System
Default Port Filter	Port	Default filter provided for the P...	System
Default Printer Filter	Printer	Default filter provided for the Pr...	System
Default Report Manager Filt...	Report	Default filter provided for the R...	System
Default Report Template Fi...	Report Template	Default Report Template Filter	System
Default Resource Filter	Managed Equipment	Default filter provided for the R...	System
EventDefinitionByName	Event Definition	Event Definition By Name	System
Open Alarms	Alarm	Open Alarms	System
Printer Related Events	Event Definition	Printer Related Events	System
ValidEventDefinitions	Event Definition	Valid Event Definitions	System

Max items displayed: 50

0 of 21 item(s) selected

For the *Basic Filter Editor*, in screens like *Group Operations*, click the filter (funnel) icon to edit an existing or create a new filter.

To create a new filter or modify an existing one in Filter Manager, you can click **New** or **Open** (to edit a selected existing filter), or you can click on the Filter command button (a key icon that appears in various locations, depending the screen). You can create or edit filters with the following editors.

- Filter Editor—For newer screens.
- Basic Filter Editor—For basic screens.

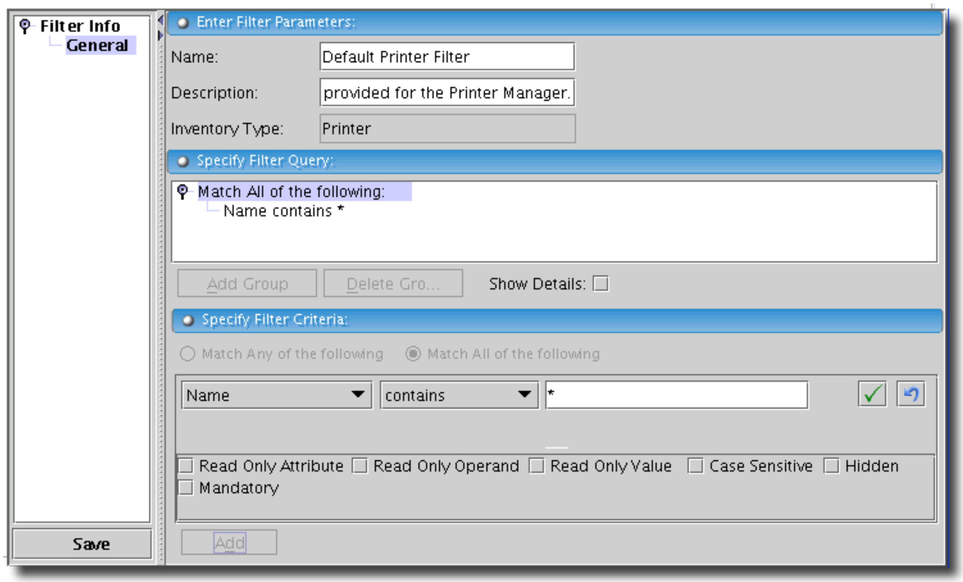
See also "Filter Wildcards" on page 215 for supported features within filters.

This application also supports view filters as described in "Filtering" on page 34.

Filter Editor

When you click the **New** menu at the top of the filter manager, you can elect to create new (or with Open ,edit existing) filters.

Figure 18-2. Filter Editor



Name: Default Printer Filter

Description: provided for the Printer Manager.

Inventory Type: Printer

Match All of the following:
Name contains *

○ Match Any of the following ● Match All of the following

Name ▾ contains ▾ *

□ Read Only Attribute □ Read Only Operand □ Read Only Value □ Case Sensitive □ Hidden
□ Mandatory

For example, you could request all equipment where the *Name* field contains the word “oware” or a wildcard (asterisk [*] means any combination of characters). The *Add / Delete* group buttons let you use group functionality, creating advanced filtering. For example you could match all values within Group 1 but any values within Group 2. For example, Group 1 could match “vendor = 'Dell'” and Group 2 could match “model number starts with '20' OR firmware version contains '2'”.

To add criteria, first click **Add Group** in the upper panel. The *Filter Attributes* radio buttons (*Match Any of the Following* or *Match All of the Following*) determine the next part of the filter’s operation.

The **Show Details** check box displays additional filter information to the right of listed criteria as they appear in the upper panel. This information displays codes for additional filtering properties you can select when you create the filter components in the lowest panel.

Available detail codes depend on the data type filtered. The *AND*ed or *OR*ed sum of the filter components' codes appears at the top level node. The codes for these attributes are the following:

Code	Meaning	Comment
H or V	Hidden / Visible	
ROO or WRO	Read Only / Read-Write Operand	
ROA or WRA	Read Only / Read-Write Attribute	
ROV or RWV	Read Only / Read-Write Value	Grays out the operand and attribute checkboxes since those are not functional if you make this read-only.
ROO or WRO	Read Only / Read-Write Operand	
ROA or WRA	Read Only / Read-Write Attribute	
M or O	Mandatory / Optional	
EL or IL	Exclude / Include Low	Valid only when you select a range of values. This determines whether you include or exclude the endpoint of the range
EH or IH	Exclude / Include High	Valid only when you select a range of values. This determines whether you include or exclude the endpoint of the range
CS or NC	Case Sensitive / Not Case Sensitive	Does not appear for numeric values.
ML or NM	Multi-line Support / No Multi-Line Support	Filter on multiple-line values (or not).

When you select *Read Only* for an attribute, operand or value, some additional impacts are that, for example, reports ordinarily let you alter filters when you manually execute them, but if they have only read-only filtering, then the report executes immediately without a pause to alter filtering.

Specifying the remaining filtering occurs when you click **Add** at the bottom of this screen. Enter attribute / operand / value combinations after clicking **Add**. To edit an existing filtered item, select the node above it and click the **Edit Filter Criteria** button (sheet of paper icon) in the lowest panel. You can delete it with the red X.

Filter Wildcards

This application supports wildcard characters for specifying entity searches of the various list fields. When applying filters to lists of objects in the application, youcan use the listed wildcard characters as part of the search criteria:

Character	Usage
*	Matches any sequence of characters in a string, including an empty sequence.
?	Matches any single character in a string.
\x	Matches the single special character "x." This provides a way of avoiding the special interpretation of the asterisk (*), **question mark (?) or bracket characters** ([ ]) in a pattern.

Filters appear at the top of most managers and inventory screens, to limit displayed

items.

Filter Wildcard Examples

If you want to match white, which and whole, then enter the filter string wh*

If you want to match fee, fie, and foe, then enter the filter string f?e.

If you want to match a special character like the asterisk or question mark then enter a backslash preceding that character. To match f**, then, you would enter a filter string like f**.

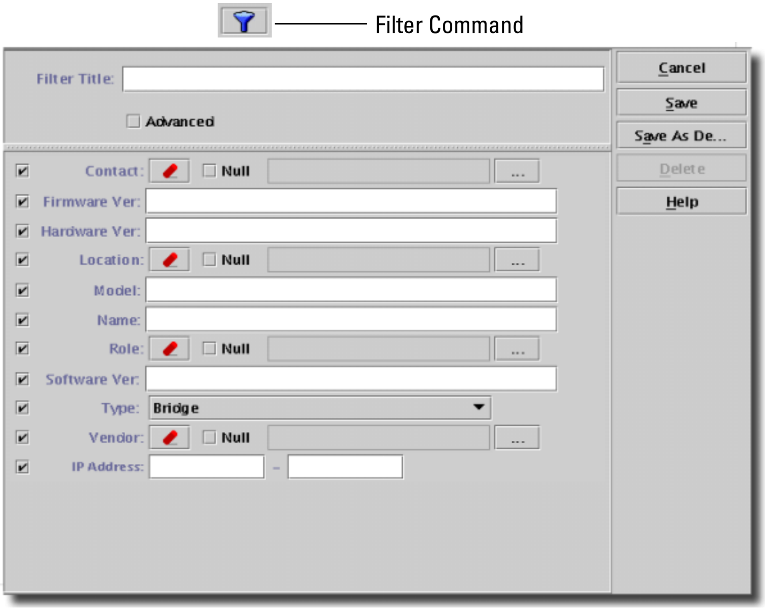
You can also combine filter strings. The string P?n* would match Pine, or Pinetop,for example.

Basic Filter Editor

In addition to clicking *New* in the Filters screen, you can create a new filter name byclicking the Filter Command Button (looks like a blue funnel) at the top of a manager, and then selecting ****New**** from the filter pick list at the top of the next screen.Enter a name in the empty *Filter Name* field that replaces the pick list, and enter filter criteria where appropriate. To modify an existing filter, select it from the *Filter Name* drop-down list and modify the appropriate filter criteria.

The data screen configures the actual filter. Its appearance varies, depending on the manager from which you configure the filter.

Figure 18-3. Key Icon Filter Editor



Filter Command

☑ Type: Bridge

NOTE: The filter may contain custom fields

Check the box to the left of each item to use it in the filter. Notice that fields are disabled, unless you check this box. The *Null* checkbox to the right of the field eraser means this filter selects only items without that value.

The following items are potential fields for the filter to match:

- **Contact**—Click on the command button to select a contact.
- **Firmware ver**—The firmware version (text).
- **Hardware ver**—The hardware version (text).
- **Location**—Click on the command button to select a location.
- **Model**—The equipment's model designation (text).
- **Name**—Enter a name or portion of a name.
- **Role**—From the drop-down list, select an equipment role.
- **Software ver**—The software version (text).
- **Type**—Select an equipment type from the drop-down list.
- **Vendor**—Click on the command button to select a vendor.
- **IP Address**—The IP Address (range) of the device (text).

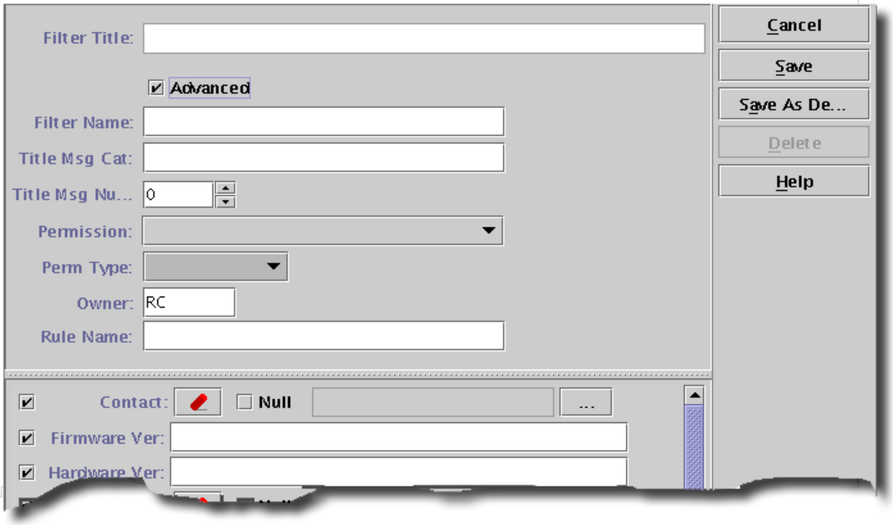
Click on **Set as Default** to set the selected filter as the default view. Clicking **Set as Default** means the configured filter automatically appears each time this screen opens. Click on **Save** to save and apply the filter. The list of items appears based on the filter you created, and the manager from which you open the filter.

NOTE: A default set of filters comes with the application. Criteria vary, depending on the manager.

Advanced Settings

This portion of the Filter Editor screen appears when you check the **Advanced** checkbox in the Filter editor. This checkbox only appears when you select a ****New**** filter, from the *Filter Title* pick list. Permission to configure these aspects of filtering is typically confined to application administrators and developers. When permissions are unavailable, the *Advanced* checkbox does not appear.

Figure 18-4. Filter Advanced Settings



Filter Title:

☑ Advanced

Filter Name:

Title Msg Cat:

Title Msg Nu... 0

Permission:

Perm Type:

Owner: RC

Rule Name:

☑ Contact: □ Null ...

☑ Firmware Ver:

☑ Hardware Ver:

This sub-panel the has the following fields:

- **Filter Title**—The title that appears with the filter.
- **Filter Name**—A unique identifier for the filter.
- **Title Msg Cat:**—The message categories that are defined in messages properties file `rcmsgsusenglish`. For Example: `RC_GENERAL, RC_EQUIPMENT, RC_QUERYNAMES`.
- **Title Msg Num**—A read-only field displaying the message number. The message numbers that are defined in messages properties file `rcmsgsusenglish`. For Example: `RC_GENERAL.11, RC_EQUIPMENT.43, RC_QUERYNAMES.10`

- **Permission**—Use the pick list to select you can select the permissions required for this filter to appear, or be applied.
- **Permission Type**—Select a permission type (*Add*, *Delete*, *Execute*, *Read*, *Write*).
- **Owner**—The owner of this filter is the product/component to which this filter belongs; in other words the product/component which creates this filter. For Example “RC” for redcell, and so on.
- **Rule Name**—The rule name along with its package, which does the query for this filter.

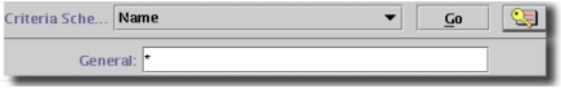
Click *Save* to persist the filter configuration your edits make.

NOTE: Exporting advanced filter options exports the Title Message category and number, but not the file to which they refer.

Quick Searches

Once you define a filter you can use a Quick Search defined there. For example, to create a Quick Search using Equipment Name, create a Filter called *Search by Name* and check the Name checkbox under the filter criteria. Do not enter a value in the text field. When you return to the Manager, you can see the *Name* field under the Filter drop-down list.

Figure 18-5. Filter Name Field



Criteria Sche... Name

General: *

Enter criteria for the Quick Search and click on *Go*.

19

Views

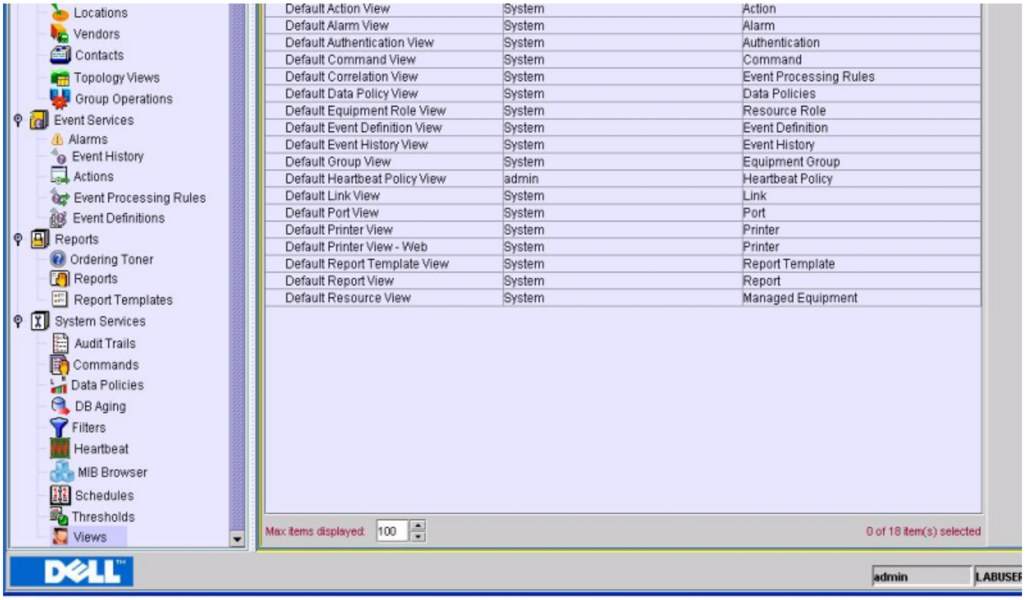
Introducing Views

To further tailor displays to your preferences, you can create and manage views. These specify columns that appear in managers, inventories and other displays.

Views

With the Views screen, you can arrange views, specifying visible columns and their order, for some inventory and manager screens.

Figure 19-1. Views screen



Default Action View	System	Action
Default Alarm View	System	Alarm
Default Authentication View	System	Authentication
Default Command View	System	Command
Default Correlation View	System	Event Processing Rules
Default Data Policy View	System	Data Policies
Default Equipment Role View	System	Resource Role
Default Event Definition View	System	Event Definition
Default Event History View	System	Event History
Default Group View	System	Equipment Group
Default Heartbeat Policy View	admin	Heartbeat Policy
Default Link View	System	Link
Default Port View	System	Port
Default Printer View	System	Printer
Default Printer View - Web	System	Printer
Default Report Template View	System	Report Template
Default Report View	System	Report
Default Resource View	System	Managed Equipment

Max items displayed: 100

0 of 18 item(s) selected

admin

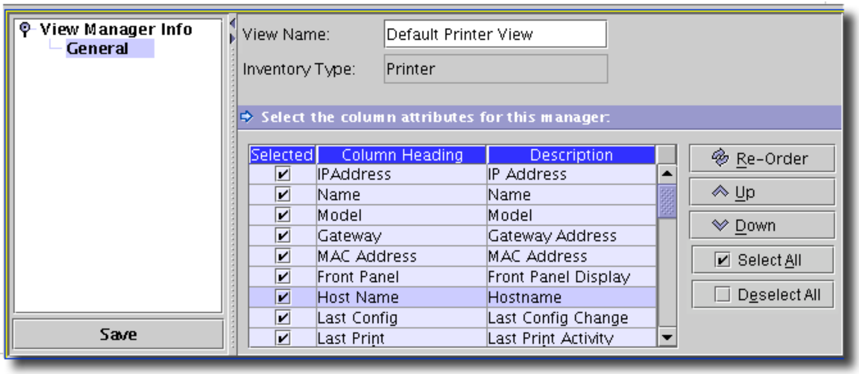
LABUSER

As with most managers, the top of this screen lets you filter the list of views, limiting it to those most useful for you. Click **New** to create a new view, or *Open* to edit a selected view. Click **Delete** to remove a selected, listed view.

View Editor

When you click **New** or **Open** in view Manager, the View Editor appears.

Figure 19-2. View Editor



View Name: Default Printer View

Inventory Type: Printer

Selected	Column Heading	Description
☑	IPAddress	IP Address
☑	Name	Name
☑	Model	Model
☑	Gateway	Gateway Address
☑	MAC Address	MAC Address
☑	Front Panel	Front Panel Display
☑	Host Name	Hostname
☑	Last Config	Last Config Change
☑	Last Print	Last Print Activity

Views apply to some managers (currently Contact, Vendor, Location, Port, and Printer) This screen has the following fields:

- **View Name**—A unique identifier for the view.
- **Inventory Type**—Select the type of inventory on the pick list. The effects of the view modifications are available when you open the manager for this type of inventory.

Select the column attributes for this manager

Below this is a list of available attributes for the selected inventory type's manager. Check the **Selected** column to include a row as the columns that appear in the manager, when open. Select a row and use the *Up/Down* arrows to the right of this list to re-order the list. The **Re-Order** button moves selected columns to the top of those listed.

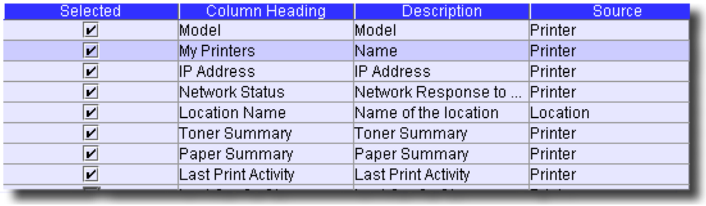
Click **Save** to preserve the view in the database. When you open the manager for the inventory type selected for the first time, the default view appears. After the first time you open a manager, the last view selected persists. This is connected to the login user. All *Admin* users, for example, would see each others' changes.

NOTE: Creating several admin users would preserve selected views.

Column Titles

Column titles that appear in views are editable here, too.

Figure 19-3. Editable Column Titles



Selected	Column Heading	Description	Source
☑	Model	Model	Printer
☑	My Printers	Name	Printer
☑	IP Address	IP Address	Printer
☑	Network Status	Network Response to ...	Printer
☑	Location Name	Name of the location	Location
☑	Toner Summary	Toner Summary	Printer
☑	Paper Summary	Paper Summary	Printer
☑	Last Print Activity	Last Print Activity	Printer

Click the contents of a column in this editor, and start typing to change the title. After you edit a column header this way, you can preserve the view it appears in, and use that view in a layout. Click **Layout→ View→ Select View** to select the altered view. If you change a layout this way, the altered view remains in the layout. Therefore, you can have several copies of the same set of columns in several views, with headers named differently in each set of columns, and use them to fit various layouts you configure.

Reports

Reports Overview

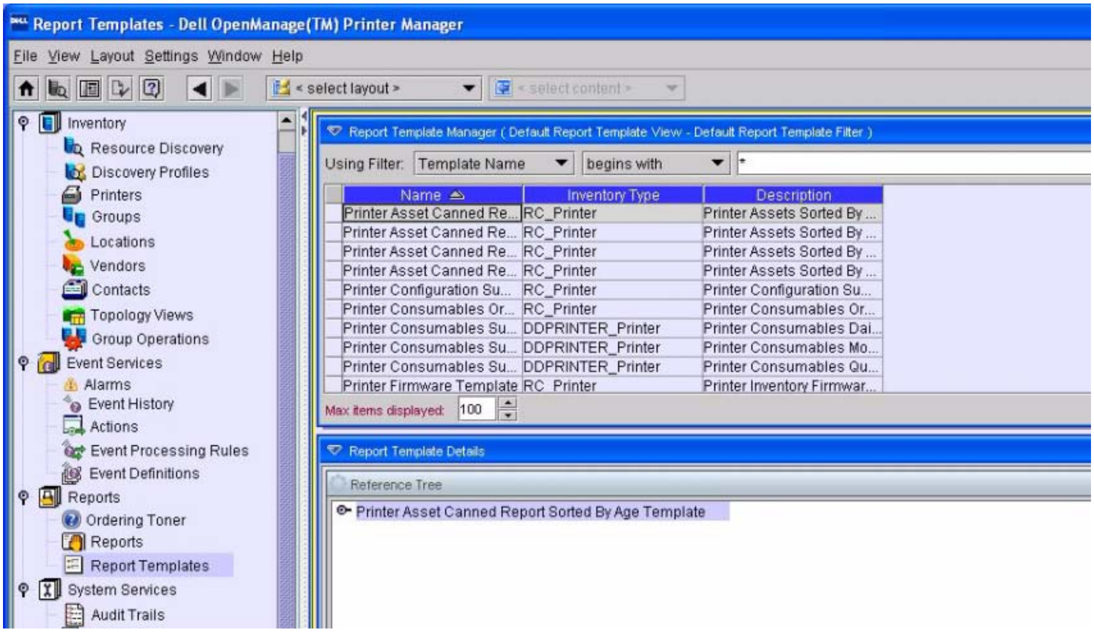
In this optional reporting application, you can configure reported attributes and layout in *Report Templates*, then apply those report templates to different portions of your managed environment. This process uses the following screens:

- Report Templates
- Reports

Report Templates

Report Template Manager lets you manage report appearance and content. You can use these templates to create individual report instances. They also let you assign them to multiple reports. A report consists of a template plus a group of devices, so the template can be “Serial Numbers”, but the reports can be “Serial Numbers for Dell,” “Serial Numbers for London,” and so on.

Figure 20-1. Report Template Manager



Report Templates - Dell OpenManage(TM) Printer Manager

Report Template Manager (Default Report Template View - Default Report Template Filter)

Using Filter: Template Name begins with *

Name	Inventory Type	Description
Printer Asset Canned Re...	RC_Printer	Printer Assets Sorted By ...
Printer Asset Canned Re...	RC_Printer	Printer Assets Sorted By ...
Printer Asset Canned Re...	RC_Printer	Printer Assets Sorted By ...
Printer Asset Canned Re...	RC_Printer	Printer Assets Sorted By ...
Printer Configuration Su...	RC_Printer	Printer Configuration Su...
Printer Consumables Or...	RC_Printer	Printer Consumables Or...
Printer Consumables Su...	DDPRINTER_Printer	Printer Consumables Dai...
Printer Consumables Su...	DDPRINTER_Printer	Printer Consumables Mo...
Printer Consumables Su...	DDPRINTER_Printer	Printer Consumables Qu...
Printer Firmware Template	RC_Printer	Printer Inventory Firmwar...

Max items displayed: 100

Report Template Details

Reference Tree

Printer Asset Canned Report Sorted By Age Template

NOTE: Installed drivers may seed templates for reports tailored to the equipment they manage. You can also modify these to suit your reporting purposes.

The reports associated with the template appear as nodes in the lower panel when you select a listed report.

Under the Action menu (or right-click), the **New** menu item creates a new template. Select a listed template and click **Open** to view it. To remove a template, select one and click **Delete**.

Re-Creating Reports after Editing Templates

You can edit any but pre-existing templates, whether it has reports attached to it or not. Consider this example:

Template T has 3 columns; A, B and C. Someone creates a report R against Template T, executes the report, saves the data as a historical report H1. Two weeks later, someone modifies the Template T, removing column C, adding column D.

When executing report R against Template T', the report now shows columns A, B and D. User saves the report as historical report H2. Here, H1 only has data for columns A, B and C. H2 has data for columns A, B and D.

If you view H1 you see Template T' is in use and this template creates a report with columns A, B and D. Unfortunately, H1 only has data for columns A, B and C, so the report created has data for columns A and B only. Column D is empty. When viewing H2 you can see Template T' is in use and can create a report with columns A, B and D. H2 has data for columns A, B and D, so all data appears.

Creating Report Templates

Click the *New* button in Template Manager to open the Template Editor where you can configure what appears in reports using this template, and how. You must select from the following types of templates: Comparison, Table, and Trend reports. The screens that appear subsequently vary slightly, depending on the selected report type.

Comparison uses current data, while trend reports rely on historical data. You must initiate polling to have historical data for the report.

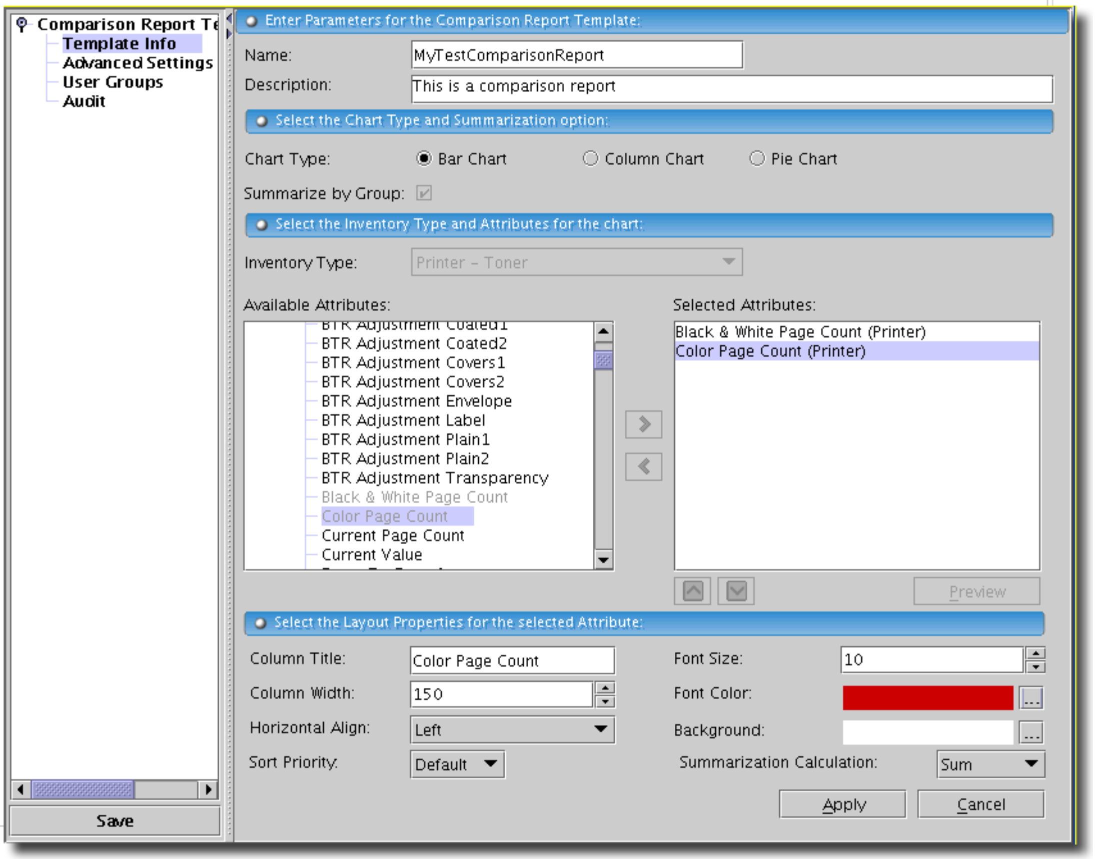
Template Editor has the following tabs:

- Template Info
- Advanced Settings
- User Groups
- Audit

Template Info

In this screen, you identify, describe and assign attributes from different classes (shown in the tree on the left) to a report. For example, you can assign attributes of *Managed Equipment*. Such a selection lets you choose from equipment values like equipment location, or contact, or inventory information.

Figure 20-2. Report Template Editor > Template Info Tab



Comparison Report Te
Template Info
Advanced Settings
User Groups
Audit

Enter Parameters for the Comparison Report Template:

Name: MyTestComparisonReport

Description: This is a comparison report

Select the Chart Type and Summarization option:

Chart Type: ● Bar Chart ○ Column Chart ○ Pie Chart

Summarize by Group: ☑

Select the Inventory Type and Attributes for the chart:

Inventory Type: Printer – Toner

Available Attributes:
BTR Adjustment Coated1
BTR Adjustment Coated2
BTR Adjustment Covers1
BTR Adjustment Covers2
BTR Adjustment Envelope
BTR Adjustment Label
BTR Adjustment Plain1
BTR Adjustment Plain2
BTR Adjustment Transparency
Black & White Page Count
Color Page Count
Current Page Count
Current Value

Selected Attributes:
Black & White Page Count (Printer)
Color Page Count (Printer)

Select the Layout Properties for the selected Attribute:

Column Title: Color Page Count

Column Width: 150

Horizontal Align: Left

Sort Priority: Default

Font Size: 10

Font Color: 🟥

Background:

Summarization Calculation: Sum

Notice the *Preview* button at the bottom right. This generates a preview of the report itself. This screen has the following fields:

- **Name**—The template's name. A unique identifier.
- **Description**—An optional text description of the template. Note that this field also appears in the Manager listing of templates.

Chart Type and Summarization

This panel appears when you select a Comparison Report, or Trend Report, not a Table Report. Comparison templates let you create a pie chart of all the attributes that are part of the Inventory Type definition. You can create bar and column charts from attributes that have numerical values.

Pie chart templates can have only one attribute, while column and bar charts can have multiple attributes.

Trend Templates produce a numerical line or bar chart that graphs data supplied by polling.

For Comparison Reports, select from the radio buttons for the type of chart this template will produce (*Bar, Column*, or *Pie*). If you want summaries by group, check **Summarize by Group**.

NOTE: You must select numeric attributes to create charts. **Also:** You must have initiated polling on the selected equipment for any data to exist for trend analysis.

For Trend Reports, select radio buttons for *Column Chart* or *Line Chart*, and check **Summarize by Group** if you want that to occur.

Inventory Type and Attributes

- **Inventory Type**—The contents of this list depend on the type of report template you are creating. For example, Trend Reports confine your template to printers, but the other report types let you select from several more: *Alarm, Card, Contact, Equipment Change Records, Equipment Components*, and so on.
- **Selected Attributes**—The attributes appearing in this panel depend on the selected inventory type. Use the arrows between the two panels to move attributes from *Available* to *Selected* (and back, if necessary). Reorder the selected attributes with the arrows at the bottom of this panel. Unless you check *Group on First Attrib*, reports generated from this template have attributes in the order they are specified here.

NOTE: The attribute types you can select for reports depend on the installed drivers and applications.

Layout Properties

When you click the **Edit** button in this panel at the bottom of the screen, you can specify additional layout information like the *Column Title Width* and *Alignment* for selected attributes. This is useful to make reports more readable if their columns are not what you wanted from automatic formatting. You can also specify the report’s header or footer information, *Font Size* and *Color*. Click **Apply** to accept your edits; **Cancel** to abandon them.

Column title—This lets you rename the column shown on the report instead of showing the default (the field name). You can adjust the column width for that attribute and define the spacing of the columns on your report instead of using the default widths.

Horizontal align defines the data’s alignment within each column (*left, center or right*). Sort Priority using the default from the Advanced Settings tab or define the attribute sort order here. You can sort within a sort, so you can sort on *Name* and then by *Location* and then by *IP Address*, and so on. Click **Apply** or **Cancel** after editing each attribute.

Report summary—When enabled, this provides a record total on the last page of the report.

Row Separators—Enabled, these provide a line between each row to help visually divide the data.

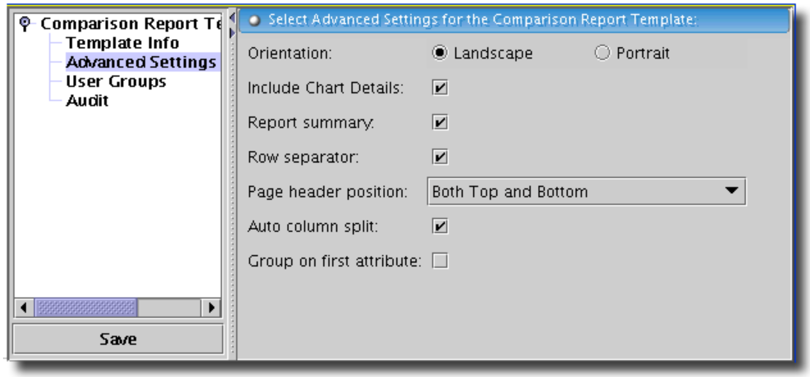
Auto Column Split—This automatically aligns the columns equally on the report providing the column widths that are most proportional. Alternatively you can define your column widths manually by editing the Column Width value in the Template Info section.

To edit, select an attribute and click the **Edit** button. Click **Apply** to accept your edits; **Cancel** to abandon them.

Advanced Settings

Users can also select more advanced settings for the report’s appearance using that tab.

Figure 20-3. Template Editor > Advanced Settings Tab



Select Advanced Settings for the Comparison Report Template:

Orientation: ● Landscape ○ Portrait

Include Chart Details: ☑

Report summary: ☑

Row separator: ☑

Page header position: Both Top and Bottom

Auto column split: ☑

Group on first attribute: □

Select from the following options:

- **Orientation**—Select either *Landscape* or *Portrait*.
- **Include Chart Details**— Check to enable. When enabled, this activates the following fields. In trend reports, it also includes the data charted as part of the report.
- **Report Summary**— Check to enable.
- **Row Separator**— Check to enable.
- **Page Header Position**—Select from *Top*, *Bottom* or *Both Top and Bottom*.
- **Auto Column Split**—Check to enable.
- **Group on First Attribute**—Check this to enable grouping the report on the leftmost attribute selected (otherwise, attributes appear in the order in the *Selected Attributes* panel). This creates groups of items in the report whenever the left most column’s value changes.

For example, with disabled, a report looks like this:

Device Name	Gig/e Port Name	Health Status
M5	ge/0/0/1	Up
M5	ge/0/0/2	Down
M5	ge/0/0/3	Up

Device Name	Gig/e Port Name	Health Status
M5	ge/0/0/4	Unknown
M18	ge/0/1/1	Up
M18	ge/0/1/2	Starting
M18	ge/0/1/3	Up
M18	ge/0/1/4	Down

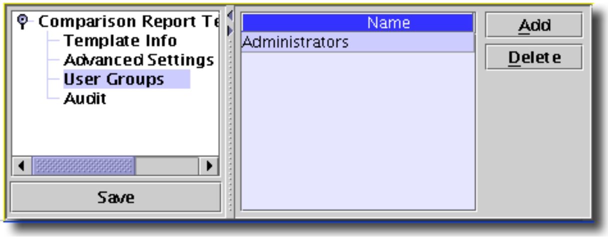
The same report looks like this with *Group on First Attribute* enabled:

Device Name	Gig/e Port Name	Health Status
M5		
	ge/0/0/1	Up
	ge/0/0/2	Down
	ge/0/0/3	Up
	ge/0/0/4	Unknown
M18		
	ge/0/1/1	Up
	ge/0/1/2	Starting
	ge/0/1/3	Up
	ge/0/1/4	Down

User Groups

You can also assign templates to be used ("owned") by specific user groups.

Figure 20-4. Template Editor > User Groups Tab



Name
Administrators

Use the *Add* or *Delete* buttons to manage the list of user groups.

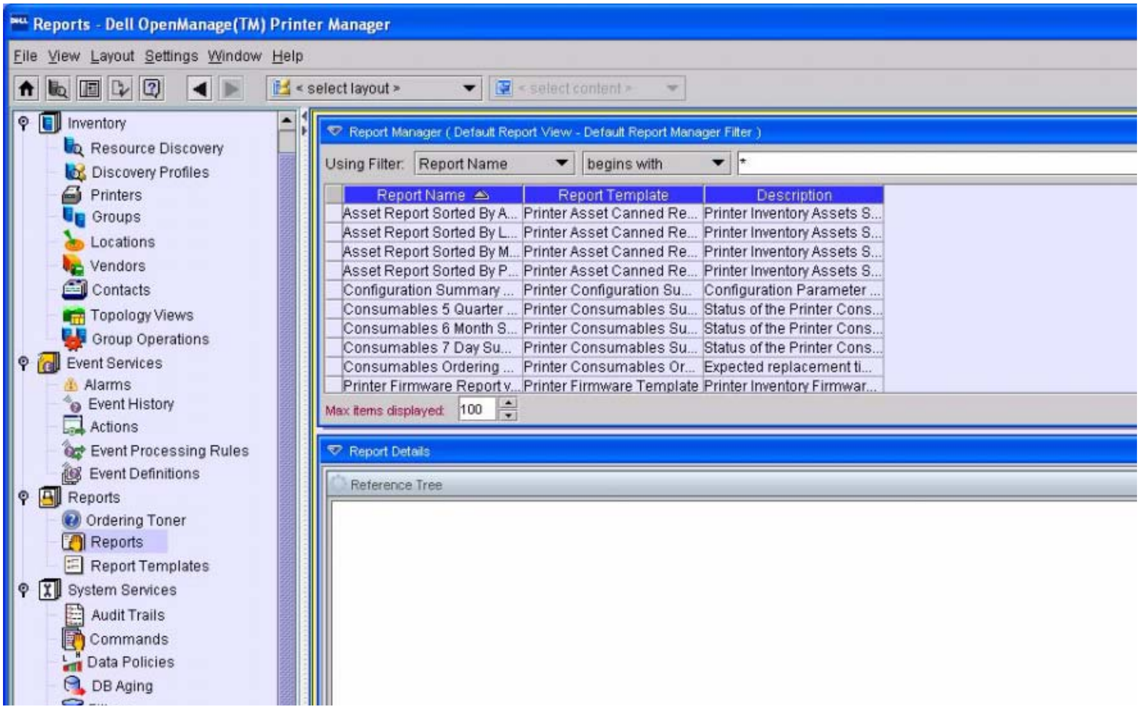
Audit

This is a standard audit screen that records the template's use. See *Audit* on page 228 for an example.

