iView^2 Getting Started Guide

Version 5.7 Build 0004

Blank page

Table of contents

Introduction 1
Purpose 1
Installation Requirements 1
Main Features 2
Graphic User Interface 2
Getting Started 4
User Login 4
User Logout 4
User Authorization 4
Network Menu Items 5
Add Device 5
Perform Device Search 7
Perform Device Save 7
Add All eWorx 300 Devices 10
Add All Advantech 5000 Devices 15
Remove Device 20
Search Device 23
Edit Device 25
Edit Description 26
Edit PROM Version 28
Edit IP Address 29
Edit MIB Definitions 32
Edit Traps 42
Edit Get/Set Community 43
Edit Users 45
Add Segment 46
Remove Segment 49
Edit Segment 52
Import Device List 55
Import Device List File Format 56
Import Device List Column Definitions 56
Export Device List 58
Tools Menu Items 60
Inventory Report 60
Inventory Report Controls Icons 61
Export Inventory Report 62
Search Inventory Report 63
PS Inventory Report 64
PS Inventory Report Controls Icons 65
Task Manager 66
Task Manager Control Icons 67
Export Report Display 68
Print Report Display 69
Task Manager - Report Display 70

Task Manager – Task Details Report Display 71
Cancel Task 73
Cancel Task Item 73
Create PROM Update Task 74
Trap Manager 79
Trap Forwarding 80
Trap Management Reporting 82
Display Trap Details: 83
Paging Through Traps: 84
Archive Traps: 84
Setting Alerts Per Page: 85
Trap Search: 86
Update Inventory 87
Display DB Config 88
Database Check 89
Refresh Device Tree 91
ZTP Configuration 92
ZTP Configuration Control Icons 94
Administration Menu Items 95
Add iView^2 User 95
Edit Current iView^2 User 96
Edit iView^2 Users 97
System Settings 98
User Session Timeout 99
Device Naming Convention 100
LDAP Settings 101
Overview: 101
Configuration: 102
Use Custom Format: 104
LDAP Matching Rules: 104
Database Backup 105
Database Restore 106
Update DB Config 108
Appendix A 109
Task Scheduling Options 109
Scheduling Guidelines 111
Scheduling Options Screenshots 112
Using the Chassis View 117
Accessing the SNMP Module 119
iMediaChassis Power Supply Identification Information 120
Appendix B 122
B+B SmartWorx Supported Modules 122
eWorx Supported Modules 124
Advantech Supported Modules 125

Introduction

Purpose

iView^2 is the Network Management System (NMS) for SNMP-based configuration and management of B&B Electronics, chassis and module products. The purpose of this document is to identify the main features of the iView^2 web-based application.

Installation Requirements

The following requirements must be met before iView^2 can be installed:

1) The Java J2SE runtime environment version 1.7 or greater must be installed
2) The Apache\Tomcat 6 or greater http server and servlet container must be installed
3) The MySQL 5.1 or greater relational database management system (rdms) must be installed

NOTES:
All the requirement applications can be found through the iView^2 installation release.

iView^2 is a Java-based solution and requires a different web container environment than Microsoft Internet Information Server (IIS). We will be recommending the Apache/Tomcat HTTP and Servlet Container. Apache/Tomcat 6 was used during development and testing.

iView^2 uses a database for all configuration information and report data. We will be recommending the MySQL database system. MySQL 5.1 was used during development and testing.

iView^2 is an Internet-based application so the main user GUI is through a web browser. The following browsers are supported:

MS Internet Explorer v10 or greater
Mozilla Firefox v15.0 or greater
Google Chrome v35 or greater

Main Features

Graphic User Interface

The iView^2 application provides a similar look and feel to the iView^2 version 1.8.x desktop application. There are 3 main sections to the iView^2 Default View: Header Section, Network Segment List Section, and Content Area Section.

Header Section
The header consists of a top banner section and a menu section.

Figure 1.1 - iView^2 Header Area

Network Segment List Section
The Network Segment List (NSL) section is located on the left side of the application just below the Header Section. The NSL is always available. The NSL can be minimized by using the mouse to click the arrow image on the top left side of the chassis tree control. As can be seen in figure 1.2, a new installation will have an unpopulated display.

There are 2 options for populating the NSL:

1) The user can manually add individual devices.
2) The user can create a list of devices and import the list into iView^2.

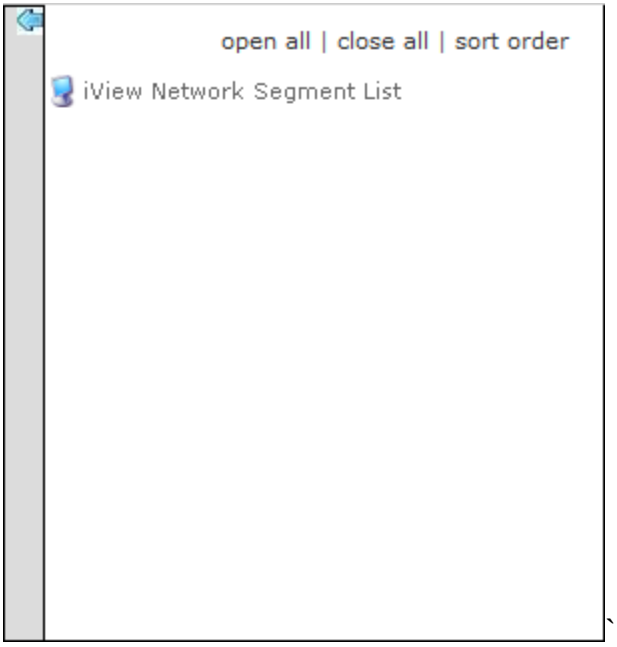


Figure 1.2 - iView^2 Network Segment List Section

Content Section

The content section is located to the right of the Network Segment List Section. This is the section of the application where most of the user interaction will be performed. As shown in figure 1.3, the default display in the content area is an iView^2 splash panel.

Figure 1.3 - iView^2 Default Display for Content Section

Getting Started

User Login

Access to iView^2 is controlled by a User Authentication process. By default there is a single login account created during installation with a User Name of “admin” and a Password of “password”.

User Logout

When a user has completed their work with iView^2 they are encouraged to logout of the application using the “Logout” selection located in right-hand side the header of the main page as shown in Figure 1.4.

Figure 1.4 – User Logout Command

User Authorization

iView^2 supports 3 different levels of user access: “User”, “Operator”, and “Administrator”.

● “User” has the minimal level of access to the system consisting of read-only access to the network components.
● “Operator” has the next level of access to the system consisting of read/write access to the network components.
● “Administrator” has the highest level of access to the system consisting of read/write access to the network components and the ability to add users and change user passwords.

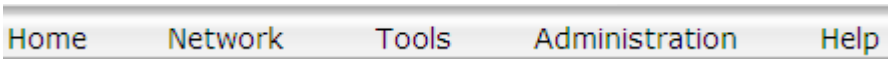


Figure 1.5 – Administrator Menu

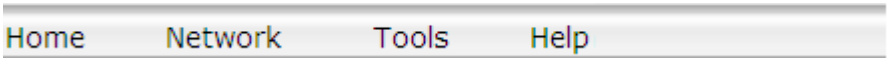


Figure 1.6 – Operator Menu

Figure 1.7 – User Menu

Network Menu Items

Add Device

The “Add Device” menu selection located in the “Network” menu commands controls the ability to add new devices. Devices are associated with the Segment to organize your network device selections. Adding a new device is a 2-step process: 1) Search for the device using the IP Address or DNS and 2) Inserting the device information into the iView^2 database.

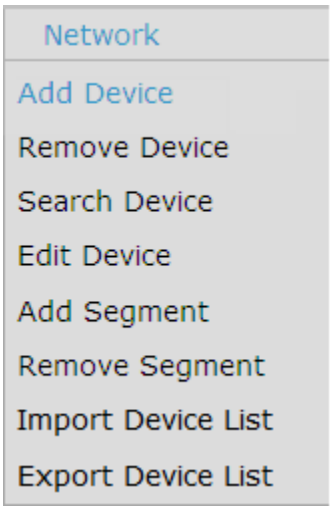


Figure 2.1 – Add Device Menu Command

Selecting "**Add Device**" from the menu will display the "Add Device" dialog box. In the "**Device IP Address:**" input area of the "Add Device" dialog box, you can enter the IP Address. Duplicate IP Addresses are not allowed. Using the "Tab" key to move to the "**Device Domain Name:**" input area or clicking on the "Device Domain Name" input area will allow the user to enter a fully qualified domain name instead of an IP Address. The "Device Domain Name" has the following formatting restrictions:

1) Valid characters in the subdomain are "a-z A-Z 0-9 - (- = dash)
2) Subdomains are limited to 63 character
3) Subdomains must be separated by a period
4) The Device Domain Name cannot exceed 255 characters

The "**Device Mfg Type**" is used to control the type of search algorithm used by iView[2] to detect devices. There are 3 selection types: "B&B Devices", "eWorx 300 Devices", "eWorx 500 Devices" ", "Advantech 5000 Devices", "Advantech 7000 Devices" , and "Advantech Sabre Devices". The "B&B Devices" include "IMC", "B&B Electronics", and "B&B SmartWorX" brands. The "eWorx 300 Devices" include the eWorx 3xx product line of switches. The "eWorx 500 Devices" include the eWorx 5xx product line of switches. The "Advantech 5000 Devices" include the EKI-5XXX product line of switches. The "Advantech 7000 Devices" include the EKI-7XXX product line of switches. The "Advantech Sabre Devices" include the CE304 and CE7028 switches.

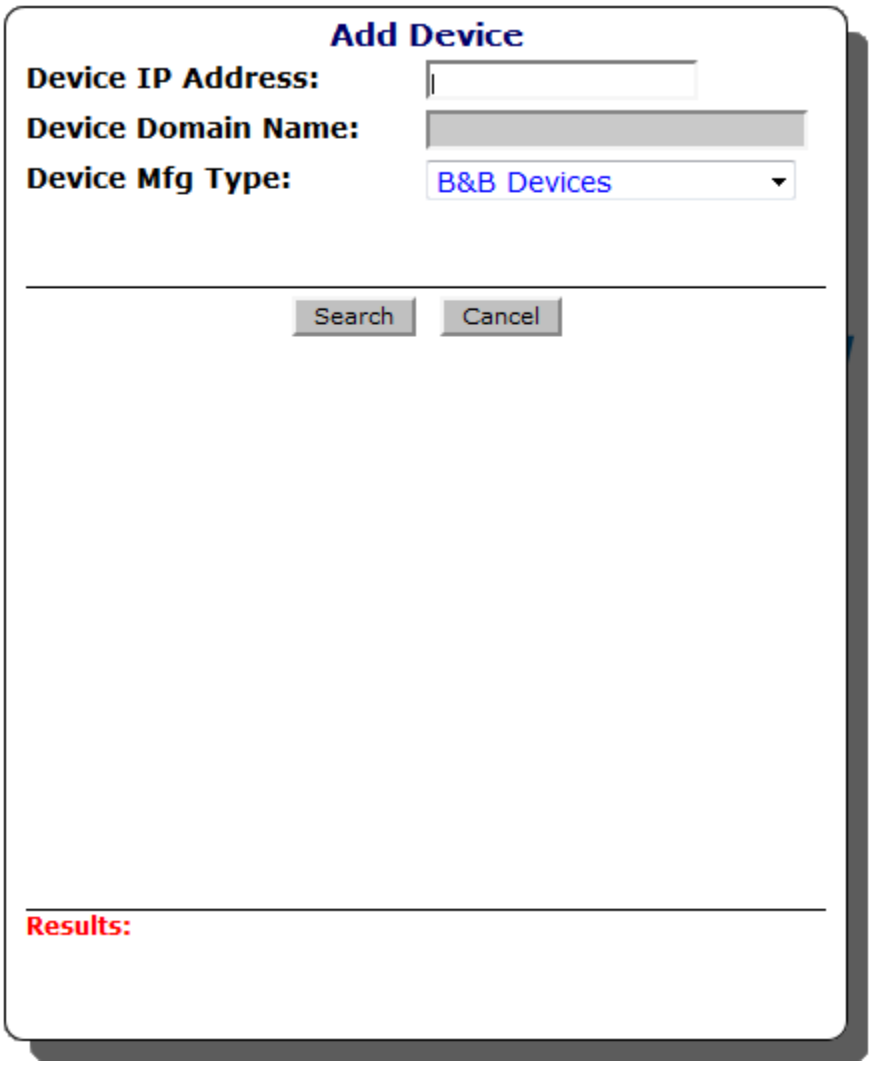


Figure 2.2 – Add Device Dialog Box

Perform Device Search

To perform a device search, enter the IP Address or Domain Name, select the Search algorithm, and press the "Search" command button. The "Search" function will validate the format and contents of the IP Address or Domain Name. A valid IP Address will then be searched for and the results displayed to the user. Refer to figure 2.3a and 2.3b for a successful search result.
NOTE: If the "eWorx 300 Devices", "eWorx 500 Devices", "Advantech 7000 Devices", "Advantech 7000 Devices" ", or "Advantech 7000 Devices" Device Mfg Type is selected, iView^2 will prompt the user for a Read/Get Community name before performing the device search.

Perform Device Save

If the device is found, the results are displayed and the user has the option of saving the device to the iView^2 database or cancelling the operation. To save a device, "Segment" where the device will be located must be selected, and "Get Community" and "Set Community" values must be entered. The "Segment" is a dropdown selection. The user can select the segment they want the new device placed. The values for "Get Community" and "Set Community" are defaulted to "public" and "public". The user can modify the "Description", "Get Community" and "Set Community" items.

Check the "Save as Default Community Strings for New Devices" to change the default values for "Get Community" and "Set Community" to something other than "public" and "public". These values will be stored on a per user basis.

Press the "Save" command button to store your information in the database and update the Network Segment List display.

Press the "Cancel" command button to erase your input and prepare for a new entry.

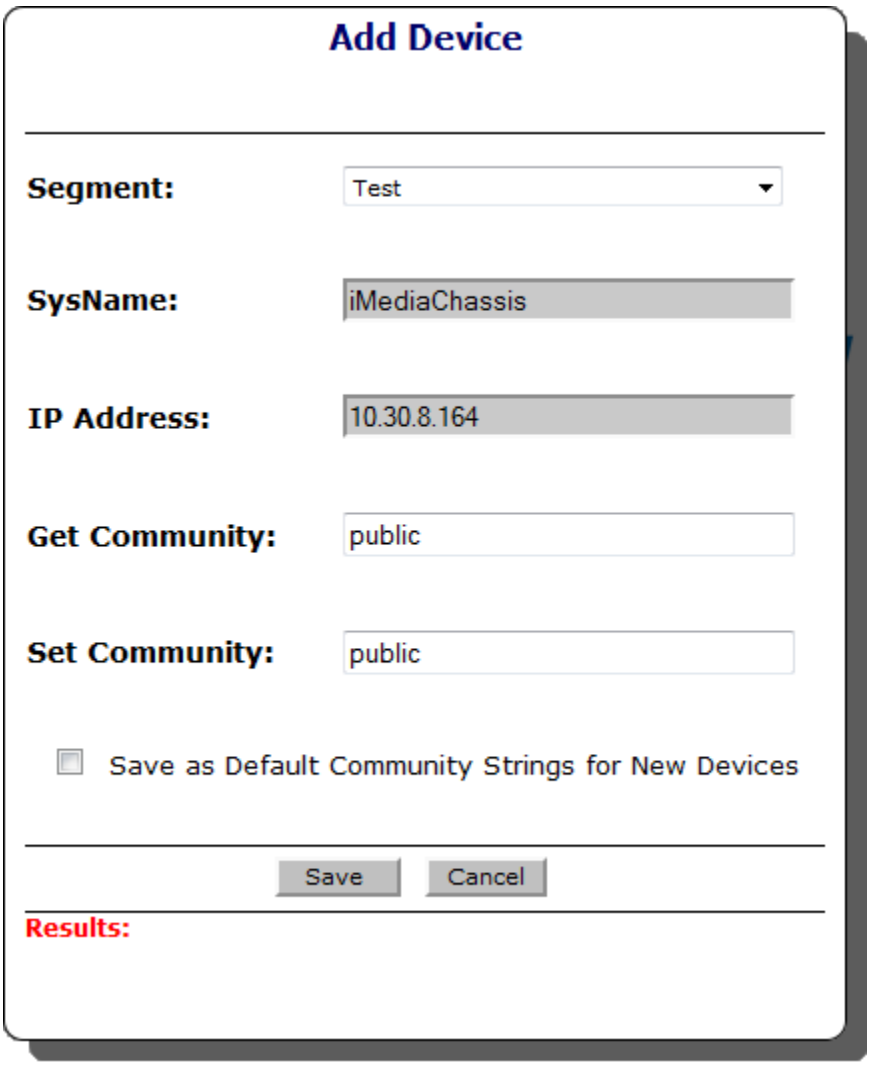


Figure 2.3 – Add Device Display after a successful Search Result

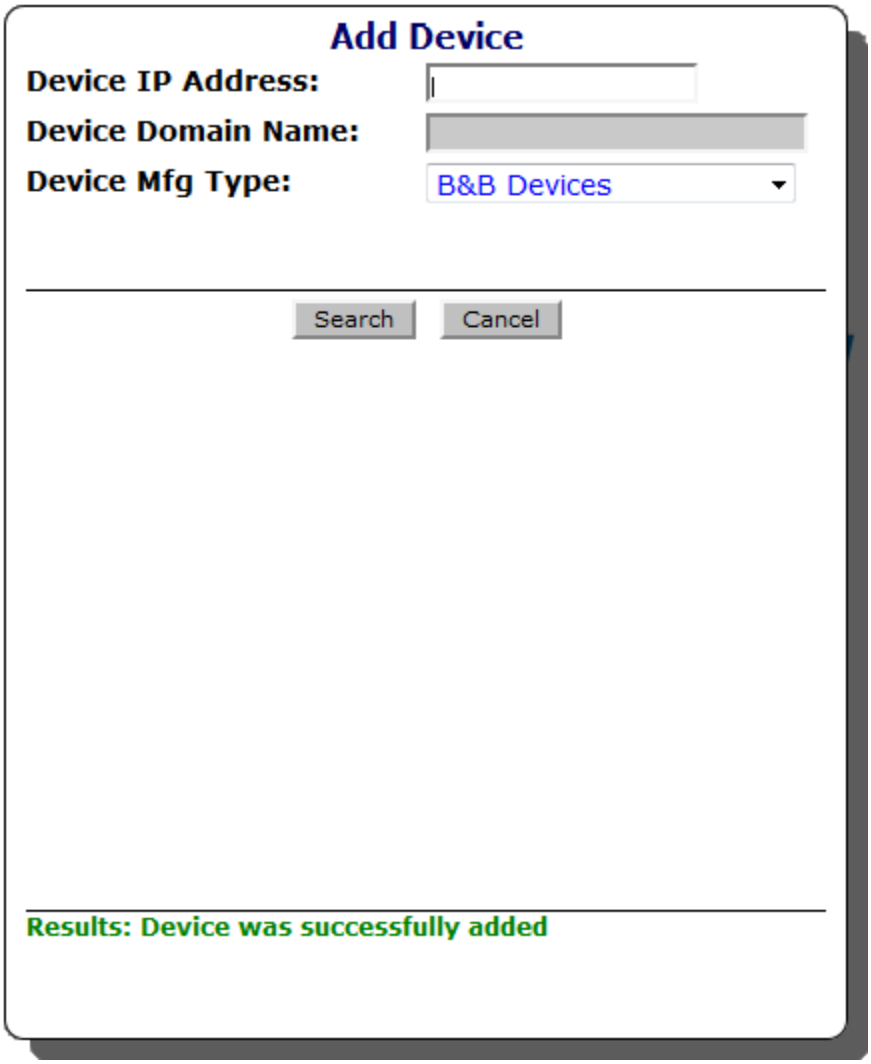


Figure 2.4 – Successful Device Addition Display

Add All eWorx 300 Devices

The "Add Device" menu selection also allows for the discovery and addition of multiple eWorx 300 devices. To access this functionality, selecting "**Add Device**" from the menu will display the "Add Device" dialog box. Leave the "**Device IP Address:**" input area of the "Add Device" dialog box **empty**, select "***eWorx 300 Devices***" from the **Device Mfg Type** dropdown, and select the "**Search**" command button.