Reports

This screen manages the specific reports that use templates you previously configured in the section described by Report Templates.

Figure 20-5. Inventory Report Manager



Using Filter: Report Name ▼ begins with ▼ *

Report Name	Report Template	Description
Asset Report Sorted By A...	Printer Asset Canned Re...	Printer Inventory Assets S...
Asset Report Sorted By L...	Printer Asset Canned Re...	Printer Inventory Assets S...
Asset Report Sorted By M...	Printer Asset Canned Re...	Printer Inventory Assets S...
Asset Report Sorted By P...	Printer Asset Canned Re...	Printer Inventory Assets S...
Configuration Summary ...	Printer Configuration Su...	Configuration Parameter ...
Consumables 5 Quarter ...	Printer Consumables Su...	Status of the Printer Cons...
Consumables 6 Month S...	Printer Consumables Su...	Status of the Printer Cons...
Consumables 7 Day Su...	Printer Consumables Su...	Status of the Printer Cons...
Consumables Ordering ...	Printer Consumables Or...	Expected replacement ti...
Printer Firmware Report v...	Printer Firmware Template	Printer Inventory Firmwar...

Max items displayed: 100

In the Action (or right-click) menu of Reports Manager, you can configure reports to run (click New or Open a selected report to configure it), and execute them (click Execute). See Executing Reportsfor more about this option. Select a report and click Delete to remove it from the available list. Click Copy to open the report editor (as in Creating A Report) with CopyOf prepended to the selected report's name. You must change this name—and any other parameters you like—before you can save the copy.

If you select Print from the Action menu, an Acrobat® report listing all available reports, their templates and description appears. If you select Help, the online help for this screen appears.

Notice that the attributes and devices referred to by a report appear in the lower (Report Details)panel of this screen when you select a report.

Creating A Report

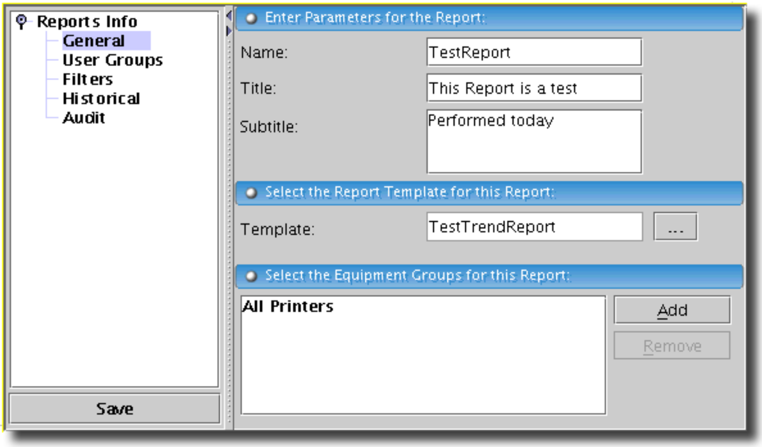
Click **New** or **Open** a selected report to edit that report's settings. The subsequent screens let you configure the report. This editor has the following screens:

- General
- User Groups
- Filters
- Historical
- Audit

General

This tab lets you configure general information about the report.

Figure 20-6. Reports Info > General



Enter Parameters for the Report:

Name: TestReport

Title: This Report is a test

Subtitle: Performed today

Select the Report Template for this Report:

Template: TestTrendReport

Select the Equipment Groups for this Report:

All Printers

This screen contains the following fields:

- **Name**—The identifier for this report.
- **Description**—An optional text description of the report.
- **Title**—The title printed in the report.

Report Template

- **Template**—Use the command button (...) to select an existing template for this report. (See *Report Templates* on page 223 for more about creating report templates)

Equipment Groups

Use the *Add* button to select equipment groups this report is to cover.

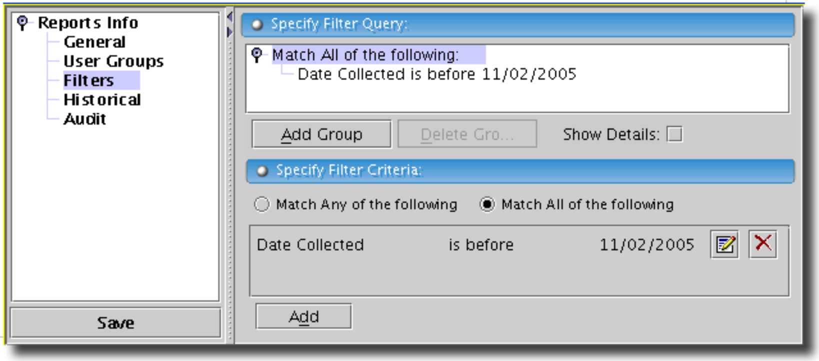
User Groups

Click *Add* to select user groups for this report. This is like the screen *User Groups on page* 228.

Filters

Here, you can add specific conditions to specify what is reported.

Figure 20-7. Reports Info > Filters



Specify Filter Query:

Match All of the following:
Date Collected is before 11/02/2005

Show Details: □

Specify Filter Criteria:

○ Match Any of the following ● Match All of the following

Date Collected is before 11/02/2005

For example, you could request all equipment where the *Name* field contains the word “oware”. The *Add / Delete* group buttons let you use group functionality, creating advanced reporting. For example you could match all values within Group 1 but any values within Group 2. For example, Group 1 could match “vendor = 'Dell'” AND “location contains 'cali'” and Group 2 could match “serial number starts with '20' OR contact name contains 'Brian'”.

To add criteria, first click *Add Group* in the upper panel. The *Filter Attributes* radio buttons (*Match Any of the Following* or *Match All of the Following*) determine part of the filter’s operation.

The *Show Details* check box displays additional filter information to the right of listed criteria as they appear in the upper panel. This information displays codes for additional filtering properties you can select when you create the filter components in the lowest panel.

Available detail codes depend on the data type filtered. The *AND*ed or *OR*ed sum of the filter components’ codes appears at the top level node. The codes for these attributes are the following:

Code	Meaning	Comment
H or V	Hidden / Visible	
ROO or WRO	Read Only / Read-Write Operand	
ROA or WRA	Read Only / Read-Write Attribute	
ROV or RWV	Read Only / Read-Write Value	Grays out the operand and attribute checkboxes since those are not functional if you make this read-only.
ROO or WRO	Read Only / Read-Write Operand	
ROA or WRA	Read Only / Read-Write Attribute	

Code	Meaning	Comment
M or O	Mandatory / Optional	
EL or IL	Exclude / Include Low	Valid only when you select a range of values. This determines whether you include or exclude the endpoint of the range
EH or IH	Exclude / Include High	Valid only when you select a range of values. This determines whether you include or exclude the endpoint of the range
CS or NC	Case Sensitive / Not Case Sensitive	Does not appear for numeric values.
ML or NM	Multi-line Support / No Multi-Line Support	Filter on multiple-line values (or not).

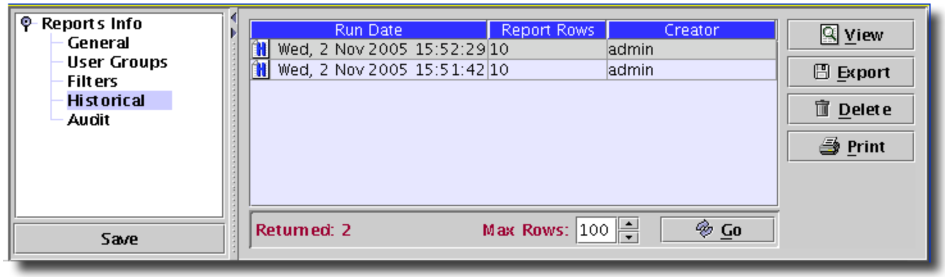
When you select *Read Only* for an attribute, operand or value, some additional impacts are that, for example, reports ordinarily let you alter filters when you manually execute them, but if they have only read-only filtering, then the report executes immediately without a pause to alter filtering.

Specifying the remaining filtering occurs when you click *Add* at the bottom of this screen. Enter attribute / operand / value combinations after clicking *Add*.

Historical

When you run reports, they generate notes in this *Historical* tab.

Figure 20-8. Reports Info > Historical



Run Date	Report Rows	Creator
Wed, 2 Nov 2005 15:52:29	10	admin
Wed, 2 Nov 2005 15:51:42	10	admin

Returned: 2 Max Rows: 100

The table listing individual reports as rows displays the *Run Date*, *Report Rows* (rows in the report), and *Creator* (the login of the user who ran the report). You can also select a report and use the following buttons:

- **View**—See the report in read-only mode.
- **Execute**—Re-run the selected report. See Executing Reports.
- **Export**—Export the report in an electronic format. These formats include XLS (Excel), pdf, comma-separated values (CSV), and HTML.

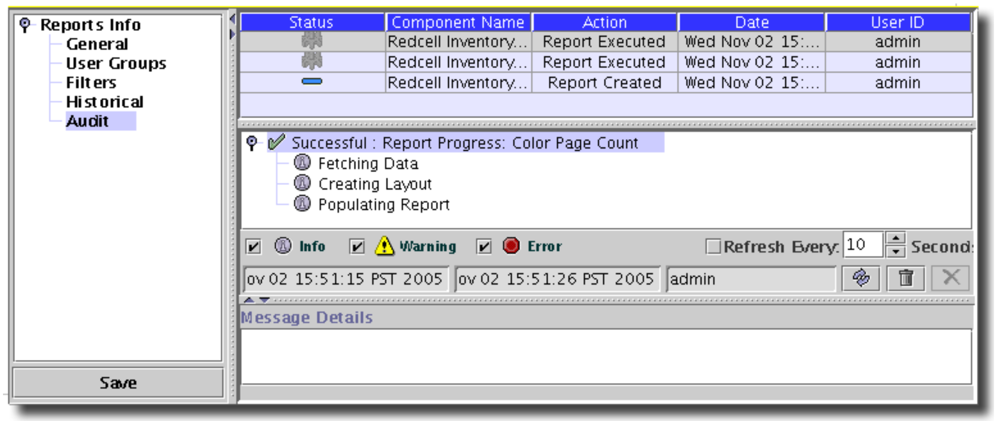
NOTE: You can save a report from the web client, but cannot export its contents.

- **Delete**—Remove the listed report.
- **Print**— Print the selected report.

Audit

This screen presents an audit trail for the selected report.

Figure 20-9. Reports Info > Audit



Status	Component Name	Action	Date	User ID
⚙	Redcell Inventory...	Report Executed	Wed Nov 02 15:...	admin
⚙	Redcell Inventory...	Report Executed	Wed Nov 02 15:...	admin
—	Redcell Inventory...	Report Created	Wed Nov 02 15:...	admin

✓ Successful : Report Progress: Color Page Count
- Fetching Data
- Creating Layout
- Populating Report

☑ Info ☑ Warning ☑ Error □ Refresh Every: 10 Second

ov 02 15:51:15 PST 2005 | ov 02 15:51:26 PST 2005 | admin

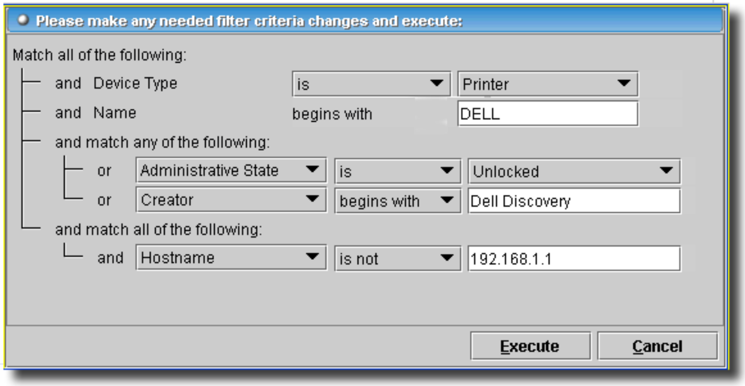
Message Details

This screen catalogs the action of running the selected report. In this you can see what made a report succeed, or fail.

Executing Reports

When you configure a report, you can *Execute* it. If you have created a filter for a particular report, then you can alter the filtering that produces the report.

Figure 20-10. Filter Screen

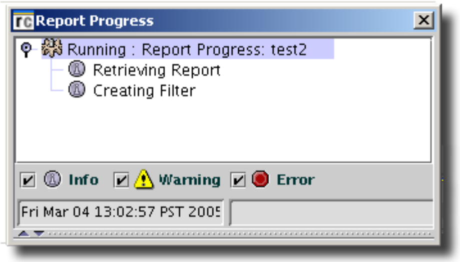

Please make any needed filter criteria changes and execute:

Match all of the following:

- and Device Type is Printer
- and Name begins with DELL
- and match any of the following:
  - or Administrative State is Unlocked
  - or Creator begins with Dell Discovery
- and match all of the following:
  - and Hostname is not 192.168.1.1

The appearance of this screen depends on what is configured in Filters. Click *Execute* after having made any appropriate alterations to the filter that ultimately produces the report, then a progress indication dialog appears his screen resembles the Audit screen.

Figure 20-11. Report Execution Progress


Report Progress

Running : Report Progress: test2
- Retrieving Report
- Creating Filter

☑ Info ☑ Warning ☑ Error

Fri Mar 04 13:02:57 PST 2005

If the filter you created for this report contains only *Read-only* values, then no interruption to alter the filter occurs. Report execution starts right away.

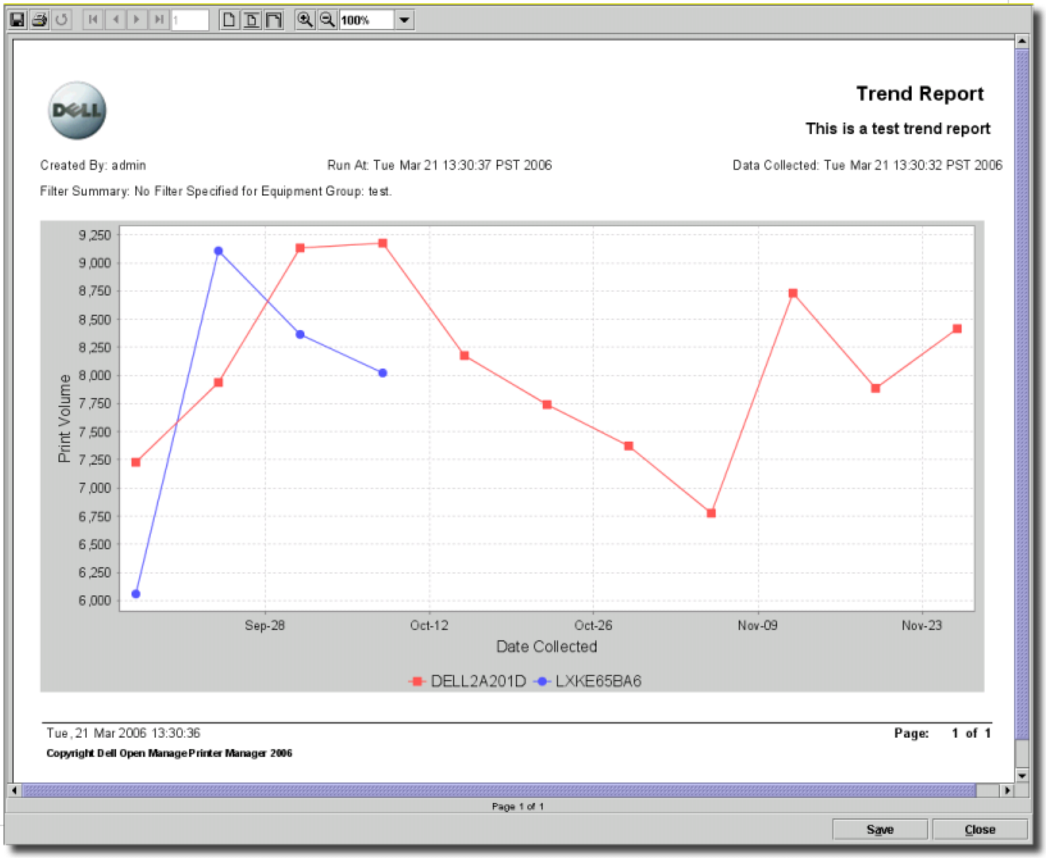
Report execution produces a preview. of the report itself

You can schedule, and re-run, execution (see Scheduling Reports). Note the *Save* button at the bottom of the frame; it saves the report for later viewing. The button bar at the top of this screen lets you navigate through multiple screens, if they exist, manage the magnification of this view, save (export), or print the report.

Trend Report

A trend report requires a matching template, and pre-existing data (stored by polling the selected equipment.

Figure 20-12. Trend Report



Trend Report

This is a test trend report

Created By: admin

Run At: Tue Mar 21 13:30:37 PST 2006

Data Collected: Tue Mar 21 13:30:32 PST 2006

Filter Summary: No Filter Specified for Equipment Group: test.

Tue, 21 Mar 2006 13:30:36

Page: 1 of 1

Copyright Dell Open Manage Printer Manager 2006

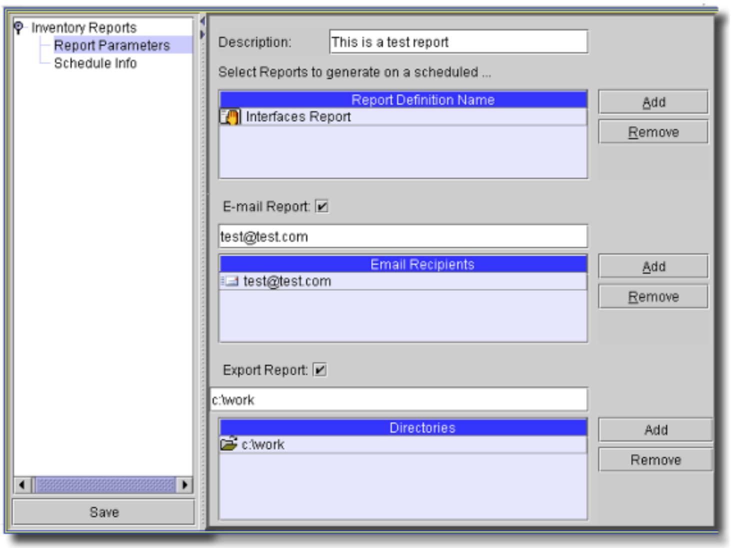
You must pre-configure the polling thresholds in the Threshold Policy Manager if you want to see useful data in this report. See Threshold Manager for more information about this.

Click *Save* to preserve this report in the database.

Scheduling Reports

You can use this application's *Schedules* screen to automate report execution. Click *New* on the *Schedules* screen, and select *Inventory Report*. The *Schedule Info* tab is where you configure the standard scheduling information (see *Schedule Info*).

Figure 20-13. Scheduling Inventory Reports– Report Parameters



Description: This is a test report

Select Reports to generate on a scheduled ...

Report Definition Name
Interfaces Report

E-mail Report: ☑

test@test.com

Email Recipients
test@test.com

Export Report: ☑

c:\work

Directories
c:\work

This screen has the following fields:

- **Description**—Enter a unique identifier for this scheduled item.
- **Select Reports**...—Click *Add* to select templates from which to generate reports. When you select a template, the list headed by *Report Definition Name* grows. See *Creating Report Templates* for instructions about how to make templates.
- **E mail Report**—If you check this checkbox, the application e-mails any generated reports to the recipient list. Enter an e-mail address in the field below the checkbox, then click *Add* to compile the list.
- **Export Report**—If you check this checkbox, the application exports any generated reports to the specified directory as an Acrobat file (pdf). Like the emailed reports, this report's name includes a time stamp and the original report's name so repeatedly scheduled reports do not overwrite each other. To enable this feature, enter a path in the field below the checkbox, then click **Add** to compile the list.

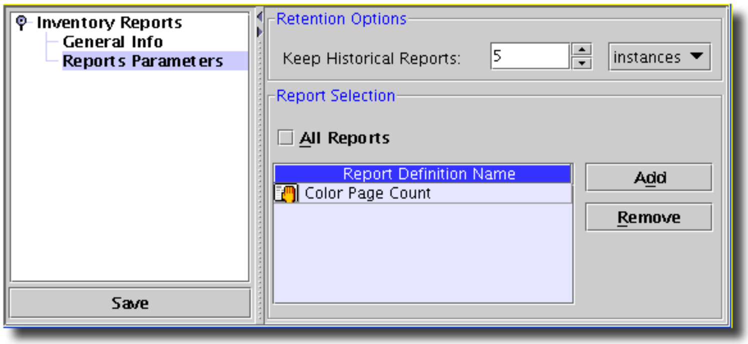
NOTE: The directory path entered is relative to the application server. The directory must be reachable, writable from the application server or exporting the report fails.

In either list, you can select an item, then click **Remove** to delete it.

Aging Report Retention

The database retains all reports unless you set database aging parameters. To do this, open the DAP Manager, and click *New*. Then select *Reports*. The first screen is generic to DAP (see General Info). On the second tab, you can configure how to retain specific reports.

Figure 20-14. Database Aging Policy–Inventory Reports



Keep Historical Reports: 5 instances

☐ All Reports

Report Definition Name
Color Page Count

On this screen you can configure the following:

Retention Options

- **Keep Historical Reports**—Fill in a number, then select from the pick list whether this number is *Instances*, *Days*, *Weeks*, *Months*, or *Years*.

Report Selection

- **All Reports**—Select this to apply this policy to all reports.

Click *Add* to select individual reports, rather than all available reports. You can select one or more reports, and they appear listed below *Report Definition Name*. Select a listed report and click *Remove* to delete it from the list.

Click *Save* when you have completed this screen and the *General Info* screen. This configuration then appears in the DAP Manager . Click *Close* in the toolbar to abandon your edits without saving.

21

Alarms

Overview

The Alarm screen lets you manage alarms and notifications (alarms are typically a subset of notifications or events). It displays information about, and let you acknowledge, received alarms or events. This screen also provide tools that help operators diagnose and correct alarms. Select *File* > *Open* > *System Services* > *Alarms* from the menu or the Navigation Pane to display Alarms.

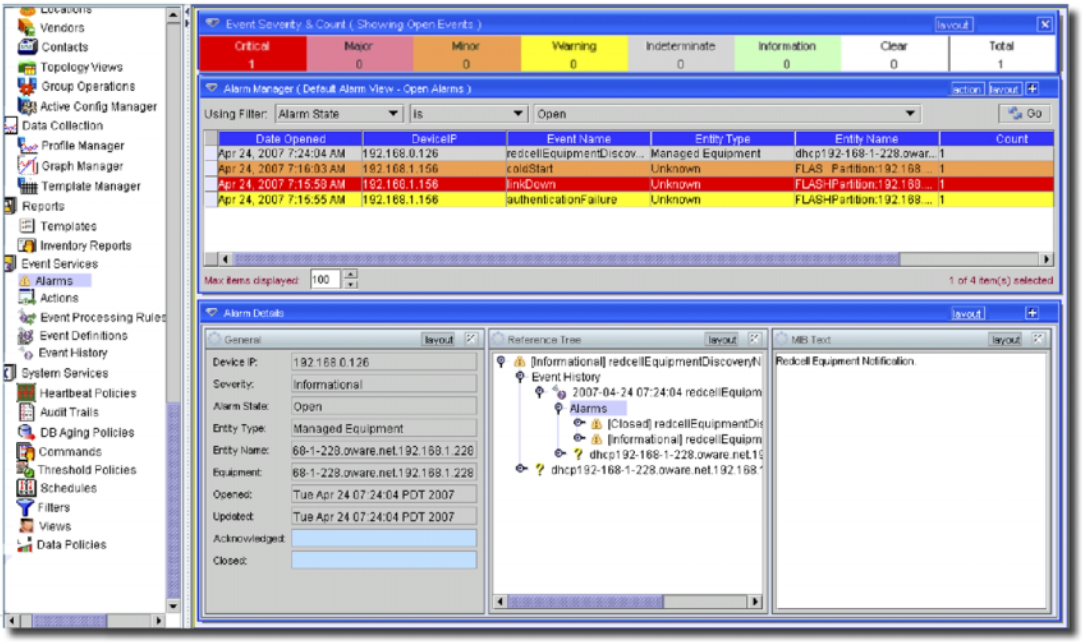
⚠ **CAUTION: While there is no theoretical limit to the number of active alarms, you can optimize application performance by keeping less than 100,000 active alarms with database aging policies.(See Data Policies specifically Alarm DAP Parameters for more about that capability).**

Event History lets you view all notifications, not just the alarm subset. See Event History.

Alarms

The Alarm screens display real time updates of new Alarms entering the system, or alarms created from the window launch time or change of view time. It can include the Alarm Severity & Count panel at the top of the screen, the *Alarm Manager* panel to display and manage events and alarms, and the *Alarm Details* panels in the lowest part of this screen that displays details about the alarm selected in the *Manager* panel.

Figure 21-1. Alarms



Event Severity & Count (Showing Open Events)

Critical	Major	Minor	Warning	Indeterminate	Information	Clear	Total
1	0	0	0	0	0	0	1

Alarm Manager (Default Alarm View - Open Alarms)

Using Filter: Alarm State | is | Open

Date Opened	DeviceIP	Event Name	Entity Type	Entity Name	Count
Apr 24, 2007 7:24:04 AM	192.168.0.126	redcellEquipmentDiscov...	Managed Equipment	dhcp192-168-1-228.owar...	1
Apr 24, 2007 7:16:03 AM	192.168.1.156	coldStart	Unknown	FLAS Partition:192.168....	1
Apr 24, 2007 7:15:59 AM	192.168.1.156	linkDown	Unknown	FLASHPartition:192.168....	1
Apr 24, 2007 7:15:55 AM	192.168.1.156	authenticationFailure	Unknown	FLASHPartition:192.168....	1

Max items displayed: 100

1 of 4 item(s) selected

Alarm Details

General

Device IP:	192.168.0.126
Severity:	Informational
Alarm State:	Open
Entity Type:	Managed Equipment
Entity Name:	68-1-228.oware.net.192.168.1.228
Equipment:	68-1-228.oware.net.192.168.1.228
Opened:	Tue Apr 24 07:24:04 PDT 2007
Updated:	Tue Apr 24 07:24:04 PDT 2007
Acknowledged:	
Closed:	

Reference Tree

```
[Informational] redcellEquipmentDiscoveryN
  Event History
    2007-04-24 07:24:04 redcellEquipm
      Alarms
        [Closed] redcellEquipmentDis
        [Informational] redcellEquipm
      dhcp192-168-1-228.oware.net.19
  dhcp192-168-1-228.oware.net.192.168.1
```

MIB Text

Redcell Equipment Notification.

The following sections discuss these related topics:

- Alarm Severity & Count
- Alarm Manager
- Alarm Table Columns
- Alarm Details
- Using Filters to Create Alarm Exports
- Archiving Alarms

See also Alarm Table Columns for a description of the columns visible in this display of alarms.

You can make changes to a view by clicking and dragging columns in the Alarm tables directly in the Alarm screen. Such changes last only for the current session. You can also change the displayed columns with the plus (+) sign above the panel displaying alarms. Available columns are described in Alarm Table Columns.

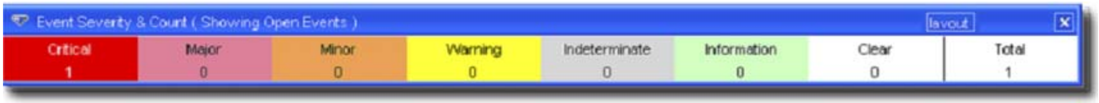
You can also do the following:

- Sort Ascending/descending.
- Remove /Insert columns. See Alarm Table Columns for a brief explanation of each Alarm attribute column type.
- Move Columns—Click the column header of the column you want to move and drag it to its new location.
- Resize Columns—Click the column header of the column you want to resize and drag to resize the column. The column margin is located between the column headers. Typically, best practice is to click the column margin to the right of the column you want to resize.

Alarm Severity & Count

This panel displays the count of Alarms by severity, and totals them on the right.

Figure 21-2. Alarm Severity & Count



Event Severity & Count (Showing Open Events)

Critical	Major	Minor	Warning	Indeterminate	Information	Clear	Total
1	0	0	0	0	0	0	1

This can either display *All Alarms* or *Open Alarms*. Change between these counts by clicking the *Layout* button. Select *Change Filter* and choose the *All Alarms* or *Open Alarms* items. The alarm counts that appear in each panel may exceed the rows of alarms in the Alarm Manager since one row can concatenate several alarms.

Alarms displayed are color-coded based on their severity, and appear until cleared. A total of uncleared alarms, listed both by category and in sum, appears at the top of the Alarm screen. The *Alarm Severity & Count* table at the top of the Alarm screen contains totals for the filtered view (all and unacknowledged), not grand totals from a database count.

See Events, Rules and Actions for information about defining events for display in the Alarm screen. Because the Alarm window is asynchronously threaded, the behavior of the progress bar may be inconsistent. It may start and stop one or more times during a transitional start (for example: changing filters).

The application ships with a set of default event/alarm severity definitions each with its own default color and sound. You can change the colors and sounds in the menu item *Settings > Configuration > Control Settings*, in the *Alarm Severities* tab.

The default severity definitions are:

- **Critical**—A service-halting condition occurs, requiring immediate corrective action. The equipment is completely out of service and you must restore its capability.
- **Major**—A service-affecting condition has developed and corrective action is required. There is a severe degradation in the equipment's capability and you must restore its full capability.

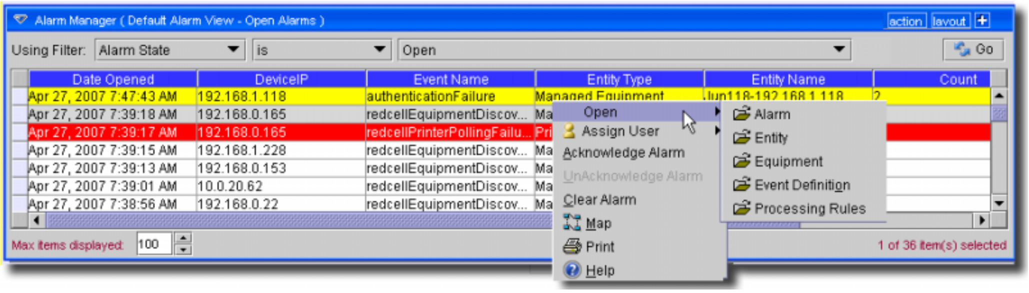
- **Minor**—A non-service-affecting fault condition exists and corrective action should be taken in order to prevent a more serious fault. The detected alarm condition is not currently degrading the capacity of the equipment.
- **Warning**—A potential or impending service-affecting fault could occur, and no significant effects have yet been felt. Action should be taken to further diagnose and correct the problem to prevent it from becoming a more serious service-affecting fault. The detected alarm condition does not currently pose a problem, but may degrade the capacity of the equipment if you do not take corrective action.
- **Indeterminate**—The severity level cannot be determined.
- **Information**—General information about the condition of the object, device, or system.
- **Cleared**—The problem is corrected, and the correlated alarm is cleared from the Active Alarm table.

Alarm Manager

In the *Default* filter, only open alarms appear on these screens. You can change displayed columns (Alarm attributes) with the plus (+) button near the top of the screen, and modify filters to restrict the alarms that appear in the display (see Filters for more information). You can filter on most attributes described in Alarm Table Columns.

For example, you could filter to see alarms that are major and above for only selected equipment.

Figure 21-3. Alarm Manager



Alarm Manager (Default Alarm View - Open Alarms)

Using Filter: Alarm State | is | Open

Date Opened	DeviceIP	Event Name	Entity Type	Entity Name	Count
Apr 27, 2007 7:47:43 AM	192.168.1.118	authenticationFailure	Managed Equipment	Jun118-192 168 1 118	2
Apr 27, 2007 7:39:18 AM	192.168.0.165	redcellEquipmentDiscov...	Ma		
Apr 27, 2007 7:39:17 AM	192.168.0.165	redcellPrinterPollingFailu...	Pri		
Apr 27, 2007 7:39:15 AM	192.168.1.228	redcellEquipmentDiscov...	Ma		
Apr 27, 2007 7:39:13 AM	192.168.0.153	redcellEquipmentDiscov...	Ma		
Apr 27, 2007 7:39:01 AM	10.0.20.62	redcellEquipmentDiscov...	Ma		
Apr 27, 2007 7:38:56 AM	192.168.0.22	redcellEquipmentDiscov...	Ma		

Max items displayed: 100

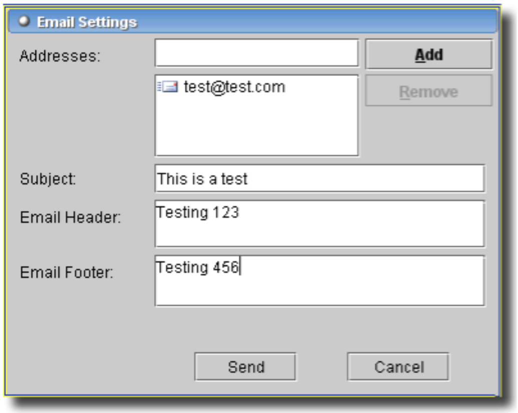
1 of 36 item(s) selected

See also Alarm Table Columns for a description of the columns visible in this display of alarms. This menu displays the following items (some installations conceal some of these):

- **Open > Entity—**This opens an editor where you can configure the device from which this alarm came.
- **Open > Alarm—**Opens a screen describing all the details of the selected alarm. See Alarm Details.
- **Open > Event Definition—**This opens an editor where you can configure the device from which this alarm came. See Event definitions .
- **Open > Equipment**—This opens an editor where you can configure the device from which this alarm came (an *Entity*, if different, is a subcomponent of the equipment).

- **Open > Processing Rules**—This opens an editor where you can configure the rules from which this alarm came. See Event Processing Rules.
- **Acknowledge Alarm**—Acknowledges the selected Alarm(s). The current date and time appear in the Ack Time field, and the name of the currently logged-on user appears in the Ack By field.
- **Unacknowledge Alarm**—Unacknowledges previously acknowledged alarm(s), and clears the entries in the Ack By and Ack Time fields.
- **Assign User—**Assign this alarm to one of the users displayed in the sub-menu by selecting that user.
- **Map**—Open a topology view displaying the equipment selected alarm(s) came from. See Overview.
- **Email Alarm—**E-mail the alarm.

Figure 21-4. Email the Alarm



Addresses: test@test.com

Subject: This is a test

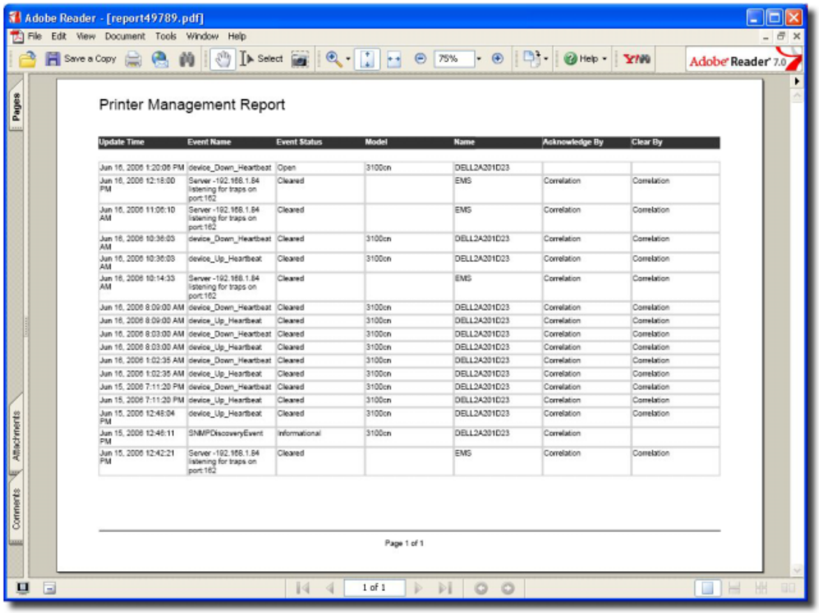
Email Header: Testing 123

Email Footer: Testing 456

Enter an e-mail address to which you want to mail the alarm's content, and click **Add** in the subsequent screen when you select this option. You can also type a subject, header and footer in the provided spaces, then click **Send**. Clicking **Cancel** ends this operation without sending e-mail.

- **Clear Alarm**—Select this option to clear the alarm.
- **Print**—Prints the displayed Alarms to a pdf file.

Figure 21-5. Printed Alarms (pdf)


Adobe Reader - [report49789.pdf]
File Edit View Document Tools Window Help
Save a Copy
Select
75%
Help
Adobe Reader 7.0
Pages
Attachments
Comments
1 of 1

Printer Management Report

Update Time	Event Name	Event Status	Model	Name	Acknowledge By	Clear By
Jun 16, 2006 1:20:06 PM	device_Down_Heartbeat	Open	3100cn	DELL2A201D23		
Jun 16, 2006 12:18:00 PM	Server -192.168.1.84 listening for traps on port:162	Cleared		EMS	Correlation	Correlation
Jun 16, 2006 11:06:10 AM	Server -192.168.1.84 listening for traps on port:162	Cleared		EMS	Correlation	Correlation
Jun 16, 2006 10:36:03 AM	device_Down_Heartbeat	Cleared	3100cn	DELL2A201D23	Correlation	Correlation
Jun 16, 2006 10:36:03 AM	device_Up_Heartbeat	Cleared	3100cn	DELL2A201D23	Correlation	Correlation
Jun 16, 2006 10:14:33 AM	Server -192.168.1.84 listening for traps on port:162	Cleared		EMS	Correlation	Correlation
Jun 16, 2006 8:09:00 AM	device_Down_Heartbeat	Cleared	3100cn	DELL2A201D23	Correlation	Correlation
Jun 16, 2006 8:09:00 AM	device_Up_Heartbeat	Cleared	3100cn	DELL2A201D23	Correlation	Correlation
Jun 16, 2006 8:03:00 AM	device_Down_Heartbeat	Cleared	3100cn	DELL2A201D23	Correlation	Correlation
Jun 16, 2006 8:03:00 AM	device_Up_Heartbeat	Cleared	3100cn	DELL2A201D23	Correlation	Correlation
Jun 16, 2006 1:02:35 AM	device_Down_Heartbeat	Cleared	3100cn	DELL2A201D23	Correlation	Correlation
Jun 16, 2006 1:02:35 AM	device_Up_Heartbeat	Cleared	3100cn	DELL2A201D23	Correlation	Correlation
Jun 15, 2006 7:11:20 PM	device_Down_Heartbeat	Cleared	3100cn	DELL2A201D23	Correlation	Correlation
Jun 15, 2006 7:11:20 PM	device_Up_Heartbeat	Cleared	3100cn	DELL2A201D23	Correlation	Correlation
Jun 15, 2006 12:48:04 PM	device_Up_Heartbeat	Cleared	3100cn	DELL2A201D23	Correlation	Correlation
Jun 15, 2006 12:46:11 PM	SNMPDiscoveryEvent	Informational	3100cn	DELL2A201D23	Correlation	
Jun 15, 2006 12:42:21 PM	Server -192.168.1.84 listening for traps on port:162	Cleared		EMS	Correlation	Correlation

Page 1 of 1

You can print or save this report from Acrobat. If you do not have the free Acrobat reader, you can download it from www.adobe.com.

- **Help**—Select this option to open online help for this screen.
- You can automate responses to alarms with Event Processing rules. For example, an alarm can trigger an e-mail. See Event Processing Rules.

Alarm Table Columns

The following describes the columns that appear in the Alarm table. You can use any or all of the attribute columns in a view, and you can use all attribute columns (except as noted). You can alter the view by dragging the column headers up to delete a column, or by clicking the plus (+) at the top right of the manager and selecting column names, then clicking *Add Column*. Added columns appear to the right of those already there. The following are the attribute columns, in alphabetic order following the default columns:

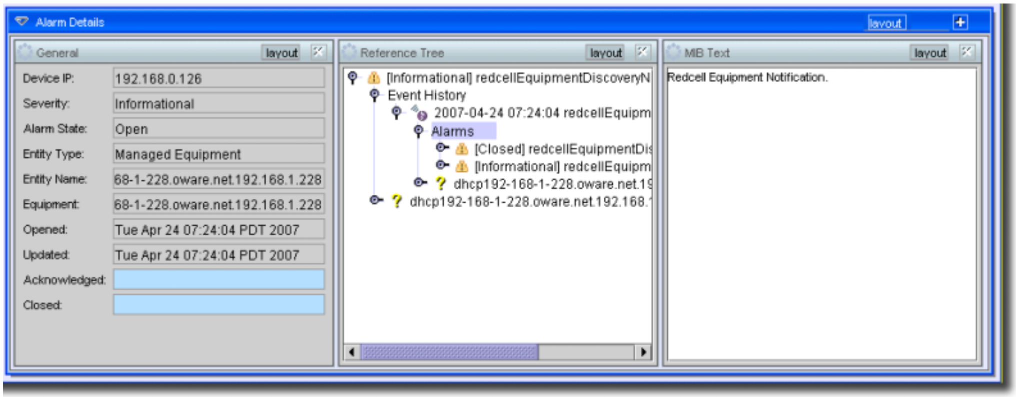
- **Ack By**—Records the user who acknowledged the alarm.
- **Ack Time**—The time the alarm was acknowledged.
- **Acknowledged**—*True* or *False*.
- **Alarm State**—The state (open / closed) of the alarm.
- **Assigned by**—The user who assigned the alarm to the *Assigned User*.
- **Assigned User**—The user who has been assigned this alarm (right click or click *Action* to do this).

- **Count**—The number of similar alarms.
- **Date Assigned**—The date and time that the alarm was assigned.
- **Date Cleared**—The date and time that the alarm was closed.
- **Date Opened**—The date the alarm appeared.
- **DeviceIP**—The IP address of the equipment where the alarm appeared.
- **Entity Name**—The entity emitting this alarm (often within the Equipment).
- **Entity Type**—The object ID of the entity related to this alarm.
- **Equipment**—The name for the entity emitting the alarm.
- **Event Name**—The name for the event at the source of the alarm.
- **Location**—The location where the entity emitting the alarm exists.
- **Message**—The alarm message.
- **Notification OID**—The identifier of the notification displayed as an alarm.
- **Region**—The region (partition) where the equipment emitting this alarm exists.
- **Severity**—The severity of the alarm. The severity only has meaning for Alarms and Security Alarms. Informational Alarms get a severity level of Indeterminate.
- **UpdateDate Time**—The time stamp for when this alarm was updated (for an additional count, the time the last duplicate was received).

Alarm Details

The Alarms screen provides a display of a selected Alarm's details at the bottom of the default layout. Display the Alarm Detail window from the Alarm screen by selecting the Alarm for which you want detailed information.

Figure 21-6. Alarm Details



Device IP:	192.168.0.126
Severity:	Informational
Alarm State:	Open
Entity Type:	Managed Equipment
Entity Name:	68-1-228.oware.net.192.168.1.228
Equipment:	68-1-228.oware.net.192.168.1.228
Opened:	Tue Apr 24 07:24:04 PDT 2007
Updated:	Tue Apr 24 07:24:04 PDT 2007
Acknowledged:	
Closed:	

```
[Informational] redcellEquipmentDiscoveryN
  Event History
    2007-04-24 07:24:04 redcellEquipm
      Alarms
        [Closed] redcellEquipmentDi
        [Informational] redcellEquipm
      dhcp192-168-1-228.oware.net.19
  dhcp192-168-1-228.oware.net.192.168.
```

Redcell Equipment Notification.

This includes the *General*, *Notification Details*, *and Reference Tree* panels: See Alarm Table Columns for a description of the fields in the general panel. Here are the fields in the *Notification Details* panel:

- **Name**—The name of the notification generating the notification.
- **Source IP**—The IP address generating the notification.
- **Receive Time**—The timestamp when this notification arrived at the application server.
- **Region**—The partition generating the notification.
- **Entity name**—The entity generating the notification.
- **Protocol**—The protocol transmitting the notification.
- **Type OID**—The object ID for the type of notification.
- **Instance ID**—The ID for the instance of this type of notification.
- **Entity OID**—The object ID for the entity generating the notification.
- **Entity Type**—The type of entity generating the notification.

The *Reference Tree* displays a graphic description of the connection between this alarm, its originating notification, and any actions and/or correlations.

The *MIB Text* panel displays any text in the MIB for the selected alarm.

The *Advisory Text* panel lets you enter any advisory text needed to accompany the selected alarm.

NOTE: To export alarms to a file, create an alarm report, then save it in the appropriate format.

Using Filters to Create Alarm Exports

For alarm reporting, the application (in the Alarm screen) lets users export data (*File > Export*) in delimited files for use in external applications like Excel. Users can set and apply any Filters or Views. Using these features, you can export any of the desired alarms out of the application for reporting purposes.

Archiving Alarms

To ensure your database does not fill up with Alarms, you can archive them with a Database Aging Policy. See Database Aging Policies (DAP) for details.

Testing Receipt of Alarms

If you want to test whether your system receives traps, you can test it with a trap generating application like Mimic or TrapGen. If you plan to test with artificially generated traps, first use the Discovery Wizard (see Advanced Discovery Wizard) to discover the device you want to initiate these traps (otherwise traps appear as “unknown”).

TrapGen is free from www.ncomtech.com. Here is an example command line for an installation of TrapGen:

```
trapgen -d [destination IP]:[port] -i [initiator’s IP] -g [trap type]
-s [specific type]
```

```
trapgen -d 192.168.0.95:162 -i 192.168.1.156 -g 0 -s 0
```

Use `trapgen -h` to see all available commands.

NOTICE: If you install a trap viewer, like the free one offered by Network Computing Technologies (they offer TrapGen), other applications competing for the trap listening port (162) do not allow this application to correctly receive traps. TrapGen is not supported as part of this application. Install and use it at your own risk.

22

System Recommendations

System Basics

System requirements for each element of your system vary depending how you use it. These numbers are meant as a guide only, not definitive figures. See the relevant upgrade guide for other prerequisites if you are upgrading your software.

You should base the minimum configuration of any system on expected peak load. Typically a configuration running all elements of a system on a single server spends 95% of its time idle and 5% of its time trying to keep pace with the resource demands. If you expect your system to perform an operation that could run create, modify or delete rules on tens or hundreds of thousands of business objects, your real system needs may be much higher.

Recommended Operating System Versions

The following are recommended operating system versions:

- Microsoft Windows®—Windows 2000 (Pro, Server, Advanced Server), Windows 2003 (Standard, Enterprise and Web), Windows XP (Pro) with current patches applied, including Service Pack 3. This is a 32-bit application, however it has been tested for Windows on both 32- and 64-bit operating system versions. Windows 2003 Server 64-bit on Dell 64-bit hardware is the reference test platform for Windows.

NOTE: Windows Terminal Server is not supported

- Linux—This application supports Redhat® (Enterprise® version 4, 4r5 or 5) and SUSE® (version 9 or 10) Linux. See 32-bit Linux Libraries for some additional requirements.

NOTE: To manage Windows systems—you must install this application on a Windows host.

32-bit Linux Libraries

For SuSE or Red Hat Enterprise 64 bit installations, you must identify the appropriate package containing 32-bit libtcl8.4.so (for example: tcl-8.4.13-3.fc6.i386.rpm for Red Hat).

NOTE: Do not use any x86_x64 rpms; these would not install the 32-bit libraries.

Any 32-bit tcl rpm that is of version 8.4 and provides `libtcl8.4.so` works.

Then issue the command:

```
rpm -ivh --force tcl-8.4.13-3.fc6.i386.rpm
```

This forces the installation of the 32-bit libraries on a 64-bit system. Ensure that your expect executable in your installation directory is properly linked by issuing the following commands:

```
[someone@RHEL5-64bit ~]$ which expect

/opt/dorado/oware3rd/expect/linux/bin/expect

[someone@RHEL5-64bit ~]$ ldd
/opt/dorado/oware3rd/expect/linux/bin/expect

linux-gate.so.1 => (0xffffe000)

libexpect5.38.so => /opt/dorado/oware3rd/expect/linux/bin/
libexpect5.38.so (0xf7fd2000)

libtcl8.4.so => /usr/lib/libtcl8.4.so (0x0094c000)

libdl.so.2 => /lib/libdl.so.2 (0x0033e000)

libm.so.6 => /lib/libm.so.6 (0x00315000)

libutil.so.1 => /lib/libutil.so.1 (0x00b8d000)

libc.so.6 => /lib/libc.so.6 (0x001ba000)

/lib/ld-linux.so.2 (0x0019d000)
```

Make sure that `libtcl8.4.so` maps to `/lib/libtcl8.4.so`

Supported Protocols

The following are supported protocols:

- TCP/IP
- SNMP
- HTTP
- UDP Multicast
- CIDR

Hardware Recommendations

	Application Server	Mediation Server	Embedded Database Server	Java Client
OMPM Configuration	• Pentium 4, 3.2 GHz CPU –2 GB RAM –20 GB available disk space –The database is 1 GB, and can grow up to 8 GB, by default	• Pentium 4, 3.2 GHz CPU –2 GB RAM –10 GB available disk space	• Pentium 4, 3.2 GHz CPU –2 GB RAM –20 GB available disk space –The database is 1 GB, and can grow up to 8 GB, by default	• Pentium 4, 2.8 GHz CPU –1 GB RAM (512 MB minimum, 1 GB for optimum performance) –1 GB available disk space
Standalone Server	P	Included on Application Server	Included on Application Server	P
Distributed	P	P	P	P
Clustered	P	P	P	P
High Availability	P	P	N/A	P

OpenManage™ Printer Manager contains an Application Server that runs all the time in the background, and a Client (the user interface you actually see). You can start and stop the client portion of the software without impacting application server (although monitoring of devices stops when you stop the applicationserver or turn off its host machine). The client can also be on a different machine than the application server. Hardware recommendations are based on the different types of installation available:

Full Installation (Application server + Client)—Pentium 4, 3.2 GHz CPU, 2GRAM, and 20G available disk space

Client only—Pentium 4, 2.8 GHz, 1G RAM (512 MB minimum, 1G for optimum performance), and 1G available disk space.

NOTE: A browser -base client is also available.

Hard drive space requirements listed here, and other hardware requirements are based on expected maximum use for average installations and are only intended to be an approximate guide.

NOTE: This software version is not compatible with Windows NT.

Memory Tuning

You can adjust the memory footprint of the local server VM by configuring it in the Heap configuration installation screen during installation.

You can also do this by making edits to

\owareapps\installprops\lib\installed.properties file.

Change these properties:

oware.server.min.heap.size=512m

oware.server.max.heap.size=512m

If 2G is available, make these properties equal to 1024m, for example. Using more memory, if it is available, generally means better performance.

NOTE: Launching the application server without sufficient memory on produces the following error: Error occurred during initialization of VM Could not reserve enough space for object heap.

You can specify memory size in bytes, kilobytes(k), megabytes(m), or gigabytes(g). Examples of these for a one gigabyte maximum java heap size are as follows:

1073741824

1048576k

1024m

1g

Best practice is to increase the minimum heap size so that it is at least half of the maximum size. Java may complain if the minimum setting is too low relative to the new maximum setting. Setting the minimum heap size to the same value as the maximum heap size improves appserver performance, and is the preferred setting.

Depending on the operating system, amount of available physical memory swap size, and other processes (for example: database server), this configuration may cause the application server to fail on startup with an out of memory error. If this occurs, decrease the minimum heap memory setting, as there is some overhead atserver startup. Decreasing the minimum by as little as 256m may solve this problem.

If this fails to solve the problem, it is likely that the maximum memory size you have specified is too large for your configuration. Retry the memory configurationwith a smaller maximum setting

Swap Files and Services

Best practice is to set the swap file for Windows to at least 1536M (larger is better), with its minimum and maximum being set to the same value to avoid resizing and fragmentation of the swap file. Ideally, it would be on its own partition or drive, separate from the OS or database.

Also, best practice is to look at what else is running on the box, including third party software *and* Windows services (`services.msc`). Stop unnecessary services and reset their startup type to manual.

For example:

If netbios is enabled over TCP/IP, it should be disabled in the A*dvanced TCP/IP properties* (*WINS* tab) for each connection, and the netbios, netbt, netbios helper and browser services should be stopped and disabled. The netbios and netbt services are not visible from the services control panel applet, but can be stopped using `net stop netbios, net stop netbt`.

Software Space Requirements

You cannot install applications unless the target drive has the required free space. Here are the minimum requirements

Software / Platform	Full Installation	Client Installation
Application Only	1080MB	330MB

The *Full* installation is really just a client plus database size. The same footprint exists for any type of installation with the actual databases being the only difference. Applications can add required space for client as well as additional space for database server. The 750MB difference in the numbers above is simply a default setting in installer that requires an additional 750MB for data space.

Configuring Shell Messages

You can change the jnp.discoveryAddress property in oware\lib\owappserver.properties to cut down on appserver shell messages.

This must be the same on *all* clients, and servers, within a cluster. Change to some acceptable multicast address: anything between [225.0.0.0 through 239.255.255.255].

Verify that you're starting the servers with the same partition name and that you have designated a config server either on the command line to `startappserver` or as part of the `pmstartup.dat` file in `oware\lib` if you're running them as Windows services.

Application Server Default Password

The default application server password is `trustnoone.` You can set (best practice: override) this in the `oware\lib\owappserver.properties` file. The default Oware Creation Center (OCC) ID is your network login, and the default OCC password is blank.

⚠ **CAUTION: Hostnames can be any length, but the initial eight characters in the names of all hosts used as servers with this application must be unique in the network.**

Client Password

The first time users log in to a client, they are prompted by the interface to change their password. The default login is *admin*, and the default password is blank (no text).

NOTE: The password is encrypted in the database.

FTP Servers on Linux/Solaris

The internal file server does not work on these operating systems. The following sections describe how to use their alternatives to that file server. Installation of FTP, TFTP, SFTP and SCP depends on having the server correctly configured on Linux.

The following installation instructions describe how to do this:

- SUSE Linux FTP—Installing on SUSE Linux.
- Red Hat Linux FTP/TFTP—Installing on Red Hat Linux

Refer to the operating system documentation for details about these, or if your operating system is not specifically mentioned below.

1. Edit `/etc/ftpd/ftpaccess`, adding the following line:

   ```
   defumask 000
   ```

2. Execute inetconv

   ```
   # inetconv
   ```

3. Verify the service is enabled

   ```
   # svcs | grep tftp

   online 10:52:15 svc:/network/tftp/udp6:default
   ```

SUSE Linux FTP

Confirm FTP is installed. Open YAST. Click on INSTALL AND REMOVE SOFTWARE on the right. When the next window comes up, type *vsftpd* into the SEARCH box, and click **SEARCH**. When the result appears on the right, click in the box to install the package. Then, click on **ACCEPT** to perform the installation.

Now that it is installed you can tell the FTP server to run in stand-alone mode. Open up a terminal window. Become superuser, and edit the `/etc/vsftpd.conf` file with a text editor.

Go to the end of the file, and uncomment the line `# listen=YES.` Save the file and close the text editor.

To make sure the FTP server run when the machine boots, you can make a small script. Log in as the superuser, and edit `/etc/init.d/vsftpd`. Paste this in:

```
#!/bin/sh

case "$1" in

start)

echo "Starting vsftpd ..."

/usr/sbin/vsftpd &
```

```
;;
stop)
echo "Stopping vsftpd ..."
killall vsftpd
;;
*)
echo "Usage: 'basename $0' {start|stop}" >&2
exit 64
;;
esac
exit 0
```

Save and close the file. While still logged into the terminal window as superuser, make this file executable with the following command:

```
chmod +x /etc/init.d/vsftpd
```

Finally, you must edit the system runlevels so the script gets executed when the machine boots next time. Run YAST. From the left pane, select SYSTEM. From the right, select *RunLevel Editor*, and when the window appears, select the *Expert Mode* radio button. Scroll down and select the vsftpd entry. Check the 3 and 5 runlevel boxes. When you are done, click **Finish**.

To test whether this is successful. Restart the machine. When it comes back up, log in.

Open a terminal window and type ps aux | grep vsftp. You should see something similar to the output below:

```
[1834][test@linux:~]$ ps aux | grep vsftp
root 1325 0.0 0.0 1840 480 ? S 16:07 0:00 /usr/sbin/vsftpd
root 1340 0.0 0.0 1220 268 ? Ss 16:07 0:00 /sbin/startpar -f
smorris 4863 0.0 0.1 2588 688 pts/1 R+ 16:08 0:00 grep vsftp
[1834][test@linux:~]$
```

A successful installation displays three lines (the second line is abbreviated in the above example). However, if you only see the last line, something is incorrect in your setup. Check each of the instructions for accuracy.

If you test the server with your favorite FTP client, remember that when you connect in as an anonymous user, you have read-only access.

The FTP server root is `/srv/ftp/.`

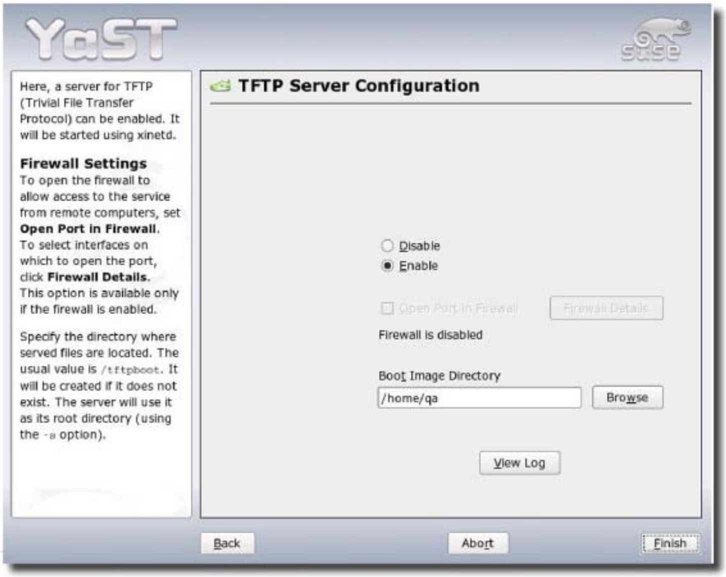
TFTP

For the tftp server, use the YAST utility. On the command line type the following:

```
/sbin/yast2 tftp-server.
```

A tftp configuration screen appear.

Figure 22-1. SUSE Linux TFTP Setup in YaST



Here, a server for TFTP (Trivial File Transfer Protocol) can be enabled. It will be started using xinetd.

Firewall Settings
To open the firewall to allow access to the service from remote computers, set **Open Port in Firewall**. To select interfaces on which to open the port, click **Firewall Details**. This option is available only if the firewall is enabled.

Specify the directory where served files are located. The usual value is `/tftpboot`. It will be created if it does not exist. The server will use it as its root directory (using the `-s` option).

TFTP Server Configuration

○ Disable
● Enable

□ Open Port in Firewall

Firewall is disabled

Boot Image Directory: /home/qa

NOTE: For NetConfig, the ftp and tftp paths must match.

Red Hat Linux FTP/TFTP

The following are steps to set up FTP and TFTP on Red Hat Linux:

1 Confirm if FTP is installed by typing the following in a shell:

```
rpm -q vsftpd
```

The following is an example response (your version may differ):

```
vsftpd-2.0.5-10.el5
```

2 Modify the `vsftpd.conf` file which is in `/etc/vsftpd`

   a Become superuser.

   b Edit `vsftpd.conf` file with a text editor.

   c Uncomment the line `#listen = YES`

d Change `umask = 000` (must be at least 011)

e Save vsftpd.conf

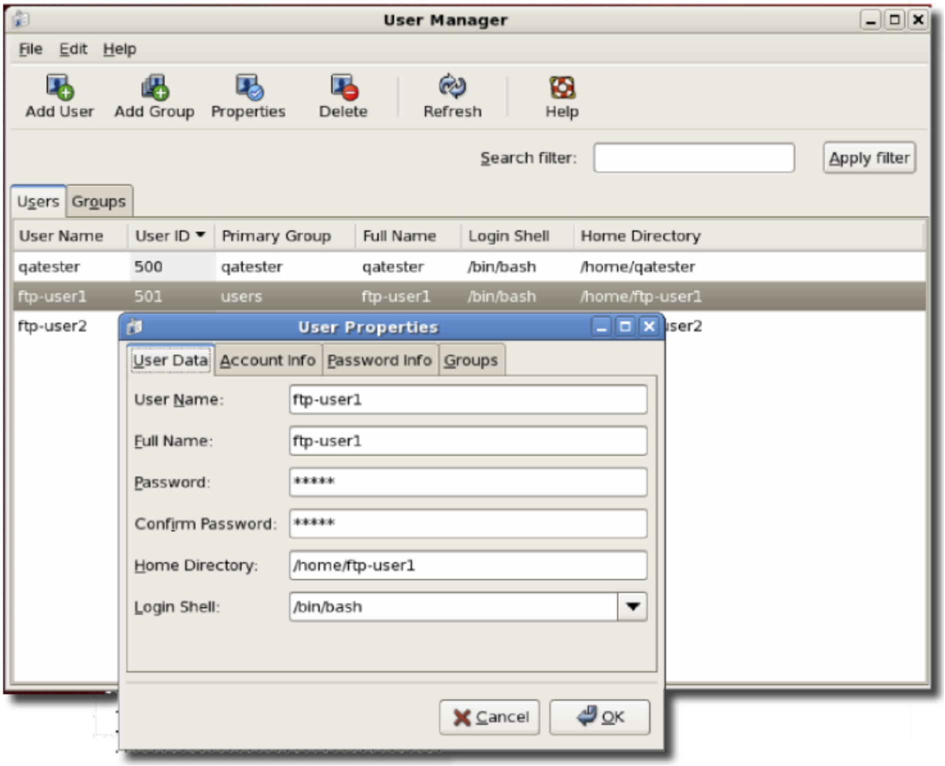
f Run this process to stop the FTP process: `/sbin/service vsftpd stop`

g Run this to restart the FTP process: `/sbin/service vsftpd start`

h Confirm the FTP process is running `netstat -a | grep ftp`

3 Create a user, for example, ftp-user1 with the home directory `= /home/ftpuser1`

Figure 22-2. Create a User



User Name	User ID	Primary Group	Full Name	Login Shell	Home Directory
qatester	500	qatester	qatester	/bin/bash	/home/qatester
ftp-user1	501	users	ftp-user1	/bin/bash	/home/ftp-user1
ftp-user2					ser2

User Name: ftp-user1

Full Name: ftp-user1

Password: *****

Confirm Password: *****

Home Directory: /home/ftp-user1

Login Shell: /bin/bash

4 Confirm TFTP is installed by running this command in a shell:

```
rpm -q tftp-server
```

The following is an example response (your version may differ)

```
tftp-server-0.42-3.1
```

5 Start TFTP with the following shell commands, once you are logged in as superuser:

```
/sbin/chkconfig -level 345 xinetd.d on
/sbin/chkconfig -level 345 tftp on
```

6 Modify the following in the TFTP file located in `/etc/xientd.d`

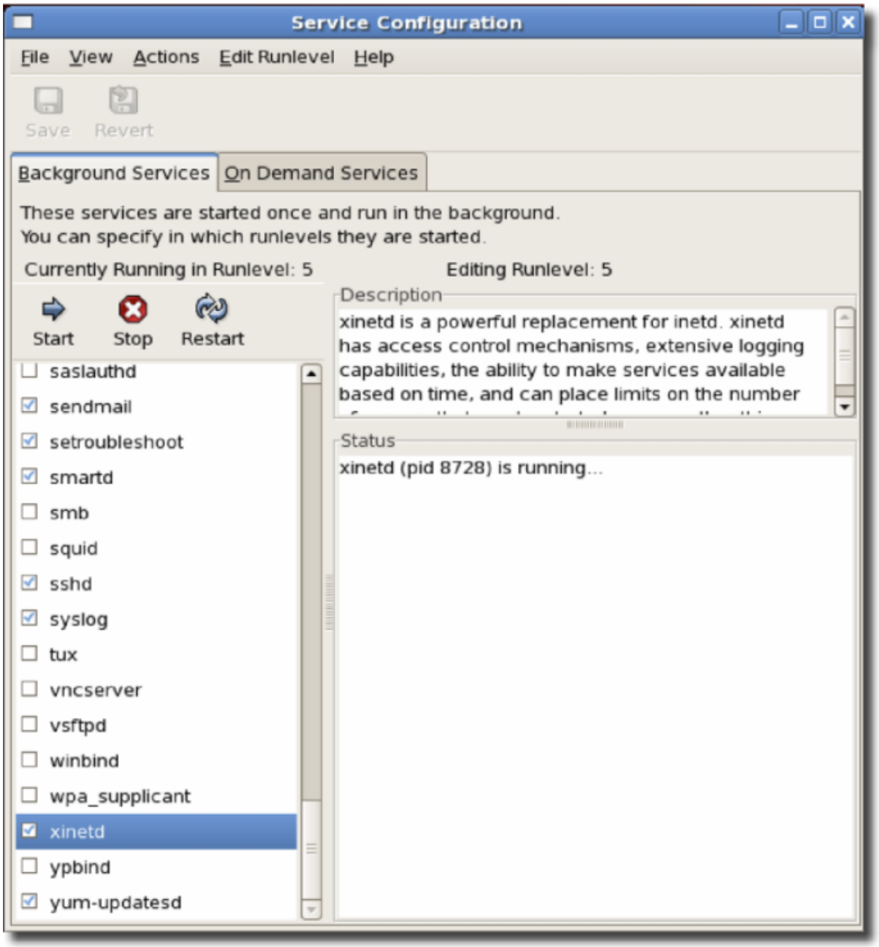
```
server_args = -u ftp-user1 -s /home/ftp-user1
```

This sets the same directory for ftp & tftp

```
disable = no
```

Save the file, then restart xinetd by going to **System**→ **Administration**→ **Server settings**→ **Services**, and enter the root password. Select xinetd a click on **Restart** or click **Stop**, then click **Start**.

Figure 22-3. Service Configuration



These services are started once and run in the background.
You can specify in which runlevels they are started.

Currently Running in Runlevel: 5

Editing Runlevel: 5

xinetd is a powerful replacement for inetd. xinetd has access control mechanisms, extensive logging capabilities, the ability to make services available based on time, and can place limits on the number

xinetd (pid 8728) is running...

- □ saslauthd
- ☑ sendmail
- ☑ setroubleshoot
- ☑ smartd
- □ smb
- □ squid
- ☑ sshd
- ☑ syslog
- □ tux
- □ vncserver
- □ vsftpd
- □ winbind
- □ wpa_supplicant
- ☑ xinetd
- □ ypbind
- ☑ yum-updatesd

7 Run the following in a shell to verify TFTP is running: `netstat -a | grep tftp`. A response should indicate such a process is running.

Ports Used

You must sometimes configure this application's port availability on firewalls. Sometimes, excluding applications from firewall interference is all that is required (see "Ports and Application To Exclude from Firewall" on page 263).

The following are some of the standard port assignments for installed components. These are often configurable (even for "standard" services like FTP or HTTP), so these are the typical or expected port numbers rather than guaranteed assignments.

Destination Ports	Service	File(s)	Notes	Used from Client
HTTP/S (Web Client)				
80[4]	oware.webservices.port	[user.root]\oware\lib\owweb services.properties	appserver	Yes
443[4, 5, 7]	org.apache.coyote.tomcat4. CoyoteConnector(Apache)	[user.root]\oware\jboss-3.2.7\server\oware\deploy\jboss web-tomcat41.sar\META-INF\ jboss-service.xml	app/medserver	No
Other Ports				
n/a[5](ICMP)	ping		MedSrv→ NtwkElement, NtwkElement→ MedSrv, ICMP ping for connection monitoring.	
20[4, 5, 7] (TCP)	FTP Data Port	n/a	(Internally configurable), "MedSrv→ FTPSrv NtwkElement→ FTPSrv" medserver[1]	No
21[4, 5, 7] (TCP	FTP Control Port	n/a	(Internally Configurable) "MedSrv→ FTPSrv NtwkElement→ FTPSrv" medserver[1]	No
22[4, 5, 7] (TCP)	SSH	n/a	MedSrv→ NtwkElement, secure craft access medserver[1]	No
23[4, 5, 7] (TCP)	Telnet	n/a	MedSrv→ NtwkElement, non-secure craftaccess medserver[1]	Yes

Destination Ports	Service	File(s)	Notes	Used from Client
25[4, 5, 7] (TCP)	com.dorado.mbeans.OWE-mailMBean(mail)	[user.root]\oware\jboss-3.2.7\owareconf\oware-service.xml	AppSrv→ SmtpRelay, communication channel to email server from Appserver	No
69[4, 5, 7] (UDP)	TFTP	n/a	(Configurable internally), F, MedSrv→ TFTPSrv NtwkElement→ TFTPSrv medserver[1]	No
161[4, 5, 7] (UDP)	com.dorado.mediation.snmp.request.listener. port (SNMP), oware.mediation.snmp.trap.forwarding.source.port	[user.root]\oware\lib\owmediationlisteners.properties,[user.root]\oware\lib\owmediation.properties	MedSrv→ NtwkElement, SNMP requestlistener and trap forwarding source medserver[1]	No
162[4, 5] (TCP)	oware.mediation.snmp.trap.forwarding.des tination.port (SNMP)	[user.root]\oware\lib\owmediation.properties	NtwkElement→ Med-Srv, SNMP trap forwarding destination port, medserver[1]	No
514[4, 5] (UDP)	com.dorado.mediation.syslog.port (syslog)		NtwkElement→ Med-Srv (mediation syslog port) medserver[1]	No
1098[4, 5, 7] (TCP)	org.jboss.naming.Naming-Service (JBOSS)	[user.root]\jboss-3.2.7\owareconf\jbossrootservice.xml	AppSrv→ MedSrv MedSrv → AppSrv user client→ AppSrv user client→ MedSrv, (JBOSS naming service), app/medserver	Yes
1099[4, 5, 7] (TCP)	org.jboss.naming.Naming-Service (JBOSS)	[user.root]\oware\jboss-3.2.7\owareconf\jbossrootservice.xml	MedSrv→ AppSrv, user client→ AppSrv, user client→ MedSrv, (JBOSS naming service & OWARE context server URL), app/medserver	Yes

Destination Ports	Service	File(s)	Notes	Used from Client
1099[2, 4, 5, 7] (TCP)	OWARE.CONTEXT.SERVER.URL		MedSrv→ AppSrv, user client→ AppSrv. user client→ MedSrv. (JBOSS naming service & OWARE context server URL)	Yes
		[user.root]\oware apps\install props\lib\installed.properties	client	
		[user.root]\oware apps\install props\medserver\lib\installed.properties	medserver[1]	
1103[4, 5] (UDP)	jnp.reply.discoveryPort (JNP)	[user.root]\oware\lib\owapp server.properties	AppSrv→ MedSrv, AppSrv→ user client, (JNP reply discovery port), app/medserver	Yes[3]
1123[4, 5] (UDP	jnp.discoveryPort (JNP)	[user.root]\oware\lib\owapp server.properties	MedSrv→ AppSrv, user client→ AppSrv, (JNP discovery port), app/medserver	Yes[3]
1812[4, 7] (TCP)	RADIUS port	[user.root]\oware\jboss-3.2.7\server\oware\conf\log in-config.xml	AppSrv→ RADIUS Srv, Appserver (RADIUS client login enabled– optional)	No
2508[4, 7]	JMS - SONICMQ_INTERBROKER_POR T (JMS)	[user.root]\oware\lib\owapp server.properties	AppSrv→ AppSrv, MedSrv→ AppSrv, (JMS - SonicMQ interborker port), app/medserver	No
3306[4, 7] (TCP)	com.dorado.jdbc.database_name.mysql	[user.root]\oware apps\install props\lib\installed.properties	AppSrv→ MySQLSrv, (JDBC database naming [MySQL]) appserver)	No
3100[4, 5, 7] (TCP) 3200[4, 5, 7]	org.jboss.ha.jndi.HANaming Service (JBOSS)	[user.root]\oware\jboss-3.2.7\owareconf\clusterservice.xml	AppSrv→ AppSrv, user client→ AppSrv AppSrv→ MedSrv MedSrv→ AppSrv user client→ AppSrv user client→ MedSrv (JBOSS HA JNDI HA Naming service [3100 is stub] app/medserver	Yes[3]

Destination Ports	Service	File(s)	Notes	Used from Client
4445[4, 5, 7] (TCP)	org.jboss.invocation.pooled. server.PooledInvoker (JBOSS)	[user.root]\oware\jboss-3.2.7\owareconf\jboss–root-service.xml	AppSrv→ MedSrv MedSrv→ AppSrv user client→ AppSrv user client→ MedSrv, app/medserver	Yes
4446[4, 5, 7] (TCP)	org.jboss.invocation.jrmp.server.JRMPInvoker (JBOSS)	[user.root]\oware\jboss-3.2.7\owareconf\jboss–root-service.xml	(AppSrv→ AppSrv, AppSrv→ MedSrv, MedSrv→ AppSrv, user client→ AppSrv, user client→ MedSrv) app/medserver	Yes
5988, 5989	WBEM Daemon (5989 is the secure port) defaults		You can add ports and daemons in monitored services. These are only the default. WBEM requires one port, and only one, per daemon.	No
6500-10[4, 5, 7] (TCP)	JBOSS		user client→ MedSrv (user client to mediation server cutthrough	Yes
8009 (TCP)	org.mort bay.http.ajp.AJP13Listener	[user.root]\oware\jboss-3.2.7\server\oware\deploy\jboss web-tomcat41.sar\META-INF\jboss-service.xml	Obsolete — appserver	No
8080[4, 5, 7] (TCP)	org.mortbay.http.SocketListener (HTTP)	user.root]\oware\jboss-3.2.7\server\oware\deploy\jboss web-tomcat41.sar\META-INF\jboss-service.xml	AppSrv→ AppSrv, mgmt client→ AppSrv, mgmt client→ Med-Srv, (Apache Coyote Tomcat4 Coyote connector) appserver/medserver	Yes2
8083 (TCP)	org.jboss.web.WebService (JBOSS)	user.root]\oware\jboss-3.2.7\owareconf\jboss–root-service.xml	not used (JBoss web services) appserver	No
8093[4, 5. 7] (TCP)	org.jboss.mq.il.uil2.UILServerILService	[user.root]\oware\jboss-3.2.7\owareconf\uil2-service.xml	MedSrv→ AppSrv, user client→ AppSrv (JBOSS mq il uil2 UIL Server-IL Server), app/medserver (Jboss JMS)	Yes

Destination Ports	Service	File(s)	Notes	Used from Client
8443[2,4, 5, 7]	org.apache.coyote.tomcat4.CoyoteConnector	[user.root]\oware\jboss-3.2.7\server\oware\deploy\jbosswebtomcat41.sar\META-INF\jboss-service.xml	user client→ AppSrv (Apache Coyote Tomcat4 Coyote connector), appserver	No
9001[4, 6, 7] (UDP)	mediation.listener.multicast.intercomm.port	[user.root]\lib\owmediationlisteners.properties	MedSrv <-> MedSrv (mediation listener multicast intercommunications port) medserver[3]	No
31310[4, 6, 7] (TCP)	JBoss		AppSrv→ AppSrv	No
54321[4,7]	Process Monitor	[user.root]\oware\lib\pmstartup.dat	mgmt client→ AppSrv, mgmt client→ MedSrv (process monitor local client for server stop/start/status) app/medserver	Yes

[2] Unused in standard configuration.
[3] Client does not connect to medserver on this port.
[4] This port is configurable.
[5] Firewall Impacting
[6] The most likely deployment scenarios will have all servers co-resident at the same physical location; as such, communications will not traverse through a firewall
[7] Bidirectional

To operate through a firewall, you may need to override default port assignments.

NOTE: To configure ports, open their file in a text editor and search for the default port number. Edit that, save the file and restart the application server and client. Make sure you change ports on all affected machines.