Add Device Dialog Box – Search for multiple eWorx 300 Devices.

Any eWorx 300 devices found will display in the Found Devices dialog. Selecting the “Edit” command button will display the “Device Configuration Settings” dialog box.

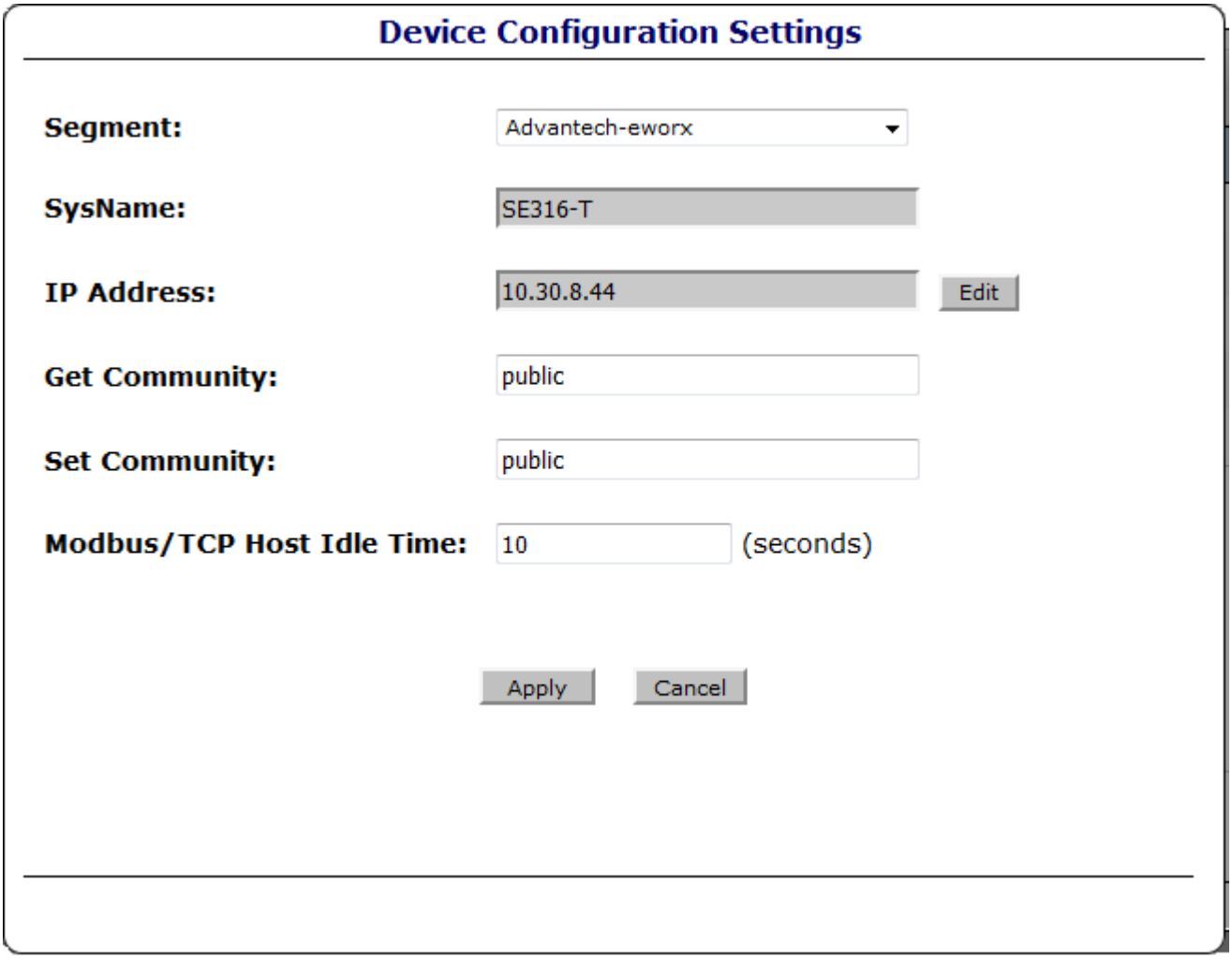
Found Devices (total = 5)

	Device Type	SysName	MAC Address	IP Address	
	SE305-T	SE305-T	00:0b:ab:ec:5a:b8	10.30.8.41	Edit
	SE316-T	SE316-T	00:d0:c9:f5:3b:70	10.30.8.44	Edit
	SEC318-2SFP-T	SEC318-2SFP-T	00:0b:ab:ec:5a:ba	10.30.8.42	Edit
	SEC310-2SFP-T	SEC310-2SFP-T	00:0b:ab:ec:75:3d	10.30.8.48	Edit
	SEG308-T	SEG308-T	00:d0:c9:f5:36:e3	10.30.8.201	Edit

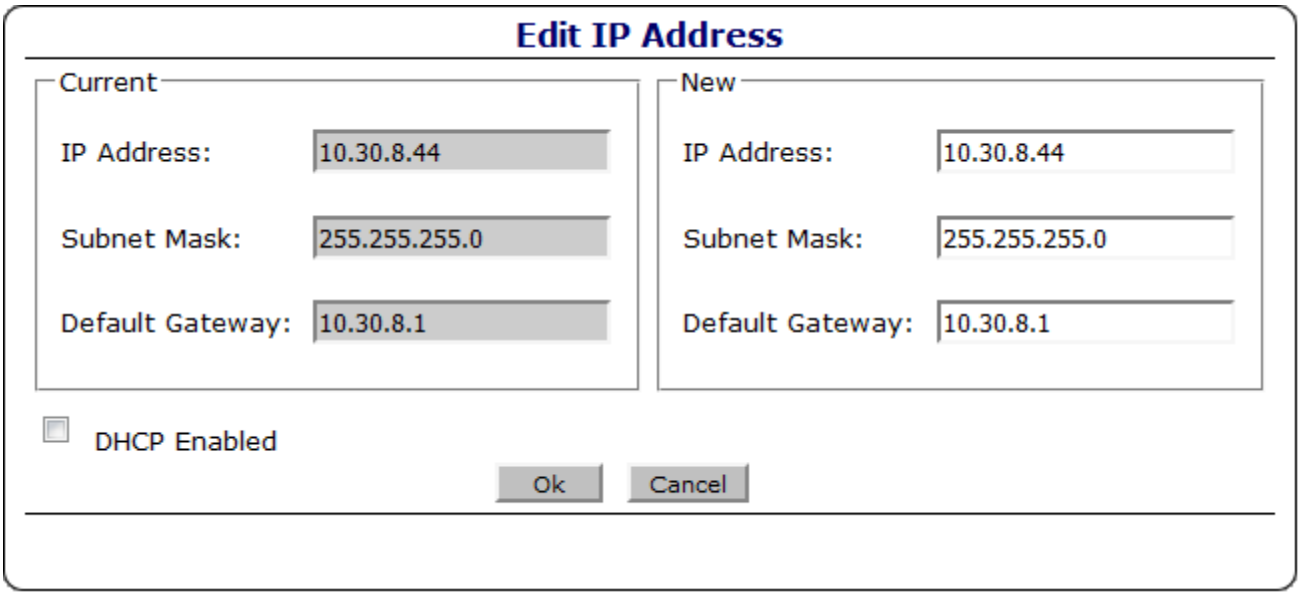
Save Cancel

Results:

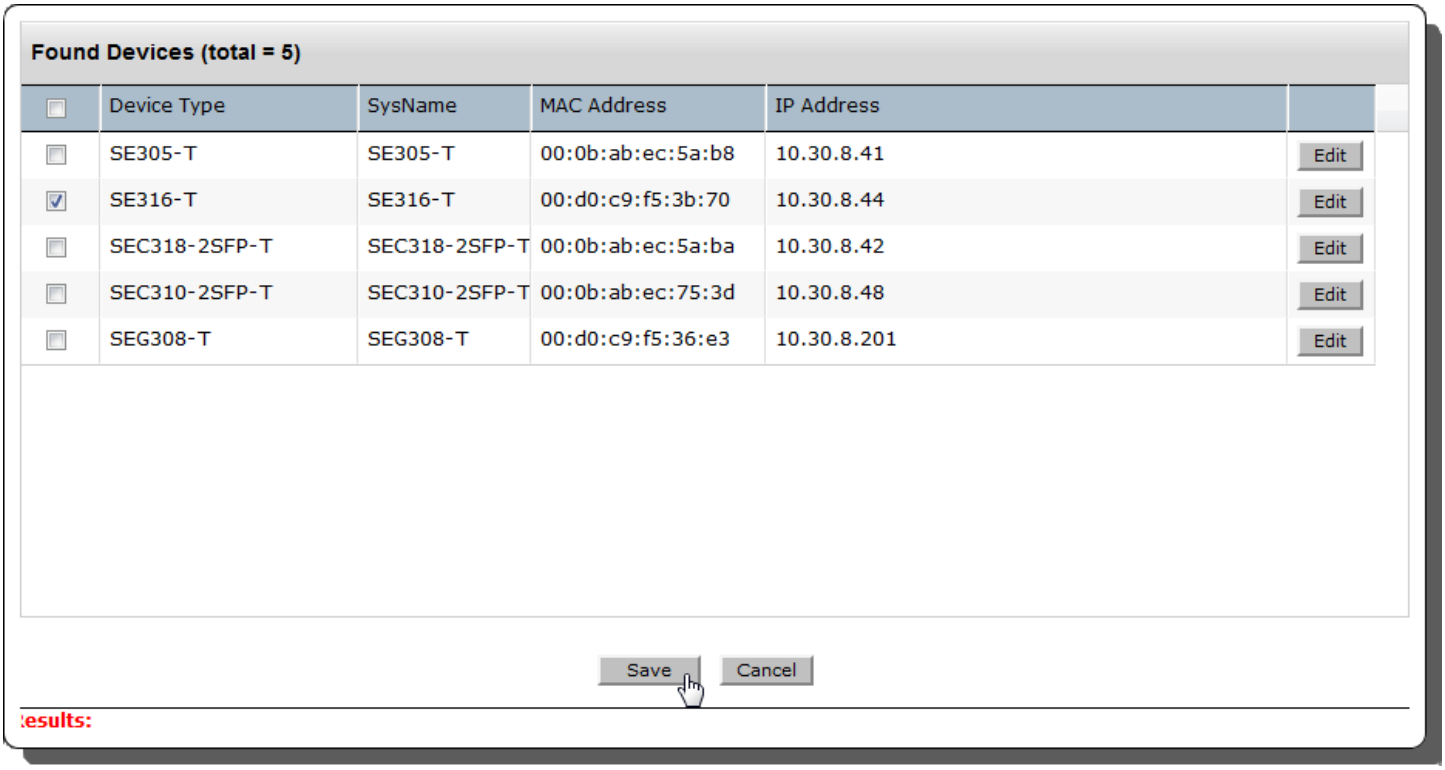
In the “Device Configuration Settings”, the “Segment” where the device should be stored can be set. The “Get Community” and “Set Community” values can be set. The “Modbus/TCP Host Idle Time” can be set. The “IP Address” can be changed by selecting the “Edit” command button which will display the “Edit IP Address” dialog. To save changes press the “Apply” command button. To exit without saving changes press the “Cancel” command button.



The “Edit IP Address” dialog can be used to change the “IP Address”, “Subnet Mask”, “Default Gateway”, and “DHCP Enabled” values. To save any changes press the “Ok” command button. To exit without saving changes press the “Cancel” command button.

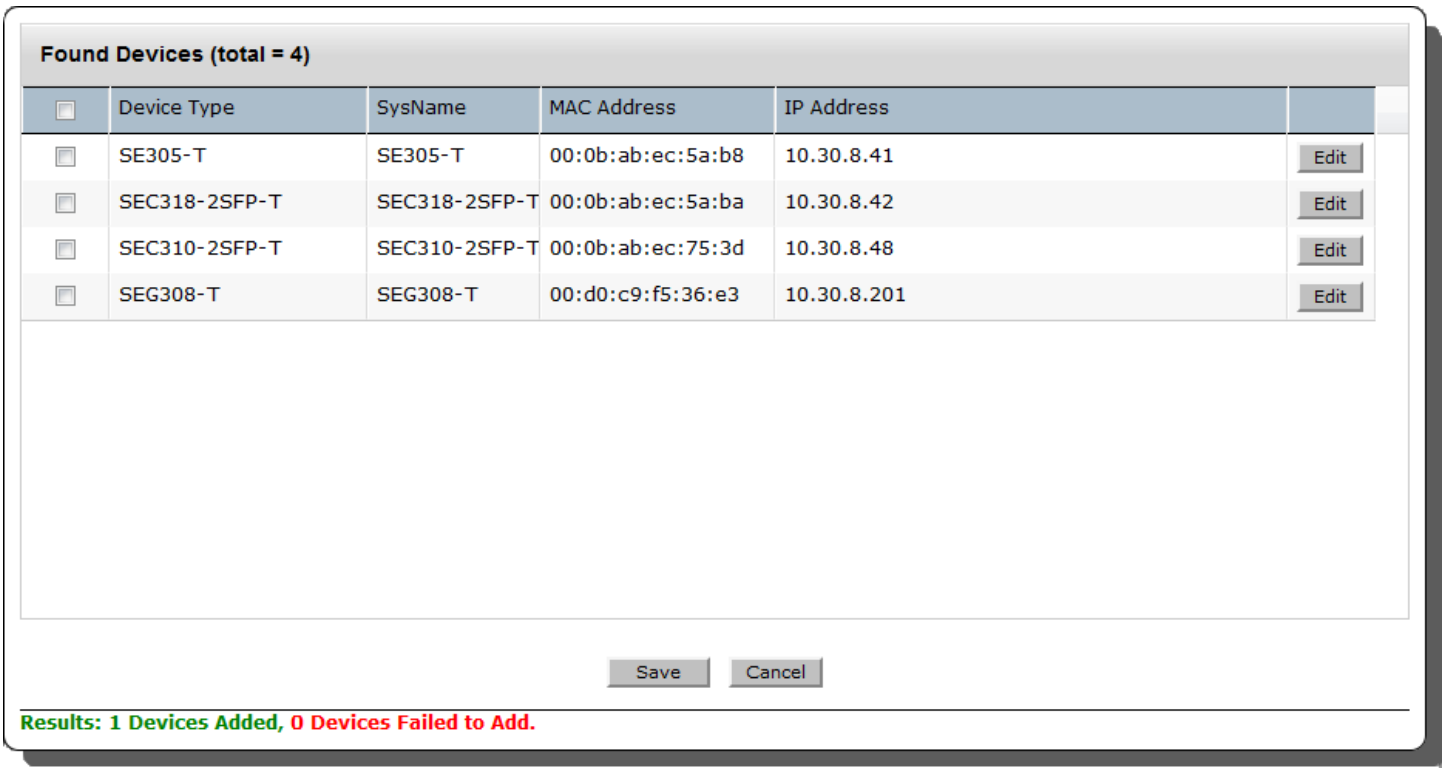


When you are done with the changes, make sure the device(s) you want added have the left side checkbox enabled and press the “Save” command button.



Device selected and ready to add.

When iView[2] is done attempting to add the device(s), a status message will display at the bottom of the display.



Results of adding a device.

Add All Advantech 5000 Devices

The "Add Device" menu selection also allows for the discovery and addition of multiple Advantech 5000 devices.

To access this functionality, selecting "**Add Device**" from the menu will display the "Add Device" dialog box. Leave the "**Device IP Address:**" input area of the "Add Device" dialog box **empty**, select "***Advantech 5000 Devices***" from the **Device Mfg Type** dropdown, and select the "**Search**" command button.

Add Device Dialog Box – Search for multiple Advantech 5000 Devices.

Any Advantech 5000 devices found will display in the Found Devices dialog. Selecting the “Edit” command button will display the “Device Configuration Settings” dialog box.