Ports and Application To Exclude from Firewall

Exclude `java.exe`, tcp port 21 and udp port 69 from firewall interference to let the application function. The java process to exclude from firewall blocking is

`<Installdir>\oware3rd\ jdk[version number]\jre\bin\java.exe..`

The embedded database process is mysqld-max-nt.exe (in Windows, the path is

`<installdir>oware3rd\mysql\[version number]\bin\mysql-max-nt.exe).`

Consult your DBA for Oracle processes, if applicable.

Installed Third Party Applications

The following applications are installed with this software. Cited version numbers are subject to change without notice

- ant v1.6.5
- cygwin v1.5.24-2
- expect v5.26
- jboss v3.2.7
- JDK v1.6.0_01
- JLoox v3.0
- MySQL v4.0.13
- Open SSH v3.6.1-p1 includes OpenSSL v0.9.7b
- TCL v8.2
- OpenLDAP
- Jasper Reports v1.3.2
- J Free Charts v1.0.8

Windows Management Interface Ports

Windows Management Interface uses the following ports:

Protocol or Function	Ports Used
RPC, TCP	135,139,445,593
SNMP, UDP	161,162
Optional:	
WINS, TCP	42
UDP	42, 137
PrintSpooler, TCP	139, 445
TCP/IP PrintServer, TCP	515

These are relevant only if you are using any Windows-based server device driver.

23

Installation

Installation Overview and Prerequisites

The installation process installs the application, including its foundation class software.

This application is incompatible with any other software using the standard SNMP ports (162, for example), or other raw sockets. Either stop the conflicting application before you install this one, or stop this one whenever you want to use the alternative. You may have to reboot to close conflicted sockets. To stop this application, you must close the client *and* stop the application server (see Stopping Servers).

Quick Start

The typical sequence of events, including installation is the following:

- **Install the software**—See Installing the Application.
- **Discover Network Devices**—See the *User Guide* for detailed instructions, or click *File > Open > Inventory > Resource Discovery* and enter the IP addresses you want to discover. You may also have to enter SNMP and Telnet login/password combinations to fully discover equipment. Once you have discovered equipment, you can manage it.
- **Begin Managing your network—**Consult the *User Guide* for details about the many options available with this software.

You can also administer your application, setting up users, and equipment access passwords, and groups for both users and equipment, as you begin to use it.

Basic Network Considerations

This application communicates with devices over a network. In fact, you must be connected to a network for application server to start successfully. Firewalls, or even SNMP management programs using the same port on the same machine where this application is installed can interfere with its ability to communicate with devices.

Your corporate network may have barriers to communication with this software that are outside the scope of these instructions. Consult with your network administrator to ensure this application has access to the devices you want to manage with the Protocols described below.

NOTE: One simple way to check connectivity with a device is to open a command shell with Start > Run `cmd`. Then, type `ping [device IP address]` at the command line. If the device responds, it is connected to the network. If not, consult your network administrator to correct this. No useful information comes from disconnected devices.

Name Resolution

If you have server and client on different machines, this application requires resolution of equipment names, whether by host files or domain name system (DNS). The application server cannot respond to clients based on its IP address alone. It may be on a different network and therefore the client would be unable to connect.

Whether it uses the OWARE.CONTEXT.SERVER URL or not, when a client connects to the application server it receives a stub with the real URL used to communicate with RMI. This stub always returns a URL with the host name, if available.

If your network does not have DNS, you can also assign hostnames in %windir%\system32\drivers\etc\hosts on Windows. You must assign a hostname in addition to an IP address in that file. Here are some example hosts file contents (including two commented lines where you would have to remove the # sign to make them effective):

```
#      102.54.94.97     rhino.acme.com          # source server

#       38.25.63.10     x.acme.com              # x client host

127.0.0.1       localhost
```

CAUTION: This software does not support installation to anything but the local file system. Avoid installing to shared drives.

Protocols

This application uses the following protocols: TCP/IP, SNMP, HTTP, UDP Multicast. You can bypass multicast, if it is disabled on your network. To allow a client to connect without multicast, add the following property to the client's owareapps\installprops\lib\installed.properties file.

```
OWARE.CONTEXT.SERVER.URL=jnp://[HostName]:1099
```

Fixed IP Address

OpenManage™ Network Manager is is a web server, among other things, and so must be installed to a host with a fixed IP address. For demonstration purposes, you can rely on dynamic IP address assignment (DHCP) with a long lease, but this is not recommended for production installations.

Windows Prerequisites

This application requires a temp directory on the host where it is being installed. If the install launcher cannot extract a Java Virtual Machine (JVM), then it cannot run. The launcher extracts a JVM to a temp directory and then starts the installer main using this temp JVM.

Windows typically has a temp directory, WINDOWS\temp. Installation expects that TEMP or TMP environment variable exists and points to this temp directory (check in a command shell with cd %TEMP% or cd %TMP%).

You can also execute the win_setup.exe installation from a command line to override temp directory locations with this command line:

```
win_setup.exe -is:tempdir c:\mytemp
```

Although it is not always necessary, during installation or uninstallation best practice is to disable any virus protection software, and any other running application. Some applications have additional services (like Norton Unerase) that prevent correct installation on Windows 2000. Stop these in Services in Control Panel's Administrative Tools.

This application cannot co-exist with other installations of Cygwin on the same Windows computer. Do not install it where Cygwin is already installed, either separately or as part of another application. If Cygwin is already installed, remove it before installing this application.

Windows 2000 installations require SP1 or higher. Firewall products should be disabled during initial installation and testing.

If they are present, turn off Microsoft Windows SNMP Services and Traps.

Linux Prerequisites

If you are installing on Linux, you must log in as a non-root user. Linux installation prompts you to run some additional scripts as root.

When installing to Linux, ensure you are installing as a user with the correct permissions, and are in the correct group. You must configure the installation directory so this user and group have all permissions (770, at least). You may install without any universal ("world") permissions. However, you must create a home directory for the installing user.

NOTE: All files created during installation respect a umask of 007. All files from setup.jar are 770. Files from ocpinstall -x are set for 660. Bin scripts from ocpinstall -x are 770.

Best practice is to install as the user designated as DBA and admin of the system. If necessary, create the appropriate user and login as this user for running the install program. The installing user must have create privileges for the target directory. By default, this directory is `/opt/dorado`.

NOTE: Linux sometimes installs a MySQL database with the operating system. Before you install this application, remove any MySQL if it exists on your Linux machine.

NOTE: To set the environment correctly for command line functions, after installation, type `oware` (or . `/etc/.dsienv in UNIX—[dot][space]/etc/[dot]dsienv)` before running the specified command. Also: This application can run on any Linux desktop environment (CDE, KDE, Gnome, and so on) but the installer will only install shortcuts for CDE.

System Capacity

System requirements for each element of your system vary depending how you use it. The numbers in this guide are suggestions only, not definitive recommendations.

You should base the minimum configuration of any system on expected peak load. Typically a configuration running all elements of the application on a single server spends 95% of its time idle and 5% of its time trying to keep pace with the resource demands. If you expect your system to perform an operation that could run create, modify or delete rules on tens or hundreds of thousands of business objects, your system requirements may be much higher.

Sizing for Printers

The following are disk space and/or database space requirements for managing printers. In addition to the sizes listed here (G = gigabyte, M = megabyte), you will need a gigabyte for system configuration and incidental data. Here are the suggested calculations:

- 4.5 M per printer
- So for each Gigabyte of memory this application can manage roughly 220 printers. For example:
- 10 G - 2200 printers
- 20 G - 4400 printers
- 14 G ~ 3000 printers

The database size for a 3,000 printer installation would be - 15 G.

We base these calculations on some key assumptions: 30 days of audit history, 30 days of job history, 30 days of event history and the default roll up polices regarding data collection. These durations are the default DAP parameters for details about how to alter these. If you adjust the DAP parameters, you must adjust the database requirements.

For example: Doubling the audit history from 30 days to 60 increases database requirements by 1M per printer. Doubling the job history from 30 days to 60 increases database requirements by 2.75M per printer.

Paths

The shell command oware makes any shell subsequently emulate a UNIX bash shell. That means either foreslash or backslash can accurately represent path separators as they may appear, depending on whether the oware command has set the environment to bash emulation. Most shell commands for this application are available in Windows/DOS equivalents structured to call the emulator, then a bash script. If you have difficulty using a command line script in Windows/DOS,then try it after you have run oware.

NOTE: Run command line scripts with -? to see their parameters.

Installing the Application

If you are installing the software on a machine with multiple Network Interface Cards (NICs), installation prompts you to select one IP address for the system you are installing.

1 Log in as a user with administrator's permissions on the Windows machine where you want to install the software or as any non-root account onLinux.

CAUTION: You must install as a non-root user with the permission to create directories in the selected installationpath. Installing to a directory that requires root level access fails.Also: Using the login "admin" to do the installation wipes out any pre-configured "admin" permissions that come with the application. Therefore do not use "admin " as the installing user account.
Also: Do not use an installing login ID that contains spaces.

2 If you are installing from CD, insert it into its drive. In Windows, the installation autoruns. If the installer does not appear, or if you have disabled autorun, you can run `win_install.exe` from a file manager.

run linux_install

A dialog appears as the Setup program initializes InstallShield. Then a Welcome Screen appears, listing the package you are about to install, and reminding you to shut down other running software (this may include anti-virus software). Click *Next*.

⚠ **CAUTION: You cannot install from a directory whose name begins with @.Also: You must extract any compressed (zipped) installation source before executing the installation.**

3 Installation performs a series of system checks to verify the target system is supported. If all checks pass, the license agreement appears.appears. You must accept the license to proceed.

4 Click *Next*.

5 The next screen displays the list of components you are about to install. Click Next.

6 The next screen lets you select the directory where the application installs. If you want to install to a different directory, type the path or click *Browse*.

After confirming the installation location, click *Next*.

7 Select the setup type from the available options.

- **Full Installation—**Installs application server, database server, mediation server, and client on the host.

  If you selected the included MySQL database, a subsequent screen (after the application installer progress completes) prompts for the data location(by default [installation root]\oware3rd\mysql), initial and maximum database size.

  If you selected Oracle as your database (on a separate machine) a subsequent screen prompts you for the Oracle connection details when installing an application server with Oracle as the chosen DBMS. Fill in initial values for Logon User and Password along with the Host, Port and SID.

- **Client Installation**—This installs client software. It does not configure the machine to run a Mediation Agent or Application Server.A subsequent screen asks you to fill in the partition where this machine is a client.

  NOTE: To allow a client to connect without multicast, add the following property to the client's owareapps\installprops\lib\installed.properties file.

  OWARE.CONTEXT.SERVER.URL=jnp://[HostName]:1099

  NOTE: This application supports a web client. Refer to the User Guide for specifics about how to use it and make it secure.

8 **If installing to a multi-homed machine (multiple NICs), choose a default IP address for use by the software. Installation automatically records this address.**

You can add the following properties to `owareapps\installprops\installed.properties` to override portions of the IP selection's impacts:

```
#
# specific interface used for all NMS initiated
# communications to the network
com.dorado.mediation.outbound.address=localhost
#
# specific interface used for binding mediation
# listeners such as SNMP trap listener
com.dorado.mediation.listener.address=localhost
#
# specific interface used for all northbound
# communications to external management system(s)
com.dorado.mediation.northbound.address=localhost
```

For any property, replace the *localhost* text with the correct IP. See Overriding Properties for more information..

9. The next screen lets you confirm the partition name (by default this is the hostname of the application server), and includes radio buttons that let you select whether to install application server as a service—something that runs even when you are logged off.
10. The next screen lets you select a heap size to tune application server performance.The default is 512 M. Best practice is to have equal amounts for minimum and maximum heap size.
11. An installation summary appears.
12. The setup program automatically installs all of the managed system software for your hardware configuration.
13. If you are installing the embedded database server (MySql), the installer either builds the database for first time use or prompts with options if a database already exists. Building an initial database may take ten minutes or more to complete.
14. A prompt appears that lets you start the service without rebooting again. If you elect to start the application server service, a monitor icon appears in the Windows tray (typically the bottom right of your screen) that is yellow as application server begins running, and green when it is up and running.
15. Finally, the application prompts you to click *Finish*. This completes the installation.

NOTE: After you complete the installation, you may want to install Adobe Acrobat Reader. An installation is included with the installation CD, or you can download a free copy from www.adobe.com. This application requires Acrobat to successfully print reports.

Default users initially have no password. Users must typically change this blank password with the first login. The login for the installing user is, by default *admin*.

Passwords are stored in the database, encrypted. You can also change this password later from the *Settings > Change Password* menu item in the application.

Starting Application Server

You can stop, start and monitor the application server service, with command lines (`pmstopall, pmstartall` and `pmgetstatus`), or use a system tray tool for controlling application server.

For security reasons, pmstopall has a security requirements similar to stopappserver. Here is a sample command line:

pmstopall <hostname>:1099 -u <username> -p <password>

Both -u and -p are optional parameters. If you omit username, the application assumes OWAdmin is the user. If you omit a password, the application assumes a blank password.

This service appears in the Windows Services dialog as Dell OpenManage Network Manager.

pmgetstatus

If you elect to autostart your application server, you can run the pmgetstatus script from a command line. If you run oware first in the shell where you run pmgetstatus, this script will automatically be on the path. Here is its usage (produced by typing the script name followed by -h):

Usage: pmgetstatus [-h <Server IP>] [-p <Server Port>] [-i <Iterations>

[-r <Refresh Rate>]]

Oware utility for reporting status on managed server processes.

By default, the local host is queried for 1 iteration.

Options:

-p <Server Port> -- Process monitor command port.

Default loaded from g:/dorado/oware/lib

/pmstartup.dat

-i <Iterations> -- Number of times to repeat command, -1 is

infinite (requires Ctl-C).

-r <Refresh Rate> -- Refresh rate of iterative command in seconds.

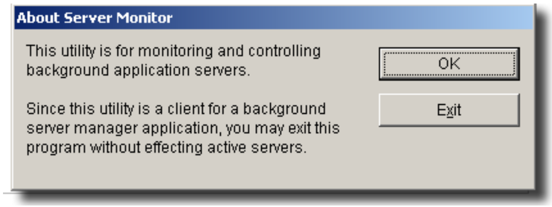
Default is 5. Requires -i option.

-? -- Show this help.

Windows Server Monitor

When you install your application as a service on Windows, you also install a server monitor. This monitor is a client to the server manager which controls starting and stopping of an application or mediation server.

Figure 23-1. Server Manager Client



About Server Monitor

This utility is for monitoring and controlling background application servers.

Since this utility is a client for a background server manager application, you may exit this program without effecting active servers.

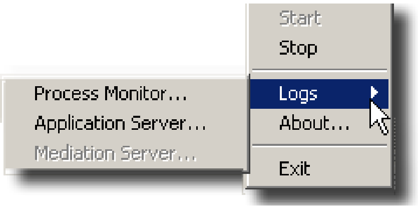
Double click the tray icon to display the about panel. *OK* closes this dialog, but maintains the icon in the tray, while *Exit* closes the Server Manager (client and tray icon).

The tray icons themselves indicate the current service condition.

Icon	Status
⊗	Offline (no status available, or not controlled by server manager)
○	Idle
🟡	Running (initializing, or shutting down)
🟢	Ready
🔴	Stopped

You can also right-click the icon to see the client menu.

Figure 23-2. Process Monitor Client Menu



The logs items let you view logged items for Server Manager, application server or mediation server. You can *Start* or *Stop* the service(s) running on your host.

NOTE: System changes can make the server monitor system tray icon disappear while the process is still running. If you cannot make your icon reappear, try running
`pmtray -r` from a command line, then restart the server monitor.

Startup Properties

The values in `installed.properties` now set most properties for the process monitor to pass when starting a server. All command-line options for the `startappserver` script are now in `installed.properties` (see Overriding Properties). These are active for each execution of the server (even a mediation server) on the machine where the override exists. Command line arguments override these properties.

The following are properties you can set in `owareapps\installprops\lib\installed.properties` to configure servers:

- Default server partition name also used by client and mediation to locate a server

  ```
  oware.client.partition.name=demo1
  ```

- Default interface used by servers and direct access cut-thru sessions.

  ```
  oware.local.ip.address=192.168.0.10
  ```

The IP address also appears in database connection properties:

```
com.dorado.meta_database.name=//192.168.0.10:3306/owmetadb
```

```
com.dorado.jdbc.database_name.mysql=//192.168.0.10:3306/owbusdb
```

To change the IP address, stop the server, set is property to the new IP and delete the `oware/temp` directory. Then restart the server.

ipaddresschange

A simpler alternative to changing properties is to use the ipaddresschange script. If you were to install this application on a machine on one network, then move your machine to another network, the IP address from your original network remains hard-coded. You must change the application's IP address to reflect the new network for the software to function correctly. Here is how to do it, once you have connected the application server machine to the new network:

a First, shut down the Oware Server Manager. Open a command shell (**Start→ Run cmd**, in Windows) then type: `net stop "Oware Server Manager"` (including the quote marks)

b Next, find out what your new IP address is. To do this type `ipconfig` in the command shell you just opened, and make note of the IP Address that appears. You will need that number in a subsequent step.

c Type oware at the command line. This sets the environment.

d In the same shell, type ipaddresschange `-n` [the IP address discovered in b]

e Restart Oware Server Manager by typing: `net start "Oware Server Manager"` (including the quote marks)

Your machine should then be able to connect to other devices on this network and function correctly.

NOTE: After the utility is done, if you are using Server Monitor, its Icon in the program tray has an x through it. You must either reboot or use Windows' Administrative facility stop the oware server manager service and restart it.

- Use only https for web services and web clients

```
oware.appserver.web.enable.https=false
```

NOTE: If you want https access to web pages ordering toner, and so on, you must alter this property on all clients as well as application server.

- Set to true when there is no graphics adaptor available for server

```
java.awt.headless=false
```

- To change the default HTTP/HTTPS port numbers for web application or web services, add the following properties to `owareapps/installprops/lib/installed.properties`:

```
oware.appserver.web.http.port=[default port number: 80 or 8080]
```

```
oware.appserver.web.https.port=443
```

You may then change the port values for these property entries and restart the application server. Special setup (outside the scope of this document) is necessary to run a web server on port numbers lower than 1024 on many operating systems.

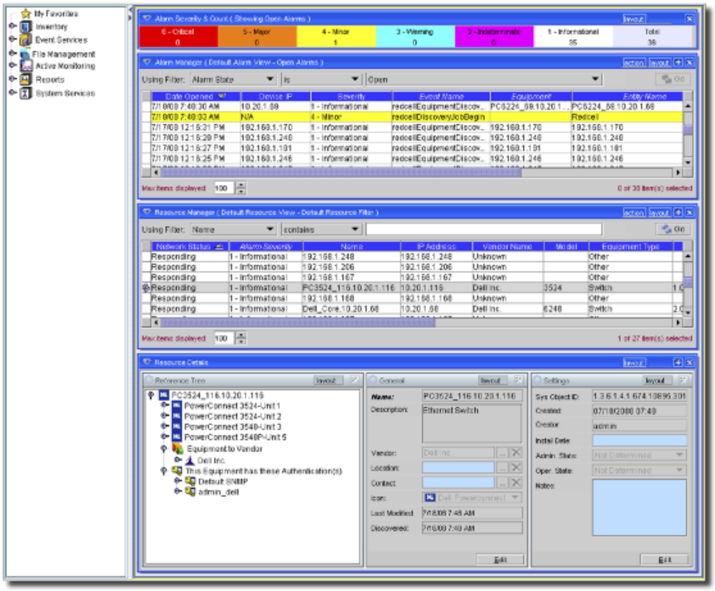
NOTE: Do not change the system time while the application server is running. If you must change the system time, shut down the server before the change, and restart it afterwards.

Discovery for Admin

The *admin* user gets a special shortcut to discovery in the screen that appears after logging in. The first time the client appears, a screen offers a shortcut to discovery.

After you click **Begin Discovery** the advanced discovery wizard opens for initial discovery of devices on your network. After completing discovery, by default, a QuickView layout appears with the discovered devices.

Figure 23-3. Quick View Layout



6 - Critical	5 - Major	4 - Minor	3 - Warning	2 - Indeterminate	1 - Informational	Total
0	0	1	0	0	35	36

Using Filter: Alarm State | is | Open

Date Opened	Device IP	Severity	Event Name	Equipment	Entity Name
7/18/08 7:48:30 AM	10.20.1.68	1 - Informational	redcellEquipmentDiscov...	PC6224_68.10.20.1...	PC6224_68.10.20.1.68
7/18/08 7:48:03 AM	N/A	4 - Minor	redcellDiscoveryJobBegin		Redcell
7/17/08 12:16:31 PM	192.168.1.170	1 - Informational	redcellEquipmentDiscov...	192.168.1.170	192.168.1.170
7/17/08 12:16:29 PM	192.168.1.248	1 - Informational	redcellEquipmentDiscov...	192.168.1.248	192.168.1.248
7/17/08 12:16:27 PM	192.168.1.181	1 - Informational	redcellEquipmentDiscov...	192.168.1.181	192.168.1.181
7/17/08 12:16:25 PM	192.168.1.246	1 - Informational	redcellEquipmentDiscov...	192.168.1.246	192.168.1.246

Max items displayed: 100 — 0 of 33 item(s) selected

Using Filter: Name | contains

Network Status	Alarm Severity	Name	IP Address	Vendor Name	Model	Equipment Type
Responding	1 - Informational	192.168.1.248	192.168.1.248	Unknown		Other
Responding	1 - Informational	192.168.1.206	192.168.1.206	Unknown		Other
Responding	1 - Informational	192.168.1.167	192.168.1.167	Unknown		Other
Responding	1 - Informational	PC3524_116.10.20.1.116	10.20.1.116	Dell Inc.	3524	Switch
Responding	1 - Informational	192.168.1.168	192.168.1.168	Unknown		Other
Responding	1 - Informational	Dell_Core.10.20.1.68	10.20.1.68	Dell Inc.	6248	Switch

Max items displayed: 100 — 1 of 27 item(s) selected

- PC3524_116.10.20.1.116
  - PowerConnect 3524-Unit 1
  - PowerConnect 3524-Unit 2
  - PowerConnect 3548-Unit 3
  - PowerConnect 3548P-Unit 5
  - Equipment to Vendor
    - Dell Inc.
  - This Equipment has these Authentication(s)
    - Default SNMP
    - admin_dell

Name: PC3524_116.10.20.1.116
Description: Ethernet Switch
Vendor: Dell Inc.
Location:
Contact:
Icon: Dell Powerconnect
Last Modified: 7/18/08 7:48 AM
Discovered: 7/18/08 7:48 AM

Sys Object ID: 1.3.6.1.4.1.674.10895.301
Created: 07/18/2008 07:48
Creator: admin
Install Date:
Admin. State: Not Determined
Oper. State: Not Determined
Notes:

Consult the online help for additional information.

Updating an Existing Installation

Always consult the manuals and CD contents for upgrade instructions. Database changes may require a migration step to preserve your data when moving to a new version.

NOTE: If you are upgrading NetConfig, you may have to update configuration file backups. Consult the NetConfig release notes for instructions about how to do this.

CAUTION: You should always perform a complete backup of your system and database before attempting an upgrade. Failures during upgrade can result in a corrupt installation.

If you have a previously-installed version of the application on your computer and attempt to run the installation program an update installation dialog appears. It reminds you that setup can update previously installed features. To change features, however, you must first uninstall the existing software.

After files install, select whether you want the installation program to rebuild the database content, otherwise, the application keeps the existing one. The installation wizard begins copying the needed files.

If your installation fails, see `setup.log`, `db_setup.log` or `app_setup.log` in the destination directory for the installation for messages that may help fix the failure.

NOTE: Servers should not be running during updates and uninstallation. Just before file transfers a screen appears, saying “Checking for active servers.” This only checks with the server manager and would not detect a server started manually. If one is running, then you are warned to stop it with an option to test further.

CAUTION: If you do an update installation, even if you elect not to rebuild the database, installation *always* re-seeds the system settings. If you have changed your settings, you may want to export these before proceeding. See the *User Guide* for more information.

Database Evolution

NOTE: Database evolution is a schema evolution process which is automated as part of the upgrade installation for MySQL users.

You can re-install an existing installation this way:

1. Back up database with the `dbbackkup` script, and copy any properties overrides and exported settings to a backup location.
2. uninstall/re-install the application and
3. restore the database, properties, and settings. (See the *User Guide* for more information.)

Also, see "Overriding Properties" on page 279—an important part of any update to your installation.

Printer Template Updates

If you have a printer management driver installed, you may want to update printer templates. These templates translate the messages and commands that pass between the managed printers and the application. To fully manage newly released or new types of printers, you must download new templates from www.dell.com, then register them to the application..

To register a template to the application, follow these steps:

1. Open a command shell. *Start* > *Run* `cmd`.
2. Type `oware` on the command line and press *Enter*.
3. Run the `registertemplate` command at the subsequent command line. Here is the syntax of that command:

   ```
   registertemplate <template_file_name>
   ```

   The `template_file_name` needs to be a complete path to the file. If you provide no filename then the script will re-register all template files in the `owareapps\printer\lib` directory. Best practice is to copy the template file to the `owareapps\printer\lib` directory and then run the registertemplate command. Once you have registered the new template, you must stop and restart polling on the new printer models. This forces the application to rebuild the polling subscription with the new template information.

   Rediscovering the printer is unnecessary. Stopping then re-enabling polling builds the polling subscription with the new values from the template. If the template addressed identification issues (serial number, MAC address or host name), page count, toner levels or toner max levels then you must stop the trend polling and restart that as well.

Cancelling the Installation

Once the installer finishes transferring files, the application is installed; you cannot cancel installation. Short of killing the installer process, you cannot cancel database initialization or component installation and seeding.The installer considers this portion of its work system configuration and not application installation so it cannot stop unless you kill the process . If you do manage to abort the install after file transfer completes (after the "creating uninstaller" message goes away), then you must run the uninstaller to remove the software.

⚠ **CAUTION: Cancellation is *not* recommended. You may strand processes that you must then manually shut down. Some directories and files would be left behind after the automatic rollback that occurs when cancelling an install.**

Uninstalling

You can uninstall the software by using Windows' control panel's *Add/Remove programs* feature (or with `win_uninstall.exe`), or by running the following on UNIX:

```
$OWARE_USER_ROOT/_uninst/linux_uninstall
```

or for console mode, run...

`OWARE_USER_ROOT/_uninst/linux_uninstall -console -is:javaconsole`.

NOTE: If you uninstall in a shell rather than using the graphic uninstaller, uninstaller cannot uninstall its own directory. This produces some errors you can ignore in a console uninstallation. Use `cd /opt` and then `rm -rf [installation target directory]` to do final cleanup.

In graphic uninstallation, as in installation, click *Next* to continue through the screens as they appear. One such screen appears listing what you want to uninstall. Confirm that you want to remove all the listed installed components. You can optionally delete all the applications' files and directories (complete removal).

⚠ **CAUTION: Uninstallation on MySql servers may delete the database and any application directories. The applications' directories also contains any installed application components and device drivers.**

The option to delete directories is primarily to support application developers having to uninstall and re-install the basic application platform without losing component files (like device drivers) on disk that were not part of the installation.

NOTE: Deletion is recommended, but not required. It removes files created after installation; temp files, database files, cache files, and files extracted from OCP/DDP files. Overall, it is the best way to get a clean uninstallation. You can back up your `oware/lib/*.properties` files or overrides before uninstalling if you want to preserve them. An alternative is overriding properties See "Overriding Properties" on page 279 for more information.

When the software has been completely uninstalled on Windows, if prompted, you must reboot your computer to complete deletion of any locked files. Best practice is to reboot right away. Uninstallation removes everything it has permissions to delete.

Stopping Servers

To stop the application server, you can either use the application server tray icon in Windows (see Starting Application Server), or stop the server from a command line. The command line to stop a server is `pmstopall`.

If you have not automated server startup, then you can use the `stopappserver` and `stopmedserver` scripts to stop these servers, even remotely. Here is the syntax:

```
stopappserver <hostname>:1099 -u <username> -p <password>

stopmedserver <hostname>:1099 -u <username> -p <password>
```

Both `-u` and `-p` are optional parameters. If you omit `username`, the application assumes `OWAdmin` is the user. If you omit a password, the application assumes a blank password.

If you have not logged in and changed the password for OWAdmin with the application's login screen the login to stop the server fails. By default, `OWAdmin` and the installing user have the role `OWServerAdmin`. Any user assigned this role can stop the appserver. Blank passwords are valid if they are defined for the user.

If you used `startappserver` in a shell to start the application server, you can stop the server by either interrupting that shell with Ctrl+C or by closing the shell. Ultimately, you can kill the Java processes on your machine to halt a server.

See "Updating an Existing Installation" on page 275 for additional notes about shutting down processes and services. If you uninstall when a server is active, the uninstallation will attempt to shut it down and failing that will prompt you to shut it down manually.

Linux Command Line Installation

You can run a Linux installation from a command line with text prompts that are equivalent to the graphic interface prompts described in "Installing the Application" on page 268, and the following pages. Here is the command line to run the text only installation:

```
install/linux/linuxinstall -console
```

Modified Files

The following system files may be modified during root installation:

```
/etc/.dsienv - installed

/etc/my.cnf - installed

/etc/rc2.d/S75owaredb – installed

/etc/rc2.d/S76oware – installed
```

The rest of the installation installs program files, does the setup functions, and performs the initial database load.

Overriding Properties

Installation typically makes all of the modifications needed to properties files, but if your installation customizes some properties, best practice is not to change default properties, but to override them. This eliminates updates or new installations overwriting property files you have configured. Best practice also includes backing up the override file(s) as described below.

To override a property, put the property itself in `installed.properties` under `owareapps\installprops\lib`. You can override selected (high availability) mediation server properties in `owareapps\installprops\medserver\lib`. Application property values are loaded first and you can override those values here.

NOTE: Installation updates or refreshes the appropriate properties in installed.properties, but does not overwrite the file, property additions you make are safe from installation changing them in this override file. New properties coming from an installtion are appended to the files.

The following is an example of property file content to override an application

cache time-out:

```
#============================================
# Dependencies
#============================================
product.dependencies=redcell

#============================================
# Application Overrides
#============================================
# set event template cache timeout to 1 minute
redcell.assurance.batch.processing.event.template.cache.expiration=
60000
```

CAUTION: If any of the dependency directory names (for example, `owareapps/redcell`) do not exist, then the application does *not* load override file.

Consult the comments in the properties files you are overriding for further information about specific properties.

Properties Loading

First the application loads all property files from the application (`/oware/lib`). Then it loads all property files from `owareapps\*\lib`. A special property `product.dependencies` that lets you control the order that files are loaded. For example setting `product.dependencies=myApp` makes owareapps properties (other than myApp) load after myApp. The product name for this property is the name of the directory under owareapps. You can also specify multiple products with a comma (,) delimited list.

Prepend and Append Keywords

One reason to have dependent property loading is to modify a property used by another product. You may need to ensure that your value comes after the other products, or vice versa. When Java reads properties, its default behavior is to override the old value with the new when encountering an identically-named property. This would compel product maintainers to change a product whenever property file changes occurred in the product on which they depend. Such maintenance would increase geometrically, especially with multiple dependencies.

This application supports property appending or prepending through keywords. If you preface the property to be modified with append. or prepend., you can put your own value after or before the original property's value(s). You must be aware of the original property's delimiters and either add one at the beginning of your value if appending, or add one at the end of your value if prepending. For example: Given a pre-existing property: oware.foo=original

```
append.oware.foo=,newappend
```

This produces oware.foo=original,newappend

```
prepend.oware.foo=newprepend,
```

This produces oware.foo=newprepend,original

If the original property is null, the first character (if appending) or last character (if prepending) is stripped (to eliminate the separator) and the property created with the resulting value. Currently, properties permit only one instance of a keyword within a given property file.

Ports Used

This application uses the following ports in a non clustered installation. Ensure your firewalls or other network security measures do not block theseports.

Port Number	Used by...
1098	Naming service (JNDI)
1099	Naming service (JNDI)
3100	HA Naming Service (JNDI)
3200	HA Naming Service (JNDI RMI)
4444	JRMP invocation (RMI)
4445	Pooled JRMP invocation (RMI)
6500 to 6510	Mediation cut-through
80	HTTP

Port Number	Used by...
443	HTTPS
8093	JMS

The client HTTP cut-through goes directly to the printer from the client. So, you must get to printers via port 8080 to demo cut-through to the embedded web server. Telnet cut-through (seldom applicable to printers) goes directly to the application server as a proxy on ports 6500-6510.

The following ports are seldom required, but are listed here in case present or future functionality requires them:

Port	Used by...
23	Telnet
1103	JNP Discovery
1123	JNP REPLY

Linux Partition Information

Suggested partitioning includes separation into several partitions including /,

swap, /usr, /opt, and /export/home.

/ (root)—The root partition contains everything that is not specifically placed on a slice/partition. The rule of thumb here is: Do not put data on this partition that is likely to grow significantly (logs, applications, data, and so on). This partition can be as little as 200MB, however best practice indicates as much as 2 GB if space is available.

swap—swap is the space allocated for the operating system to use as part of its virtual memory to augment physical memory. If something in memory has not been used for a while, the operating system will move it to disk temporarily. Recommendations for this are typically for two to three times the physical memory, however we usually determine the amount available based on physical memory. If you have 512 MB, specify 1.5-2.0 GB. As physical memory increases, still specify 1-2 times the physical memory so you have enough disk space for the operating system. The following are instructions about setting swap:

- **a** Check your current swap space setting with `swap -l`
- **b** su to root (if not already).
- **c** Issue `mkfile (size required) (filename)`
- **d** Execute `swap -a (pathname)`. This adds the swap file. You must use an absolute path name.
- **e** Check with `swap -l` to confirm the new swap addition.

/usr—Typically holds operating system commands and utilities related to the operating system. `/usr` can also contain the documentation associated with these commands. This partition should be a minimum of 1.5 GB for a full installation. Best practice is to specify 2 GB and potentially more if you know you will be adding operating system utilities.

/etc—It is recommended that this be located on the root partition, not on its own partition. The data here may change from time to time, but the typically does not grow significantly.

/var—Best practice is to create a partition for `/var`. This contains the syslog data, print spool, mail, and so on. This partition could grow significantly from the required amount of disk space depending on the applications running on the system. We recommend you allow at least 2 GB.

/opt—The `/opt` partition holds application software that is added to the system. Redcell would be an application that should be installed here. The size of this partition should depend on the required disk space for applications including Redcell. Both the application's software and data reside in the same directory structure, however, so you can add more volumes to another partition.

/export/home—`/export/home` is typically for user data. Most systems have user home drives specified in this space (for example: /export/home/auser). This should have enough space for all user data.

/<some_partition_name>—With a RAID configuration, you can specify a large amount of disk space for data purposes.

You must also enable process monitor with the appropriate property set to true in `oware/lib/pmstartup.dat`. The property relates to either application server `(application.server.active=true or false)` or mediation server `(mediation.server.active=false or true)`, not both.

24

Configuring the Runtime Environment

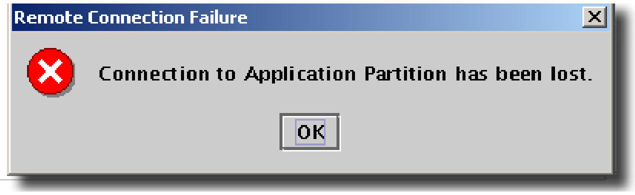
Runtime Requirements

This application runs as a thin client. It gets services from an application server, which must be up and running before any clients start.

Application Server

Clients do not run if they cannot connect to an application server. Instead, a warning appears and the clients shut down.

If a client loses connection to the application server (for example, if the application server restarts) a *Connection Lost* dialog appears. Click **Re-start** to reestablish the connection to the application server.



Remote Connection Failure

Connection to Application Partition has been lost.

When the Application Server finishes loading, the application server log displays `Rule Load Complete`. After you see this message you can start clients.

NOTE: Clients may need two or three minutes to reestablish an application server connection if the server fails and goes down. You can also restart clients to reconnect them to the application server.

Server Options

Application server can run from a command line that lets you start up with several options. Consult Application Server for details.

Configuring the Server

You typically configure the application server during or immediately after its installation. Application server configuration settings are in `oware\lib` in the files `owappserverstartup.properties` and `owappserver.properties`, and you can edit these with any text editor. See "Overriding Properties" on page 279 for more information about configuring application server. See Properties ,for additional details. See also the results of `startappserver -h` from a command line or the application server section of the *User Guide* discussing additional command line options.

Mediation Service

The Mediation Service provides an interface to external systems and devices. Mediation Services come from one or more Mediation Agents. In a single host installation, application server typically also starts the mediation service.

Except for authentication (logins and passwords for devices) and connectivity to the managed network, device drivers automate most mediation configuration. For example, if you want to manage XYZ devices, connect your hardware to the network with those devices and install the application's XYZ device driver (XYZ is an example, not a real driver). You supply the login and password for those devices during device discovery.

NOTE: Dell Device drivers are automatically installed with the application. Other types of device drivers are available too.

Default external protocols supported can include:

- General ASCII
- TL1
- SNMP
- Web Services
- ICMP
- MML
- Partial Q3

A Mediation Agent contains Managed Beans (MBeans) that manage the physical connections to a mediation target system or device. Connections might include communications with serial port devices, telnet sessions, TCP sockets, and external databases. The mediation agent executes dialogs with the mediation target (at the instruction of the client application) to retrieve and/or send data with the connection.

The Mediation Agent is essential for all operations involving communications with external systems and devices. If one is not running, you can still make administrative changes to the system, but it processes no traps or other external communication.

Database Timeout

When managing large networks or equipment with many interfaces, you may have to increase `the com.dorado.bom.lock_timeout` property in `owdatabase.properties`. Increase this setting based on the size of the equipment being managed. Generally, you should set this value to the maximum number of interfaces you expect your network elements to have. For example, if the element is expected to have 500 logical interfaces then the timeout value should be set to 500.

NOTE: The minimum recommended timeout value is 60 seconds.

Client Logging

This application preserves the client log files by appending the user id and current timestamp to the log file name (otherwise files would be overwritten).

As a result, client log files are never overwritten; they accumulate in the log directory (`owareapps\redcell\logs`). Therefore, you must periodically clean up client logs files. The `client-log4j.xml` file in `owareapps\redcell\lib` directory controls the filename for the client log. By default, it contains the following setting:

```
${oware.user.root}/owareapps/redcell/logs/client-
   ${com.dorado.redcell.RCSessionId}.log
```

Here, `com.dorado.redcell.RCSessionId` is the user id and timestamp (`admin-1056133530200` for example). If you do not want to preserve the log file for each client session and want to overwrite the previous log file then modify the above line to -

```
${oware.user.root}/owareapps/redcell/logs/client.log
```

This means you do not need to periodically clean up log files.

Other Logging

The *getlogs* script is now included with your software. It creates a `logs.jar` file in the root installation directory, and moves any existing copy of `logs.jar` to `oware\temp`. This jar compresses all logs necessary for troubleshooting. Read the jar yourself, or forward this jar to Dell technical support to help troubleshoot.

When troubleshooting (or contacting technical support), you may find pertinent information in logs located in the following directories:

```
..\oware\jboss-3.0.8\server\oware\log

..\oware\temp\soniqmq.log

..\app_setup.log

..\db_setup.log
```

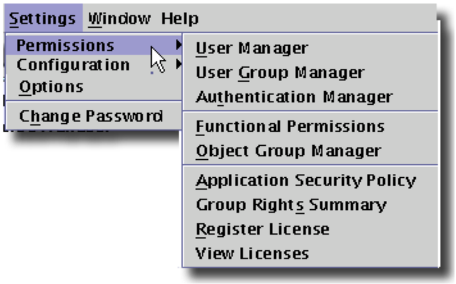
25

Security

Security Overview

This application enforces security several ways, including permissions, authentication, and security policies. The various Managers and interfaces that set and view security settings appear in the Permissions submenu, shown below. Access it by selecting *Settings* > *Permissions*.

Figure 25-1. Permissions Submenu



⚠ **CAUTION: All users inherit OWPublic's permissions. You must remove OWPublic's read permissions from things in Object Group Manager to conceal those items.**
Also: Functional permissions are application-wide (see *Functional Permissions Editor* on page 309). When concatenated with other permissions they are additive (unions, not intersections).

Security Events

This application emits security events. The base security event is *OWSecurityEvent*. Here are the rest of the Security Events, with comments where their title does not make their function self-evident:

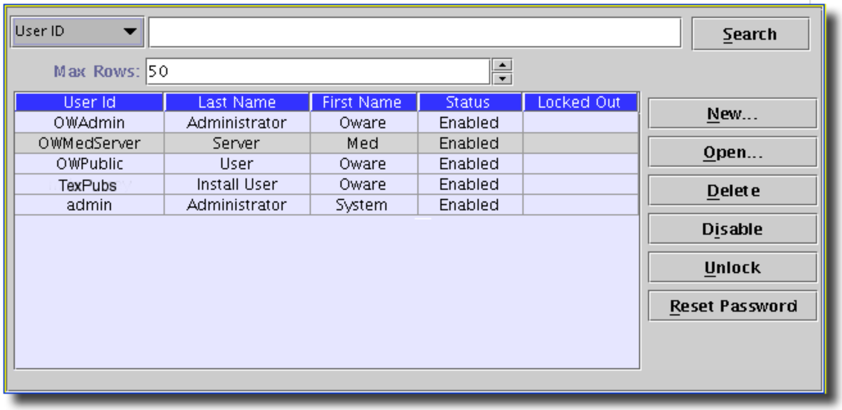
- OWSecurityAccountResetEvent
- OWSecurityClientTerminationEvent — Success of previous event request, emitted just before client termination.
- OWSecurityLoggedOnEvent — Response to previous event's request; user monitor listens to build list of active clients.
- OWSecurityLogoffEvent
- OWSecurityLogonEvent
- OWSecurityPasswordChangeEvent

- OWSecurityPasswordResetEvent
- OWSecurityRequestEvent — The base class extended by all OWSecurity* RequestEvents.
- OWSecurityResponseEvent — Base class extended by all non-OWSecurity*
- OWSecurityUserDisabledEvent
- OWSecurityUserLockedOutEvent

User Manager

The application's User Manager, shown below, lets you create and manage users, and associate information with them like passwords, group membership, and contact information. Select *Settings > Permissions > User Manager* to display the User Manager.

Figure 25-2. User Manager



User ID

Max Rows: 50

User Id	Last Name	First Name	Status	Locked Out
OWAdmin	Administrator	Oware	Enabled	
OWMedServer	Server	Med	Enabled	
OWPublic	User	Oware	Enabled	
TexPubs	Install User	Oware	Enabled	
admin	Administrator	System	Enabled	

The User Manager displays the *User ID*, *First* and *Last Name*, *Status* (enabled or disabled) and whether the user is *Locked Out*. Use the *Max Rows* field to limit the number of records that appear at once on screen. You can also filter the display to show a select subset of users, and can sort so users appear in the order you like.

To filter the display:

Select a filter parameter (*UserID*, *Last Name*, *Groups*) from the tab at the top left of this screen, enter the corresponding search text in the text field, and click *Search*.

If you select *Groups* as the filter criteria, a drop-down menu appears in place of the text field. Select one of the groups from this menu and click *Search*.

To sort the display:

Click on any column header to sort the display based on that column’s contents. The initial click sorts the column in ascending order; the next click sorts in descending order. Subsequent clicks toggle the sort between ascending and descending.

The User Manager has these controls:

- **New** — Opens a dialog where you can add new users to the system. See Adding or Modifying a User for more information.

  NOTE: Best practice is to add new users rather than making changes to administrative privileges.

- **Open** — Opens an edit dialog populated with the information for the selected user. See Adding or Modifying a User for more information.
- **Delete**—Removes the selected user from the list (and the application).
- **Disable** — Prevents the selected user from logging on to the application by setting the user’s Expiration Date to the current date.
- **Unlock** — Releases the lock on the selected user. (Locks are indicated by an entry in the *Locked Out* field.) Users are locked out if they try to log in with an incorrect password too many times (default = 4). When this happens the date and time of lock out appears in the *Locked out* column. Administrators can configure the number of attempts allowed users before they are locked out (see Login Policy).

  Unless otherwise configured, locked-out users cannot gain entry into the system until an administrator releases their locks. Unlocking a locked-out user sets the user’s password to a blank. The password change screen automatically appears with the newly-enabled user’s first login.

- **Reset Password** — Displays a dialog where you can specify a new password for the selected user. Enter the new password in the *New Password* field and again in the *Re-enter Password* field and click OK to implement the change.

NOTE: *OWAdmin* without any password exists by default as an alternative user with administrative privileges. If you want your installation to be extremely secure, delete this user, but understand that you will have to re-install if other, authorized administrators cannot log in for some reason.

Default Users

Installation automatically seeds the following users

- **OWMedServer**—An internal user (principal) used by the system. You can neither log in with this account nor delete it.
- **OWPublic**—An internal user that provides base permissions across all users. You can neither log in with this account nor delete it.
- **<installing user>**—The installing user is seeded during database creation during installation (not for client installations). The login is the operating system's name for the installing user. You can neither log in with this account nor delete it.
- **OWAdmin**—A seeded administrative account. You can log in with this account, and cannot disable it, but you can change its password. You cannot delete this account.
- **admin**—A seeded administrative account, which is the core application component. You can login using this account. You cannot disable this account, but you can change the password. You cannot delete this account.

Adding or Modifying a User

Click *New* to create a new User, or select an existing user and click *Open* to modify that user's properties. A three-tab User Editor appears, open to the General tab.

To create a user:

Click New to display the User Editor, enter the appropriate information, and click Save. Most of the information associated with a user is optional. However, the following entries are required:

- User ID
- Password
- Confirmation of Password

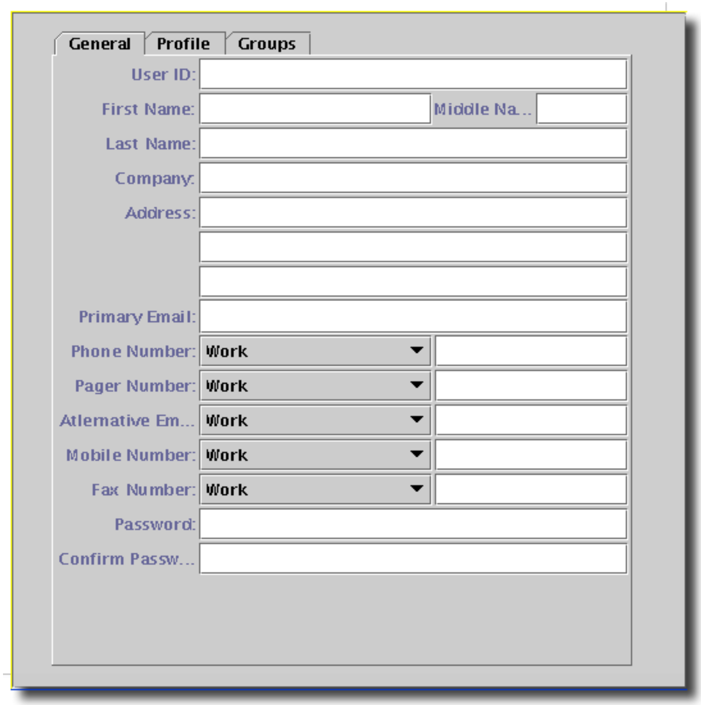
NOTE: Windows user names should contain neither an apostrophe (') nor a space.

In addition to these entries, you may want to associate the user with a Group. This confers a predetermined set of permissions to the user. See Groups Tab for more information.

General Tab

The General tab lets you enter and edit identifying and contact information for the selected (or newly created) user.

Figure 25-3. User Manager: General Tab



Phone Number: Work

Pager Number: Work

Alternative Em... Work

Mobile Number: Work

Fax Number: Work

The following are the fields on this tab (described when not self-evident):

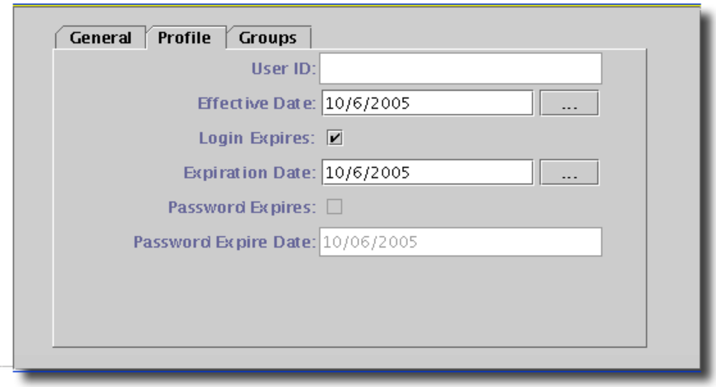
- **User ID** — (Required) Enter an ID for this user. If you are modifying an existing user, this field is read-only. The User ID must be unique; if it matches an existing User ID, the application generates an error.
- **First Name** — First Name
- **Middle Name** — Middle Name
- **Last Name** — Last Name
- **Company** — Company
- **Address** — Address
- **Primary Email** — Primary Email
- **Phone Number** — Select a phone number type from the drop-down list, then enter a phone number for the selected user.

- **Pager Number** — Select a pager number type from the drop-down list, then enter a pager number for the selected user.
- **Alternative Email**—Select an email type from the drop-down list, then enter an email address.
- **Mobile Number** — Select a mobile number type from the drop-down list, then enter a mobile number for the selected user.
- **Fax Number** — Select a fax number type from the drop-down list, then enter a fax number for the user.
- **Password** — (Required) Enter the password for this user. For security purposes, the characters appear as a series of asterisks. The default security does not require the password to contain mixed-case letters, numbers, or special characters. Once a user has been created, this field becomes read-only.
- **Confirm Password** — (Required) Re-enter the password for this user. If this entry does not match the Password entry, an error dialog appears and both password fields empty.

Profile Tab

The Profile tab provides access to password and login parameters like expiration policy and expiration date, and lets Administrators reset the expiration dates of "locked-out" users.

Figure 25-4. Profile Tab



User ID:

Effective Date: 10/6/2005

Login Expires: ☑

Expiration Date: 10/6/2005

Password Expires: □

Password Expire Date: 10/06/2005

The following are fields on this tab:

- **User ID** — The (read-only) ID for the selected user.
- **Effective Date** — (Required) The date when this account becomes effective. This field lets you create accounts in advance. The accounts remain dormant until the Effective Date arrives.
- **Login Expires** — Indicates whether the login for this user expires. If you select this option, the application activates the Expiration Date field.

- **Expiration Date** — Specifies the date on which the login expires. This field is not active unless you select the Login Expires option.

  Specify an expiration date by entering the date directly in the text field, in the proper format (by default: month/day/year). You can also click the Command button (...) and select a date from the calendar graphic that appears.

  If a user is disabled, typically by login failure, the Expiration Date becomes the current date. The user cannot log in again until you reset the Expiration Date to some future date or clear the *Login Expires* option.

- **Password Expires** — When selected, this option sets an expiration policy for the password of the associated user. If you set password expiration, you must set an expiration date. If you do not set password expiration, the password for this user never expires.

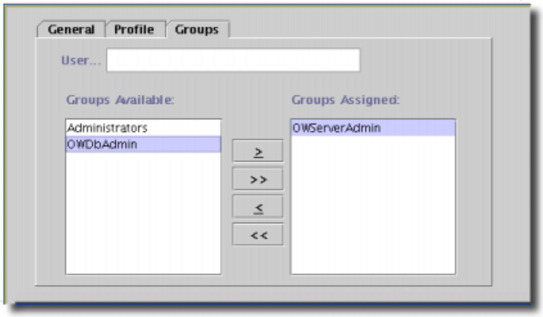
Password Expire Date — This field is active only if you selected the *Password Expires* option.

Groups Tab

The Groups tab lets you determine which user groups, if any, to associate with a user (see User Group Manager for information about how to create the groups that appear here). Since you grant permissions to defined groups, you can grant or deny users access to certain functions based on their group associations.

The ID for the selected user appears at the top of the tab. Available groups appear in the left tab, and groups currently assigned to the selected user appear in the right tab.

Figure 25-5. Groups Tab



Use the controls in this tab to assign groups to or remove assignments from the current user.

To Add Group Assignments:

Select one or more groups from the left pane (*Groups Available*) and click the right-arrow (>) button to move those groups into the right pane (*Groups Assigned*). Ctrl+click to select multiple non-contiguous items, or click on one item and Shift-click on another to select a range of consecutive items. Click the double-right-arrow (>>) button to move all of the groups from the left to the right pane. Click OK to store the results.

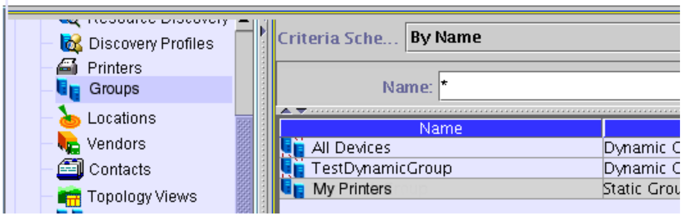
To Remove Group Assignments:

Select one or more groups from the right (Groups Assigned) pane and click the left-arrow (<) button to move those groups into the left pane. Ctrl+click to select multiple non-contiguous items, or click on one item and Shift-click on another to select a range of consecutive items. Click the double-left-arrow (<<) button to move all of the groups from the right to the left pane. Click OK to store the results.

User Group Manager

The User Group Manager lets you create user groups (see *User Manager* on page 288 for instructions about creating users themselves). Open this manager from *Settings > Permissions > User Group Manager*. Initially, a Group is nothing more than a name and a description.

Figure 25-6. User Group Manager



Criteria Sche... By Name

Name: *

Name	
All Devices	Dynamic C
TestDynamicGroup	Dynamic C
My Printers	Static Grou

Click New or select a group and click Open to modify a group. See Adding or Modifying a Group for a description of the editor. To remove a group, select it, then select **Delete**. You cannot delete some groups; for example, you cannot delete **Administrators**.

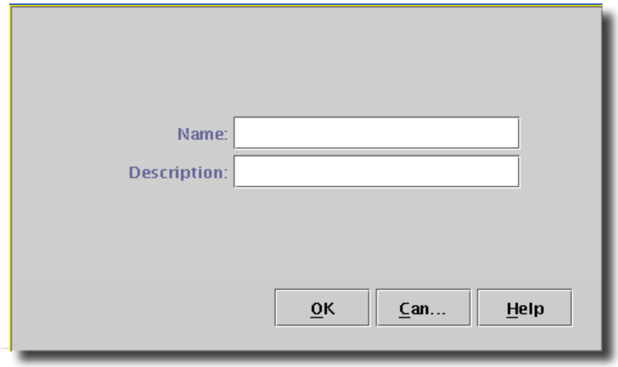
Once created, however, you can associate individual users with groups (See *Groups Tab* on page 293), and grant permissions to users based on their association with a group (See *Functional Permissions* on page 307). By default, new groups have no permissions.

Adding or Modifying a Group

Adding groups and modifying groups are similar operations using the same interface.To add a new group, Click *New...* To modify an existing group, Select the group in the Group Manager and Click *Open...*

In both cases, an editor dialog (shown below) appears. If you are editing an existing group, the dialog contains the information for that group. If you are creating a new group, the dialog is blank.

Figure 25-7. Group Editor



Enter or modify the appropriate information in the Group Editor's fields and click OK to save the entry. The following are the fields in this dialog:

Name — The name of the group (read-only if editing, rather than creating). This entry is required, and must be unique.

Description — A description of the group. This entry is optional.

Default Role and User

By default, a role (user group) and two users exist when you install your application. Here are the defaults:

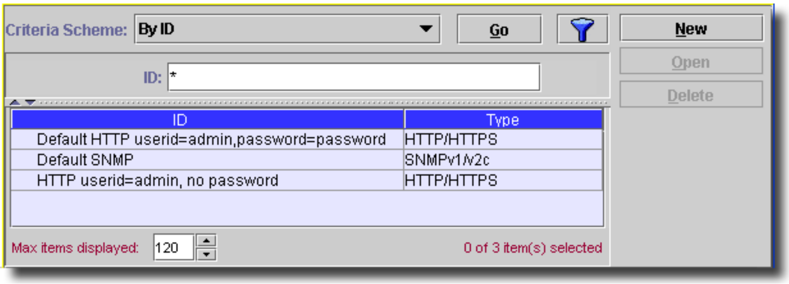
- **Role**: Administrator
- **User**: admin (a case-sensitive login).

Windows installations create a user with the same name as the login for whoever did the installation. This user is not attached to any role. It is also often unused.

Authentication Manager

The Authentication Manager lets you create and manage Authentication Objects. These objects let the application establish a set of credentials for various network elements, including login IDs and passwords. These restrict access to certain functions and/or information to authorized users.

Figure 25-8. Authentication Manager



Criteria Scheme: By ID

ID: *

ID	Type
Default HTTP userid=admin,password=password	HTTP/HTTPS
Default SNMP	SNMPv1/v2c
HTTP userid=admin, no password	HTTP/HTTPS

Max items displayed: 120

0 of 3 item(s) selected

As with most managers, you can filter the authentication objects listed with the Filter at the top of the screen. Right click a listed authentication object, or click the Action button to display the following menu items:

New—Opens an editor (see Creating and Modifying Authentication Objects, the

next section).

Open—Edits a selected authentication object (see Authenticator Editor on page

265).

Print—Create an Acrobat report of the items displayed in the inventory (change the filter and click Go to change this display). You must have the free Acrobatreader installed for this to function. See www.adobe.com to download and install this application.

Delete—Removes the selected authentication object from those listed.

Import / Export—This appears in the menu accessible in the Action button, and imports / exports information about all authentications as a text file.

Exported files can serve as backups or as seed files, and can be imported by clients running on other servers.

⚠ **CAUTION: The exported file exposes passwords in plain text.**

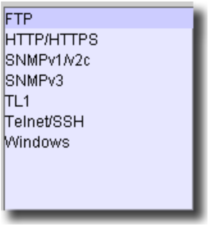
NOTE: This report limits the number of columns to those that can fit on a single page width.

Help—Opens the help for this screen.

Creating and Modifying Authentication Objects

The process for creating and editing Authentication Objects is similar to other managers: click *New* to create a new object, or select an existing object from the list and click *Open* to modify it. Delete an object by first selecting it and then clicking *Delete*. See the *Authenticator Editor* on page 297 for specific details about the entries associated with authentication objects.

Figure 25-9. Authentication Type


FTP
HTTP/HTTPS
SNMPv1/v2c
SNMPv3
TL1
Telnet/SSH
Windows

NOTE: The types that appear in this dialog depend on the installed device drivers.

When performing deep discovery, you must typically have the correct device driver installed and at least one authentication object (for example: an SNMP authentication object specifying a public read community). If you want to interact with a device using a command-line interface (like Telnet), you must create a Telnet/SSH authentication object.

Authenticator Editor

The Authenticator Editor is the interface where you create and modify authentication objects. It contains the following pages: *General*, *Equipment*, and *User Groups*. The General page is different, depending on the Authentication Type. These types include:

- FTP
- HTTP/HTTPS
- SNMP v1/v2
- SNMP v3
- TL1
- Telnet / SSH
- Windows

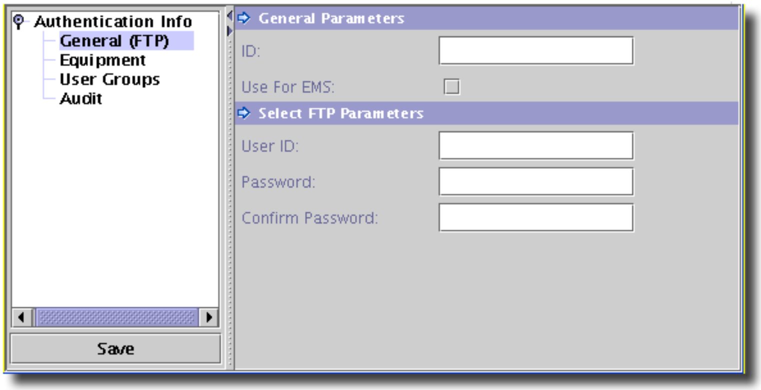
NOTE: The Audit section of this manager catalogs actions in which the application used the authentication.

NOTE: Check the *Use for EMS* checkbox in your authentications. This lets the entire element management system (EMS) use this authentication. Otherwise, authentications are only available to individual users who have permissions to use them. This is necessary for other (non-admin) users to do discrete configuration.

FTP

You can also enter authentication information for FTP:

Figure 25-10. General (FTP) Page



General Parameters

ID:

Use For EMS: □

Select FTP Parameters

User ID:

Password:

Confirm Password:

Enter the following fields:

General Parameters

- **ID**—The FTP authentication object name.
- **Use for EMS**—Checking this lets this application—the entire element management system (EMS)—use this authentication. Otherwise, authentications are only available to individual users who have permissions to use them.

If none of the associated credentials are marked Use for EMS then the software chooses the set of authentications to which the current user has access.Administrators typically use this capability to control access to cut-thru session capabilities (read vs. read-write) when a command line interface is present to the managed device.

NOTE: *Resync fails if you do not check this box.*

Select FTP Parameters

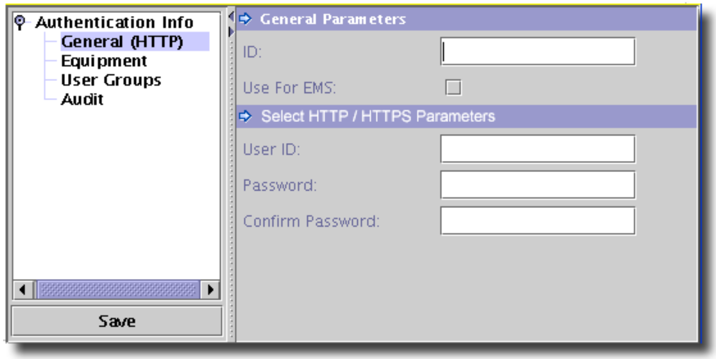
- **User ID** — The login ID.
- **Confirm Password** — Confirm the password.

Confirm your entries here with *File > Save* or by clicking on the *Save* icon or button.

HTTP/HTTPS

These authentication objects serve as logins for http or https connections.

Figure 25-11. General (HTTP/HTTPS) Page



Here are the fields:

General Parameters

ID — A unique identifier for this authentication object.

Use for EMS— Checking this lets this application—the entire element management system (EMS)—use this authentication. Otherwise, authentications are only available to individual users who have permissions to use them.

If none of the associated credentials are marked Use for EMS then the software chooses the set of authentications to which the current user has access.Administrators typically use this capability to control access to cut-thru session capabilities (read vs. read-write) when a command line interface ispresent to the managed device.

Select HTTP/HTTPS Parameters

UserID — The login ID.

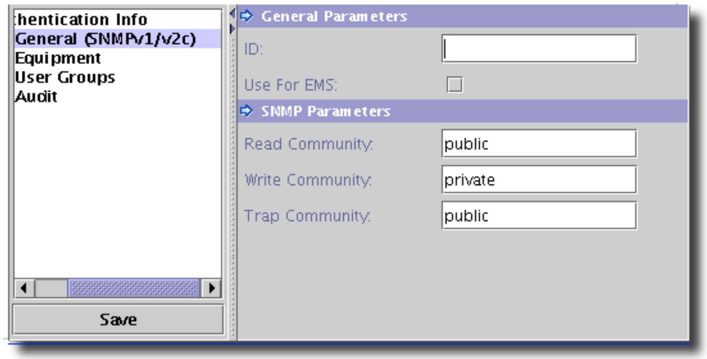
Confirm Password — Confirm the password.

Confirm your entries here with File > Save or by clicking on the Save icon or button.

SNMP v1/v2

Enter information for v1 or v2 SNMP authenticators through the General (SNMP) page, shown below. Some fields — Read Community, Write Community, and Trap Community—pre-fill with default values.

Figure 25-12. Authenticator Editor — General (SNMP) Page



ID:

Use For EMS: □

Read Community: public

Write Community: private

Trap Community: public

The following are the fields in the General (SNMP) page:

General Parameters

- **ID** — (Required) This entry must be unique; it identifies the authentication object.
- **Use for EMS**—Checking this lets this application—the entire element management system (EMS)—use this authentication. Otherwise, authentications are only available to individual users who have permissions to use them

If none of the associated credentials are marked Use for EMS then the software chooses the set of authentications to which the current user has access.Administrators typically use this capability to control access to cut-thru session capabilities (read vs. read-write) when a command line interface is present to the managed device.

NOTE: *Resync fails if you do not check this box.*

Select HTTP/HTTPS Parameters

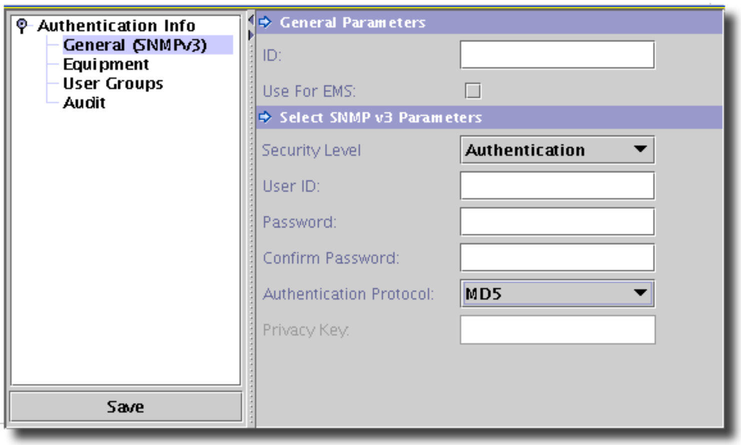
- **Read Community** —The default is *public*.
- **Write Community** —The default is *private*.
- **Trap Community**— The default is *public*.

Confirm your entries here with *File* > *Save* or by clicking on the *Save* button or icon.

SNMP v3

Enter information for v3 SNMP authenticators through the General (SNMP) page, shown below. Some fields — Version, Read Community, Write Community, and Trap Community, pre-fill with default values.

Figure 25-13. Authenticator Editor — General (SNMP) Page



General Parameters

ID:

Use For EMS: □

Select SNMP v3 Parameters

Security Level: Authentication

User ID:

Password:

Confirm Password:

Authentication Protocol: MD5

Privacy Key:

This screen has the following fields:

General Parameters

- **ID** — (Required) This entry must be unique; it identifies the authentication object. The ID is only a label name under which you store the authentication and has no effect on the SNMPv3 Authentication itself.
- **Use for EMS**—Disregard. This entity does not support SNMP v3.
- Select SNMP v3 Parameters
- **Security Level**—Defines the three security levels that can be used. They are:

  No Authentication–Sends SNMP messages without authentication and without privacy. This requires only a valid User ID, known by the device's SNMP agent.

  Authentication (No Privacy)—Sends SNMP messages with authentication but without privacy. Requires only a valid User ID and a password.

  Authentication with Privacy—Sends SNMP messages with authentication and privacy. This requires a valid User ID, password, authentication Protocol and Privacy Key.

- **User ID**—Specifies the User Name for this object. The Security user name represents the user in a format that is Security Model-independent.
- **Password** — Specify the password for this user.
- **Confirm Password** — Confirm the password.

- **Authentication Protocol** — Select the protocol from the pick list (*MD5* or *SHA*). Used with the Privacy Key to produce a secret key in which to validate the connection.
- **Privacy Key**— Enter the privacy key. The application uses this to generate a secret key. Specifying MD5 requires the privacy key to be 16 characters long while SHA requires the privacy key to be 20 characters long.

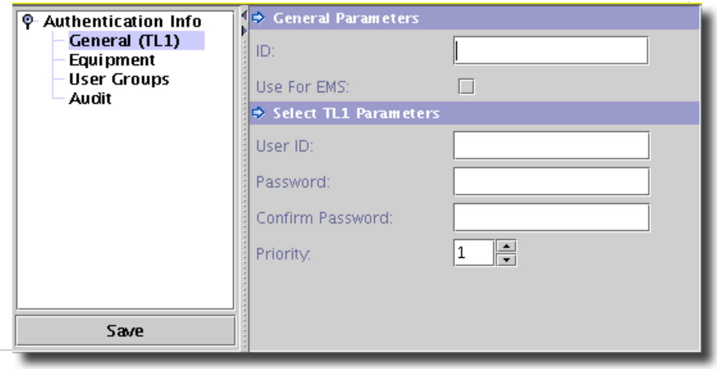
Confirm your entries here with *File > Save* or by clicking on the *Save* button or icon.

NOTE: For the application to correctly receive SNMP v3 traps, you must configure the authentication for a device in the Equipment Editor Authentication (Management Interfaces) screen.

TL1

Enter information for TL1 Authenticators through the General (TL1) page.

Figure 25-14. General (TL1) Page



The following are the fields in the General (TL1) page:

General Parameters

- **ID** — An identifying name for this authentication object.
- **Use for EMS**—Checking this lets this application—the entire element management system (EMS)—use this authentication. Otherwise, authentications are only available to individual users who have permissions to use them .

If none of the associated credentials are marked Use for EMS then the software chooses the set of authentications to which the current user has access.Administrators typically use this capability to control access to cut-thru session capabilities (read vs. read-write) when a command line interface is present to the managed device.

NOTE: *Resync fails if you do not check this box.*

Select TL1 Parameters

- **User ID** — The User ID that this object uses.

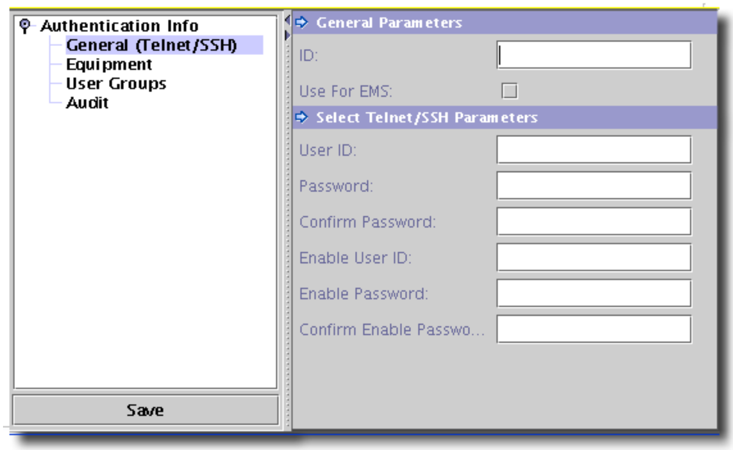
- **Password** — The password for the User ID this object uses.
- **Confirm Password** — Confirm the password.
- **Priority** — The priority attached to this request. Lower numbers receive a higher priority.

Confirm your entries here with *File* > *Save* or by clicking on the *Save* button or icon.

Telnet / SSH

You can use Telnet / SSH authentication objects for either SSH (default: port 22) or Telnet (default: port 23) logins. Select which type of login by selecting the port when you use them in the Resource Discovery Wizard.

Figure 25-15. General (Telnet / SSH) Page



The following are the authentication object fields for Telnet/SSH (ASCII) logins.

General Parameters

- **ID**—The Telnet or SSH authentication object name.
- **Use for EMS**—Checking this lets this application—the entire element management system (EMS)—use this authentication. Otherwise, authentications are only available to individual users who have permissions to use them .

  If none of the associated credentials are marked *Use for EMS* then the software chooses the set of authentications to which the current user has access. Administrators typically use this capability to control access to cut-thru session capabilities (read vs. read-write) when a command line interface is present to the managed device.

Resync fails if you do not check this box.

Select Telnet / SSH Parameters

- **User ID**—The user login.

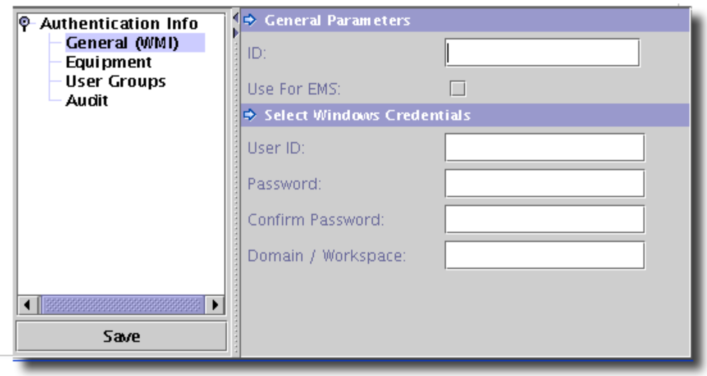
- **Password** — The password for the User ID this object uses.
- **Confirm Password** — Confirm the password.
- **Enable User ID**—The user login, if the device needs a different login for an enabled user. Consult your device's manuals for more about this.
- **Enable Password / Confirm Enable Password**—The user password (and confirmation), if the device needs a different password for an enabled user.

Confirm your entries here with *File > Save* or by clicking on the *Save* icon or button.

Windows

These authentication objects serve as logins for Windows (WMI) connections.

Figure 25-16. General (Windows) Page



This screen has the following fields:

General Parameters

- **ID**—A unique identifier for this authentication object.
- **Use for EMS**—Checking this lets this application—the entire element management system (EMS)—use this authentication. Otherwise, authentications are only available to individual users who have permissions to use them .

  If none of the associated credentials are marked *Use for EMS* then the software chooses the set of authentications to which the current user has access. Administrators typically use this capability to control access to cut-thru session capabilities (read vs. read-write) when a command line interface is present to the managed device.

NOTE: *Resync fails if you do not check this box.*

Select Telnet / SSH Parameters

- **UserID**—The login ID.
- **Confirm Password** — Confirm the password.

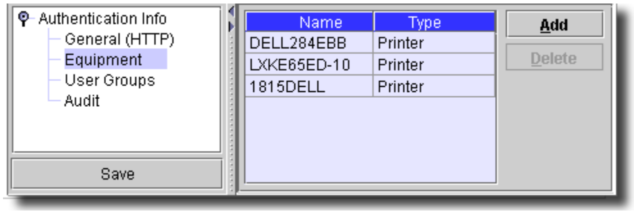
- **Domain / Workspace**—Enter the Windows domain.

Confirm your entries here with *File* > *Save* or by clicking on the *Save* icon or button.

Equipment

The Equipment page provides an interface through which you can associate managed equipment with the authentication object you are creating or editing.

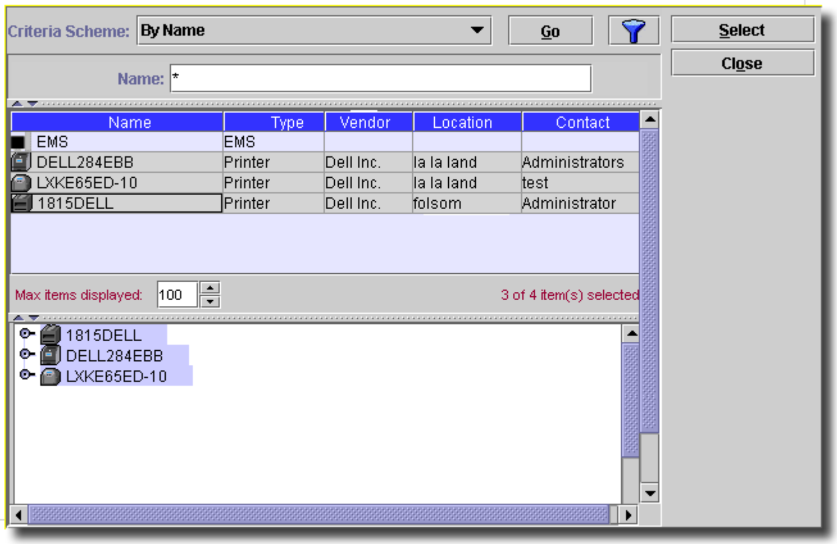
Figure 25-17. Equipment Page



Name	Type
DELL284EBB	Printer
LXKE65ED-10	Printer
1815DELL	Printer

- **To add equipment**—Click *Add*. The Select *Equipment* page appears.

Figure 25-18. Equipment Selection



Criteria Scheme: By Name

Name: *

Name	Type	Vendor	Location	Contact
EMS	EMS			
DELL284EBB	Printer	Dell Inc.	la la land	Administrators
LXKE65ED-10	Printer	Dell Inc.	la la land	test
1815DELL	Printer	Dell Inc.	folsom	Administrator

Max items displayed: 100

3 of 4 item(s) selected

1815DELL
DELL284EBB
LXKE65ED-10

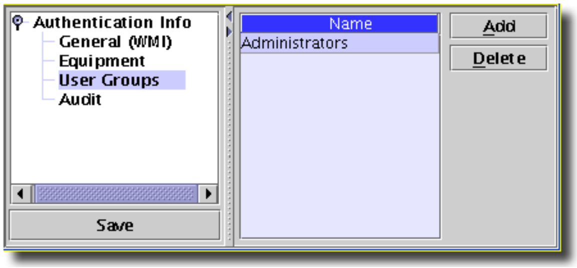
Click an equipment object in the list to select it; the selected object then appears in the lower pane. A turn key icon appears if the selected object contains subcomponents (cards and ports, for example); click on the turn key to display a tree representation of those subcomponents. Click on any individual item in the tree to select it; click *OK* to add the selected equipment to the list associated with the authentication object.