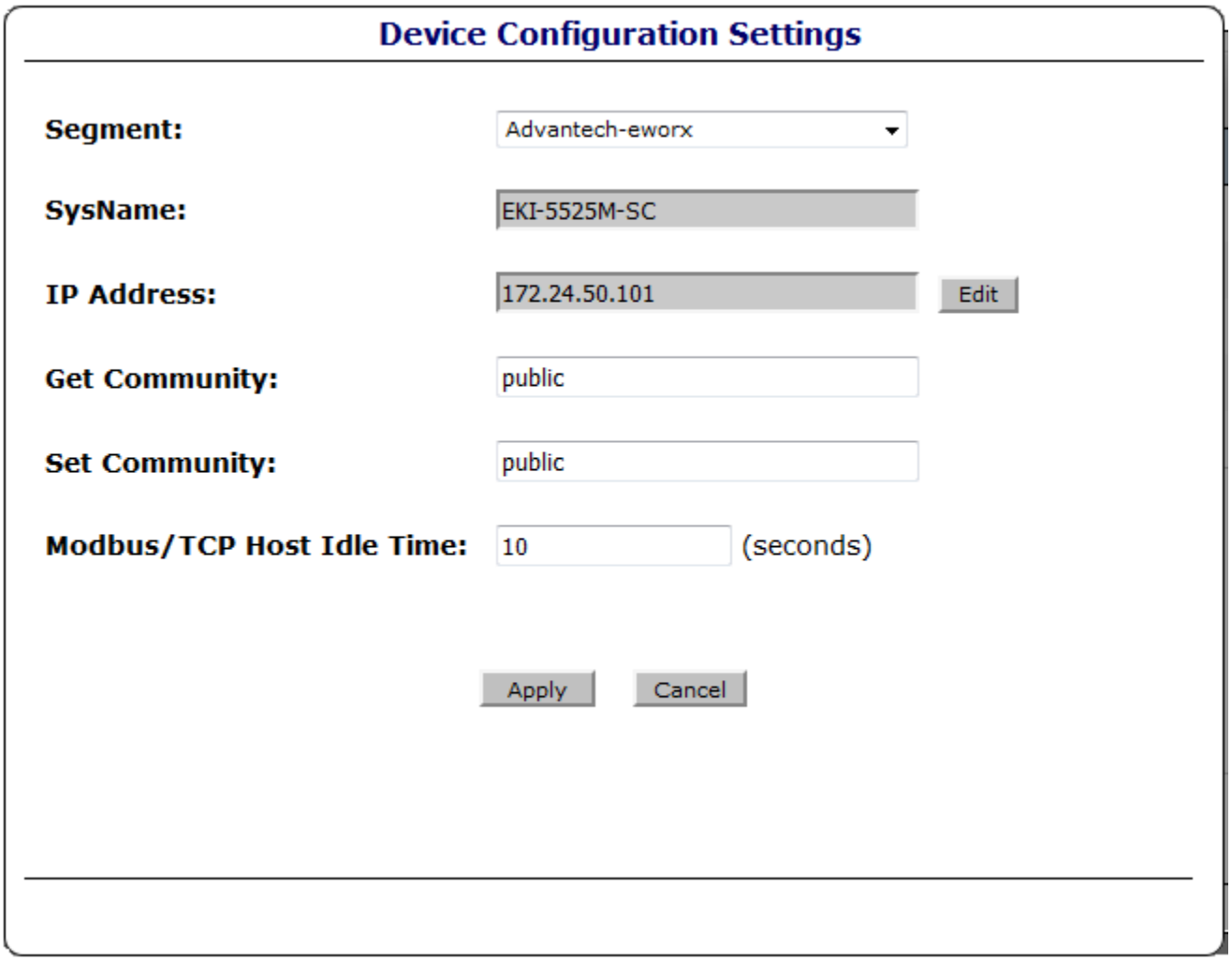
Found Devices (total = 4)

	Device Type	SysName	MAC Address	IP Address	
	EKI-5525M-SC	EKI-5525M-SC	00:d0:c9:f5:43:67	172.24.50.101	Edit
	EKI-5524MM-SC	EKI-5524MM-SC	00:d0:c9:f5:3f:b3	172.24.50.102	Edit
	EKI-5725	EKI-5725	00:d0:c9:f5:1a:94	172.24.50.103	Edit
	EKI-5729F	EKI-5729F	00:d0:c9:f5:1d:ae	172.24.50.105	Edit

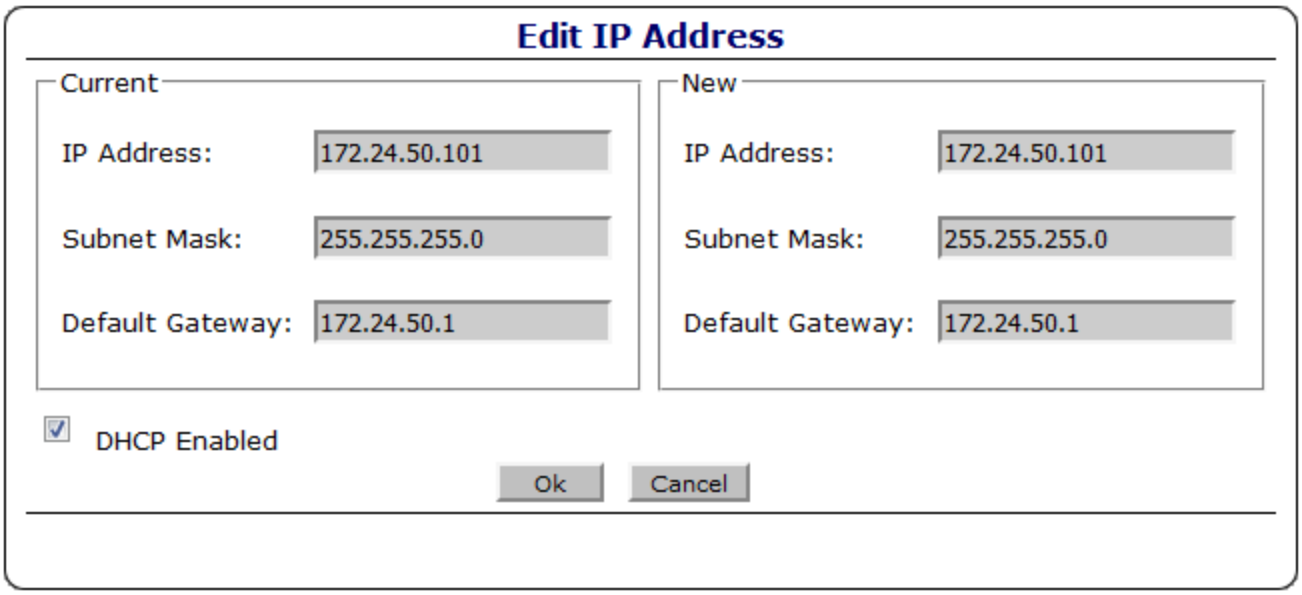
Save Cancel

Results:

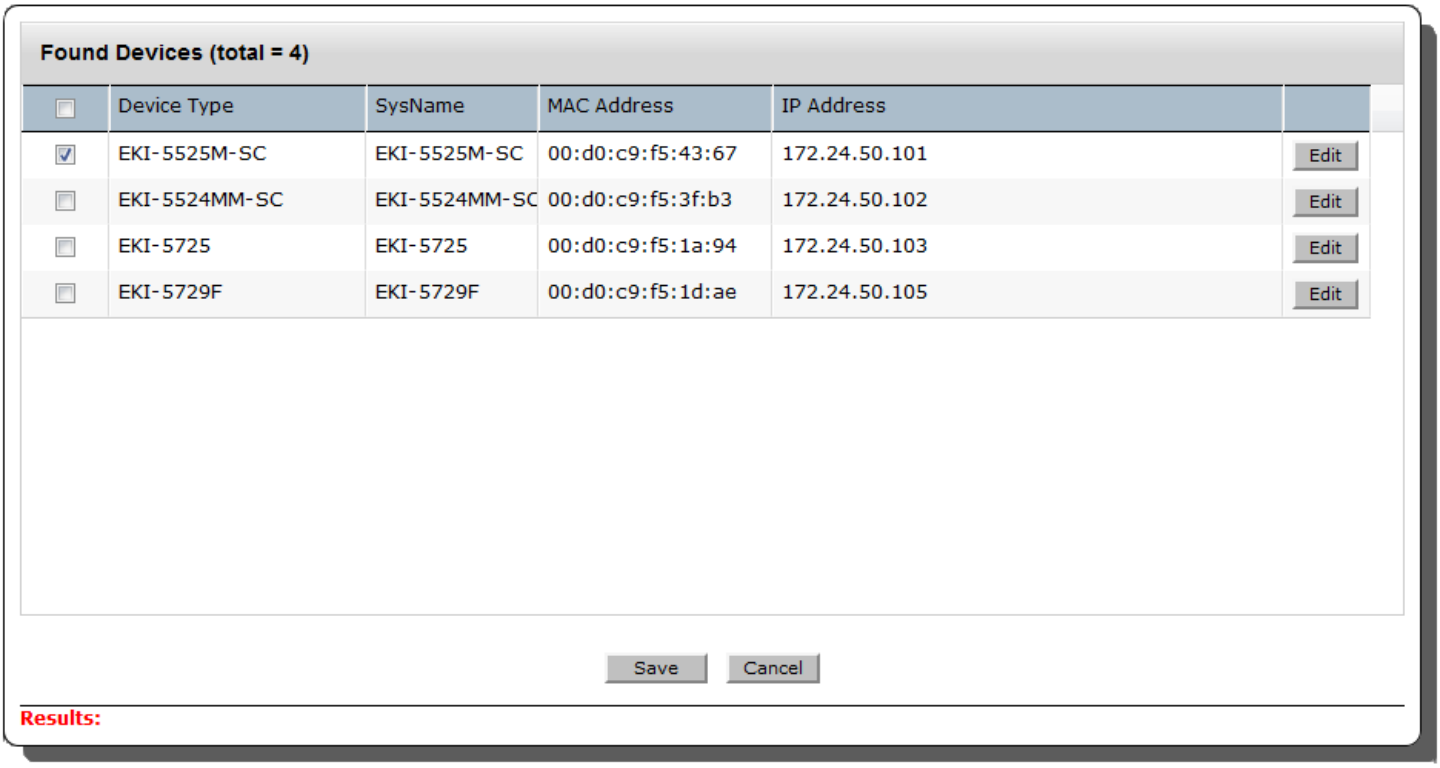
In the “Device Configuration Settings”, the “Segment” where the device should be stored can be set. The “Get Community” and “Set Community” values can be set. The “Modbus/TCP Host Idle Time” can be set. The “IP Address” can be changed by selecting the “Edit” command button which will display the “Edit IP Address” dialog. To save changes press the “Apply” command button. To exit without saving changes press the “Cancel” command button.



The “Edit IP Address” dialog can be used to change the “IP Address”, “Subnet Mask”, “Default Gateway”, and “DHCP Enabled” values. To save any changes press the “Ok” command button. To exit without saving changes press the “Cancel” command button.

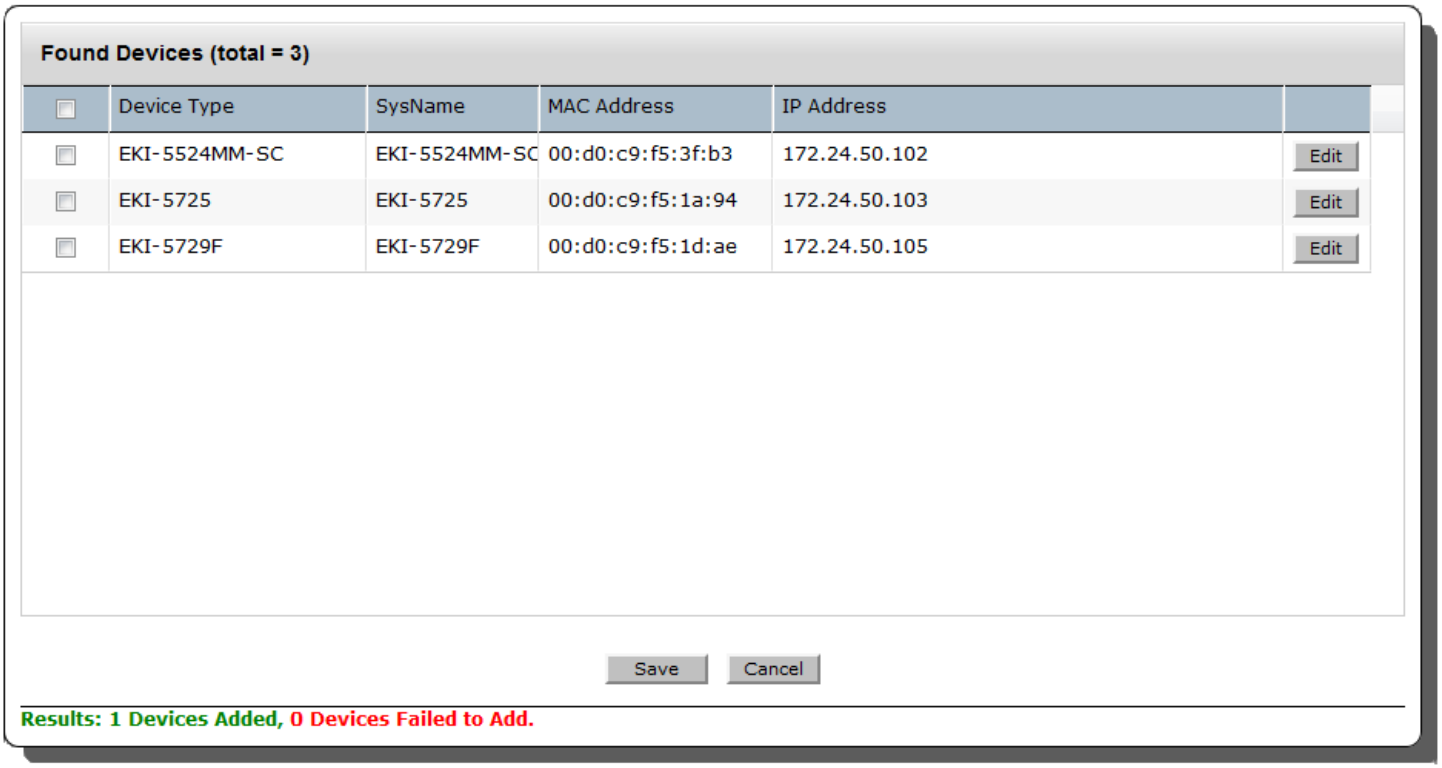


When you are done with the changes, make sure the device(s) you want added have the left side checkbox enabled and press the “Save” command button.



Device selected and ready to add.

When iView[2] is done attempting to add the device(s), a status message will display at the bottom of the display.



Results of adding a device.

Remove Device

The “Remove Device” menu selection located in the “Network” menu commands controls the ability to remove devices. Devices are associated with the categories are used to organize your IMC network device selections. Removing device is a 3-step process:

1) Select the Segment containing the device
2) Select the device(s) you want to remove
3) Remove the device information from the iView^2 database

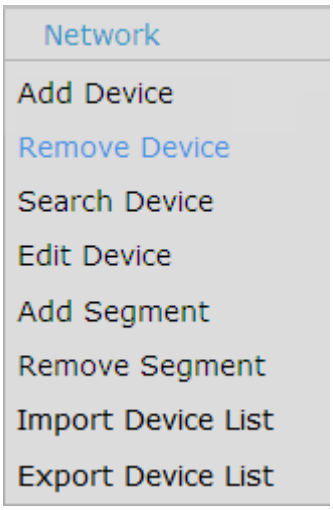


Figure 2.5 – Remove Device Menu Command

1) Select the Segment containing the device – The Remove Device dialog contains a dropdown list containing all the Segments in your Network Segment List. Selecting a Segment will display all the devices associated with that Segment under the “Description” section as shown in Figure 2.6.

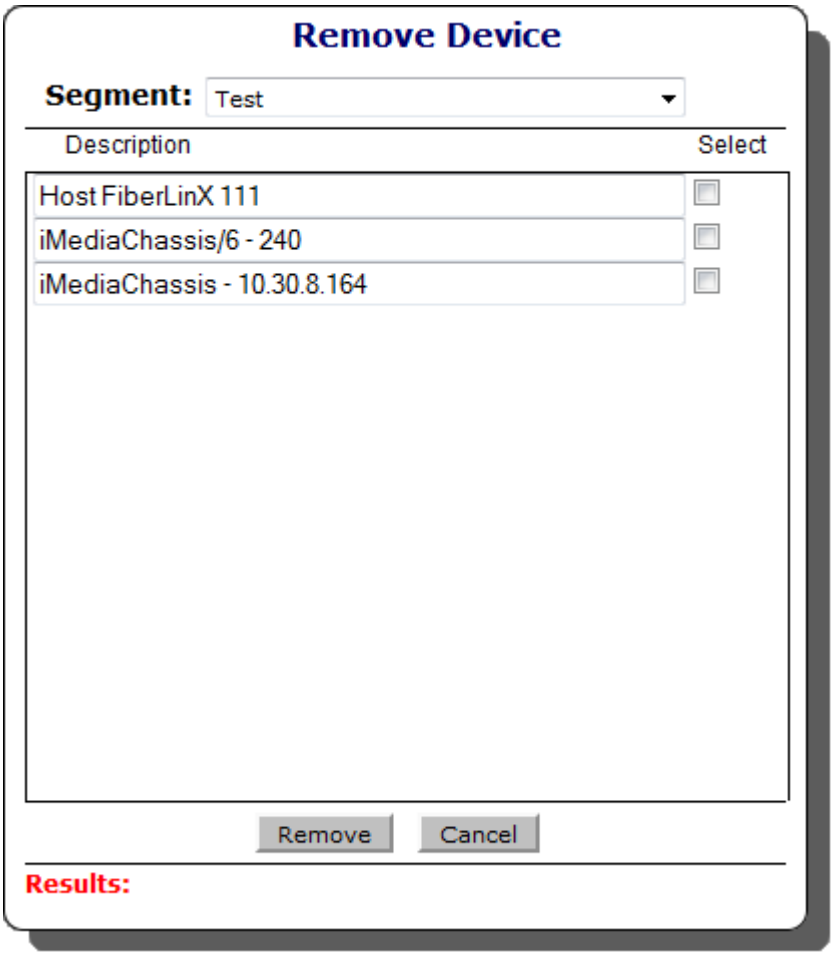


Figure 2.6 – Remove Device Menu Command

2) Select the device(s) you want to remove – Use the mouse to click in the “Select” square to the right of the device description information. Every device with the “Select” square checked will be subject to removal.

3) Remove the device information from the iView^2 database – After you have completed selecting the devices to remove press the “Remove” command button. This will display a message box listing your selections and ask you if you are sure you want to remove the device(s), as shown in figure 2.7. Pressing the “OK” command button will execute the device removal process. Pressing the “Cancel” command button will bring you back to the main Remove Device display.

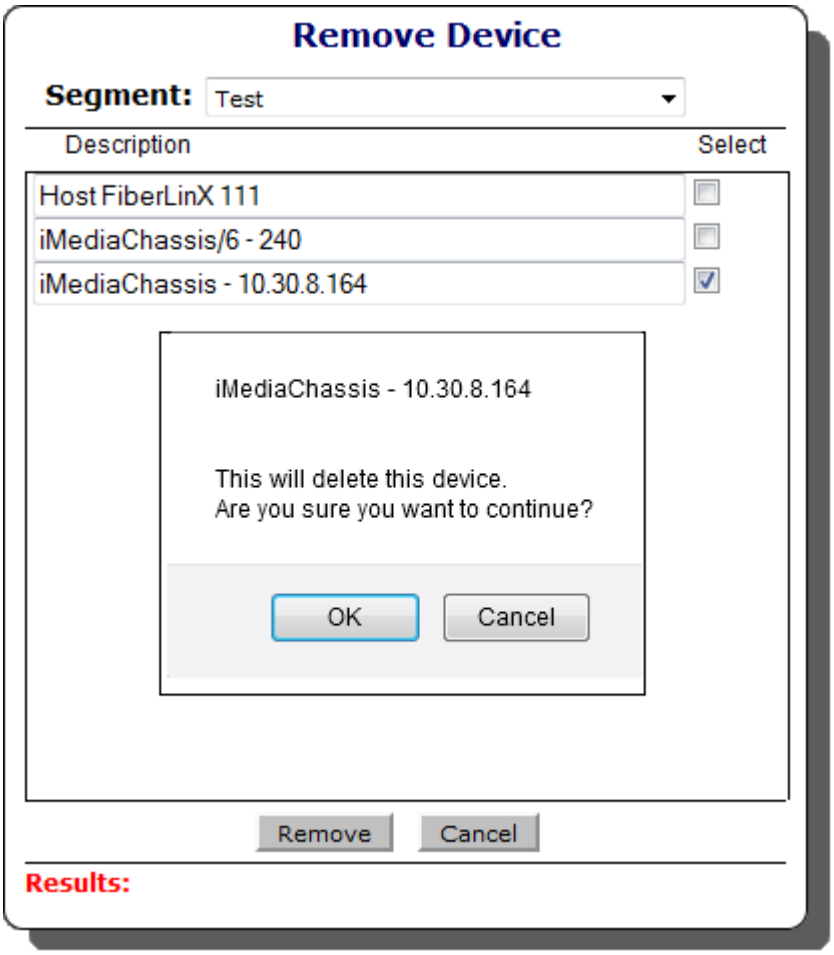


Figure 2.7 – Remove Device Confirmation

Search Device

The “Search Device” menu selection located in the “Network” menu commands and provides the user with the ability to search for IMC network devices using IP Addresses and Community strings to temporarily monitor a device.

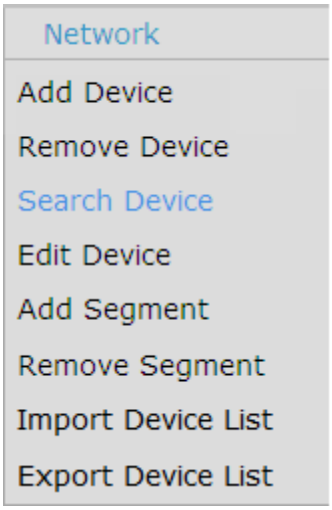


Figure 2.8 – Search Device Menu Command

1) Enter the Device IP Address OR Device Domain Name, Get Community, and Set Community in the Search Device Dialog Display as shown in Figure 6.2.

2) Press the “Search” command button to start the device search.

3) A successful search will display the device.

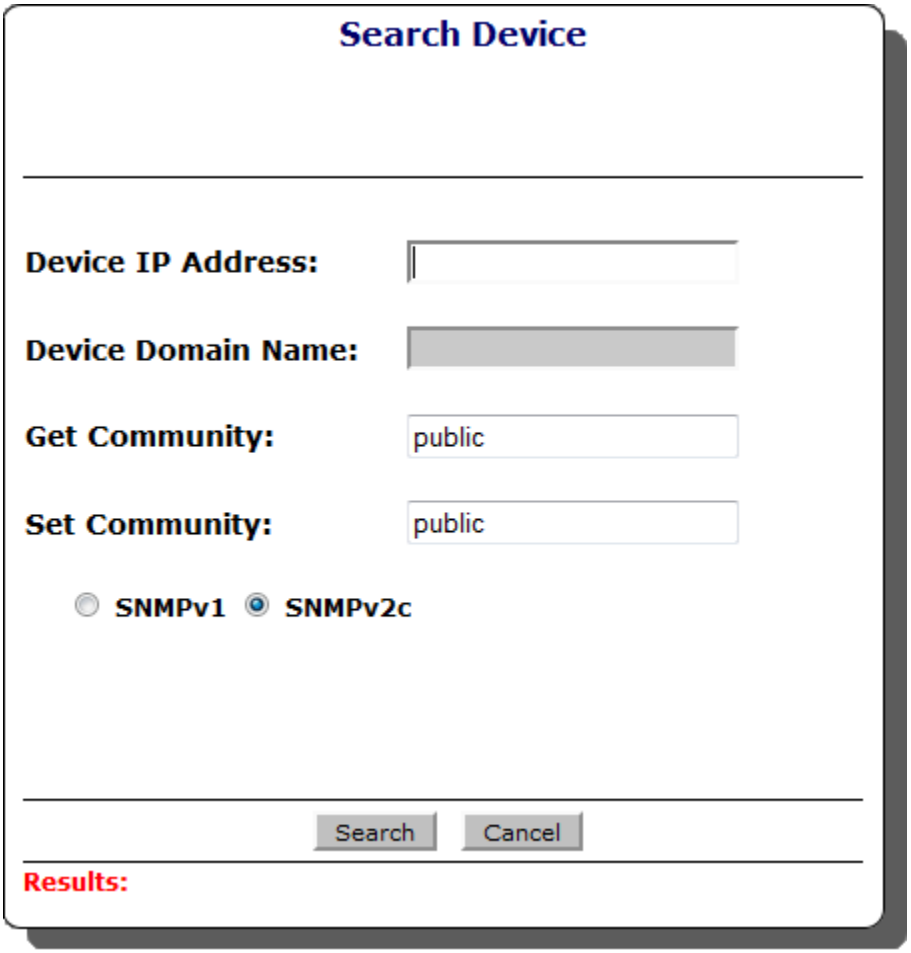


Figure 2.9 – Search Device Dialog Display

Edit Device

The “Edit Device” menu selection is located in the “Network” menu commands. This provides the user the ability to modify the “Description” for a device or update the “PROM Version”.
NOTE: The “Edit Device” menu is only for “B&B Devices”.

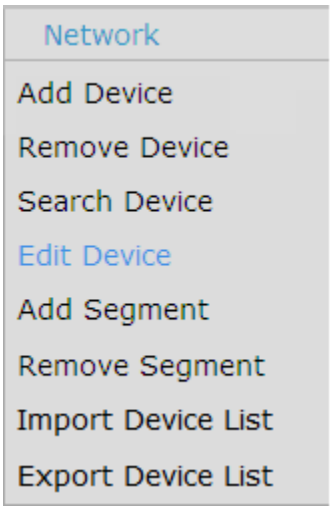


Figure 2.10 – Edit Device Menu Command

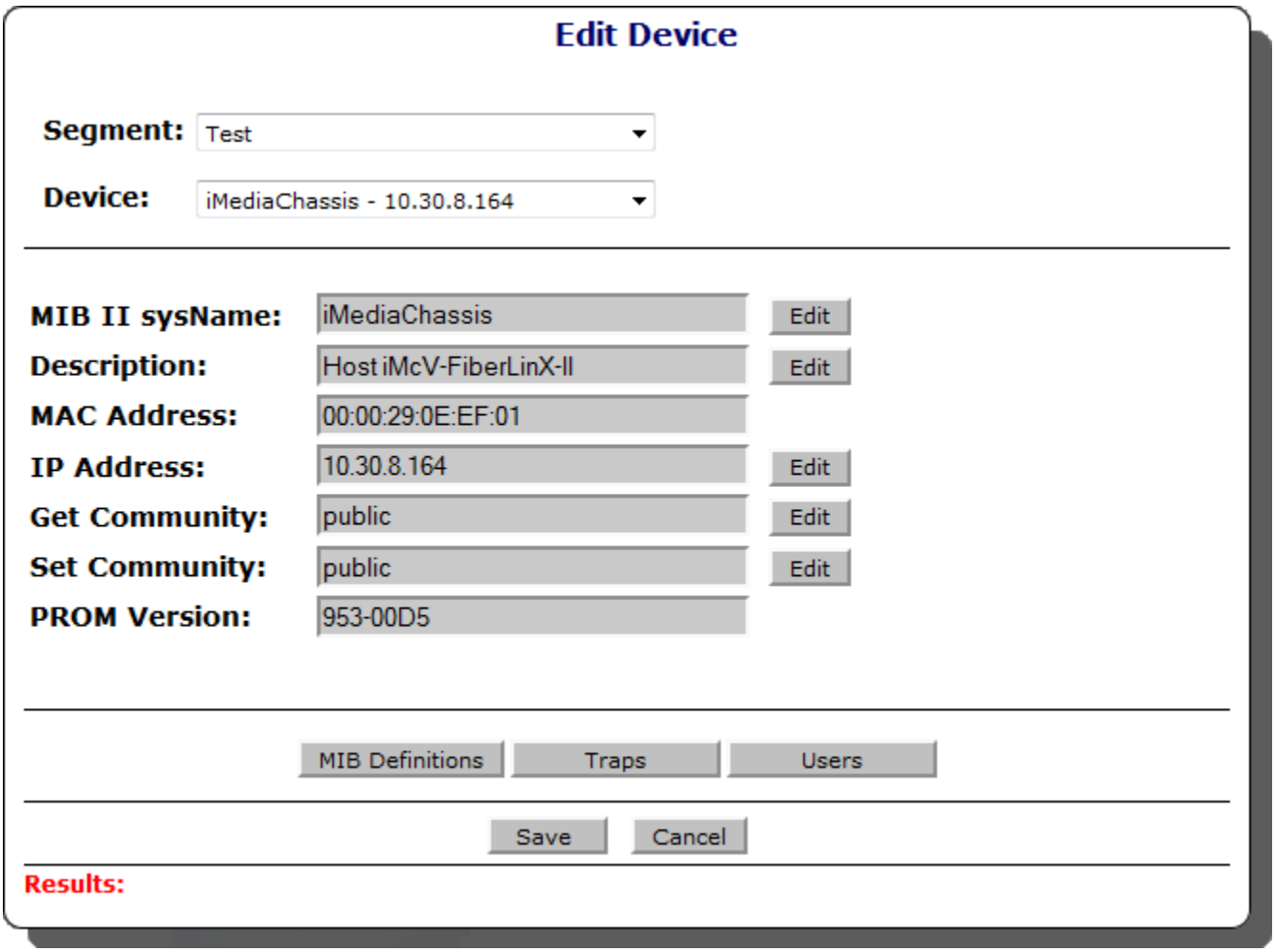


Figure 2.11 – Edit Device Dialog Display

Edit Description

To change the device description, select the "Description" "Edit" command button, enter the new device description in the "Description" field and press the "Save" command button. A successful operation will display "Operation Completed Successfully" in the "Results" section and the new description will display in the "iView Network Segment List". Figure 2.12a shows the results of changing a device description to "Host Giga-FiberLinX-III (.196)".

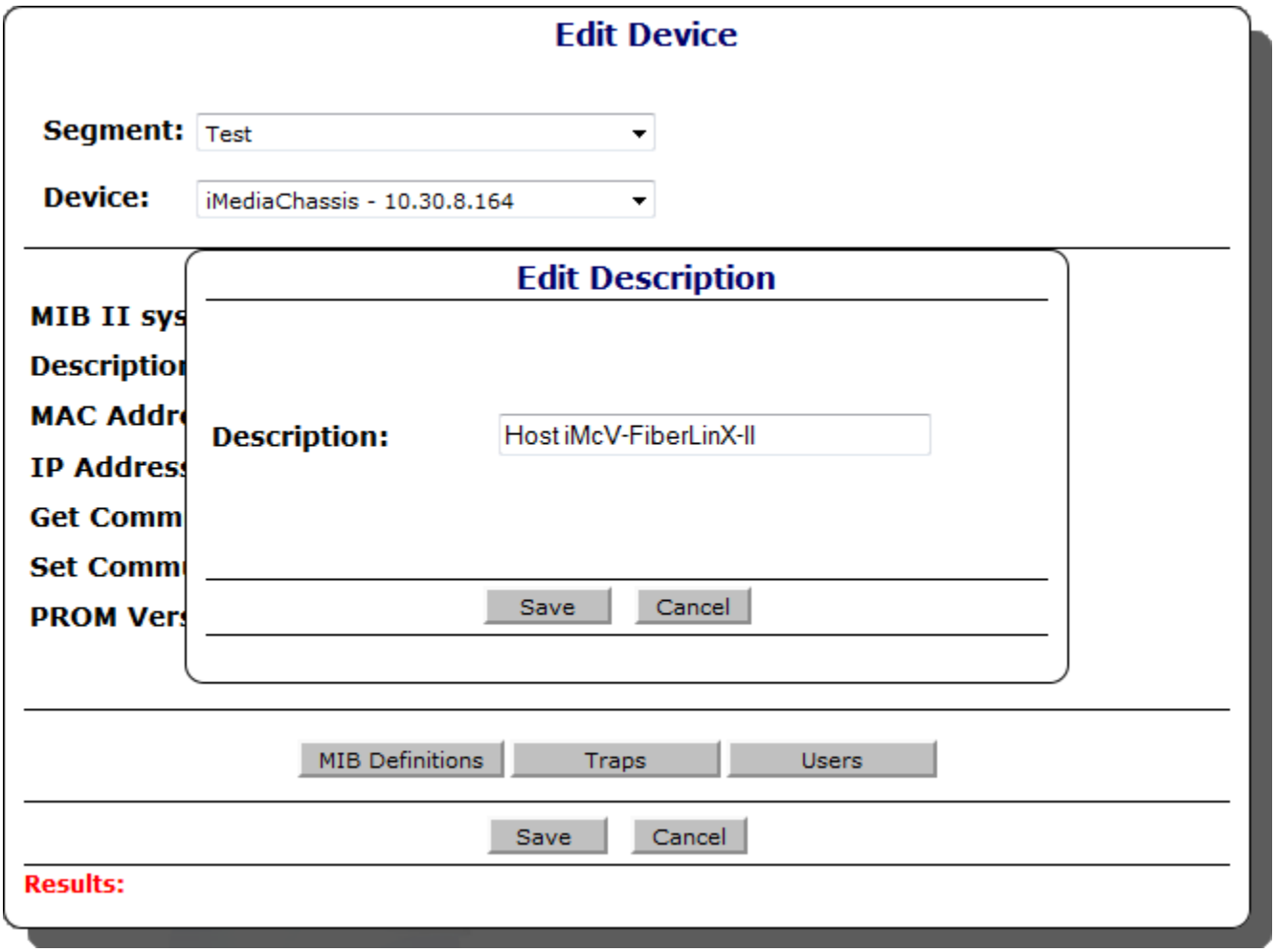


Figure 2.12a – Edit Device Description

Edit PROM Version

To update the device "PROM Version", follow the Task Manager instructions to select the device, set the scheduling options, and submit for processing.

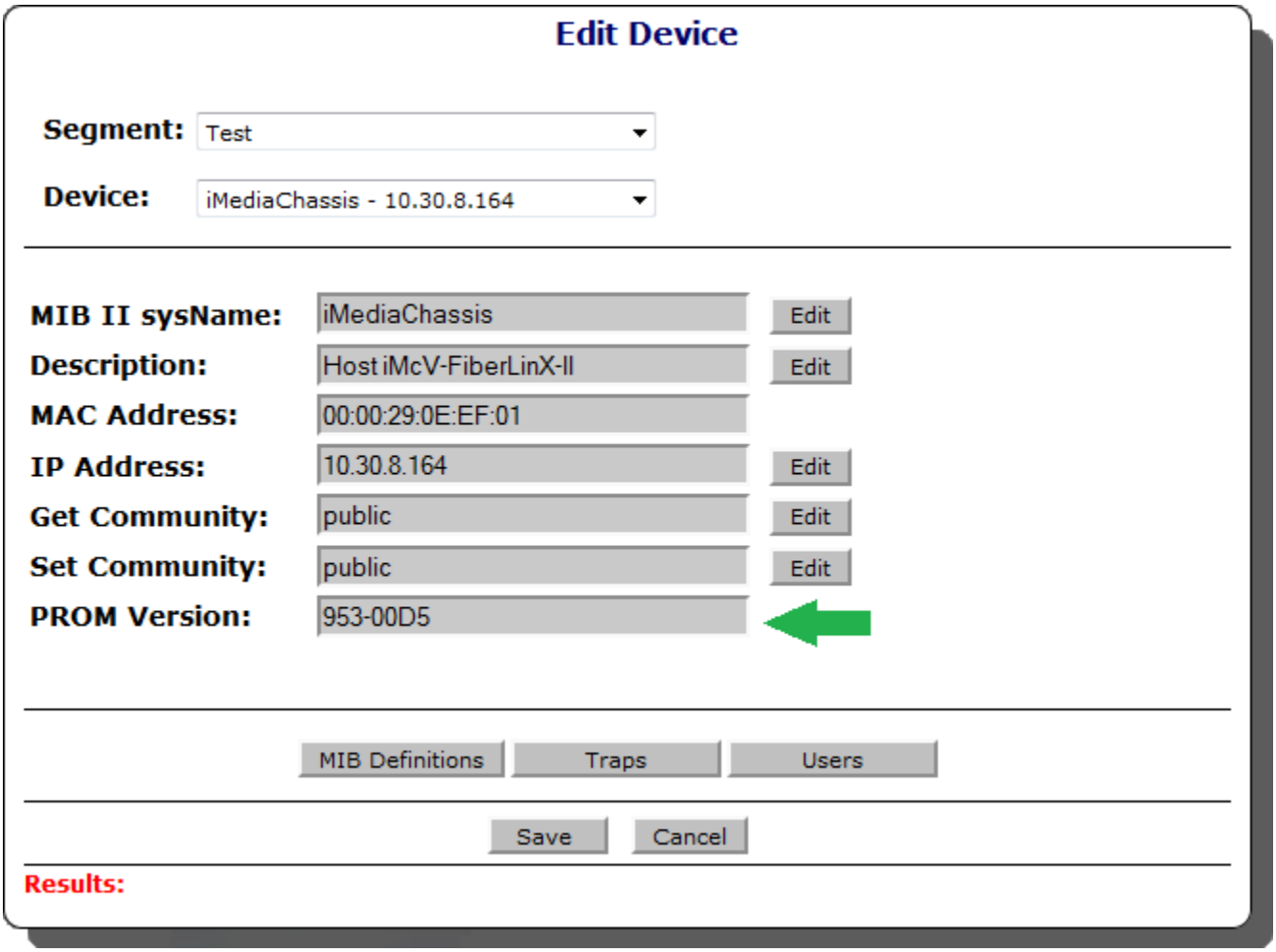


Figure 2.12b – Update PROM File

Edit IP Address

To change the device “IP Address” press the “Edit” command button to the right of the “IP Address” text box in the Edit Device Dialog display to display the “Edit IP Address” dialog as shown in Figure 2.13.