- **To Delete Equipment** — Select the equipment object in the list and click *Delete*.

User Groups

This page lets you associate User Groups with authentication objects. The created authentication object is visible only to users who are members of the associated group. The initial display (Figure 25-19 is an example) lists the groups associated with this object.

Figure 25-19. User Groups Page



To add a group, click *Add*. To remove a group from the list, select it and click *Delete*. When adding groups, the Group Manager dialog, appears. (For more information on the Group Manager, see *User Group Manager* on page 294.)

Select a group from the displayed list (or click *New...* to define a new group) and click OK to implement your selection.

RADIUS Authentication

If you want to use RADIUS authentication for this application's clients, you must create a RADIUS user matching the login in the application (and assign that user the correct groups and functional permissions in the application).

The property file that needs to change is on the application server(s) in

```
oware\jboss-3.2.3\server\oware\conf\login-config.xml.
```

By default, RADIUS authentication is commented out in this file. To use RADIUS, uncomment this section (changing <!-- to < and --> to >). Then, configure the options (example server, secret, prompts, NAS-IP-Address).

Here is an example of the application's freeradius implementation on helix.

```
<authentication>
           <!--login-module code = "com.theorem.radius3.login.RADIUSLogin"
             flag = "sufficient">
             <module-option name = "authtype">CHAP</module-option>
             <module-option name = "debug">true</module-option>
```

```
          <module-option name = "server">127.0.0.1</module-option>
          <module-option name = "port">1812</module-option>
          <module-option name = "timeout">1</module-option>
          <module-option name = "secret">secret</module-option>
          <module-option name = "namePrompt">Name:</module-option>
<module-option name = "passwordPrompt">Password:</module-option>
<module-option name = "NAS-IP-Address">@127.0.0.1</module-option>
<module-option name = "NAS-Port">#1</module-option>
<module-option name = "Framed-Protocol">#PPP</module-option>
          <module-option name = "Service-Type">#Login</module-option>
        </login-module-->
        <login-module code = "com.dorado.extensions.OWLoginModule"
          flag = "sufficient">
        </login-module>
    </authentication>
```

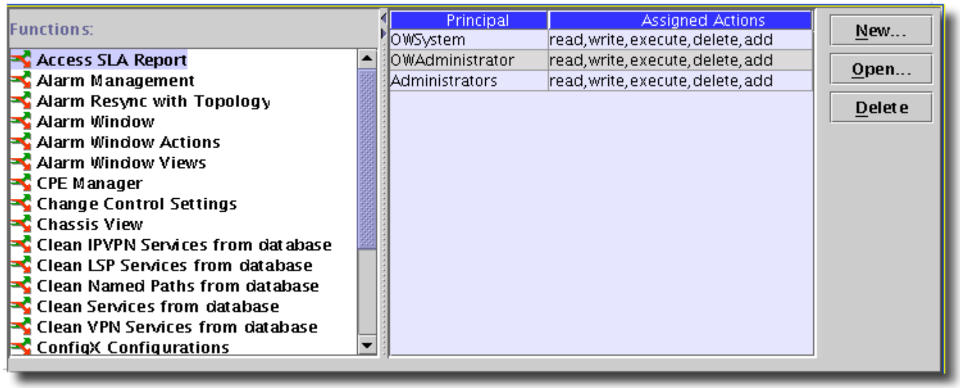
Functional Permissions

This page lets you associate system functions (permissions) with individual users or with user groups. Select Settings > Permissions > Functional Permissions to display the Functional Permissions page, shown below.

NOTE: Functional permissions are global and additive with other permissions. If you have a group permission and a functional permission set, the result is a union, not an intersection of the two.
Also: Best practice is to add users rather than alter administrative functional permissions.

Grant permissions by selecting a predefined function and then create a list of groups and/or individual users authorized to perform that function. You can further refine permissions by defining a set of actions (read, write, execute, and so on) that each group or user can perform when exercising the function.

Figure 25-20. Functional Permissions Page



Access SLA Report
Alarm Management
Alarm Resync with Topology
Alarm Window
Alarm Window Actions
Alarm Window Views
CPE Manager
Change Control Settings
Chassis View
Clean IPVPN Services from database
Clean LSP Services from database
Clean Named Paths from database
Clean Services from database
Clean VPN Services from database
ConfigX Configurations

Principal	Assigned Actions
OWSystem	read,write,execute,delete,add
OWAdministrator	read,write,execute,delete,add
Administrators	read,write,execute,delete,add

- **Functions Panel** — The Functions panel displays the available functions. Select a function by clicking it; the groups and users who have been granted permission to perform this function appear, along with the permitted actions (read, write, execute, and delete, for example.)
- **Permissions Panel** — The Permissions panel displays the Principal — the groups allowed to perform the selected function in the Functions page — and the Assigned Actions for each group or individual associated with that function.
- **New** — Lets you associate a new Principal with the selected function and assign actions to that Principal. Clicking *New...* opens the Functional Permissions editor with the *Principal* (Group) drop-down menu active.

Possible functional permissions authorize the following:

- **read**—retrieve data from the database
- **write**—update data in the database
- **execute**—execute some application function
- **delete**—delete data from the database
- **add**—create new data

Function Associations

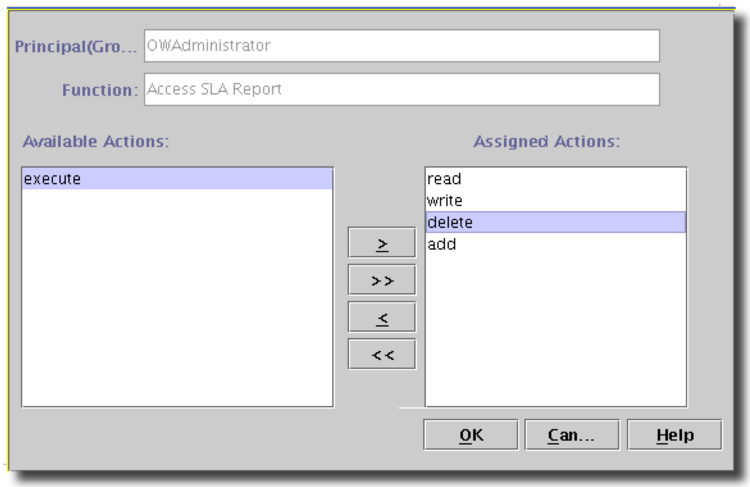
You can do the following with the association of Groups or Principals with functions:

- **Associating a New Principal or Group with a Function**—Select a function in the Function page of the Functional Permissions Manager and click *New*.
- **Modifying Actions Permitted a Principal or Group for a Function**—Select a function in the Function page of the Functional Permissions Manager. Select the *Principal* or *Group* for which you want to modify the assigned actions and click *Open...*
- **Removing Associations Between Principal or Group and a Function**—Select a function in the Function page of the Functional Permissions Manager, select the *Principal* or *Group* whose association you want to remove and click *Delete*.

Functional Permissions Editor

Alter functional permissions through the Functional Permissions editor, as illustrated below.

Figure 25-21. Functional Permissions Editor



Principal(Gro...: OWAdministrator

Function: Access SLA Report

Available Actions:

execute

Assigned Actions:

read
write
delete
add

The following are the fields in this editor:

- **Principal (User)**— Drop-down menu (when adding a new Principal) from which you can select a User Group or individual. The *Show Groups/Show Users* button determines the state of this menu (groups or individuals), and the menu displays its state in the parenthetical expression. If the menu is in *Users* mode, the title reads *Principal(User)*. If it is in *Groups* mode, the title reads *Principal(Groups)*.

During Edit operations, the *Principal* field is a read-only area, not a menu, that displays the Principal (either a Group or a User) whose permissions you are editing.

- **Show Groups/ Show Users** — Mode selector for the *Principal* menu. Click this button to change the mode of the Principal menu from Groups to Users, or vice versa. If the Principal menu is in *Groups* mode, this button reads *Show Users*. If the Principal menu is in *Users* mode, this button reads *Shows Groups*.
- **Function** — This read-only field displays the function whose associations or permissions you are editing.
- **Available Actions** — Displays a list of actions available, but not assigned, for the selected function. To assign actions from this list to the current group or user, select one or more actions and click the underlined right (>) arrow. Assign all the available actions by clicking the double right arrow (>>).
- **Assigned Actions** — Displays a list of actions assigned, for this function, to the current group or user. To remove assigned actions, select one or more from the list and click the underlined left (<) arrow. Remove all assigned actions by clicking the double left arrow (<<).

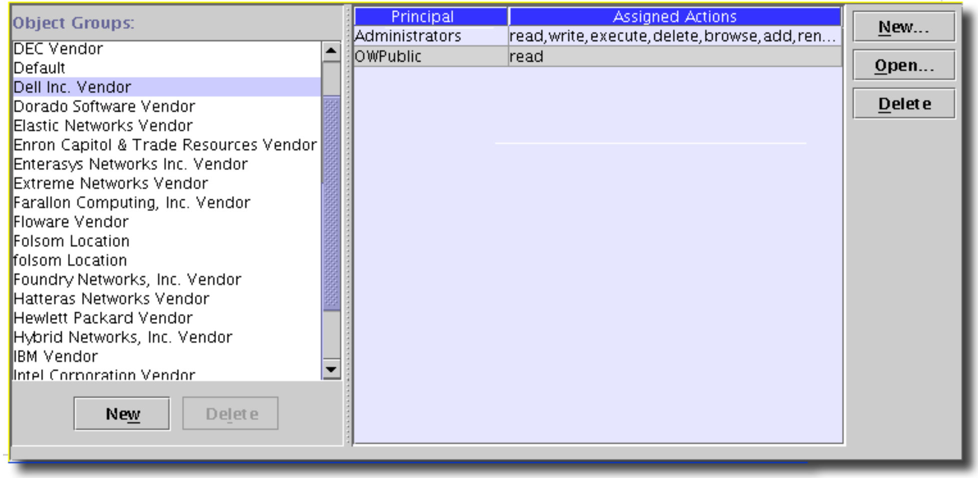
Click *OK* to implement any changes you have made, or click *Cancel* to close the dialog and discard your changes.

NOTE: Functional permissions are cached on the client. Changes in those permissions may take as long as the “time to live” for this cache. The cache is set in the `redcell.cacheentrylivetime` property in seconds. This property defaults to 300 seconds, and is in `owareapps\redcell\ lib\redcell.properties`, and best practice is to override rather than change such properties.

Object Group Manager

The Object Group Manager lets you group objects and then associate them with individual users or user groups. Open it with the *Settings > Permissions > Object Group Manager* menu item. Permissions are attached to each association. For example, you can associate the principals *Administrators* and *Trainees* with a Dell Vendor object group, and can attach one set of permissions (*read*, *write*) to the association between Administrators and the Dell Vendor object group, while attaching another set of permissions (read) to the association between Trainees and the Dell Vendor object group.

Figure 25-22. Object Group Manager



Object Groups:

DEC Vendor
Default
Dell Inc. Vendor
Dorado Software Vendor
Elastic Networks Vendor
Enron Capitol & Trade Resources Vendor
Enterasys Networks Inc. Vendor
Extreme Networks Vendor
Farallon Computing, Inc. Vendor
Floware Vendor
Folsom Location
folsom Location
Foundry Networks, Inc. Vendor
Hatteras Networks Vendor
Hewlett Packard Vendor
Hybrid Networks, Inc. Vendor
IBM Vendor
Intel Corporation Vendor

Principal	Assigned Actions
Administrators	read,write,execute,delete,browse,add,ren...
OWPublic	read

This application also provides “natural groupings,” automatically creating a dynamic object group whenever you add an entity belonging to one of the natural groups the system. The following are some examples of natural groups:

- **Object Vendor** — All objects that refer to a particular vendor.
- **Location** — All objects that refer to a given location.
- **Role** — Within this application, objects can refer to a role. The role can describe the use those objects have within the network — core router, for example, as opposed to edge router.

NOTE: You cannot make individual interfaces part of an object group, but you can assign a role to them. Roles make natural groups, and you can use those role-based groups to manage the access to individual interfaces.

The system administrator and add-on products can add other groups to this list, and can add objects to those groups.

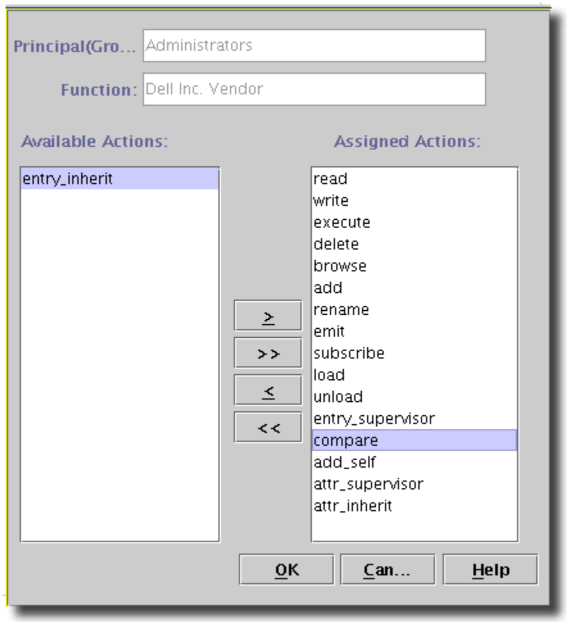
To add a new object group, click *New* below the list of available groups and name the group in the subsequent screen. Accept that name to add it to those listed.

CAUTION: All users inherit OWPublic's permissions. You must remove OWPublic's read permissions from things in Object Group Manager to conceal those items.

Adding or Modifying Object Groups

When you click *New*, you can create a new association between either user or object groups and permissions. Select from *User Groups* (see *User Group Manager* on page 294 for instructions about how to make and manage these groups) or individual users (see *User Manager* on page 288 for more information about these). The button at the top right of this screen toggles between individual users and groups displayed in the pick list in the top center of the screen (Figure 25-23).

Figure 25-23. Adding Object Group Permissions



Principal(Gro... Administrators

Function: Dell Inc. Vendor

Available Actions:

- entry_inherit

Assigned Actions:

- read
- write
- execute
- delete
- browse
- add
- rename
- emit
- subscribe
- load
- unload
- entry_supervisor
- compare
- add_self
- attr_supervisor
- attr_inherit

Select a *Principal (Group or User)*, if you are creating new permissions. Otherwise this and the *Function* field, reminding you of the object group previously selected, are read-only. Then use the selection lists below to arrange the available permissions. Click *OK* to confirm your selection.

⚠ **CAUTION: Because devices can belong to different object groups, restricting permissions to a single group may not remove a device from a prohibited user's control. Permissions for *Vendor, Location, Equipment Role*, manually created *Object Group* and *Services* are applied with a logical AND, so similar advice applies about them.**

Application Security Policy

The Application Security interface lets you specify security policies governing user login and passwords. Open the Application Security Policy page by selecting *Settings > Permissions > Application Security Policy*.

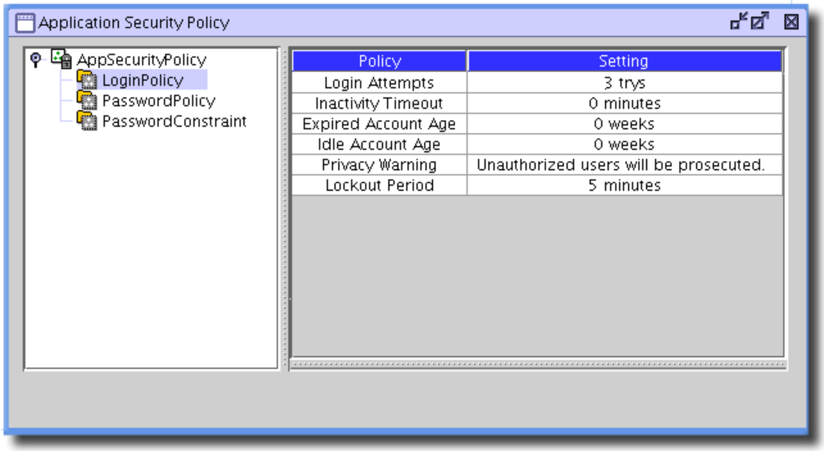
The following are types of application security policies described in this section:

- Login Policy
- Password Policy
- Password Constraint

Login Policy

The LoginPolicy section of the Application Security Policy page sets policies about user logins. These policies govern the message that appears in the login screen and the various security measures applied to user's attempts to log in.

Figure 25-24. Login Policy Page



Policy	Setting
Login Attempts	3 trys
Inactivity Timeout	0 minutes
Expired Account Age	0 weeks
Idle Account Age	0 weeks
Privacy Warning	Unauthorized users will be prosecuted.
Lockout Period	5 minutes

The individual policies available from the Login Policy Page are:

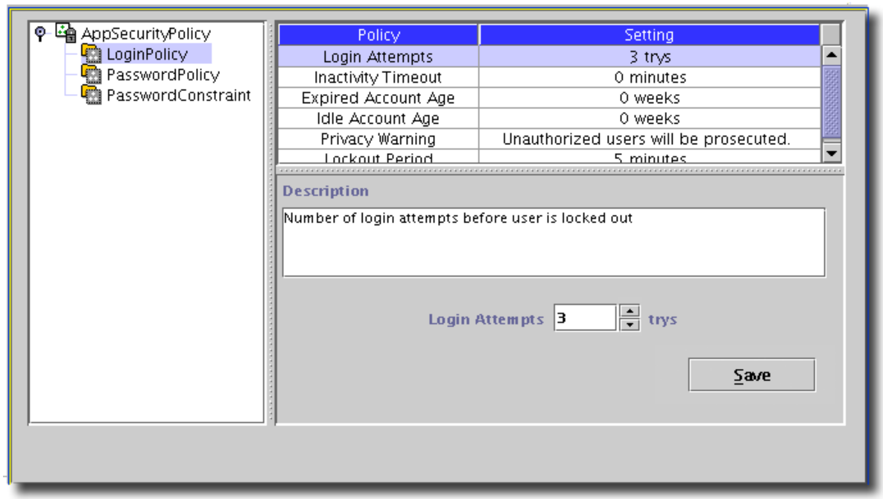
- Login Attempts
- Inactivity Timeout
- Expired Account Age
- Idle Account Age
- Privacy Warning
- Lockout Period

Each Login Policy appears in the list along with its current setting. Edit a policy by clicking it; an editor appropriate to that setting appears in the lower portion of the page.

Login Attempts

The Login Attempts setting specifies how many consecutive unsuccessful login attempts are allowed before a user is locked out.

Figure 25-25. Login Attempts



Policy	Setting
Login Attempts	3 trys
Inactivity Timeout	0 minutes
Expired Account Age	0 weeks
Idle Account Age	0 weeks
Privacy Warning	Unauthorized users will be prosecuted.
Lockout Period	5 minutes

Description

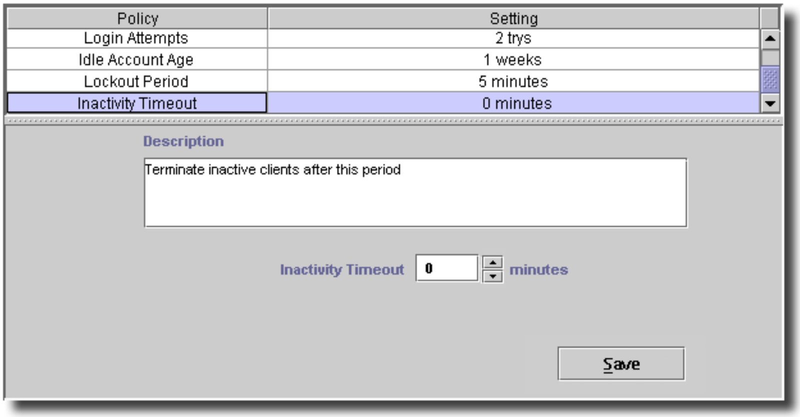
Number of login attempts before user is locked out

Login Attempts 3 trys

Inactivity Timeout

The Inactivity Timeout setting determines how long a terminal can remain inactive before the client is shut down. A setting of 0 effectively disables this setting, allowing users to remain inactive indefinitely.

Figure 25-26. Inactivity Timeout



Policy	Setting
Login Attempts	2 trys
Idle Account Age	1 weeks
Lockout Period	5 minutes
Inactivity Timeout	0 minutes

Description

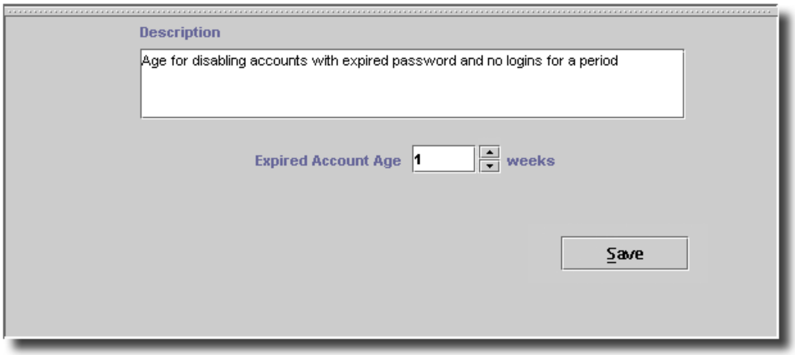
Terminate inactive clients after this period

Inactivity Timeout 0 minutes

Expired Account Age

The Expired Account Age setting determines how many weeks an account can remain active if it has an expired password and no logins. Once this threshold is reached, the account is disabled and can only be reactivated by an administrator.

Figure 25-27. Expired Account Age



Description

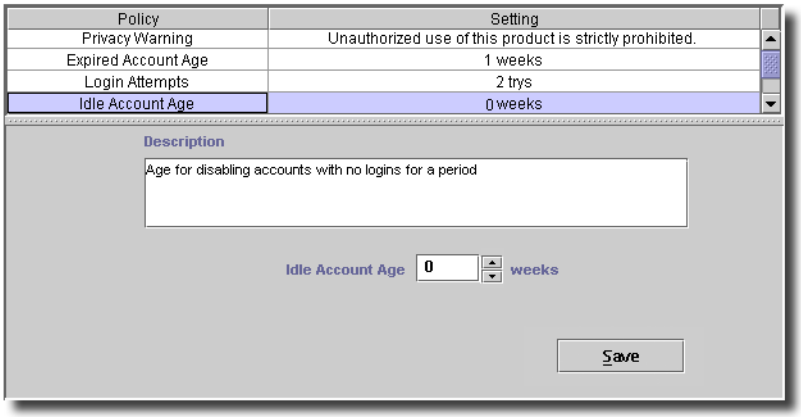
Age for disabling accounts with expired password and no logins for a period

Expired Account Age 1 weeks

Idle Account Age

The Idle Account Age determines how long an account can remain inactive (have no logins) before it is disabled.

Figure 25-28. Idle Account Age



Policy	Setting
Privacy Warning	Unauthorized use of this product is strictly prohibited.
Expired Account Age	1 weeks
Login Attempts	2 trys
Idle Account Age	0 weeks

Description

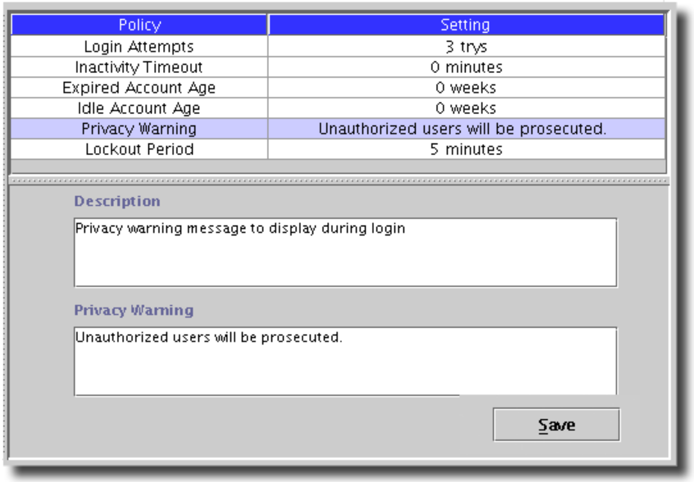
Age for disabling accounts with no logins for a period

Idle Account Age 0 weeks

Privacy Warning

The Privacy Warning appears every time a user logs on. Enter your desired text in the Privacy Warning field and click *Save* to implement the change.

Figure 25-29. Privacy Warning



Policy	Setting
Login Attempts	3 trys
Inactivity Timeout	0 minutes
Expired Account Age	0 weeks
Idle Account Age	0 weeks
Privacy Warning	Unauthorized users will be prosecuted.
Lockout Period	5 minutes

Description

Privacy warning message to display during login

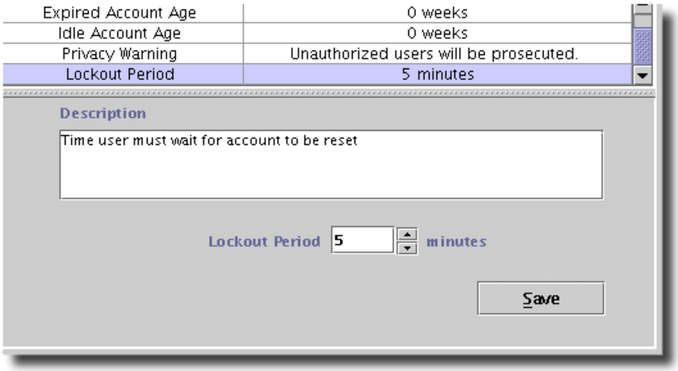
Privacy Warning

Unauthorized users will be prosecuted.

Lockout Period

The Lockout Period determines how long a user must wait, after a failed login attempt, before a new attempt is allowed.

Figure 25-30. Lockout Period



Expired Account Age	0 weeks
Idle Account Age	0 weeks
Privacy Warning	Unauthorized users will be prosecuted.
Lockout Period	5 minutes

Description

Time user must wait for account to be reset

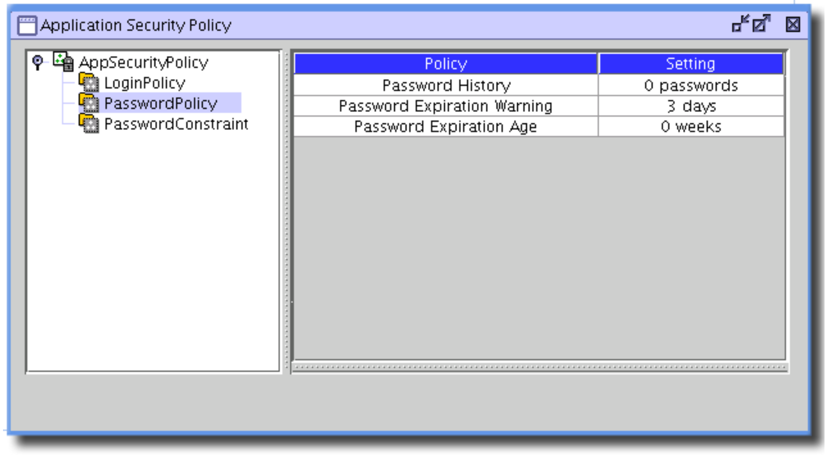
Lockout Period 5 minutes

Password Policy

The settings associated with Password Policy determine whether (and how long) users can keep passwords, how many unique passwords a user must have before the oldest can be re-used, and how much warning they get before their password expires.

Display the password policies by clicking the PasswordPolicy icon in the navigation page. The individual policies appear in the right page.

Figure 25-31. Application Security Policy Page — Password Policies



Policy	Setting
Password History	0 passwords
Password Expiration Warning	3 days
Password Expiration Age	0 weeks

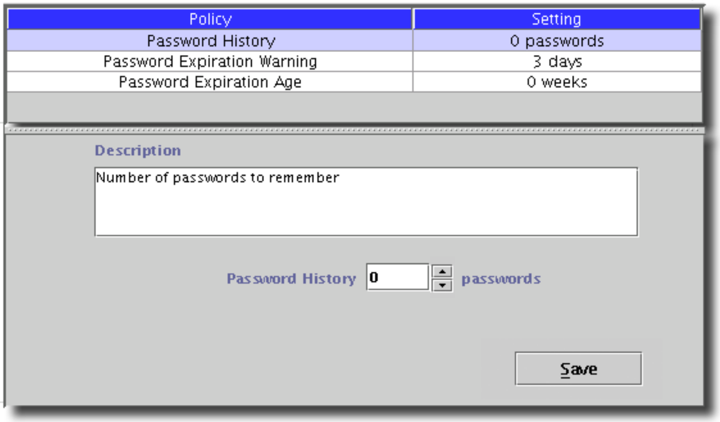
Edit a policy by clicking it; an editor appropriate to that policy appears in the lower portion of the page.This policy editor lets you manage the following:

- Password History
- Password Expiration Warning
- Password Expiration Age
- Allow Password Reuse
- Minimum Password Length
- Require a special character
- Require a special characternumber
- Require Mixed Case
- Allow UserId in Password
- Allow Reverse UserId in Password
- Allow Same Character Consecutively
- Require PasswordMatch Regular Expression

Password History

Enter the *Password History* setting in conjunction with the *Allow Password Reuse* setting (see *This specifies whether users must include a number in their passwords —house2magnet, for example.* on page 322). If password reuse is not allowed, the system tracks passwords in a FIFO (First In, First Out) queue, up to the number specified by this setting.

Figure 25-32. Password History



Policy	Setting
Password History	0 passwords
Password Expiration Warning	3 days
Password Expiration Age	0 weeks

Description

Number of passwords to remember

Password History 0 passwords

You can reuse an old password after the specified a number of other passwords have been used. For example: If you do not enable *Allow Password Reuse* and Password History is set to three, a user's sequence of passwords might look like this:

```
House*Magnet
Fig@Bumper
Rose-Window
Standard+Disclaimer
House*Magnet
```

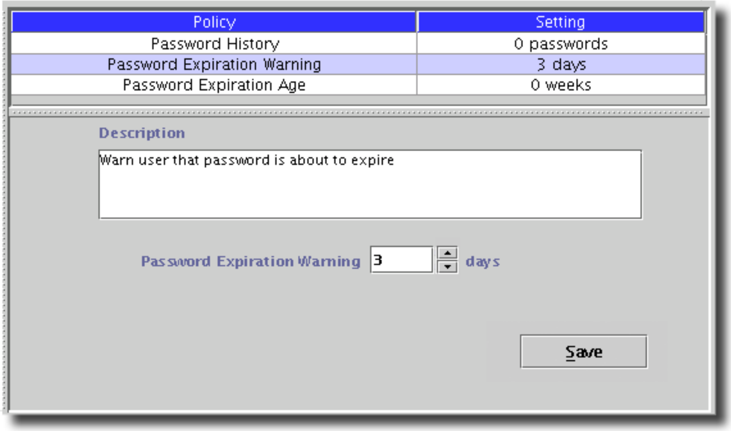
You can reuse `House*Magnet`, since three other passwords have been used since `House*Magnet`.

NOTE: A setting of zero, as shown in the example, effectively enables immediate password reuse even if you do not set Allow Password Reuse.

Password Expiration Warning

This warning goes to users whose password is about to expire. The setting determines, in days, how much advance warning they receive (the warning appears every login attempt during the warning period). Enter a value directly in the *Password Expiration Warning* field, or use the up and down arrows to change the displayed value.

Figure 25-33. Password Expiration Warning



Policy	Setting
Password History	0 passwords
Password Expiration Warning	3 days
Password Expiration Age	0 weeks

Description

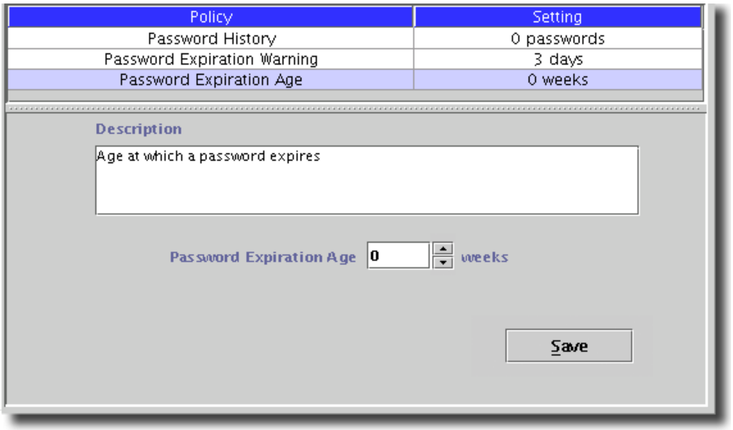
Warn user that password is about to expire

Password Expiration Warning 3 days

Password Expiration Age

The Password Expiration Age setting determines how long a user can keep a password before a new one must be selected. Enter a value directly in the Password Expiration Age field, or use the up and down arrows to change the displayed value.

Figure 25-34. Password Expiration Age



Policy	Setting
Password History	0 passwords
Password Expiration Warning	3 days
Password Expiration Age	0 weeks

Description

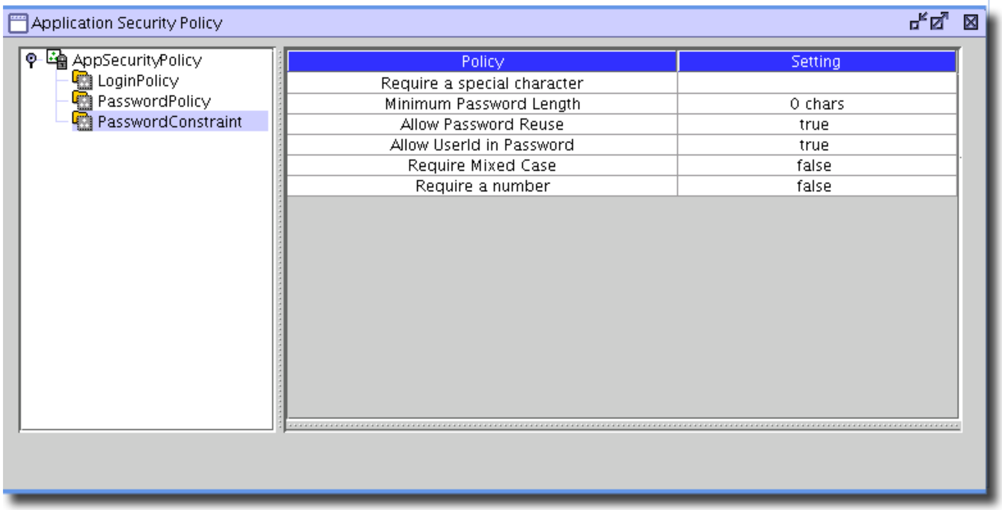
Age at which a password expires

Password Expiration Age 0 weeks

Password Constraint

Password Constraint policies specify how you can construct passwords. Display them by clicking the PasswordConstraint icon in the navigation page. The display shows each policy and its current setting. Edit a policy by selecting it; the edit dialog appears in the lower portion of the page.

Figure 25-35. Password Constraint



Policy	Setting
Require a special character	
Minimum Password Length	0 chars
Allow Password Reuse	true
Allow UserId in Password	true
Require Mixed Case	false
Require a number	false

This includes the following sections:

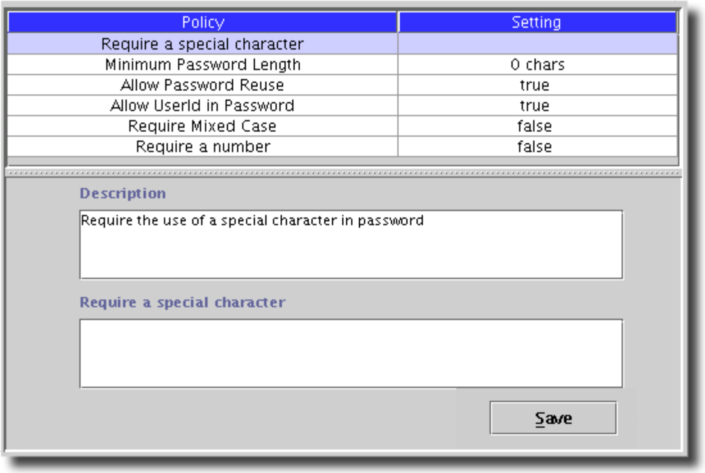
- Allow Password Reuse
- Allow UserId in Password
- Require Mixed Case
- Require a special characternumber
- Require Mixed Case
- Allow UserId in Password
- Allow Reverse UserId in Password
- Allow Same Character Consecutively
- Require PasswordMatch Regular Expression

You can set the initial, default password too. See *General* on page 336 for more information.

Require a special character

This requires a special character be part of a user's password — house*magnet, for example. Activate this option by entering the special characters considered acceptable in the *Require a special character* field. In the example above, an asterisk (*) is among the acceptable special characters.

Figure 25-36. Require a special character



Policy	Setting
Require a special character	
Minimum Password Length	0 chars
Allow Password Reuse	true
Allow UserId in Password	true
Require Mixed Case	false
Require a number	false

Description

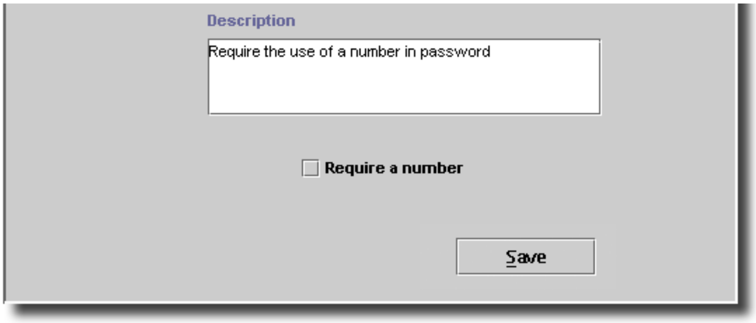
Require the use of a special character in password

Require a special character

Require a number

This specifies whether users must include a number in their passwords —house2magnet, for example.