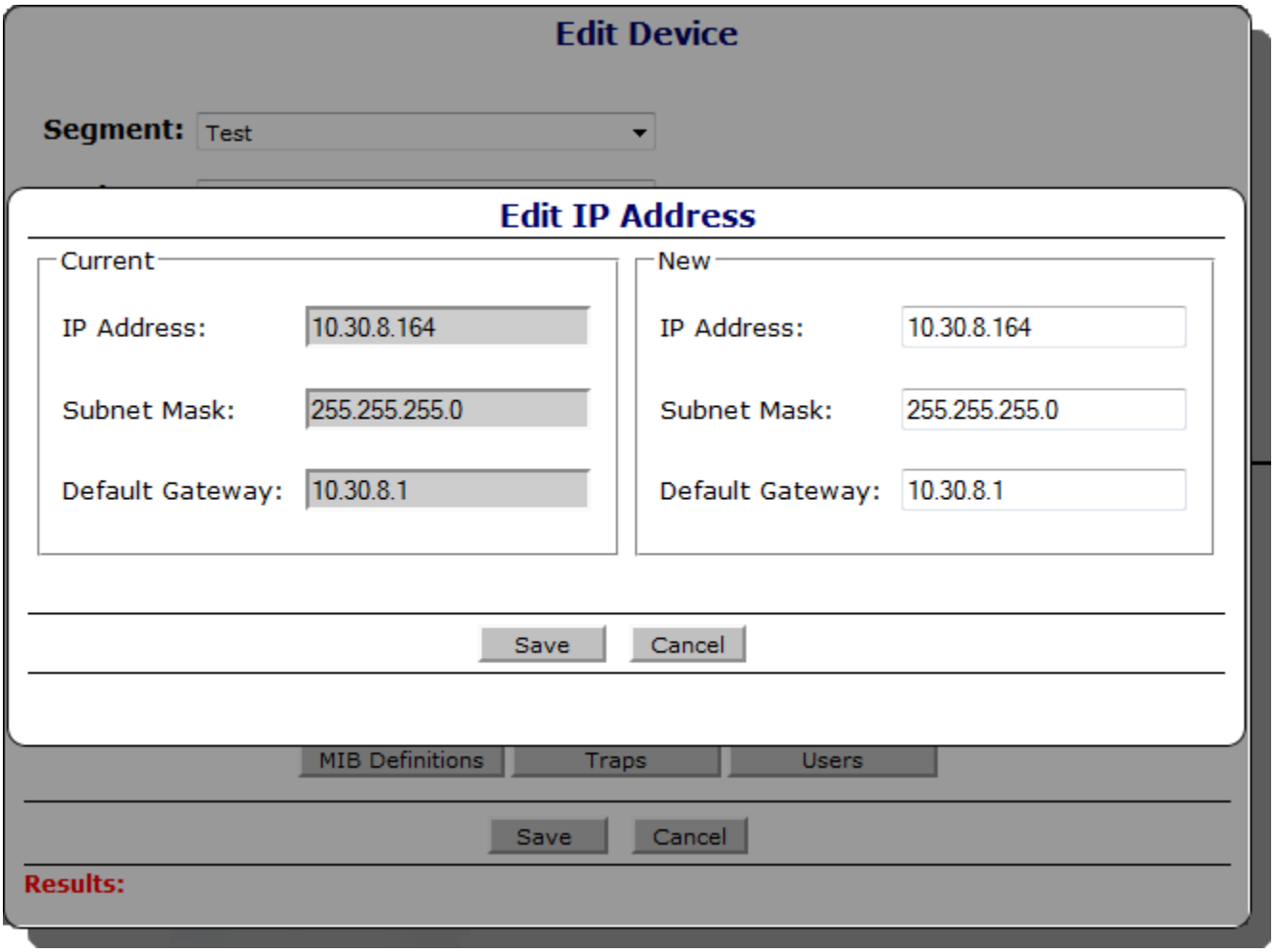


Figure 2.13 – Edit IP Address Dialog

1) Enter the addressing information that needs to be changed into the appropriate field in the “New” section.

2) Press the “Save” command button to write the new addressing information to the device. The entered information will be checked for appropriate format as an IPv4 address. An error message will be displayed if any of the fields is blank or is not formatted correctly.

3) Press the “Cancel” command button to close the “Edit IP Address” dialog without saving any changes.

4) Pressing “Save” command button to write the new addressing information to the device will cause the “IP Address Verification” dialog to display as shown in Figure 7.2e. The “Change IP Address Verification” dialog displays because writing the new addressing information to the device will cause the device to reboot when the write operation is complete.

Figure 2.14 – Change IP Address Verification Dialog

5) The system will display a “Processing Request” display while the new addressing information is being written to the device. When the operation is complete the results will be displayed as shown in Figure 2.15.

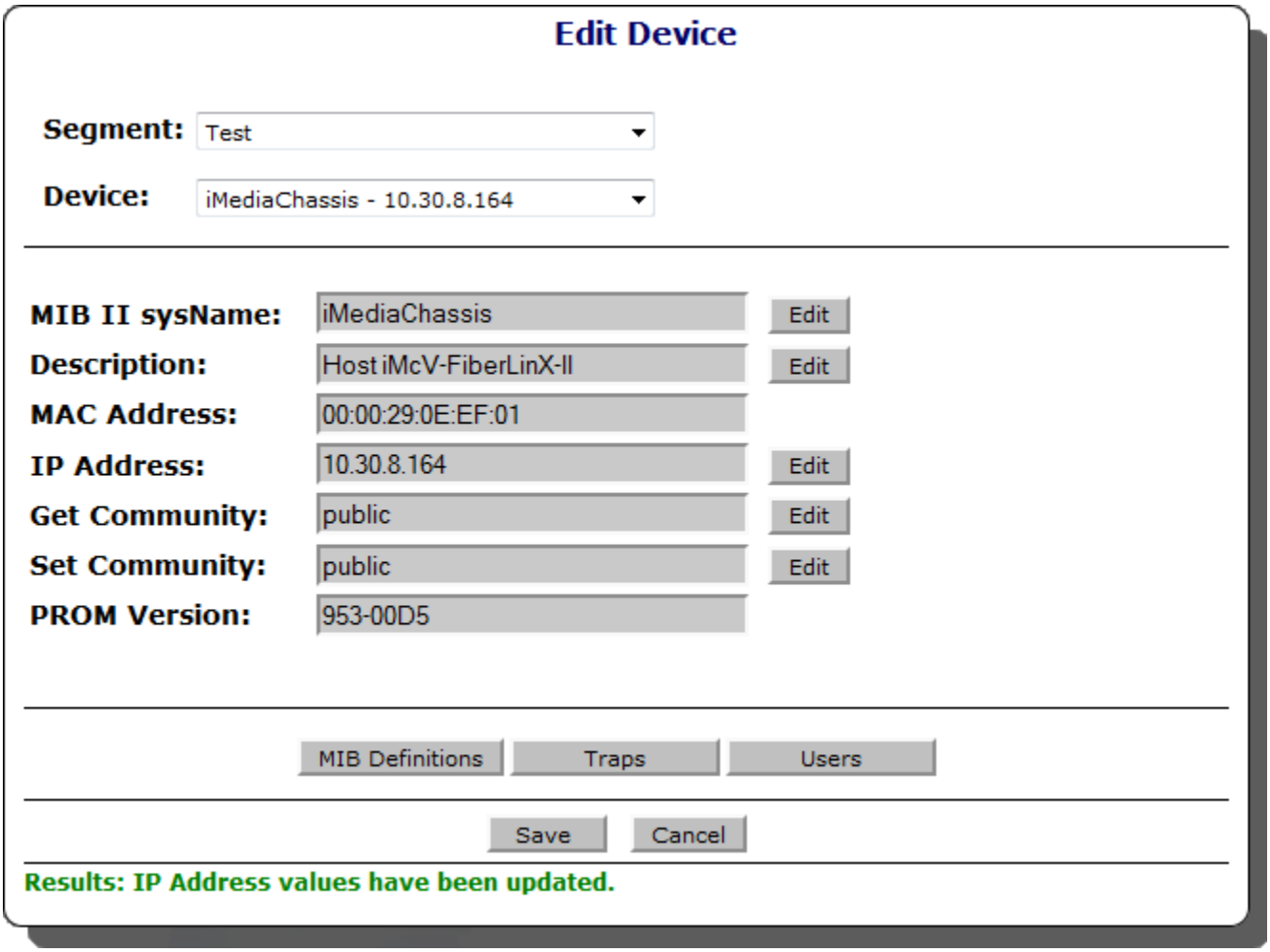


Figure 2.15 – IP Address Change Results Display

Edit MIB Definitions

To change the device “MIB Definitions” press the “MIB Definitions” command button in the Edit Device Dialog display as shown in Figure 7.2g. The “MIB Definitions” page allows you to: Add a New Community, Edit a Community, Delete a Community, Add Authentication to a Community, Edit the Authentication, or Delete the Authentication from a Community.

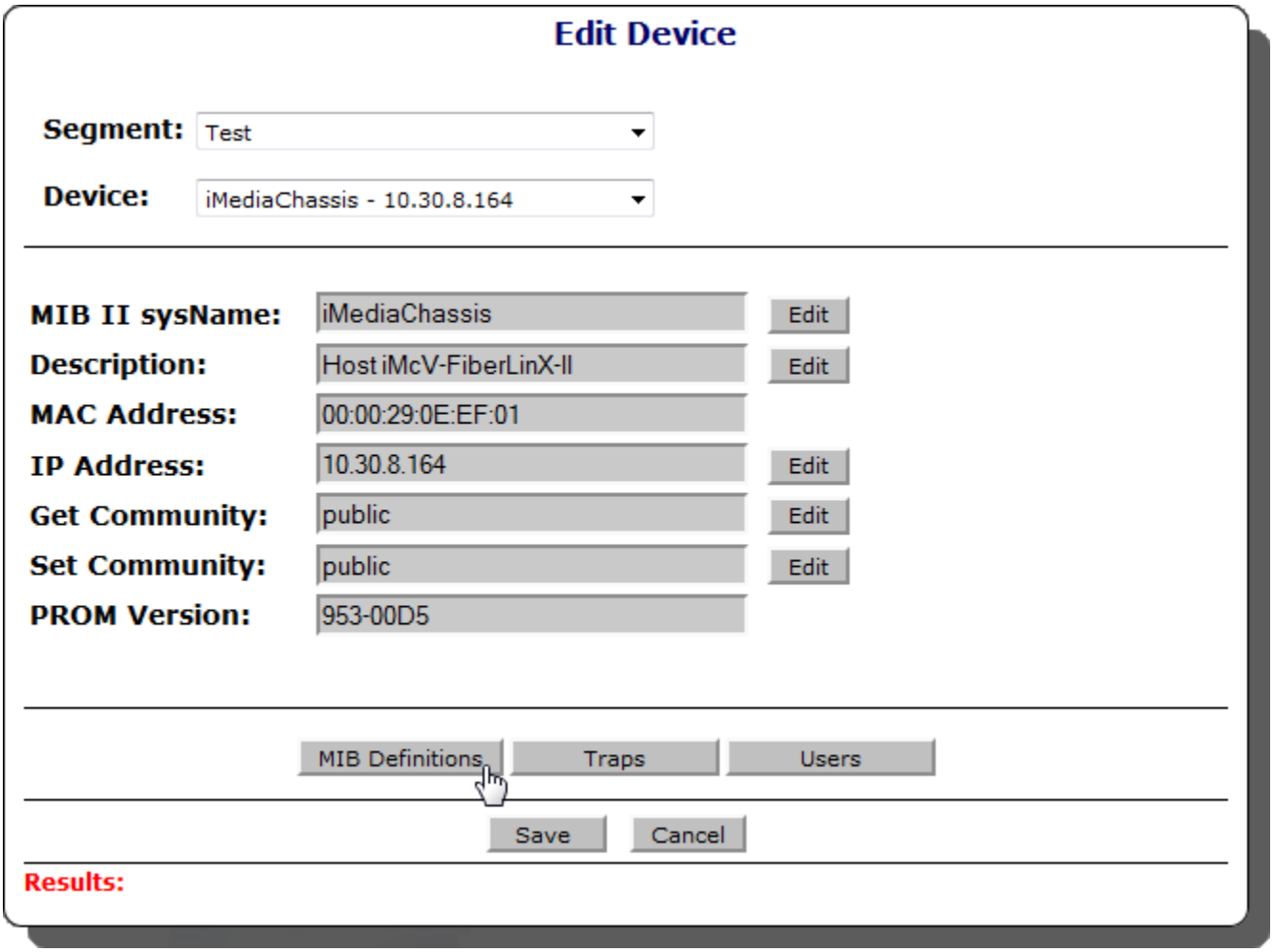


Figure 2.16 – MIB Definitions Command Button

Add a New Community

1) Press the “MIB Definitions” command button in the Edit Device Dialog display to open the “Edit MIB Definitions” dialog box. The “Edit MIB Definitions” dialog box is shown in Figure 2.17.

2) Press the “Add” command button in the “Edit MIB Definitions” dialog to display the “Edit Community” dialog. The “Edit Community” dialog allows the user the ability to define a new community.

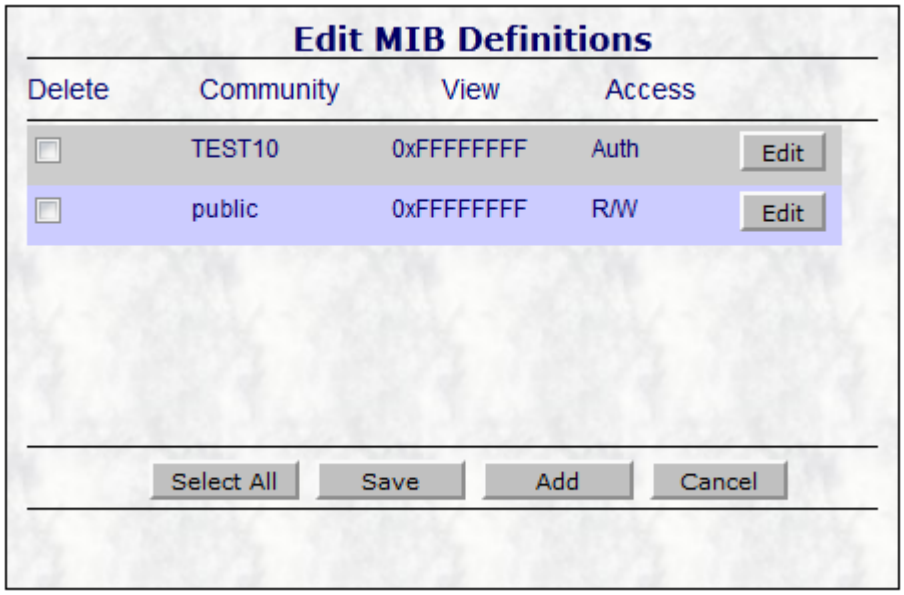


Figure 2.17 - Edit MIB Definitions dialog

3) In the “Edit Community” dialog box enter the “Name” of the new community.

Figure 2.18 – Edit Community Dialog

4) Click the “Groups” command button to display the “Edit View Privileges” dialog box. From the “Edit View Privileges” dialog box (refer to Figure 2.19) you can enable the MIB groups you want the community to have access to by checking the box next to the appropriate selection.

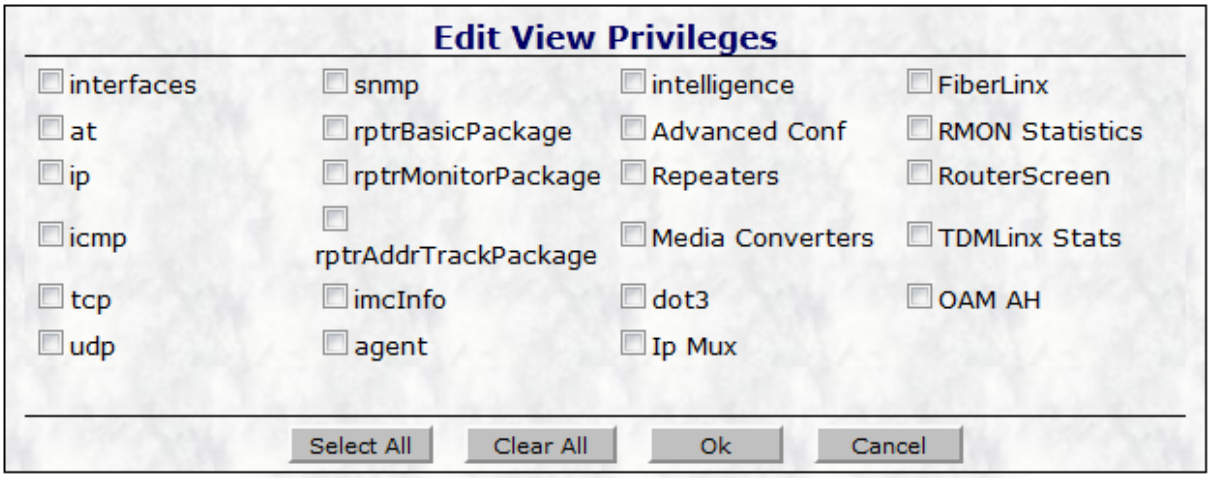


Figure 2.19 – Edit View Privileges Dialog

5) Press the "Ok" command button to exit the "Edit View Privileges" dialog box once you have made your MIB groups selections.

6) Select the "Access Type" from the "Edit Community" dialog box.

7) Press the "Ok" command button in the "Edit Community" dialog box to return to the "Edit MIB Definitions" dialog box.

8) In the "Edit MIB Definitions" dialog box press the "Save" command button as shown in Figure 2.20.

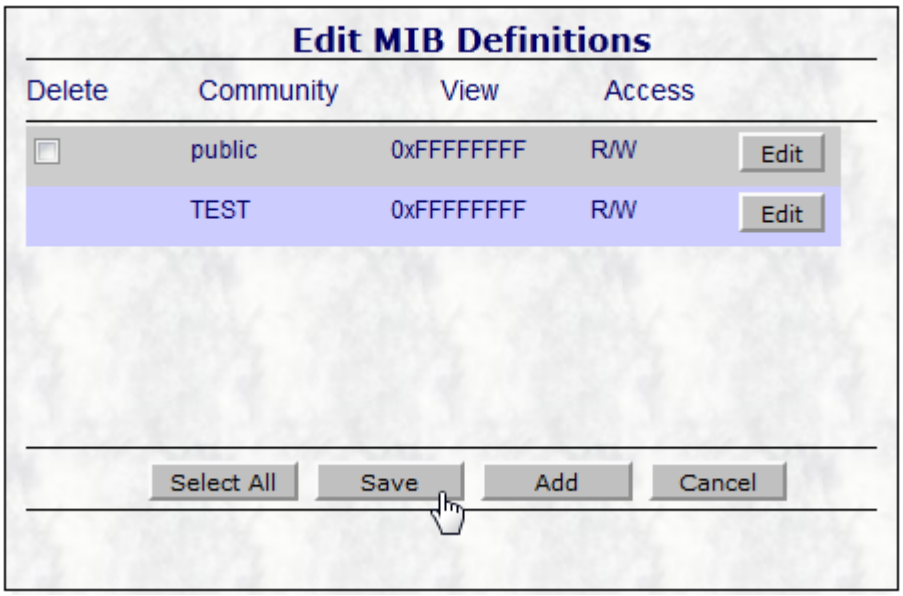


Figure 2.20 – Press "Save" to store "TEST" community to device.

9) The "Processing Request" display will appear while the new community is written to the device as shown in Figure 2.2l.

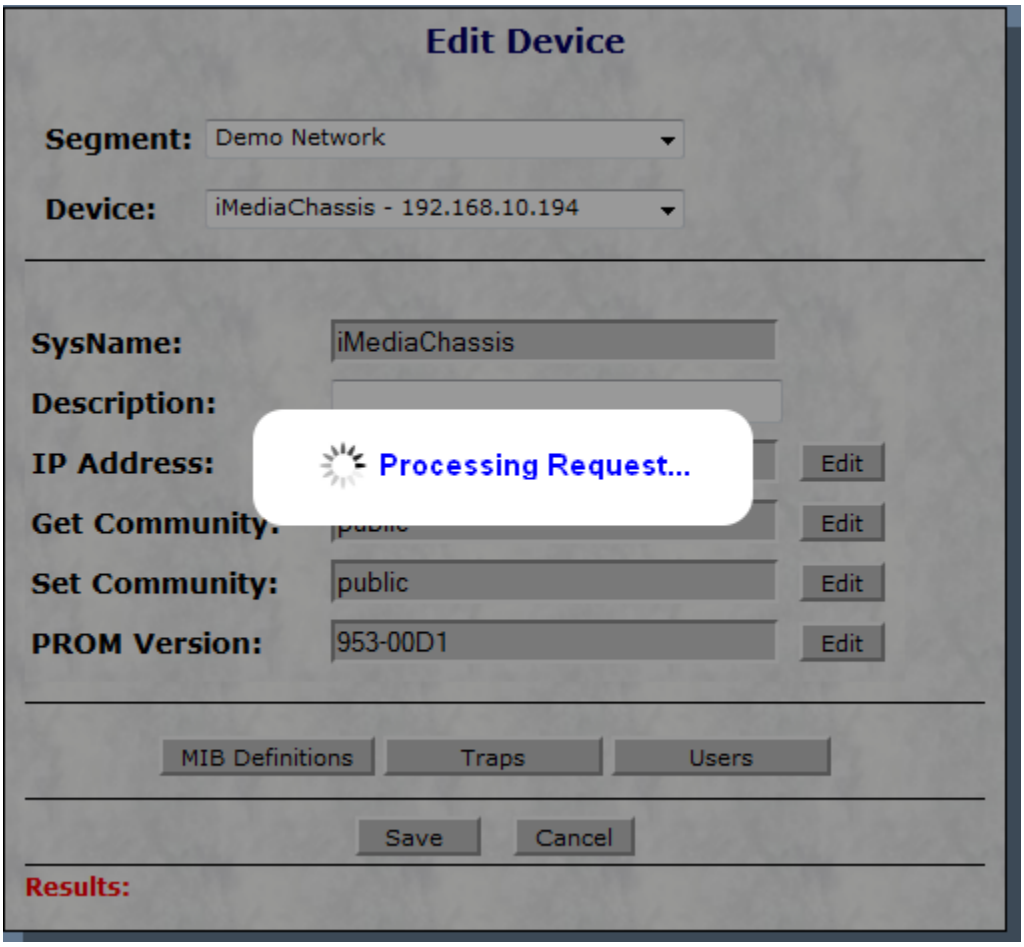


Figure 2.2l – Example processing Add Community request.

10) When the write community to device request is finished processing the results of the operation will appear in the “Results” section of the “Edit Device” dialog as shown in Figure 2.22.

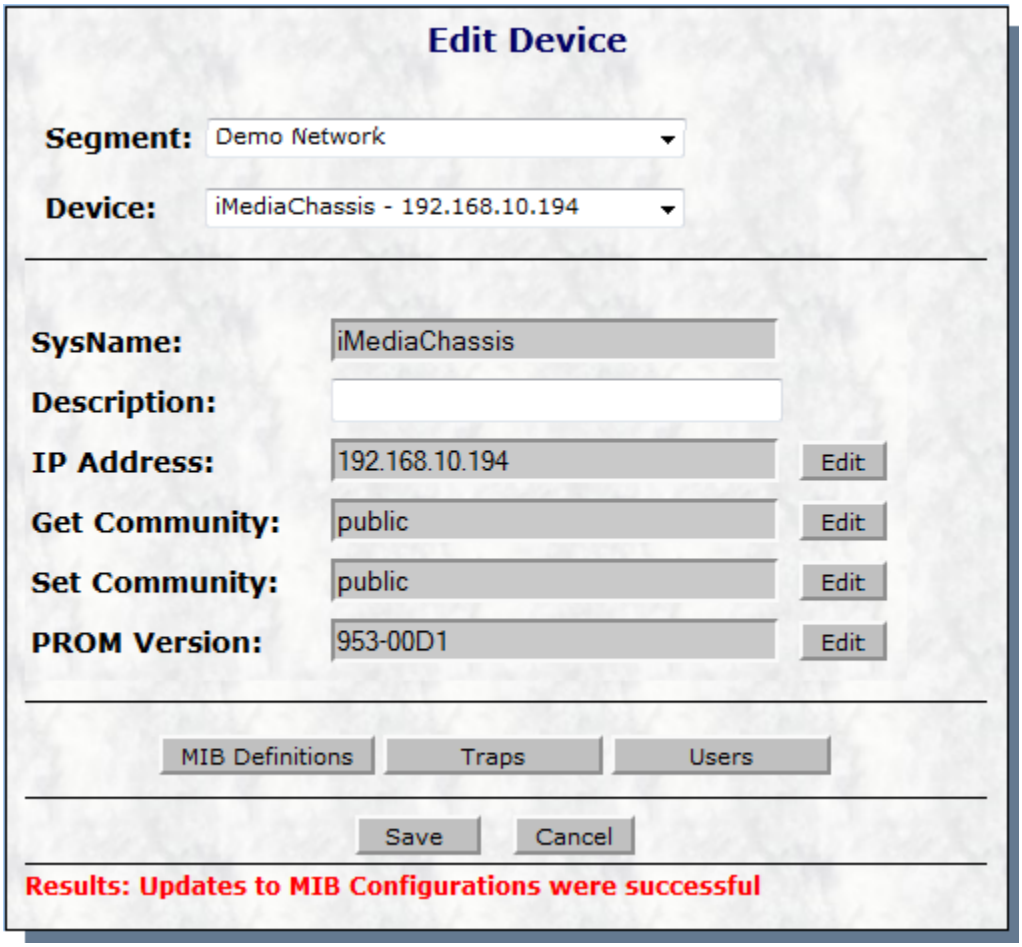


Figure 2.22 – Add Community Results Display

Edit a Community

1) Press the “MIB Definitions” command button in the Edit Device Dialog display to open the “Edit MIB Definitions” dialog box. The “Edit MIB Definitions” dialog box is shown in Figure 2.23.

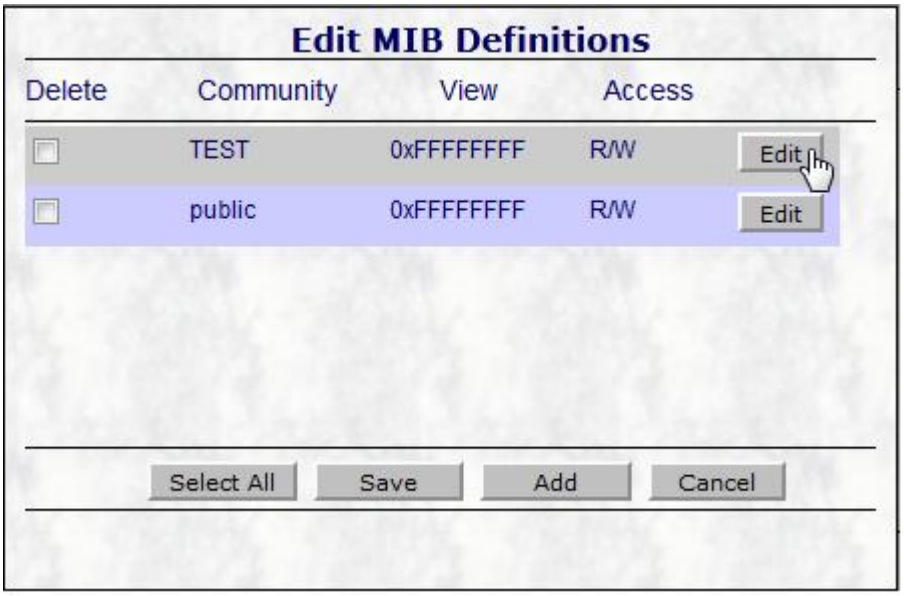


Figure 2.23 – Edit Community

2) Press the “Edit” command button in the “Edit MIB Definitions” dialog to the right of the community you want to change. The “Edit Community” dialog will appear (Figure 2.24) which will allow the user the ability to change the “Groups” associated with the community or the “Access” rights of the community.

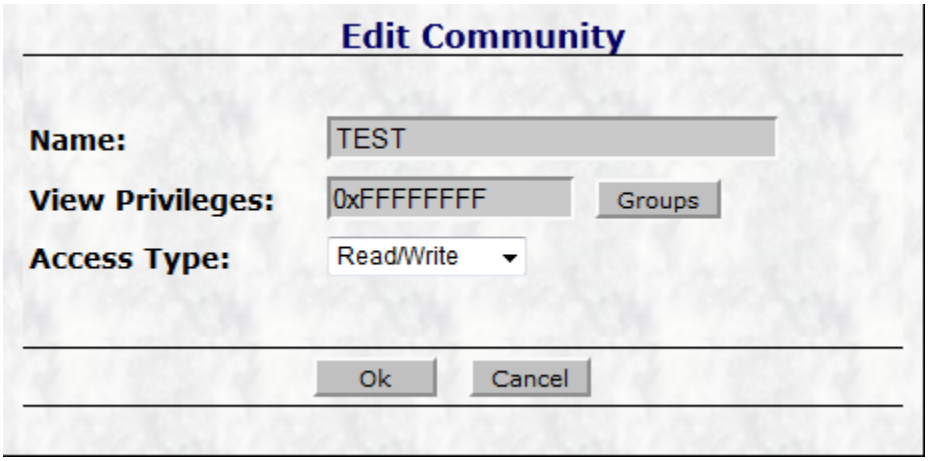


Figure 2.24 – Edit existing community

3) Press the “Ok” command button in the “Edit Community” dialog box to return to the “Edit MIB Definitions” dialog box.

4) In the “Edit MIB Definitions” dialog box press the “Save” command button.

5) The “Processing Request” display will appear while the community changes are written to the device.

6) When the write community to device request is finished processing the results of the operation will appear in the “Results” section of the “Edit Device” dialog.

Delete a Community

1) Press the “MIB Definitions” command button in the Edit Device Dialog display to open the “Edit MIB Definitions” dialog box.

2) Select the MIB Definition(s) you want to delete by using the mouse to set the check in the “Delete” checkbox next to the community you want to delete. The example in Figure 2.25 shows that the “TEST” community is selected for deletion.

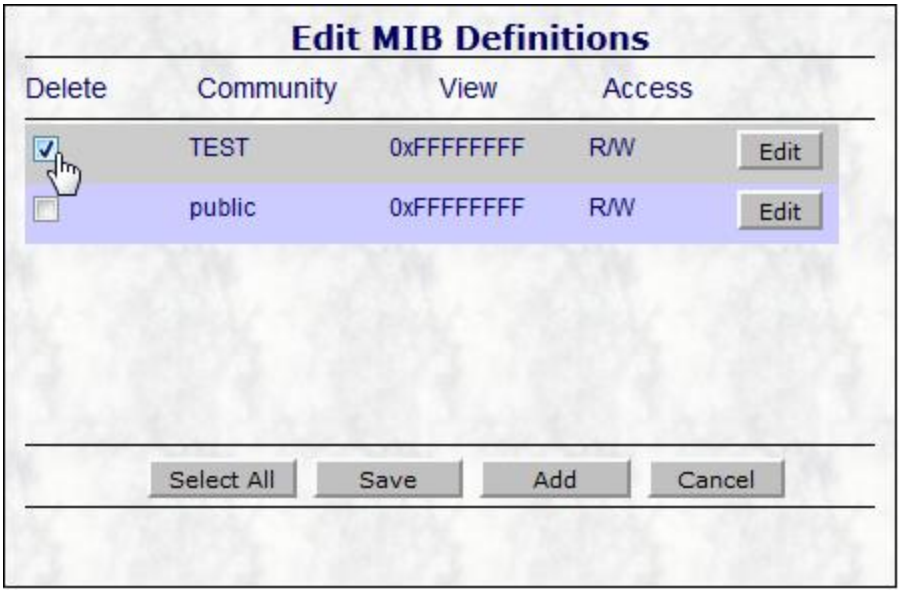


Figure 2.25 – Selecting a community to delete

3) In the “Edit MIB Definitions” dialog box press the “Save” command button.

4) The “Processing Request” display will appear while the community changes are written to the device.

5) When the write community to device request is finished processing the results of the operation will appear in the “Results” section of the “Edit Device” dialog.

Add Authentication to a Community

Authentication provides the user the ability to provide certain IP Address more or less access within a community.

1) Press the “MIB Definitions” command button in the Edit Device Dialog display to open the “Edit MIB Definitions” dialog box.

2) Press the “Edit” command button in the “Edit MIB Definitions” dialog to the right of the community you want to change.

3) Change the “Access Type” to “Authentication”. This will change the “Access Type” of the community and display the “Authentication” command button as shown in Figures 2.27 and 2.28.

Figure 2.27 – Changing “Access Type” to Authentication

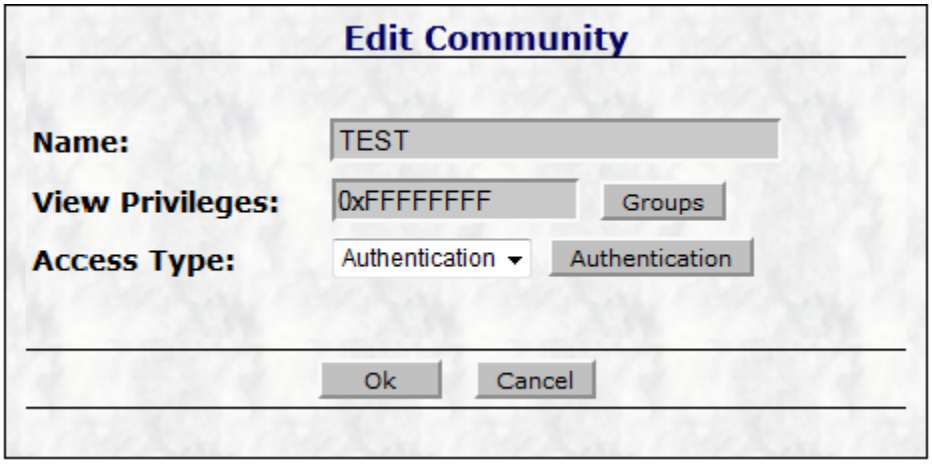


Figure 2.28 – Availability of “Authentication” command button

4) Press the “Authentication” command button to display the “Authentication List” dialog box. The “Authentication List” dialog box allows the user the ability to “Add” IP Address and their associated access restrictions to the selected community.

Figure 2.29 - “Authentication List” dialog box

5) Press the “Add” command button in the “Authentication List” dialog box to display the “Add Authentication” dialog box.

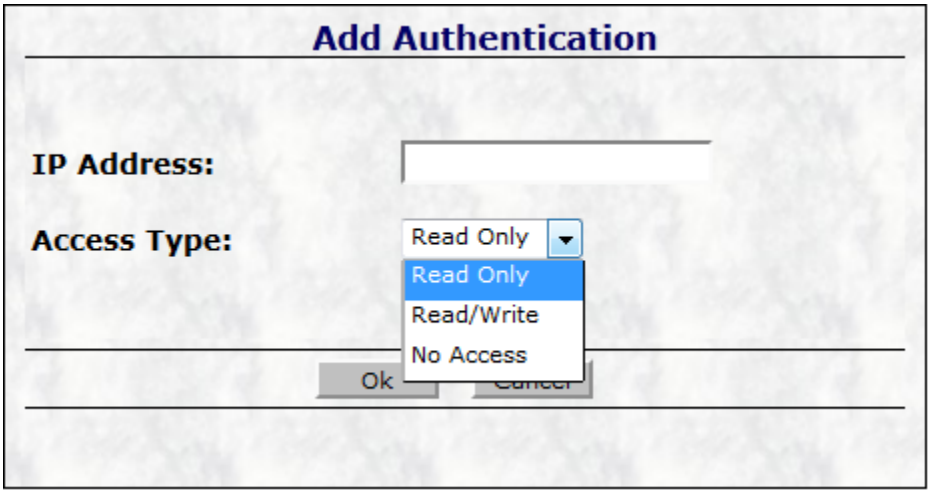


Figure 2.30 – “Add Authentication” dialog box

6) Enter an “IP Address” and select the appropriate “Access Type” from the selections.

Read Only – The entered IP Address will only have read only SNMP access to the device
Read/Write – The entered IP Address will have read and write SNMP access to the device
No Access – The entered IP Address will have no SNMP access to the device

NOTE: The authentication access type associated with a community will only allow those IP Addresses associated with the community the applicable SNMP access. Any IP Address not in the “Authentication List” will not have any SNMP access to devices through the authenticated community.

7) Press the “Ok” command button in the “Add Authentication” dialog box.

8) Press the “Ok” command button in the “Authentication List” dialog box.

9) Press the “Ok” command button in the “Edit Community” dialog box.

10) In the “Edit MIB Definitions” dialog box press the “Save” command button.

11) The “Processing Request” display will appear while the community changes are written to the device.

12) When the write community to device request is finished processing the results of the operation will appear in the “Results” section of the “Edit Device” dialog.

Delete the Authentication from a Community

1) Press the “MIB Definitions” command button in the Edit Device Dialog display to open the “Edit MIB Definitions” dialog box.

2) Press the “Edit” command button in the “Edit MIB Definitions” dialog to the right of the community you want to change.

4) Press the “Authentication” command button to display the “Authentication List” dialog box.

5) Select the authentication you want to delete by using the mouse to set the check in the “Delete” checkbox.

6) Press the “Ok” command button in the “Authentication List” dialog box.

7) Press the “Ok” command button in the “Edit Community” dialog box.

8) In the “Edit MIB Definitions” dialog box press the “Save” command button.

9) The “Processing Request” display will appear while the community changes are written to the device.

10) When the write community to device request is finished processing the results of the operation will appear in the “Results” section of the “Edit Device” dialog.

Edit Traps

Most Trap operations in iView[2] are controlled through the "Trap Manager" functions. The "Edit Device" dialog box also allows a user the ability to add trap operations for ip addresses that are not associated with the iView[2] server.