Figure 25-37. Require a number



Description

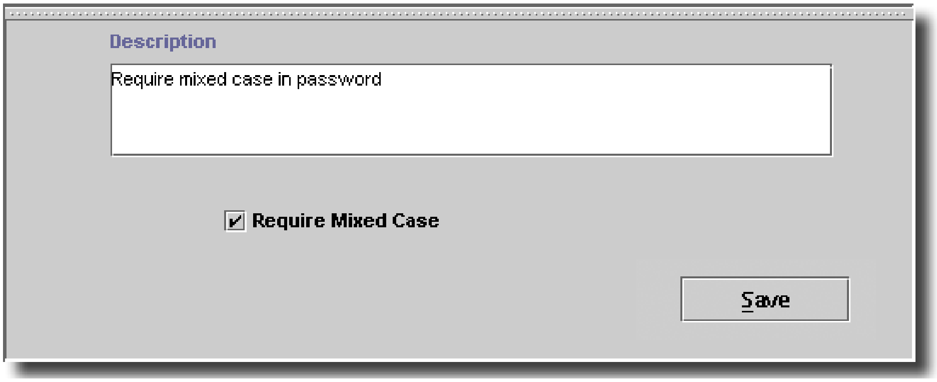
Require the use of a number in password

□ Require a number

Require Mixed Case

This requires a user's password to include both upper and lowercase characters —`HouseMagnet`, for example.

Figure 25-38. Require Mixed Case



Description

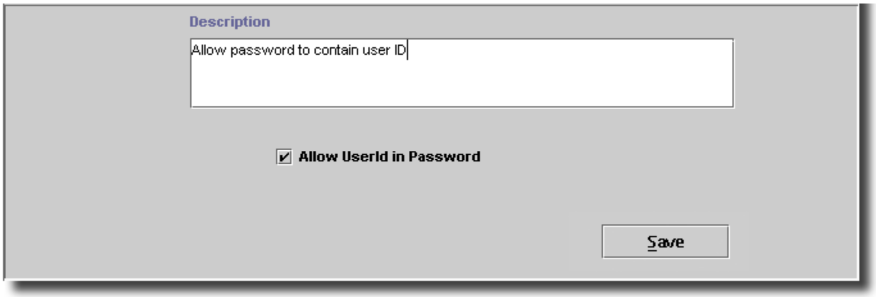
Require mixed case in password

☑ Require Mixed Case

Allow UserId in Password

This lets users include their User ID in their passwords. For example, user MyUser could to create *house*MyUser*magnet* as a password.

Figure 25-39. Allow UserID in Password



Description

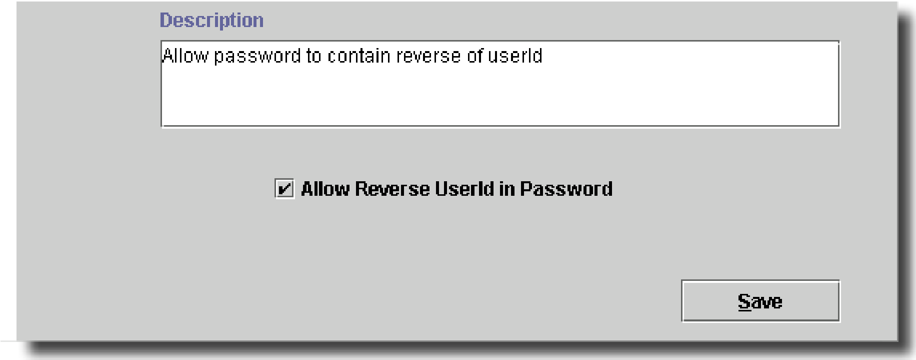
Allow password to contain user ID

☑ Allow UserId in Password

Allow Reverse UserId in Password

This lets users include a backward version of their User ID in their passwords. For example, user MyUser could to create house*resUyM*magnet as a password.

Figure 25-40. Allow Reverse UserID in password.



Description

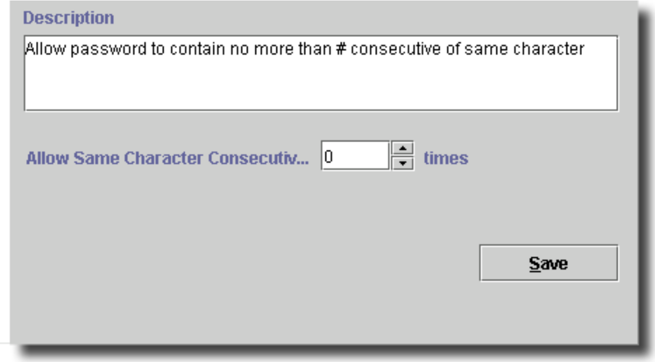
Allow password to contain reverse of userId

☑ Allow Reverse UserId in Password

Allow Same Character Consecutively

This lets users include consecutive identical characters in their passwords. For example, user you could to create hoooouse*MyUser*magnet as a password.

Figure 25-41. Allow same characters consecutivly



Description

Allow password to contain no more than # consecutive of same character

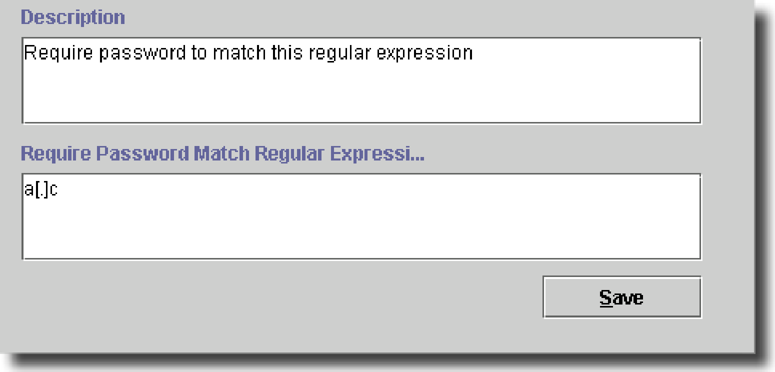
Allow Same Character Consecutiv... 0 times

Use the spinner to select how many consecutive characters to permit.

Require PasswordMatch Regular Expression

This lets administrators restrict passwords to those that match a regular expression.

Figure 25-42. Require password match regular expression



Description

Require password to match this regular expression

Require Password Match Regular Expressi...

a[.]c

Allow UserID in Password

For example, this allows administrators to supply an expression like this:

[^[:digit:]\\\'\;\"\:\?\/\>\<\,\.\=\-].*([[:digit:]\\\'\;\"\:\?\/
\>\<\,\.\=\-]).*[^[:digit:]\\\'\;\"\:\?\/\>\<\,\.\=\-]

This expression specifies that the password must contain, but not start or end with, a numeric or special character, where a special character is defined as any of the following: \";:?/><,.=-

Permitted regular expressions are of the type "RE_SYNTAX_POSIX_AWK". This specifies, among other things, that special characters must be escaped using the backslash.

You can find additional descriptions of the syntax of regular expressions at the following URLs:

http://nlp.stanford.edu/nlp/javadoc/gnu-regexp-docs/

http://www.cs.utah.edu/dept/old/texinfo/regex/regex.html#SEC18

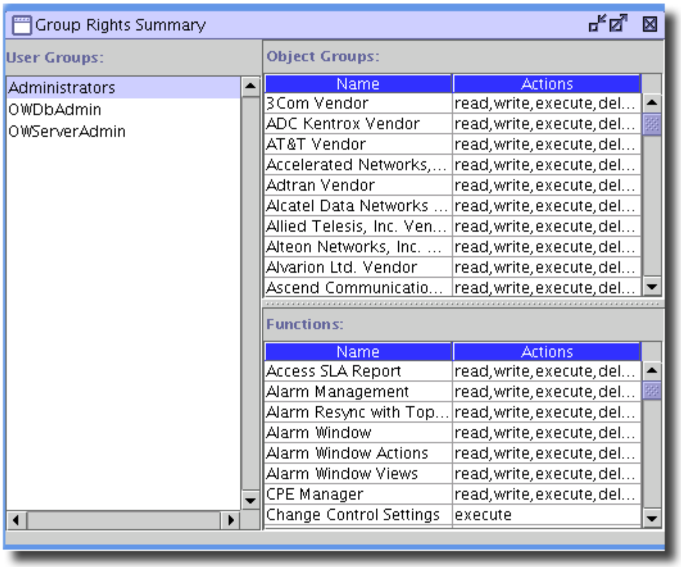
http://www.eli.sdsu.edu/courses/fall98/cs596/notes/regexp/regexp.html

This policy defaults to an empty regular expression.

Group Rights Summary

The Group Rights Summary page provides a read-only summary of user groups, as defined in the *User Group Manager* on page 294, and each group's assigned functions and actions, as defined in the *Functional Permissions* on page 307.

Figure 25-43. Group Rights Summary Page



Group Rights Summary

User Groups:

- Administrators
- OWDbAdmin
- OWServerAdmin

Object Groups:

Name	Actions
3Com Vendor	read,write,execute,del...
ADC Kentrox Vendor	read,write,execute,del...
AT&T Vendor	read,write,execute,del...
Accelerated Networks,...	read,write,execute,del...
Adtran Vendor	read,write,execute,del...
Alcatel Data Networks ...	read,write,execute,del...
Allied Telesis, Inc. Ven...	read,write,execute,del...
Alteon Networks, Inc. ...	read,write,execute,del...
Alvarion Ltd. Vendor	read,write,execute,del...
Ascend Communicatio...	read,write,execute,del...

Functions:

Name	Actions
Access SLA Report	read,write,execute,del...
Alarm Management	read,write,execute,del...
Alarm Resync with Top...	read,write,execute,del...
Alarm Window	read,write,execute,del...
Alarm Window Actions	read,write,execute,del...
Alarm Window Views	read,write,execute,del...
CPE Manager	read,write,execute,del...
Change Control Settings	execute

To display the information for a user group, select that group in the left (User Groups) page.

26

Licensing and System Controls

Overview

Some capabilities for this application require licensing. You view installed licenses with the License Viewer, described below.

The various panels that populate the Controls Manager provide for configuration of application modules and services. Select *Settings* > *Configuration* > *Control Settings* to display the Controls Manager. This Manager consists of tabbed panels representing groups of functions. Those functions appear in this section in alphabetical order.

NOTE: The configuration of the Controls Manager depends upon the specific installation. The examples in this section demonstrate one possible configuration, but do not exhaust all possibilities. Some controls may do nothing without additional, installed options.

- Assure Properties
- General
- Graphics
- Properties
- Color Editor

CAUTION: If you see a panel in the application, but not in the document, changes to that panel are unsupported in your version of the application.

Licenses

Some products require you to register a license. Use the *Settings* > *Permissions* > *Register License* menu item to open a dialog that lets you locate the license file. Select the file, and click *Register License* in the dialog, and you can use the licensed product.

Here are the steps to register a license file in this application:

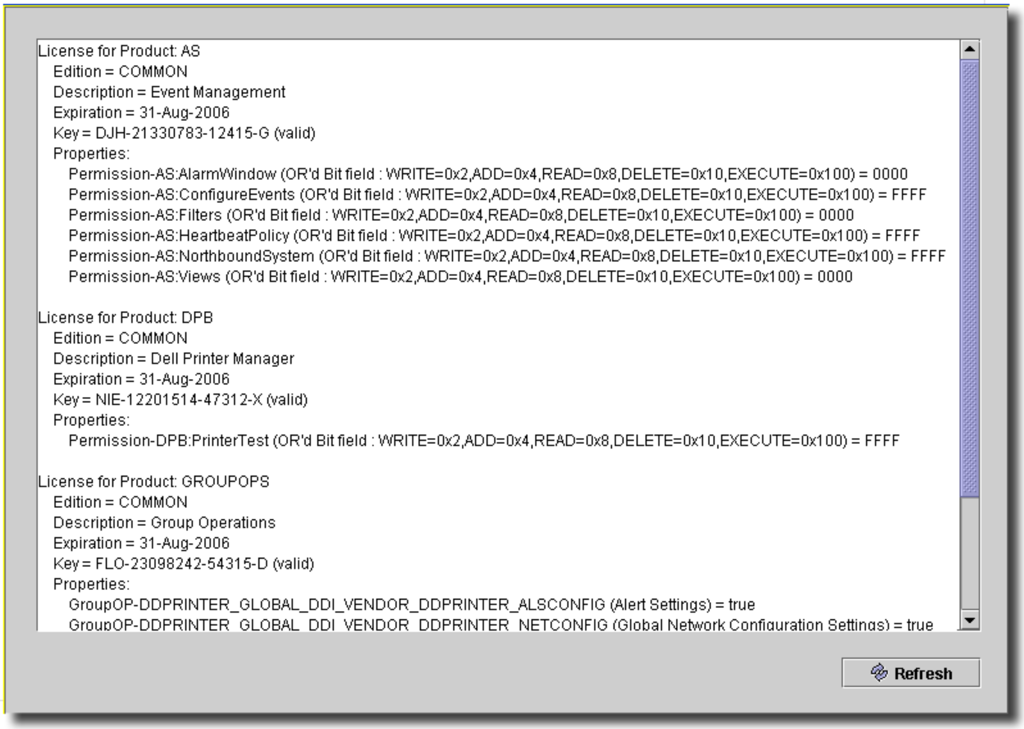
1. Copy the license.xml file to an accessible local directory, for example the owareapps directory.
2. Open *Settings* > *Permissions* > *Register License*.
3. In the *Select License File* window browse to the `license.xml` file location and select the file.
4. Click the *Register License* button to import and register the license file.
5. The *License File Registered* dialog should appear. Click *OK*.

The License is now registered and the licensed product/functionality is now available.

License Viewer

Open the application's license viewer with *Settings > Permissions > View Licenses*. This viewer displays the currently available licenses for the application.

Figure 26-1. License Viewer



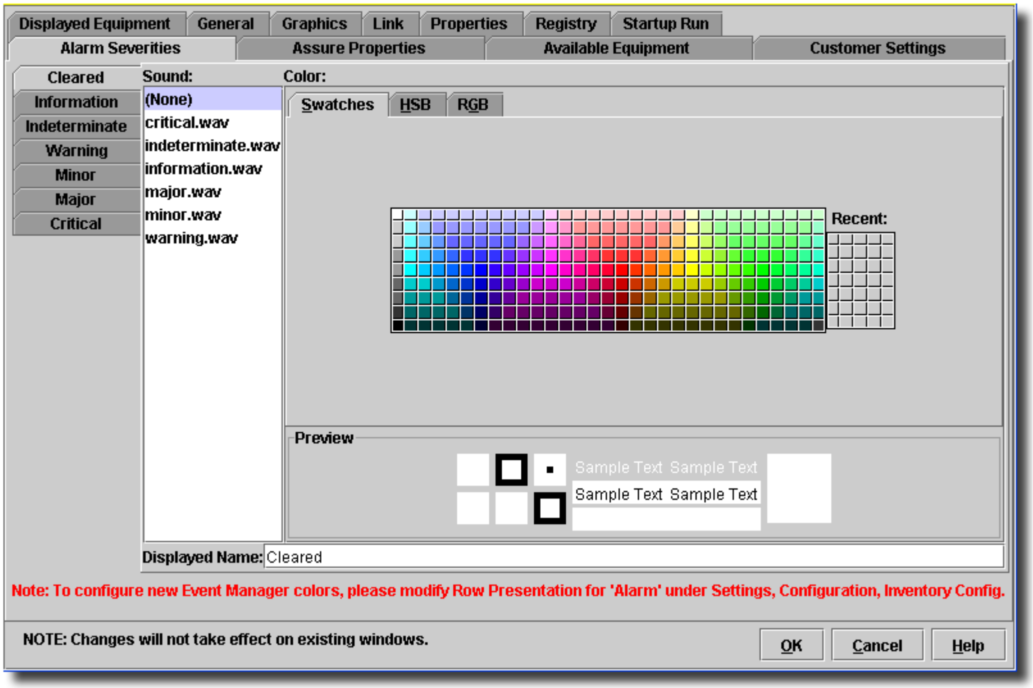
```
License for Product: AS
  Edition = COMMON
  Description = Event Management
  Expiration = 31-Aug-2006
  Key = DJH-21330783-12415-G (valid)
  Properties:
    Permission-AS:AlarmWindow (OR'd Bit field : WRITE=0x2,ADD=0x4,READ=0x8,DELETE=0x10,EXECUTE=0x100) = 0000
    Permission-AS:ConfigureEvents (OR'd Bit field : WRITE=0x2,ADD=0x4,READ=0x8,DELETE=0x10,EXECUTE=0x100) = FFFF
    Permission-AS:Filters (OR'd Bit field : WRITE=0x2,ADD=0x4,READ=0x8,DELETE=0x10,EXECUTE=0x100) = 0000
    Permission-AS:HeartbeatPolicy (OR'd Bit field : WRITE=0x2,ADD=0x4,READ=0x8,DELETE=0x10,EXECUTE=0x100) = FFFF
    Permission-AS:NorthboundSystem (OR'd Bit field : WRITE=0x2,ADD=0x4,READ=0x8,DELETE=0x10,EXECUTE=0x100) = FFFF
    Permission-AS:Views (OR'd Bit field : WRITE=0x2,ADD=0x4,READ=0x8,DELETE=0x10,EXECUTE=0x100) = 0000

License for Product: DPB
  Edition = COMMON
  Description = Dell Printer Manager
  Expiration = 31-Aug-2006
  Key = NIE-12201514-47312-X (valid)
  Properties:
    Permission-DPB:PrinterTest (OR'd Bit field : WRITE=0x2,ADD=0x4,READ=0x8,DELETE=0x10,EXECUTE=0x100) = FFFF

License for Product: GROUPOPS
  Edition = COMMON
  Description = Group Operations
  Expiration = 31-Aug-2006
  Key = FLO-23098242-54315-D (valid)
  Properties:
    GroupOP-DDPRINTER_GLOBAL_DDI_VENDOR_DDPRINTER_ALSCONFIG (Alert Settings) = true
    GroupOP-DDPRINTER_GLOBAL_DDI_VENDOR_DDPRINTER_NETCONFIG (Global Network Configuration Settings) = true
```

Licenses appear listed in this screen. Click *Refresh* to query for additional licenses.

Alarm Severities

To access this and the panels described in the following sections, click *Settings > Configuration > Control Settings* and click the appropriate tab on the subsequent screen. Use the *Alarm Severities* panel to associate alarm severities with colors and sounds. Sound files are in `owareapps\assure\media\sounds`.

Figure 26-2. Alarm Severities



Displayed Name: Cleared

Note: To configure new Event Manager colors, please modify Row Presentation for 'Alarm' under Settings, Configuration, Inventory Config.

NOTE: Changes will not take effect on existing windows.

Select an alarm, then click the sound, or *(None)* to assign it to that alarm. You can make any `.wav` file alert you to the presence of an alarm by naming it correctly and putting it in `owareapps\assure\media\sounds`. You must also set `redcell.assure.fault.audible.alarms.enabled` to *true* as instructed in *Properties on page* 339.

You can also change the text displayed (*Displayed Name*) for an alarm severity at the bottom of this tab. See *Color Editor* on page 329 for additional information.

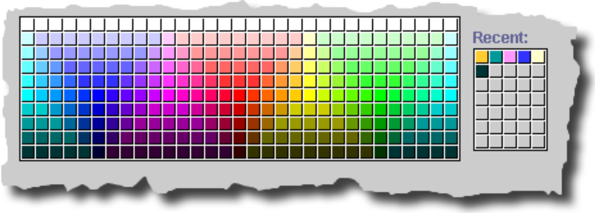
NOTE: OMPM best practice is not to use this screen, but to use the methods described in *Inventory Config* on page 46 instead.

Click *OK* to accept your edits, or *Cancel* to abandon them.

Color Editor

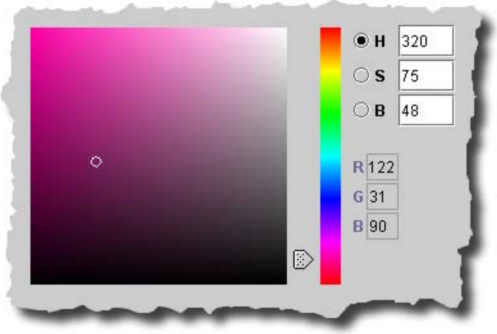
The Color Editor is how various application modules select colors. It provides three modes of color selection: swatches, HSB values, and RGB values.

- **Swatches**—This color model presents the available colors as a grid of 310 boxes. Click on any box to select that color.



The *Recent* portion of this panel displays the 35 most recently selected swatch colors; you can select any of these colors by clicking on the appropriate box.

- **HSB**—This color model lets you specify a color by its Hue, Saturation, and Brightness values. You can select and adjust one component (H, S, or B) at a time.



● H 320
○ S 75
○ B 48
R 122
G 31
B 90

The large square in this panel displays a range for the selected component with respect to the other two components. For example, if you select a Hue value of 200, the square displays that hue with the saturation ranging from 100 (right) to 0 (left), and the brightness ranging from 0 (bottom) to 100 (top).

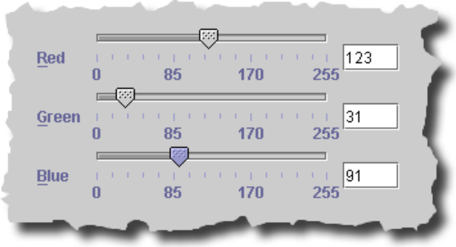
The slider in the middle displays the range of values for the selected component.

The H, S, and B radio buttons to the right of the panel let you select the color component to adjust, and let you directly specify the value for each component. The following are acceptable values:

- **H**—Hue is measured on a color wheel, and is specified in degrees. Acceptable values range from 0 to 360.
- **S**—Saturation (the amount of the specified hue present) is specified as a percentage. Acceptable values range from 0 to 100.
- **B**—Brightness is specified as a percentage. Acceptable values range from 0 to 100.

  The R, G, and B values on the lower right side of this panel indicate the equivalent Red, Green, and Blue values for the selected color.

- **RGB**—This color model lets you specify a color by its Red, Green, and Blue components.



Red 123

Green 31

Blue 91

Each color component (Red, Green, and Blue) has an associated slider. Move the slider to the right or left to change the value, or type a component value ranging from 0 to 255 in the text box to the right of the appropriate slider.

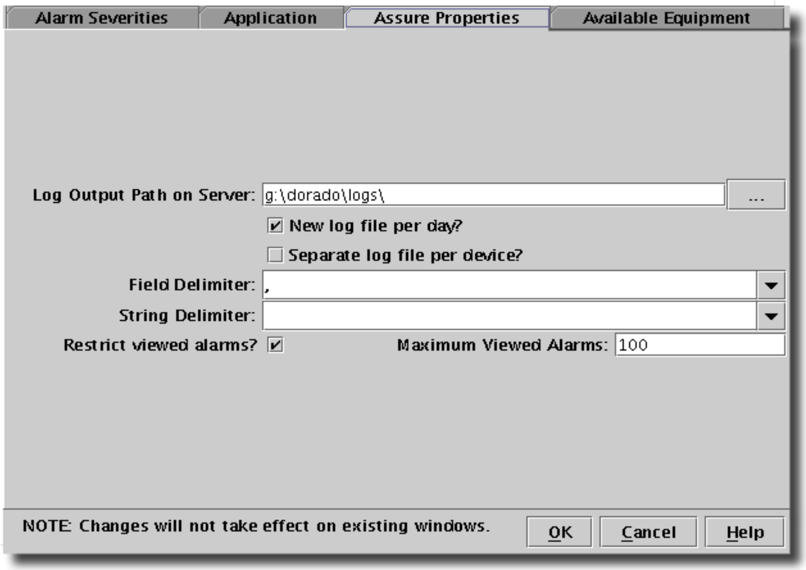
For all three color models, the Preview portion of this dialog shows you what your current color looks like as the text color against a grey background, as the background for white text, and as the text color against a white background.

When you are satisfied with the color, click on *OK* to implement it. Click on *Cancel* to cancel the operation.

Assure Properties

Use this tab to configure various properties in the Assure blade (the Event Services application managing alarms).

Figure 26-3. Assure Properties



Log Output Path on Server: g:\dorado\logs\

☑ New log file per day?

□ Separate log file per device?

Field Delimiter: ,

String Delimiter:

Restrict viewed alarms? ☑ Maximum Viewed Alarms: 100

NOTE: Changes will not take effect on existing windows.

The following are the fields and checkboxes you can modify:

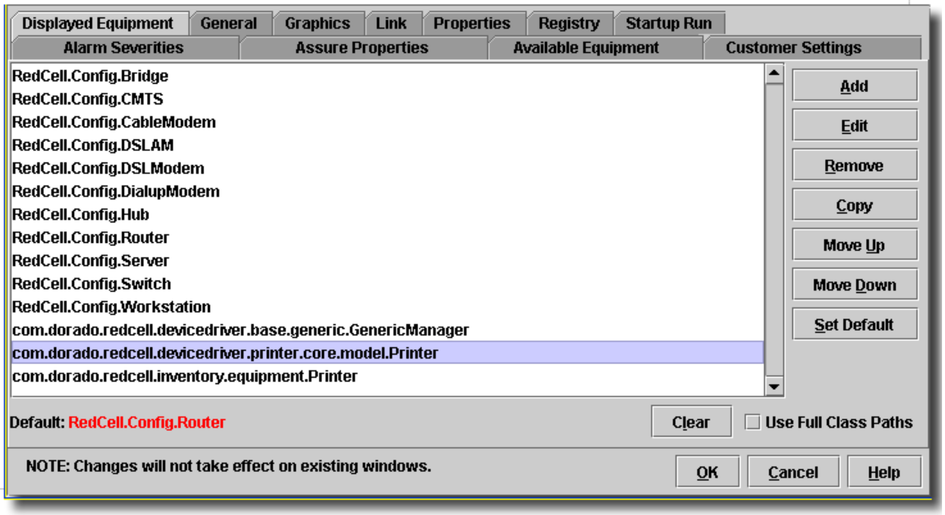
- **Log Output Path**—Type a path for the output log file, or select one with the command button (...).
- **New Log File Per Day**—Check if you want a new log file produced daily. If this is not checked, the same log file continues to grow.
- **Separate Log File Per Device?**—Separates logs by device rather than including all devices in a single log.
- **Field Delimiter**—Select from the pick list of field delimiters. The default is a comma.
- **String Delimiter**—Select from the pick list of string delimiters. The default is no delimiter.
- **Restrict Viewed Alarms**, and **Maximum Viewed Alarms**—Work in tandem to ensure a limit to the number of displayed alarms. The application continues to track even undisplayed alarms.

  You can also control the display and querying of alarms in the Alarm History and Alarm Monitor windows with the by creating an Assure system property: `redcell.assure.fault.alarmwindow.maximumallowed`. This number determines the limit you can type in the *Max View Size* spinner in both windows. See *Overriding Properties* on page 347 for more information.

Available Equipment

The Available Equipment control panel determines which equipment classes are available for management. Only previously defined or seeded equipment classes appear in this list.

Figure 26-4. Available Equipment Panel



RedCell.Config.Bridge
RedCell.Config.CMTS
RedCell.Config.CableModem
RedCell.Config.DSLAM
RedCell.Config.DSLModem
RedCell.Config.DialupModem
RedCell.Config.Hub
RedCell.Config.Router
RedCell.Config.Server
RedCell.Config.Switch
RedCell.Config.Workstation
com.dorado.redcell.devicedriver.base.generic.GenericManager
com.dorado.redcell.devicedriver.printer.core.model.Printer
com.dorado.redcell.inventory.equipment.Printer

Default: RedCell.Config.Router

□ Use Full Class Paths

NOTE: Changes will not take effect on existing windows.

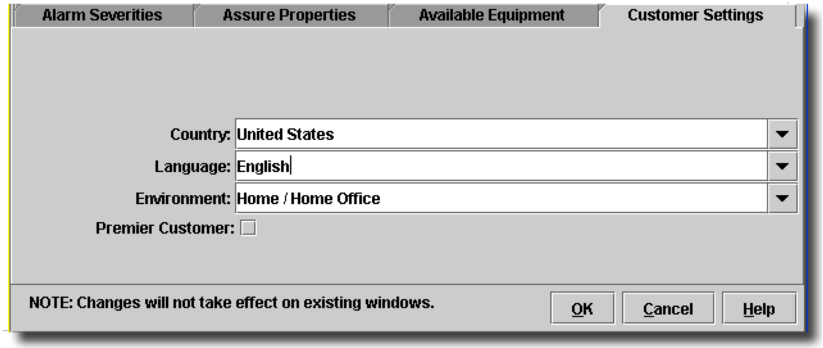
The following are the controls in this panel:

- **Add**—Displays a dialog so you can add equipment classes to the Available Equipment list.
- **Edit**—Displays a dialog populated with the selected equipment class name. Edit the name and click *OK* to accept the changes.
- **Remove**—Removes the selected equipment class.
- **Copy**—Makes a copy of the selected equipment class name.
- **Move Up/Down**—Move the selected equipment up or down the list.
- **Set Default**—Sets the selected equipment class as the default. The *Available Equipment* menu in the Equipment Manager displays this equipment class as the default.
- **Clear**—Clears the default specification.
- **Use Full Class Paths**—Select this option to display full class paths in the Available Equipment list.

Customer Settings

This screen configures customer settings for the selected installation if you have the Dell Printer driver installed.

Figure 26-5. Customer Settings



Country: United States

Language: English

Environment: Home / Home Office

Premier Customer: □

NOTE: Changes will not take effect on existing windows.

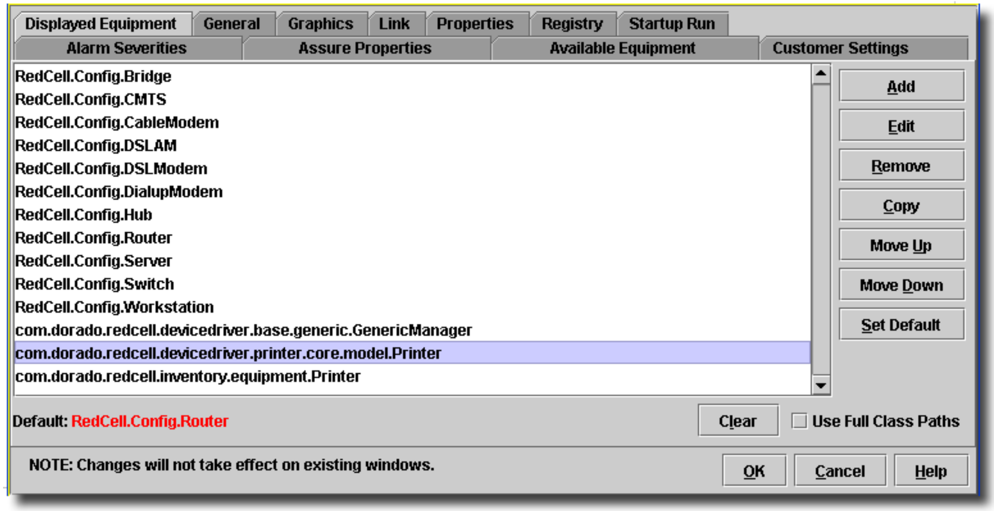
Settings here influence the web page that appears when you order supplies. The following are the controls on this panel:

- **Country**—Select a country from those available on the pick list.
- **Language**—Select a language from those available on the pick list.
- **Environment**—Select an environment from those available on the pick list.
- **Premier Customer**—Check to activate.

Displayed Equipment

The *Displayed Equipment* control panel determines which classes of equipment are available to the Equipment Manager for creating new equipment objects. Classes listed depend on the drivers installed with your application.

Figure 26-6. Displayed Equipment Panel



RedCell.Config.Bridge
RedCell.Config.CMTS
RedCell.Config.CableModem
RedCell.Config.DSLAM
RedCell.Config.DSLModem
RedCell.Config.DialupModem
RedCell.Config.Hub
RedCell.Config.Router
RedCell.Config.Server
RedCell.Config.Switch
RedCell.Config.Workstation
com.dorado.redcell.devicedriver.base.generic.GenericManager
com.dorado.redcell.devicedriver.printer.core.model.Printer
com.dorado.redcell.inventory.equipment.Printer

Default: RedCell.Config.Router

□ Use Full Class Paths

NOTE: Changes will not take effect on existing windows.

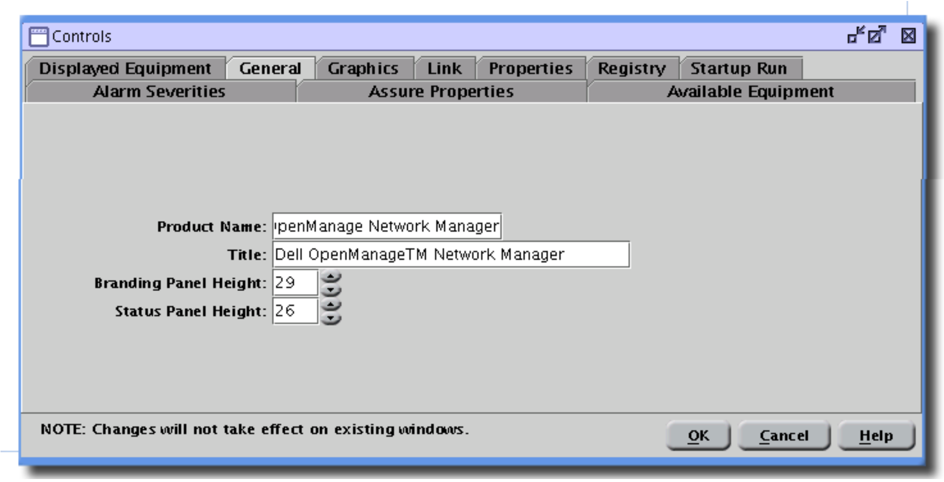
The following are the controls in this panel:

- Add—Opens a dialog where you can specify an equipment class to add. The equipment class you add must also exist in the Available Equipment list.
- Edit—Displays a dialog containing the selected equipment class. Edit the name or path of the equipment class as appropriate and click *OK* to implement the changes.
- Remove—Deletes the selected equipment class from the list of displayed equipment.
- Copy—Makes a copy of the selected equipment class.
- Move Up/Down—Move the selected item up or down the list.
- Set Default—Sets the selected equipment class as the default when new classes are added to the Equipment Manager.
- Clear—Clears the default equipment class specification.
- User Full Class Paths—When selected, specifies that full class paths are to appear in the Displayed Equipment control panel.

General

The General panel lets you specify the product name and screen appearance.

Figure 26-7. General Panel



Product Name: penManage Network Manager

Title: Dell OpenManageTM Network Manager

Branding Panel Height: 29

Status Panel Height: 26

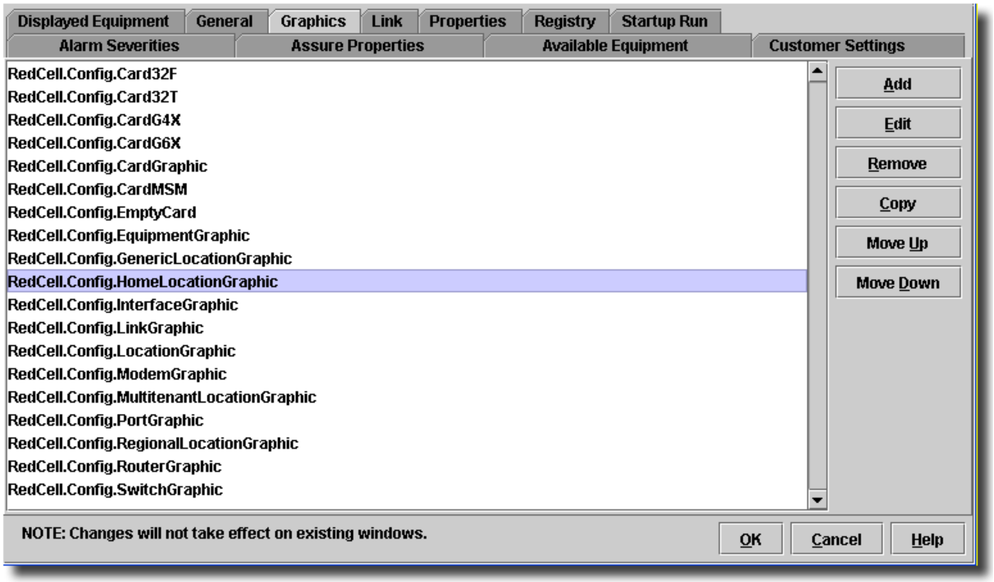
NOTE: Changes will not take effect on existing windows.

- **Product Name:**—Enter a product name in the *Product Name* field.
- **Title**—This text appears in the portal form title bar.
- **Branding Panel Height**—The height (in pixels) of the panel that appears under the menus.
- **Status Panel Height**—The height (in pixels) of the panel that appears beneath the work area in the portal form.

Graphics

The Graphics panel lets you specify which graphics are available to associate with managed objects in Topology (maps are a separate issue). The controls in this panel let you add, copy, edit, remove graphics from the list, and reorder them in the display. See the *Topology* chapter of the *User Guide* for information about changing Topology map graphics.

Figure 26-8. Graphics Panel



RedCell.Config.Card32F
RedCell.Config.Card32T
RedCell.Config.CardG4X
RedCell.Config.CardG6X
RedCell.Config.CardGraphic
RedCell.Config.CardMSM
RedCell.Config.EmptyCard
RedCell.Config.EquipmentGraphic
RedCell.Config.GenericLocationGraphic
RedCell.Config.HomeLocationGraphic
RedCell.Config.InterfaceGraphic
RedCell.Config.LinkGraphic
RedCell.Config.LocationGraphic
RedCell.Config.ModemGraphic
RedCell.Config.MultitenantLocationGraphic
RedCell.Config.PortGraphic
RedCell.Config.RegionalLocationGraphic
RedCell.Config.RouterGraphic
RedCell.Config.SwitchGraphic

NOTE: Changes will not take effect on existing windows.

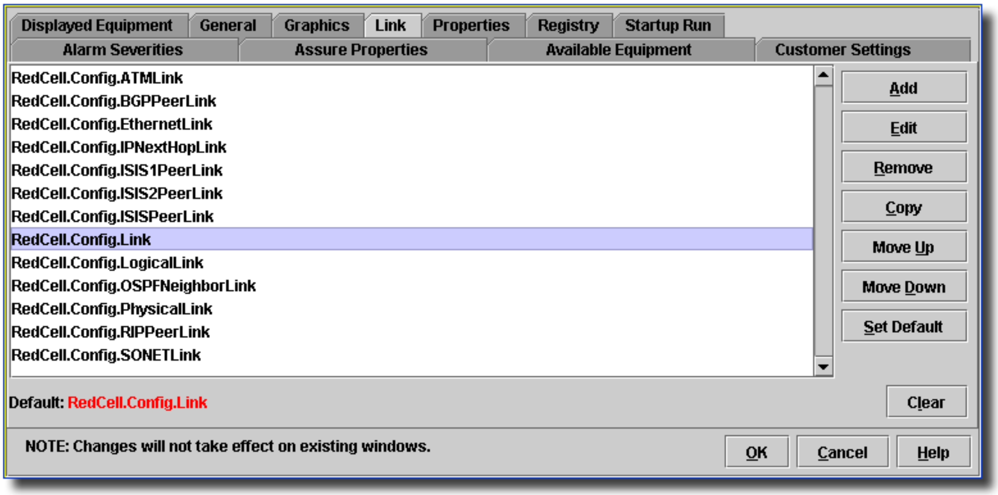
The Graphics panel offers the following controls:

- **Add**—Lets you specify a graphic, with full class path, available for association with a managed object—`RedCell.Config.HomeLocationGraphic`, for example. (The Topology viewer uses this graphic.)
- **Edit**—Displays an edit dialog, through which you can change the name or path of the selected graphic.
- **Remove**—Deletes the selected graphic.
- **Copy**—Makes a copy of the selected graphic.
- **Move Up/Down**—Move the selected item up or down the list.

Link

The Link panel lets you specify which classes are available for link creation. The classes listed in this panel must be in the application already, and populate the Class Selection menu in the Link Manager.

Figure 26-9. Link Panel



RedCell.Config.ATMLink
RedCell.Config.BGPPeerLink
RedCell.Config.EthernetLink
RedCell.Config.IPNextHopLink
RedCell.Config.ISIS1PeerLink
RedCell.Config.ISIS2PeerLink
RedCell.Config.ISISPeerLink
RedCell.Config.Link
RedCell.Config.LogicalLink
RedCell.Config.OSPFNeighborLink
RedCell.Config.PhysicalLink
RedCell.Config.RIPPeerLink
RedCell.Config.SONETLink

Default: RedCell.Config.Link

NOTE: Changes will not take effect on existing windows.

The following are the Link panel controls:

- Add—Adds a new class to the list of classes from which you can create link objects.
- Edit—Opens a dialog populated with the selected class. Change the name or path as appropriate and click *OK* to implement your changes.
- Remove—Deletes the selected class from the list.
- Copy—Makes a copy of the selected class.
- Move Up/Down—Move the selected item up or down the list.
- Set Default—Sets the selected class as the default. This class appears as the default selection in the *Class Selection* menu of the Link Manager. New Link objects instantiate from this class unless otherwise specified.
- Clear—Clears the default specification.

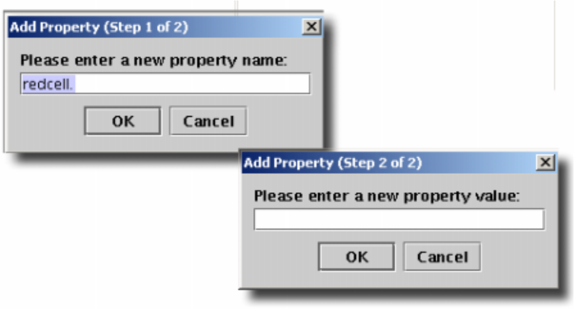
NOTE: This screen is not used for OMPM.

Properties

The Properties control panel provides an interface into the application's `settings.txt` file (in `owareapps\redcell\db`) and lets you view, add, delete, edit, and sort the entries in that file. The contents of this panel may vary if you have optional products or drivers installed.

The Properties panel features the following controls:

- Add—Opens a two-step dialog through which you can add a new property. Both steps appear below. In the first step, enter the name of the new property and click *OK*. Then enter a value for the new property and click *OK* to save it.



Add Property (Step 1 of 2)

Please enter a new property name:

redcell.

Add Property (Step 2 of 2)

Please enter a new property value:

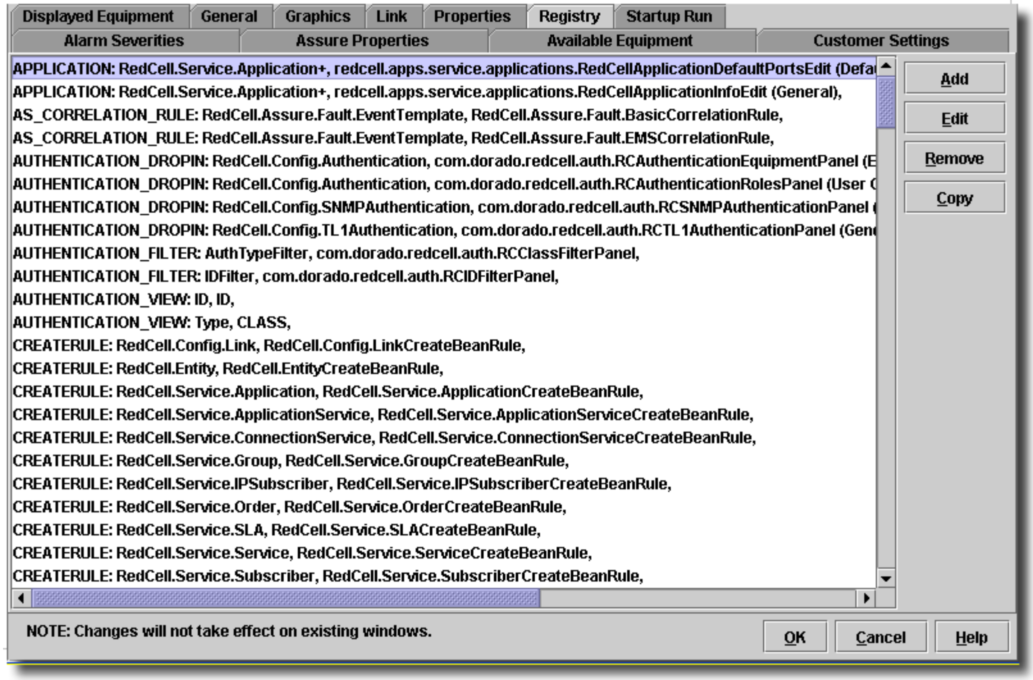
- Edit—Opens a two-step dialog populated with the selected property. Change the name or path as appropriate and click *OK* to move to the second step. Specify the appropriate property value in the second dialog and click *OK* to implement your changes.
- Remove—Deletes the selected property from the list.
- Copy—Makes a copy of the selected property.
- Move Up/Down—Orders the list appearance. Note that the list is exported to the `settings.txt` file in the order of this panel; changing the sort order also changes the export order. This is for readability only.
- Sort—Sorts the listed properties alphabetically. A subsequent dialog asks you to confirm that you also want to change the order of properties exported to a `settings.txt` file.

NOTE: Settings for alarm count and view size settings may have a performance impact.

Registry

The Registry panel provides a graphical interface to manage the application's registry. The Registry lets the application access new classes. The parameters for each individual registry item determine how to interpret the entry, and let you specify default values and behaviors for that entry.

Figure 26-10. Registry Panel



```
APPLICATION: RedCell.Service.Application+, redcell.apps.service.applications.RedCellApplicationDefaultPortsEdit (Defa
APPLICATION: RedCell.Service.Application+, redcell.apps.service.applications.RedCellApplicationInfoEdit (General),
AS_CORRELATION_RULE: RedCell.Assure.Fault.EventTemplate, RedCell.Assure.Fault.BasicCorrelationRule,
AS_CORRELATION_RULE: RedCell.Assure.Fault.EventTemplate, RedCell.Assure.Fault.EMSCorrelationRule,
AUTHENTICATION_DROPIN: RedCell.Config.Authentication, com.dorado.redcell.auth.RCAuthenticationEquipmentPanel (E
AUTHENTICATION_DROPIN: RedCell.Config.Authentication, com.dorado.redcell.auth.RCAuthenticationRolesPanel (User C
AUTHENTICATION_DROPIN: RedCell.Config.SNMPAuthentication, com.dorado.redcell.auth.RCSNMPAuthenticationPanel (
AUTHENTICATION_DROPIN: RedCell.Config.TL1Authentication, com.dorado.redcell.auth.RCTL1AuthenticationPanel (Gen
AUTHENTICATION_FILTER: AuthTypeFilter, com.dorado.redcell.auth.RCClassFilterPanel,
AUTHENTICATION_FILTER: IDFilter, com.dorado.redcell.auth.RCIDFilterPanel,
AUTHENTICATION_VIEW: ID, ID,
AUTHENTICATION_VIEW: Type, CLASS,
CREATERULE: RedCell.Config.Link, RedCell.Config.LinkCreateBeanRule,
CREATERULE: RedCell.Entity, RedCell.EntityCreateBeanRule,
CREATERULE: RedCell.Service.Application, RedCell.Service.ApplicationCreateBeanRule,
CREATERULE: RedCell.Service.ApplicationService, RedCell.Service.ApplicationServiceCreateBeanRule,
CREATERULE: RedCell.Service.ConnectionService, RedCell.Service.ConnectionServiceCreateBeanRule,
CREATERULE: RedCell.Service.Group, RedCell.Service.GroupCreateBeanRule,
CREATERULE: RedCell.Service.IPSubscriber, RedCell.Service.IPSubscriberCreateBeanRule,
CREATERULE: RedCell.Service.Order, RedCell.Service.OrderCreateBeanRule,
CREATERULE: RedCell.Service.SLA, RedCell.Service.SLACreateBeanRule,
CREATERULE: RedCell.Service.Service, RedCell.Service.ServiceCreateBeanRule,
CREATERULE: RedCell.Service.Subscriber, RedCell.Service.SubscriberCreateBeanRule,
```

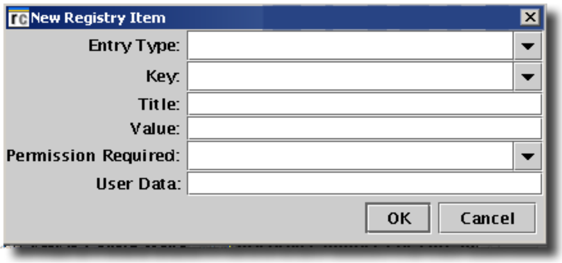
NOTE: Changes will not take effect on existing windows.

⚠ **CAUTION: Changes to this panel are *not* recommended. Changes here can impair the application.**

The Registry panel has the following controls:

Add—Displays the *Editing Registry Item* dialog, where you can specify a new class. The class must already exist (created in the Oware Creation Center). Add an entry by filling out the fields in the *Editing Registry Item* dialog, shown below. Click *OK* to add the entry to the database.

Figure 26-11. Registry Edits

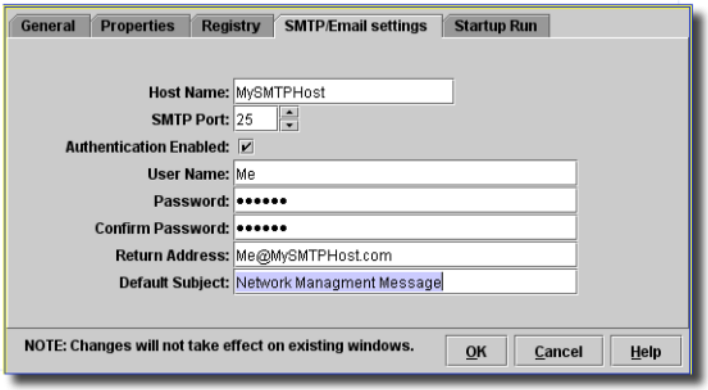


- **Edit**—Opens a dialog populated with the selected class. Make the appropriate changes and click *OK* to implement your changes.
- **Remove**—Deletes the selected class from the list.
- **Copy**—Makes a copy of the selected entry.

SMTP / Email Settings

This screen sets up the Simple Mail Transport Protocol (SMTP) and other e-mail settings for this application to send mail.

Figure 26-12. SMTP / Email Settings



Host Name: MySMTPHost

SMTP Port: 25

Authentication Enabled: ☑

User Name: Me

Password: ••••••

Confirm Password: ••••••

Return Address: Me@MySMTPHost.com

Default Subject: Network Managment Message

NOTE: Changes will not take effect on existing windows.

This screen has the following fields:

Host Name—The name of the SMTP server.

SMTP Port—Use the spinner to enter the port for SMTP on the named host.

Authentication Enabled—Check to enable authentication on this host.

User Name—The login name to access the SMTP server.

Password / Confirm Password—The password, and its confirmation, to access the SMTP server.

Return Address—The return e-mail address for mail sent by this application.

Default Subject—The subject that appears by default in any mail sent by the application. Other mail specifics may override this subject.

NOTE: This screen's settings override any properties settings. See "E-mail Settings" on page 343.

Startup Run

The Startup Run Manager lets you specify which rules run when the application starts. The contents of this panel may vary if you have optional applications or drivers installed.

⚠ **CAUTION: Changes to this panel are *not* recommended. Such changes can impair the application.**

The following are the controls in this manager:

- **Add**—Opens a dialog where you can specify the rule to run, and its parameters.
- **Edit**—Opens a dialog populated with the selected entry. Edit the entry as appropriate and click *OK* to implement your changes.
- **Remove**—Deletes the selected entry.
- **Copy**—Makes a copy of the selected entry.
- **Move Up/Down**—Orders the list appearance. Startup rules run in list order.

27

Properties

Overview

You can modify the application through the `.properties` files, typically in `oware\lib, oware\medserver\lib` and in `owareapps\<application>\lib`, for example: `owareapps\redcell\lib`. These are text files you can edit with any text editor. The application does not modify local files during the course of normal system operations. When an administrator or user modifies files, like properties or seed files, best practice is to note which files changed and back up that data. (This application stores all its operational data in its database.)

Particularly if you reinstall your application, installation recreates some properties files in their original form. If you modified those files since the original installation, reinstallation overwrites any changes. Therefore, it is safest to use the application's override capacity see Overriding Properties for files which may change through daily operation, and must therefore be restored from backup (unless you override properties) after reinstallation.

Commonly Modified Properties

Among other things, properties files configure the application's e-mail and use the Win32 print driver and scheduler defaults. Pound signs (#) indicate comments.

See Overriding Properties for advice about modifying properties. You can override individual properties, regardless of where the originals are located.

E-mail Settings

This entry specifies the SMTP host name and return address (overridden in `installed.properties`, this is originally in `owareapps\redcell\lib\SMTP.properties`). The application uses this host name whenever it sends an e-mail; it uses the return address when e-mailing alarms from the Alarm Window.

```
#************************************************************
# SERVER SETUP FOR EMAIL (SMTP) SERVER CONFIGURATION #
#----------------------------------------------------------#
# Uncomment the following lines and populate the value to #
# configure the mail server used by this software to send #
# emails like alerts and scheduled reports. #
# #
# (substitute appropriate values without parenthesis) #
#------------------------------------------------------------#
# This file goes in
#------------------------------------------------------------#
311 Reidell
# NOTE: Message subject is appended to the actual message
# subject that generate the email item.
#redcell.smtphost=(put SMTP server name or IP here)
#redcell.smtphost.authentication.enabled=true
#redcell.smtphost.username=(user name here)
#redcell.smtphost.password=(password here)
#redcell.returnaddress=(return address)
#redcell.notification.message=(default message subject)
# EXAMPLE values
#redcell.smtphost=postoffice.myserver.com
#redcell.smtphost.authentication.enabled=true
#redcell.smtphost.username=John
#redcell.smtphost.password=secret
#redcell.returnaddress=EMAIL@postoffice.myserver.com
redcell.returnaddress=redcell@doradosoftware.com
```

Typically, you can send e-mail within your SMTP host's domain without a login or password. The `SMTP.properites` (or `installed.properties` override) e-mail configuration overrides the following, if you need to set login and password.

In the unusual event that you must send mail outside your domain, set the login/password for the application in three properties that are now in `redcell.properties` for connecting to SMTP server using username and password.

```
redcell.smtphost.authentication.enabled=false
redcell.smtphost.username=admin
redcell.smtphost.password=password
```

Set the `redcell.smtphost.authentication.enabled` property to *true* and provide the username and password information for authenticating the application server with SMTP Server..

To receive email from event templates that trigger e-mails, the destination user must have an e-mail address in this software. See User Manager on page 257 for details. To e-mail from actions/mapping, you just need to type in email account in the actions and then map the actions. No need to add anything to the user manager.

Win32 Print Driver

This Boolean value lets the application use the Win32 custom print driver.

```
# Set to true to enable the use of the
# Win32 custom print driver,
# which speeds up printing of large reports in the application.
StyleReport.useCustomDriver=true
```

Printer Properties

The following polling properties are in `oware\lib\owmediation.properties`. Increase them if you manage a network with more than 1000 printers. As with all properties, best practice is to override them (see Overriding Properties).

```
    # Polling Engine Properties
    # The properties below should be used for controlling the network bandwidth
    # and managing the number of network entities.

    # The property specifies a threshold limit, which if crossed will put the
    # pending subscriptions on hold till the threshold is recovered.
    oware.mediation.polling.max.network.bytes=10240000

    # This property defines the max number of subscriptions in a time slot.
    oware.mediation.polling.max.subscriptions.per.timeslot=25

    # This property defines the timeslot bandwidth.
    oware.mediation.polling.max.bytes.per.timeslot=1024000

    # This property defines the thread pool size used for executing subscriptions.
    # This property should be changed depending on the network entities to be polled.

    oware.mediation.polling.mbean.thread.pool.size=10
```

NOTE: These properties are relevant only if you have a printer driver installed.

Defaults

This section of the properties file sets the default runtime of the application scheduler and specifies whether or not a reverse lookup, to associate a host name with an IP address, occurs during discovery.

```
# Defaults
#
```

```
redcell.scheduler.defaulttime=02:00 AM

#
# if true, reverse lookup is performed in GenericDiscoveryRule
# (scheduled Device Discovery) to obtain host name.
# if false, host name is populated with IP address
#
redcell.discovery.usedns=true
```

installed.properties

This file (`owareapps\installprops\lib\installed.properties`) contains defaults installed with your package. An example of this file appears below. Installation automates the insertion of the `[host name]` variable:

```
#*************************************************************
#  The following properties override those found in         *
#  oware/lib/*.properties in order to establish valid       *
#  properties for this installation.                        *
#*************************************************************

oware.database.host=[host name ]
com.dorado.bom_dbms.preferred_db_type=rdbms
oware.installed.package.name=[Package Name]
oware.installed.package.version=[Package Version]
OWARE.CONTEXT.SERVER.URL=jnp://[host name]:1099
```

Dell installations explicitly set the server URL on clients. This URL assumes the application server is running on the default port range. If ports conflict, use the `-n [Node Number]` parameter in a command line to start application server so it uses something other than a default port range.

If your client cannot connect and the server log shows it cannot bind to port 1099 (or 11099, and so on), then stopping application server from the client does not work; client applications cannot communicate with the application server. In this case, to stop application server, you must kill the `java.exe` processes on the server machine. The tray icon should then indicate the application server is stopped.

To change the port range for application server, modify the node number property for appserver in `oware\lib\pmstartup.dat`. By default (upon installation) the property is as follows:

```
application.server.node.number=0
```

To use a different part range, change zero (0) to 1, 2 or 3.

Once the application server starts and listens (no bind errors), you still have to change port settings for the client connections. For each installation (server and client) modify a URL setting in `owareapps\installprops\lib installed.properties`. An example of default setting (hostname varies) would be as follows:

```
OWARE.CONTEXT.SERVER.URL=jnp://hostname:1099
```

The application server node number should prefix the `1099` port if greater than 0. For example, using `application.server.node.number=1` in `pmstartup.dat` would imply all installations need the following setting in installed.properties:

```
OWARE.CONTEXT.SERVER.URL=jnp://hostname:11099
```

NOTE: For a complete list of port settings and protocols used by this application, see the installation guide.

Overriding Properties

Best practice is not to change default properties, but to override them. This eliminates updates or new installations overwriting property files you have tuned. If you override values, then backing up the override file(s) is essential.

To override a property controlling all but mediation, put it in a file (whose name ends in .`properties`) in the following directory under `owareapps`: `installprops\lib`. You can override mediation server properties in `owareapps\installprops\medserver\lib`. Application property values are loaded first and you can override those values here.

The following is an example of property file content to override a cache timeout:

```
#=============================================
# Dependencies
#=============================================
product.dependencies=redcell

#=============================================
# Redcell Assurance Overrides
#=============================================
# set event template cache timeout to 1 minute
redcell.assurance.batch.processing.event.template.cache.expiration=60000
```

If you have more than one product dependency, add another product.dependency property.

CAUTION: If any of the dependency directory names (for example, `owareapps\redcell`) do not exist, then the application does *not* load the override file.

Consult the comments in the properties files you are overriding for further information about specific properties.

Properties Files

The following files contain properties that might be modified by the application's users and administrators. Best practice is to override any properties you want to change in these files. See Overriding Properties for instructions.

NOTE: Client installations where no DNS exists (for example across a VPN) require you to replace your application server's local host name with its IP address in the application's properties files in `oware\lib` and `oware\medserver\lib`.

Best practice is to backup these files, or those that override them. All paths are given relative to the installation directory. Note that this is not an exhaustive list. Some properties files are unique to addons or third-party products, and are not included.

oware\addons\ezmediation\lib

allmsgs_en_US.properties

jaxb-xjc-1.0-ea.jar

owclasspath.properties

owezcli.properties

owezexports.jar

owezmediation.jar

oware\addons\transactionengine\lib

temsgusenglish.properties

transengine.properties

oware\addons\workflow\lib

workflowapp.properties

workflowbase.properties

workflowdemo.properties

workflowlogicon.properties

oware\addons\workflow\resourcebundles

workflowmsg_en_US.properties

oware\examples\ClusterMonitor\Cluster

Cluster.properties

oware\lib

Oware.properties

allmsgs_en_US.properties

debugger.properties

<username>_formsettings.properties

owappserver.properties

owappserverstartup.proper

owcorba.properties

owdatabase.properties

oweditorsettings.properti

owfc.properties

owfc_web.properties

owframework.properties

owimportjdbctables.properties

owjdbcstorage.properties

owjms.properties

owlicense.properties

owlogicworkspace.properties

owmediation.properties

owmediationlisteners.prop

owmisc.properties

owpartition.properties

owsce.properties

owsecurity.properties

owstoredprocedures.properties

owwebservices.properties

services.properties

oware\medserver\lib

Oware.properties

owappserverstartup.proper

owexternalapp.properties

owinternal.properties

owlicense.properties

owmediation.properties

owmediationlisteners.prop

owmisc.properties

owsecurity.properties

owareapps\assure\lib

asmsgs_en_US.properties

assure.properties

assurecompmgr.properties

sla.properties

owareapps\redcell\lib

owuserappserver.properties

owuserclasspath.properties

rccompmgr.properties

rcmsgsusenglish.properties

redcell.properties

28

Functional Permissions

Functions

This application ships with a default set of Functions and Actions (see Default Actions)—tasks that users and operators are expected to perform, and the authorizing permissions. See *Functional Permissions* on page 307 for more background information about these. You must typically restart the application client (re-login) for changes in these permissions to take effect. By default, new groups have permissions for no functions.

NOTE: In setting functional permissions, if a client loses connection to the server a Java BOM Error appears. This typically occurs if you leave the application idle for about 15 minutes. This is a benign error that you may safely ignore.

The following table lists and explains the most significant default set of functions, and explains them when not self-evident. Typically, the action *Execute* lets you see the manager, *Read* lets you query, *Add* lets you create a new element, *Write* lets you update an existing element, and *Delete* lets you remove an element.

Functions (available actions)	Description / Applied on…
Alarm Management	Not used
Alarm Resync with Topology	Topology alarm state view may go out of sync with the open alarms in the system. Enabling alarm resync brings topology in sync with assure alarm states
Alarm Window Actions	Not used
Change Control Settings	Configures users' access to the Settings > Configuration > Control Settings dialog, General Tab
Configure Audit Access 0 and Access 1 read permissions	In the audit manager, different types of audit records can have different levels of security associated with them. This setting lets you hide more secure audit actions from the average user. Currently all actions are specified at access level of 1. Soon the user management and password policy actions will be at access level 0
Configure Audit Trail (read, delete, execute)	Audit Trail Manager
Configure Authentication (add, read, write, delete, execute)	Configures Authentication Manager under Settings > Permissions.

Functions (available actions)	Description / Applied on…
Configure Classes (add, read, write, delete, execute)	Class Manager access
Configure Contacts (add, read, write, delete, execute)	Contact Manager access
Configure DAPs	Database Aging Policies access
Configure Devices	This controls the ability to do discrete configuration. Read lets users get values from the equipment (without read they do not even see the entry in the tree) Write lets users change those values
Configure Equipment Group (add, read, write, delete, execute)	Equipment Group Manager access
Configure Events	Configures Event Template Manager access
Configure Filters (execute)	Applies to all managers (except Link). Execute – this action enables the gear button (access to Filter Manager) on the filter
Configure Locations (add, read, write, delete, execute)	Location Manager access
Configure Notifications	Configures Notification Mapping Manager access
Configure Schedule Manage (add, read, write, delete, execute)	Schedule Manager under network services->system services
Configure Users	Configures User Manager access
Configure Vendors (add, read, write, delete, execute)	Vendor Manager access
Cut-Thru (Direct Access) to any host (execute)	Enables the *Telnet* and *HTTP* buttons on the Discovery Results panel of the Resource Discovery Wizard
Device Discovery (add, read, write, delete, execute)	Device Discovery Scheduler write – enables the *Parameters and Schedule* button
Device Discovery (execute)	Device Discovery Wizard access
Device Resync (add, read, write, delete, execute)	Device Resync Scheduler write – enables the *Parameters and Schedule* button
Event Details	Configures access to the event details panel
Event Inventory	Configures access to the event inventory
Generate Printer Test Data	Execute permission adds an item to the printer manager action menu to generate test data for printer reports that require long-term polling

Functions (available actions)	**Description / Applied on…**
Inventory Configuration	(Execute) allows access to the Inventory Config Manager under Settings > Configuration > Inventory Config. This manager configures the Custom fields for various Inventory Types
Inventory Filters	Manages access to filtering function in inventory managers
Inventory Historical Reports	Manages access to historical reports about inventory
Inventory Layouts	Manages access to editing layouts
Inventory Printers	Manages access to printer manager
Inventory Report Manager (write, delete, execute)	Report Manager delete – enables the *Delete* button write – enables the *Save* button
Inventory Report Template Manager	Manages access to report template manager
Inventory Views	Manages access to inventory views in managers, configuring columns and so on.
Launch Device Heartbeat	Execute permission allows a user to start heartbeat polling.
Manage Permissions (add, read, write, delete, execute)	Access for all menu items under Permissions
Northbound System Manager	Enable/Disable the access to the *Northbound Manager* menu item/window Used only for seeding Northbound Manger and Editor's context sensitive menu items, drop-in buttons, filters. See the details in the following tables
Execute	Users can see/access the *Northbound Manager* menu items/windows
Read	Enables filters and help in *Northbound Manager* and *Editor* screens
SecurityAlarm	Enables/Disables displaying Security Alarms in *Event History* view.
No Permissions	Disables display of Security Alarms in Event History view and in Fault Reports.
Execute	No Effect
Read	Enables/Disables displaying Security Alarms in *Event History* view.
Add	No Effect
Write	No Effect
Delete	No Effect
Threshold Policy	Manages access to setting thresholds.
Topology (add, delete, execute)	Delete & add – if both are present the items can be moved on the map

The optional Report Framework (Inventory Report Manager, Inventory Report Template Manager, and Inventory Historical Reports) adds more functional permissions when installed. These control the managers and the reports generated through that framework.

Default Actions

This application ships with a default set of actions. In varying combinations, these actions are associated with permissions, and determine what a user can and cannot do within the application.

Action	Default Behavior
execute	This action determines whether a particular manager form can launch.
add	This action enables the *New* button on the manager panel. If this action is not assigned then the *New* button is hidden.
read	This action renames the *Edit* button to *View (*View opens the editor in read only mode). That is, the *Ok* button is disabled. If neither read nor edit action is assigned, then this button is hidden
write	This action shows the *Edit* button on the manager, which when clicked opens the editor would open in edit mode.
delete	This action enables the *Delete* button on the manager panel. If this action is not assigned the *Delete* button does not appear.

29

Database Management

Introducing Databases

This chapter discusses database management procedures. This discussion includes installation with the embedded MySQL database.

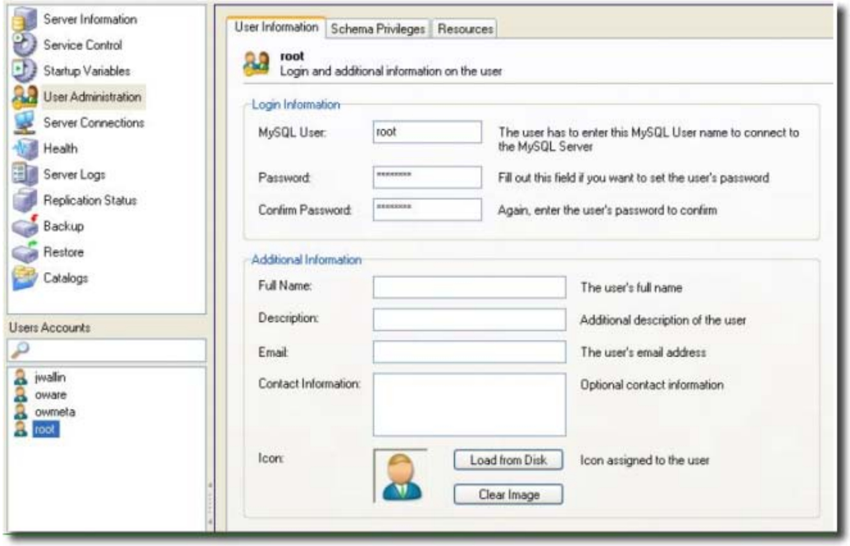
In addition to correctly sizing your database, best practice is to develop a plan to regularly back up the database, including steps to verify this backup with recovery. The frequency of backups depends upon your environment, but you should back up often enough to minimize data loss.

Administration Basics

You can download the MySQL administrator from `http://dev.mysql.com/downloads/administrator/1.0.html`, you can get its manual at `http://dev.mysql.com/doc/administrator/en/index.html`. This optional tool has a graphical user interface, and provides an overview of the MySQL settings. It displays performance indicators graphically, making it easier to determine and tune server settings.

Start this tool to view databases. When you install the embedded database, installation creates two databases: `owmetadb` and `owbusdb`. The installation also creates a `root` and `<O/S user>` login (users *oware* and *owmeta* are created, too).

Figure 29-1. MySQL Users



root
Login and additional information on the user

Login Information

MySQL User: root — The user has to enter this MySQL User name to connect to the MySQL Server

Password: ******** — Fill out this field if you want to set the user's password

Confirm Password: ******** — Again, enter the user's password to confirm

Additional Information

Full Name: — The user's full name

Description: — Additional description of the user

Email: — The user's email address

Contact Information: — Optional contact information

Icon: — Icon assigned to the user

The default password for database access is *dorado*. Read the tool's instructions for specifics about how to use it.

Database Timeout

When managing large networks or equipment with many interfaces, you may have to increase a timeout property: the `com.dorado.bom.lock_timeout` property in `owareapps\installprops\lib\installed.properties` (originally in `owdatabase.properties`).

Copy that property into `installed.properties`, then increase this setting based on the equipment managed. Generally, you should set this value to the maximum number of interfaces you expect your network elements to have. For example, if the element is expected to have 500 logical interfaces then the timeout value should be set to 500.

NOTE: The minimum recommended timeout value is 60 seconds.

Embedded Database Sizing

The initially installed Embedded Database is a relatively small instance—possibly too small for your application. This is important to note because errors occur when you reach the size limit of the database. Therefore, after installing, you may want to resize the Embedded Databases to fit your application. See Modifying the MySQL File Systems for instructions about modifying an existing, installed system, and Embedded Database Administration Utilities on page 358 for information about the tools to do this.

Modifying the MySQL File Systems

If you have upgraded from older operating systems (Windows® 3.1, for example),you may still have a FAT file system that limits your database size or expansion beyond 2GB. The database is a file as far as the operating system is concerned, and FAT limits file size. There is also a 4GB limit on early versions of NTFS that may linger because of upgrades.

To change the installed database sizes, you must edit the configuration file:

- Windows: `%SystemRoot%\my.ini`

The following line controls maximum database size (at end):

```
innodb_data_file_path =
d:/work/oware3rd/mysql/4_0_13/ibdata/ibdata1:600M:autoextend:max:2000M
```

To recreate database after modifying config file, use the following command from the application server:

```
        loaddb -q -d -m
```

Syntax details:

```
innodb_data_file_path =
pathtodatafile:sizespecification;pathtodatafile:sizespecification;...
```

```
innodb_data_file_path = ...
;pathtodatafile:sizespecification[:autoextend[:max:sizespecification]]
```

If you specify the last datafile with the *autoextend* option, InnoDB will extend the last datafile if it runs out of free space in the tablespace. The increment is 8 MB at a time. An example:

```
                innodb_data_file_path = /ibdata/ibdata1:100M:autoextend
```

This instructs InnoDB to create just a single datafile whose initial size is 100 MB and which is extended in 8 MB blocks when space runs out.

If the disk becomes full you may want to add another datafile to another disk, for example. Then you must look at the size of `ibdata1', round the size downward to the closest multiple of 1024 * 1024 bytes (= 1 MB), and specify the rounded size of `ibdata1' explicitly in `innodb_data_file_path`. After that you can add another datafile:

```
innodb_data_file_path =
/ibdata/ibdata1:988M;/disk2/ibdata2:50M:autoextend
```

Be cautious on filesystems where the maximum file-size is 2 GB. InnoDB is not aware of the operating system's maximum file-size. On those filesystems you might want to specify the max size for the datafile:

```
innodb_data_file_path = /ibdata/ibdata1:100M:autoextend:max:2000M
```

Some additional caveats:

- You must use foreslashes (/) instead of backslashes (\) when you specify the path.
- The subdirectory iblogs must be used by MySQL exclusively
- Make sure you enough disk space available on the data path specified

- You can add as many entries as you like. However, you can use `autoextend` only in the last entry.
- The name of filepath must be valid on the filesystems. However, you must always have your leaf directory in the path as ibdata.

Database Backup / Restoration

The recommended procedures for database backup and restoration for the embedded database follows. Best practice is to develop backup plans using these procedures for the sake of database reliability.

For MySQL (embedded) databases, use this database's native backup/restore utilities to backup the `owbusdb` database. Refer to the manual available at www.mysql.com for instructions about backup and restoration.

Developer Backup

Licensed application developers must do additional database backup to back up `owmetadb` as well as `owbusdb` databases. To (offline) backup all applications and development metadatabases, use the supplied scripts:

```
dbbackup
dbrestore
```

These automate backup and restore of all databases. To run these scripts, type `oware` at a command line (press Enter), then type the script name at the command line. For more specifics, see Embedded Database Administration Utilities on page 358.

Embedded Database Administration Utilities

The Embedded Database-provided utilities to administer this application's databases.

Download the MySQL documents from www.mysql.com for tips about performance tuning your hardware for the embedded database.

You can determine the version installed with your software by the directory structure. For example: `oware3rd\mysql\4_0_13.`

You can use the following utility scripts with the Embedded Database (use the `-h` parameter for full usage):

- **dbbackup—**This backs up a database.
- **dbrestore—**This restores a previously backed-up database.
- **loaddb**—This re-creates an empty database.

30

The Application Server

Introducing the Application Server

The Application Server is the central engine for all components on both server and client systems, relieving clients of significant programming infrastructure overhead. The Application Server is a set of Enterprise JavaBeans (EJBs) embedded within EJBs provide remote access from clients to other components—the Virtual Rule Machine (VRM), Mediation Services, the Event Channel, and other services. For example, a client application that needs to check information in the classes database does not access application databases directly. Instead, the Application Server's EJB mediates any insertions, queries, updates, or deletes.

Starting the Server

You must start Application Server so you can use most of the Execution Center (OEC) components.

NOTE: You can ensure command lines referred to in the following steps have set your command shell environment correctly with the `oware` command (Windows). Although these commands are optional, they are recommended.

To start application server, from the command line enter `startappserver`. Once an Application Server starts, the name of the log file appears in its shell. To see its progress, use this command:

```
tail -f <logname>
```

Logging

When you start application server as a service any console output writes to a log file in `$OWARE_ROOT/jboss_<versionnumber>/server/oware/log` (for mediation server, see `$OWARE_ROOT/jboss_<version number>/server/owaremed1/log`). If you want to see the console output as it is generated, then run `startappserver` at a command line rather than having it start as a server.

Command Line Options

The following is a transcript of this command line:

```
startappserver -?
```

Read this to understand the options available when starting application server, particularly for clustering. See

```
Usage: startappserver [-c CONFIG_SERVER] [-p PARTITION_NAME]  [-m
MULTICAST_IP] [-n NODE_NUM] [-s]


  NOTE: When clustering with multiple servers CONFIG_SERVER,
PARTITION_NAME, MULTICAST_IP, and NODE_NUM must be the same for all
instances.


The [PARTITION_NAME] value is a unique name used for clustering and
client discovery of the server. If you do not provide the PARTITION_NAME,
the application defaults to the entry in  owpartition.properties. If you
provide a PARTITION_NAME, the application uses that {PARTITION_NAME}.


The [CONFIG_SERVER] value is the assigned First Primary server assigned
for the cluster.  This server must be up for any other server to join.


The [MULTICAST_IP] value is the MultiCast IP the partition uses to
communicate.

NOTE: for clustering with multiple servers, this must be the same for all
instances. If not supplied one, the application dynamically creates one
using the local IP address for seeding.

For example 192.168.8.1 would be assigned 239.0.8.1 as the default
multicast address.

The valid range for multicast addresses is 224.0.0.0 through
239.255.255.255

Avoid addresses 224.0.0.0 through 225.0.0.0.  Network equipment uses
these heavily.

This also means that you may only run the default instance of EITHER the
appserver or medserver.
```

The optional [NODE_NUM] value is an integer (1-5) used to modify the three ports bound by the server. You need to choose unique NODE_NUM values for both appserver and medserver instances.

The -s option is used when the application server is started by the process monitor, and prevents the application server from shutting when a user logs off the system under Windows NT.

Properties Best Practices

Best practice is to configure application and mediation servers by overriding properties that configure them. Do this in the files `owareapps\installinfo`. You can read the properties files overridden in `oware\lib` and in `owareapps\ <application name>\lib` for details about what can change. If you put a property in a file with a `properties` extension in `owareapps\installinfo`, that value overrides the defaults.

NOTE: For better performance when overriding, use the IP address rather than *localhost* for the database server name.

Index