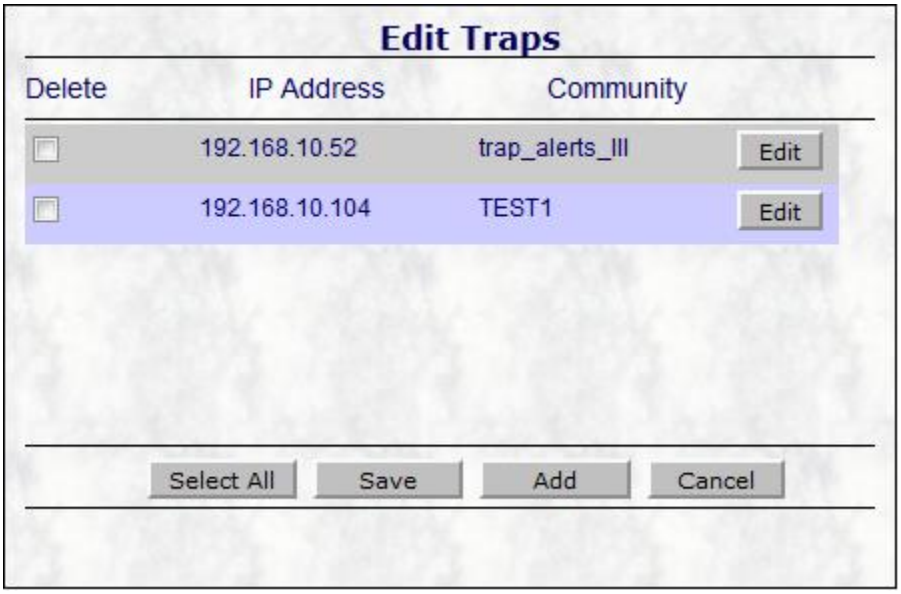


Figure 2.31 – "Edit Traps" dialog box

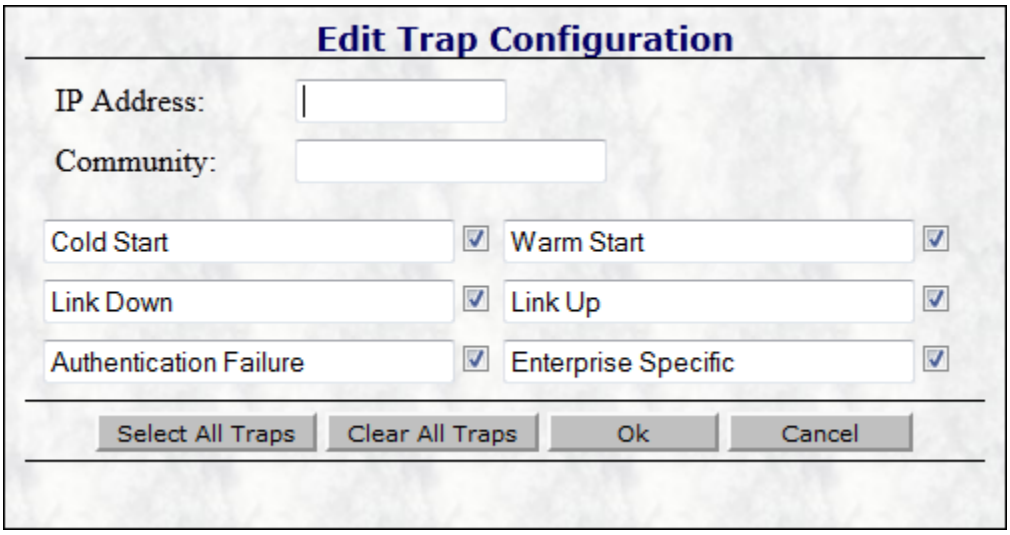


Figure 2.32 – Edit Trap Configuration Dialog Box

Edit Get/Set Community

The Get Community and Set Community for a device can be changed through the “Edit Device” dialog by pressing the “Edit” command button to the right of the “Get Community” or “Set Community” display.

Figure 2.33 – “Edit Device” dialog box

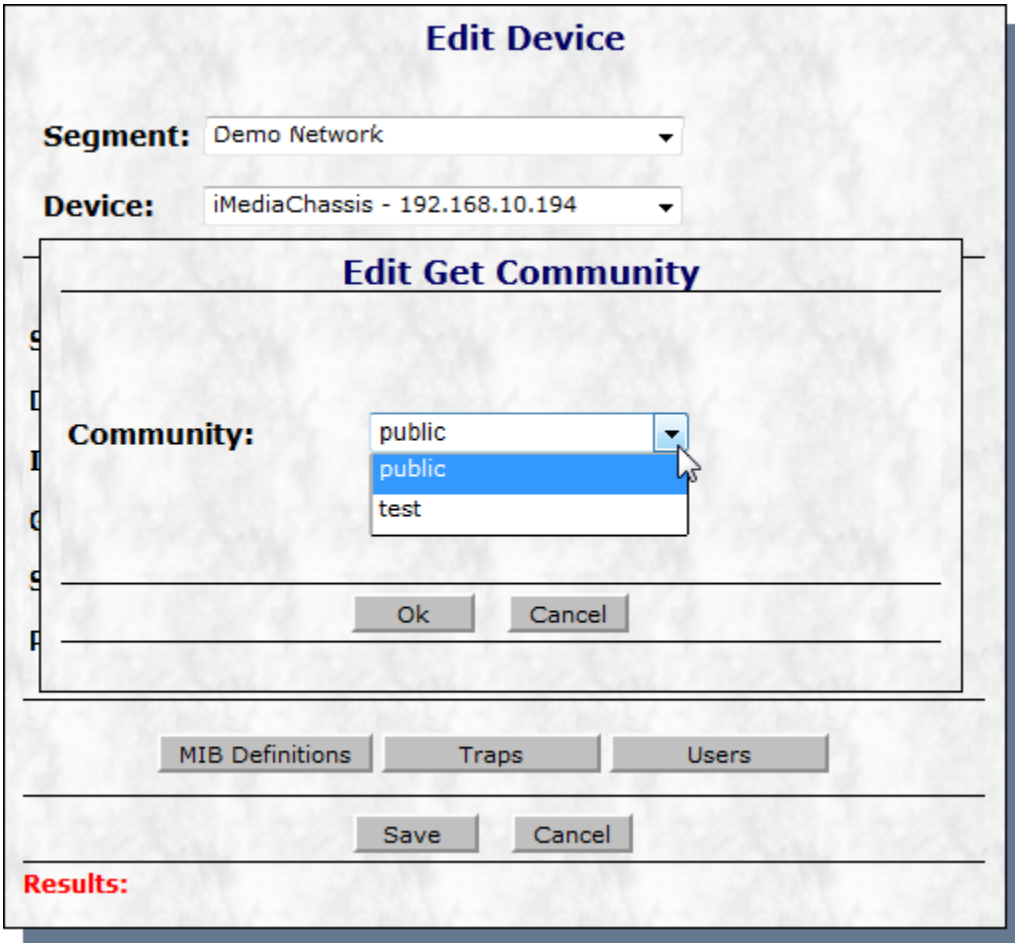


Figure 2.34 – “Edit Get Community” dialog

Edit Users

The “Users” command button in the “Edit Device” dialog box allows for the definition of names, passwords, and access rights for configuration and administration of the device. There are three levels of access rights that can be assigned:
Admin – Provides full read and write access.
Operator – Provides full read and write access except for “Users” and PROM file updates.
User – Provides read only for settings and no access for “Users” and PROM file updates.

Add a User

1) Press the “Users” command button in the “Edit Device” Dialog display to open the “Edit Device Users” dialog box.

2) Press the “Add” command button in the “Edit Device Users” dialog box to display the “User Settings” dialog box.

3) In the “User Settings” dialog box enter the appropriate user information.

4) Press the “Ok” command button in the “User Settings” dialog box.

5) Press the “Save” command button in the “Edit Device Users” dialog box.

7) The “Processing Request” display will appear while the community changes are written to the device.

8) When the write community to device request is finished processing the results of the operation will appear in the “Results” section of the “Edit Device” dialog.

Figure 2.35 – “Edit Device Users” dialog box

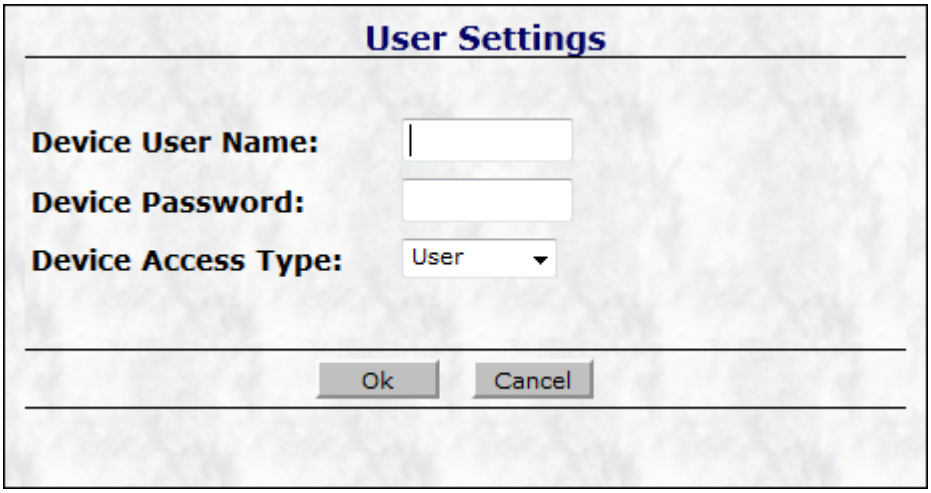


Figure 2.36 – “User Settings” dialog box

Delete a User

1) Press the “Users” command button in the “Edit Device” Dialog display to open the “Edit Device Users” dialog box.

2) Select the user(s) you want to delete by using the mouse to set the check in the “Delete” checkbox.

3) Press the “Save” command button in the “Edit Device Users” dialog box.

4) The “Processing Request” display will appear while the community changes are written to the device.

5) When the write community to device request is finished processing the results of the operation will appear in the “Results” section of the “Edit Device” dialog.

Add Segment

The “Add Segment” menu selection located in the “Network” menu commands controls the ability to add new segments. Segments are used to organize your IMC network device selections. You must enter at least 1 segment before you can add any devices.

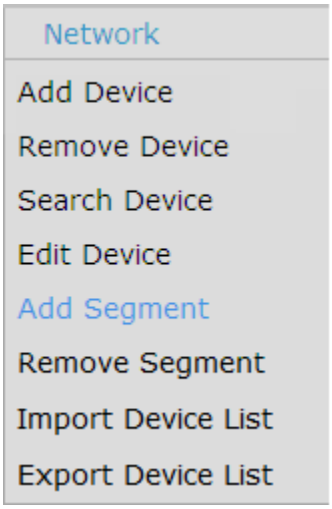


Figure 2.37 – Add Segment Menu Command

In the “Segment:” input area of the “Add Segment Display” you can enter your segment identification information. This can consist of up to 50 alphanumeric characters. Duplicate segments are not allowed.

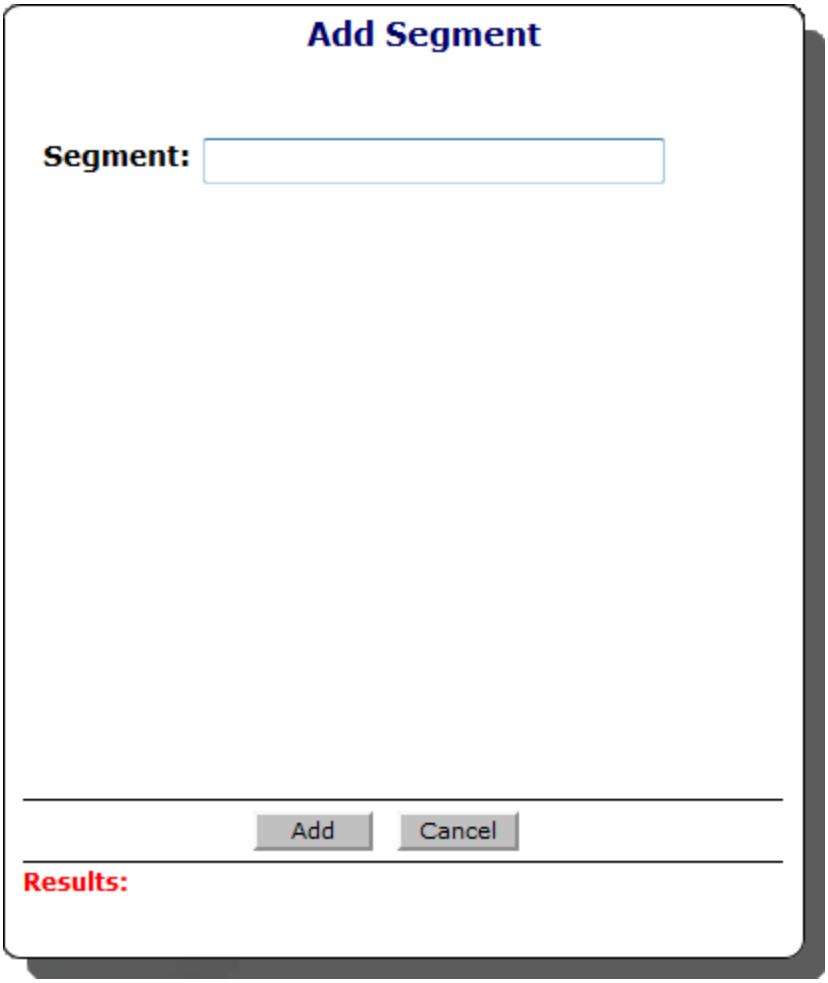


Figure 2.38 – Add Segment Display

Press the “Add” command button to store your information in the database and update the Network Segment List display.

Press the “Cancel” command button to erase your input and prepare for a new entry.

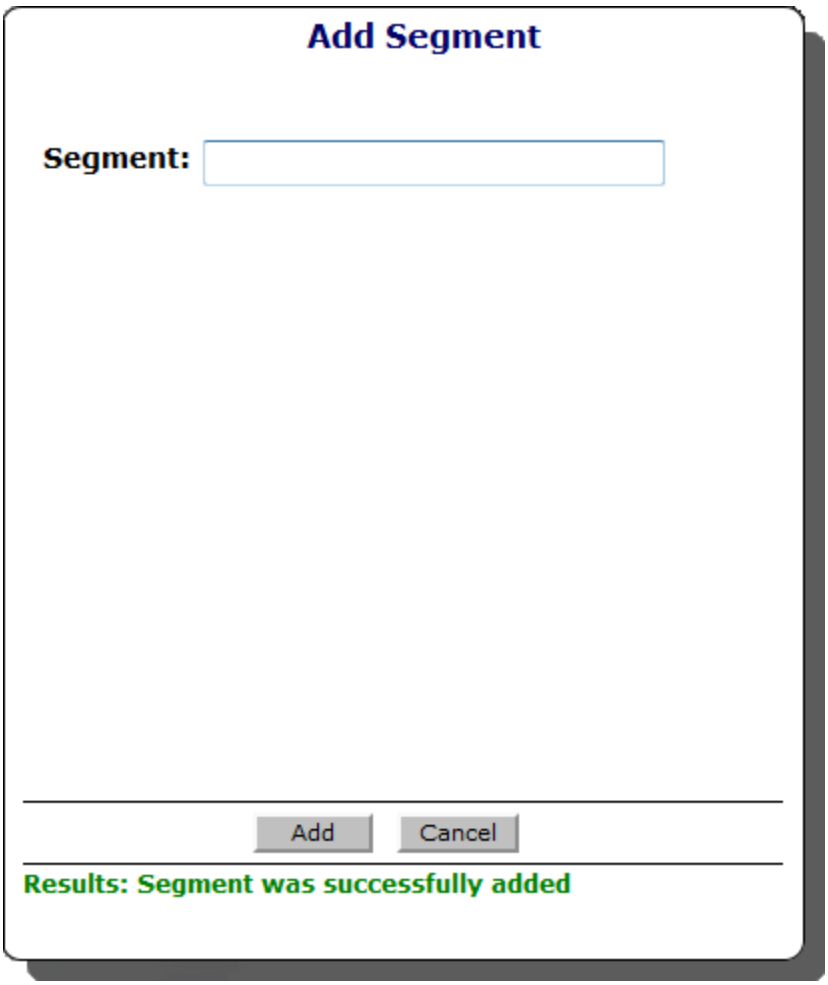


Figure 2.39 – Successful Segment Addition Display

Remove Segment

The “Remove Segment” menu selection located in the “Network” menu commands controls the ability to remove segments. Segments are used to organize your IMC network device selections. Removing a segment is a 2-step process: 1) Select the Segment(s) for deletion and 2) Remove the Segment information into the iView^2 database. **NOTE: Removing a segment will also remove any devices associated with that Segment.**

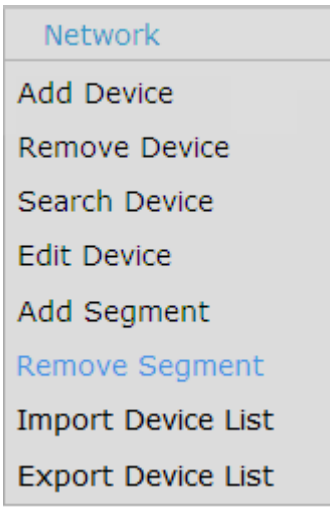


Figure 2.40 – Remove Segment Menu Command

1) Select the Segment(s) for deletion – Selections are made from the Remove Segment dialog as shown in figure 2.41. Each Segment in the Segment Network List is displayed using the Segment description. Use the mouse to click in the "Select" square to the right of the device description information. Every device with the "Select" square checked will be subject to removal.

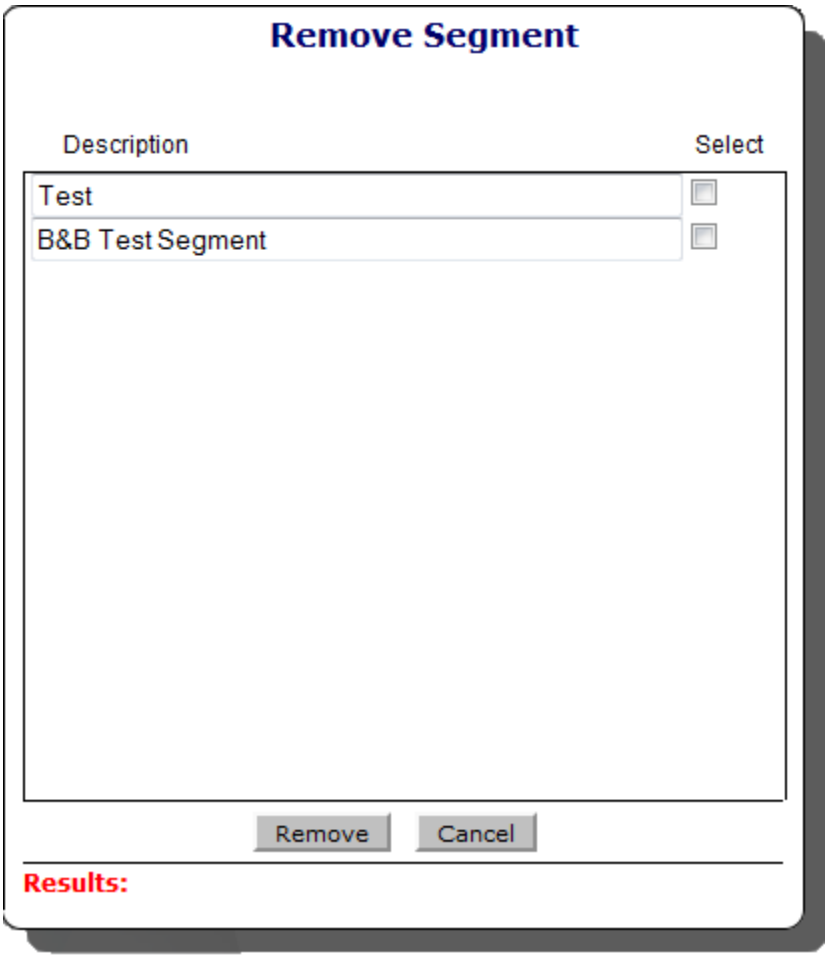


Figure 2.41 – Remove Segment Dialog

2) Remove the Segment information from the iView^2 database – After you have completed selecting the Segments to remove press the "Remove" command button. This will display a message box listing your selections and ask you if you are sure you want to remove the Segments(s), as shown in figure 3.6. Pressing the "OK" command button will execute the device removal process. Pressing the "Cancel" command button will bring you back to the main Remove Segment display. **NOTE: Removing a segment will also remove any devices associated with that Segment.**

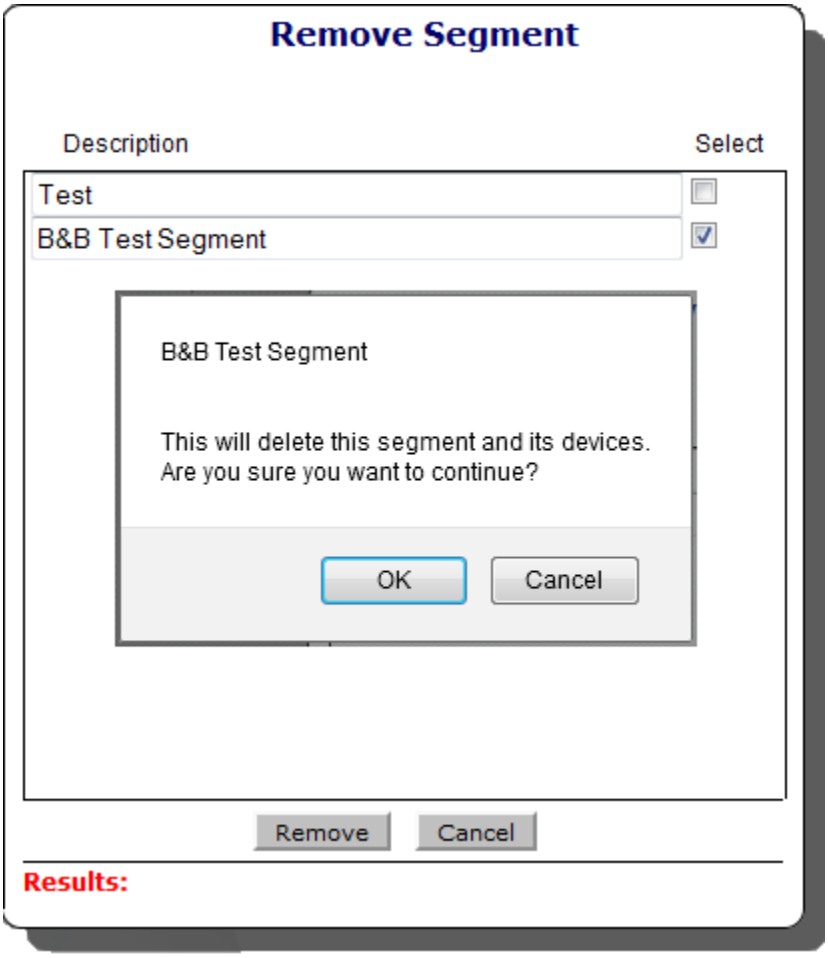


Figure 2.42 – Remove Segment Confirmation Display

Edit Segment

The “Edit Segment” menu selection located in the “Network” menu commands controls the ability to edit segment names. Segments are used to organize your IMC network device selections. Editing a segment is a 3-step process: 1) Select the Segment(s) to edit, 2) Enter the new Segment naming information, and 3) Select the “Save” command button.

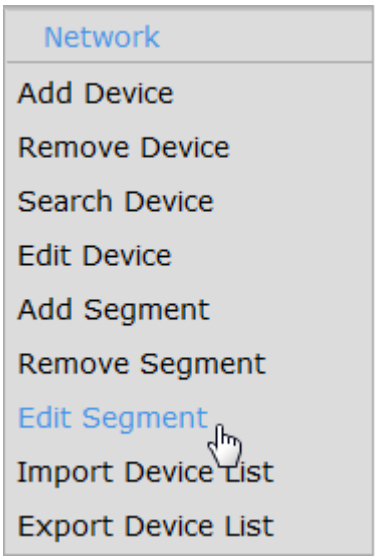


Figure 2.43 – Edit Segment Menu Command

1) Select the Segment(s) to edit – Selections are made from the Edit Segment dialog as shown in figure 2.44. Each Segment in the Segment Network List is displayed using the Segment description. Use the mouse to click in the “Select” square to the right of the Segment description information. Every device with the “Select” square checked will be subject to editing.

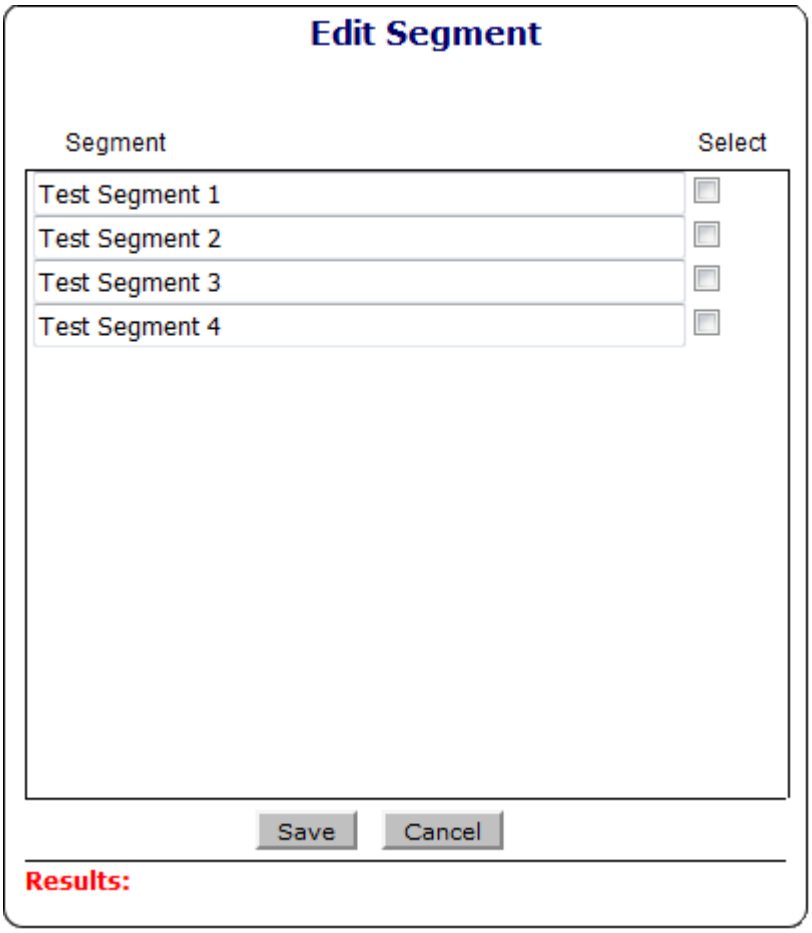


Figure 2.44 – Edit Segment Dialog

2) Enter the changes – Entered the desired Segment naming changes. Refer to figure 2.45, in this example we are changing “Test Segment 1” to “Test Segment 100”.

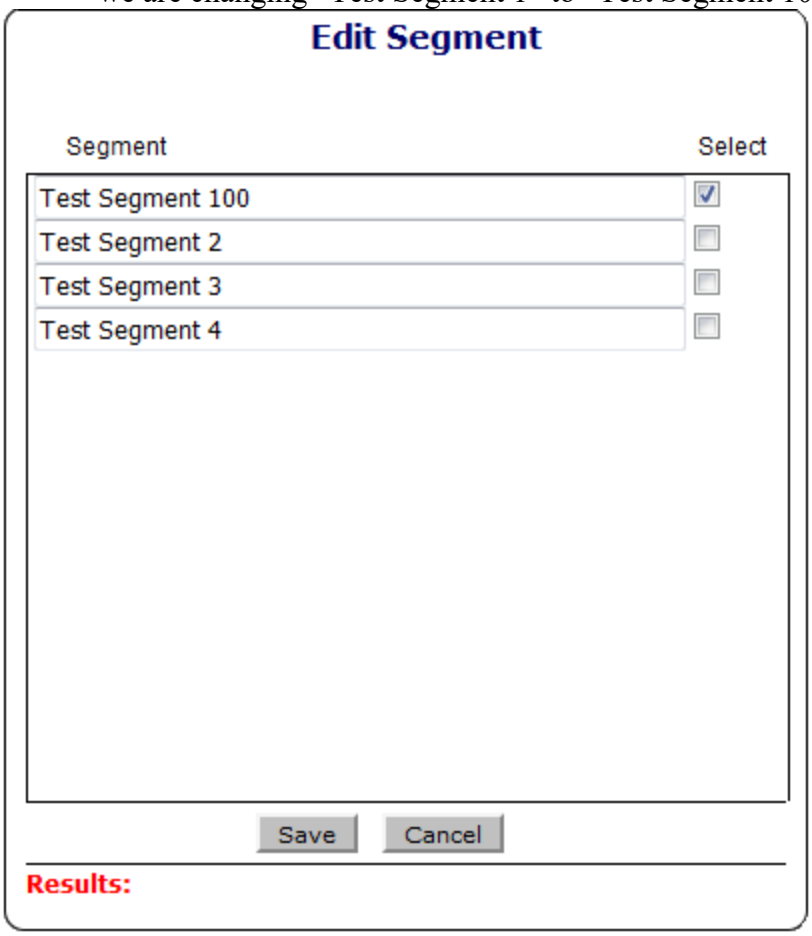


Figure 2.45 – Enter Segment name change

3) Save the changes – Select the “Save” command button to save the Segment naming changes to the database.

Import Device List

The “Import Device List” menu selection located in the “Network” menu commands controls the ability add devices to iView^2 using a comma separated value (csv) file. Selecting the "Import Device List" from the menu will display the "Import Device List" dialog box.

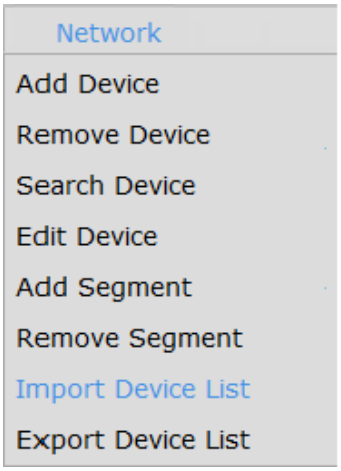


Figure 2.46 – Import Device List Menu Command

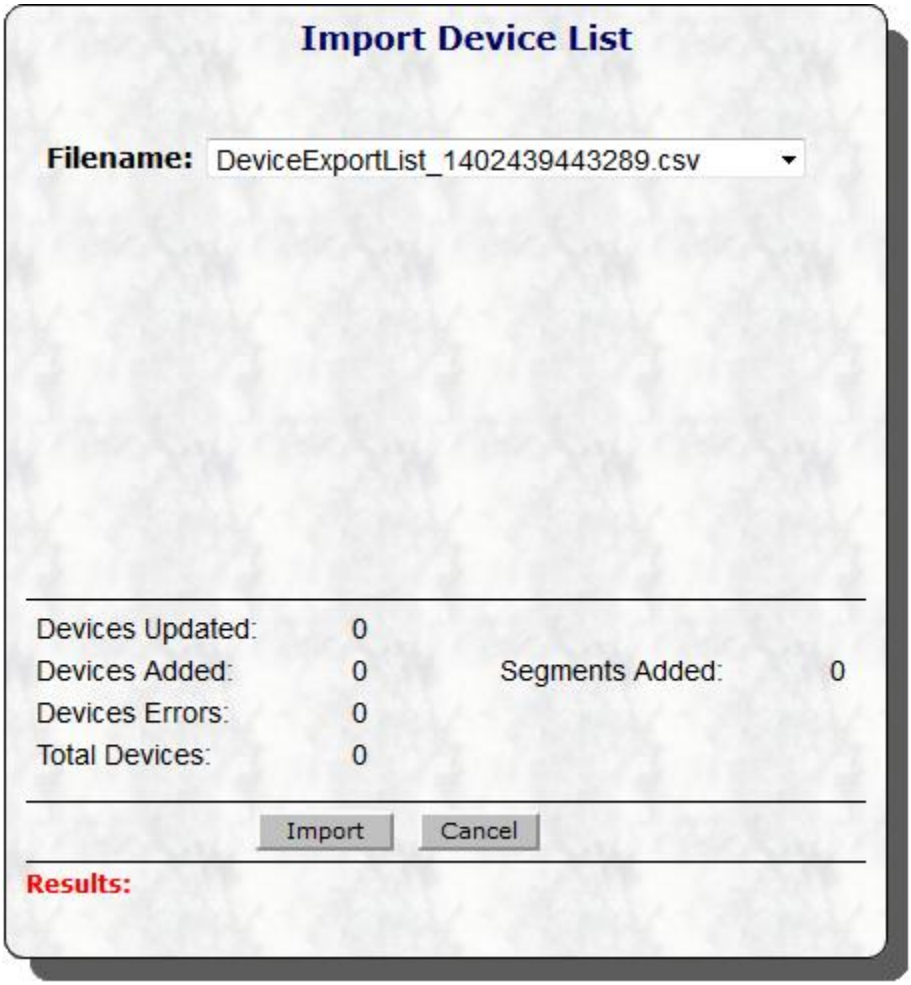


Figure 2.47 – Import Device List Dialog Box

The server will look into the "Import Files Path" identified in the iView^2 System Settings and bring back the last 10 device import files it finds. The "Import Device List" dialog box will display these in order from most current to least current. The user can select the file they want to import and press the "Import" control button. The file name selected by the user will be sent to the server. The server will read the file and extract the device information.

If a device is already contained in the "iview" database the following fields in the "device_tree_table" will be updated: nParentId, strIPAddress, strDNS, strMACAddress, strGetCommunity, strSetCommunity, strDeviceUser, and strDevicePassword will be updated with the information contained in the import file.

If the device is not in the "iview", the device will be added as new using the standard iView^2 Add Device functionality.

If the "Segment" listed for the device in the import file does not exist, iView^2 will create the segment and associate the device with it.

When iView^2 is done with the import it will display the following information to the user: "Devices Updated", "Devices Added", "Devices Errors", "Total Devices", and “Segments Added”.

Import Device List File Format

● The device list import file must have a “.csv” extension.
● The first row in the device list import file must contain the following column identifiers:
Device Id, Segment, Device Type, IP Address, Device Domain Name, MAC Address, Get Community, SET Community, Device User, Device Password
● The second row in the device list import file must contain the first device definition, for example:
5,North_Segment,iMediaChassis,10.30.8.162,,00:00:29:0E:1A:24,public,public,admin,admin
● Subsequent rows contain any other device definitions

Import Device List Column Definitions

Device Id – This is an integer value which uniquely identifies a device in the iView^2 database. New devices will contain a zero in this field.

Segment – This is a string value which uniquely identifies the segment that will group the device. This field must contain the unique name of an existing segment in iView^2 or the unique name of a new segment to add to iView^2.

Device Type – This is a string value which serves as a generic identifier for a family of devices. This field can be left as an empty string (““) if the device type is not known and will be filled in automatically by iView^2.

IP Address – This is a string value that will contain a properly formatted ip address. In the case where a device domain name will be used this to access the device, this field can be left as an empty string (“”).

Device Domain Name – This is a string value that will contain a properly formatted device domain name. In the case where an ip address will be used to access the device, this field can be left as an empty string (“”).

MAC Address – This is a string value that will contain a properly formatted mac address. This field can be left as an empty string (““) if the mac address is not known and will be filled in automatically by iView^2.
Get Community – This is a string value that will contain the get community name that will be used by iView^2 for SNMP get access.

Get Community – This is a string value that will contain the get community name that will be used by iView2 for SNMP set access.

Set Community – This is a string value that will contain the set community name that will be used by iView^2 for SNMP set access.

Device User – This is a string value that will contain the user name that will be used by iView^2 for device access authentication.

Device Password - This is a string value that will contain the user password that will be used by iView^2 for device access authentication.

Check – This is an optional column. If included, this column takes an integer value of 0 or 1. A 1 means that iView^2 should not try to access the device during installation because this device is not yet active on the network, but it should still be added. By default iView^2 will not add devices that it cannot access during installation. A 0 means that iView^2 should try to access the device during installation.

Export Device List

The “Export Device List” menu selection located in the “Network” menu commands controls the ability to export the devices listed in the iView[2] “Network Segment List” to a comma separated value (csv) file. Selecting the "Export Device List" from the menu will display the "Export Device List" dialog box.

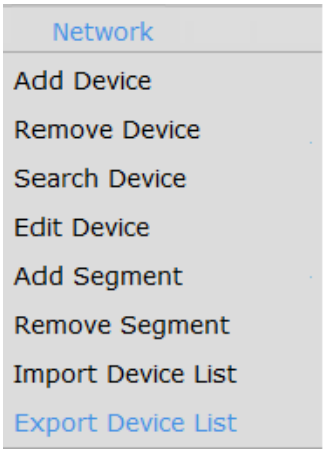


Figure 2.48 – Export Device List Menu Command

Figure 2.49 – Export Device List Dialog Box

A default file name is displayed with a ".csv" extension. The user can change the file name, but the ".csv" extension is required. Pressing the "Export" control button will display the "Please Wait" message while the request is sent to the server for processing. The server will create a comma separated value (csv) file listing all the devices in the iView^2 “Network Segment List" display. This file will be stored in the "Export Files Path" identified in the iView^2 “System Settings”.

Tools Menu Items

Inventory Report

The “Inventory Report” menu selection is located in the “Tools” menu commands. This command will display a list of the devices contained in the “iView Network Segment List”. The devices are displayed in a paged manner. The size of the page is determined by the “Devices Per Page” setting as shown in Figure 3.2. The user can page forward and backwards to view the devices.

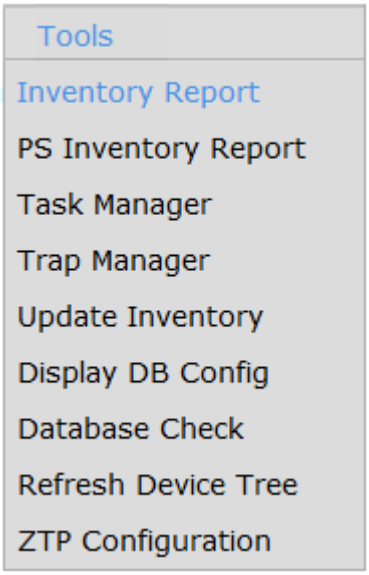
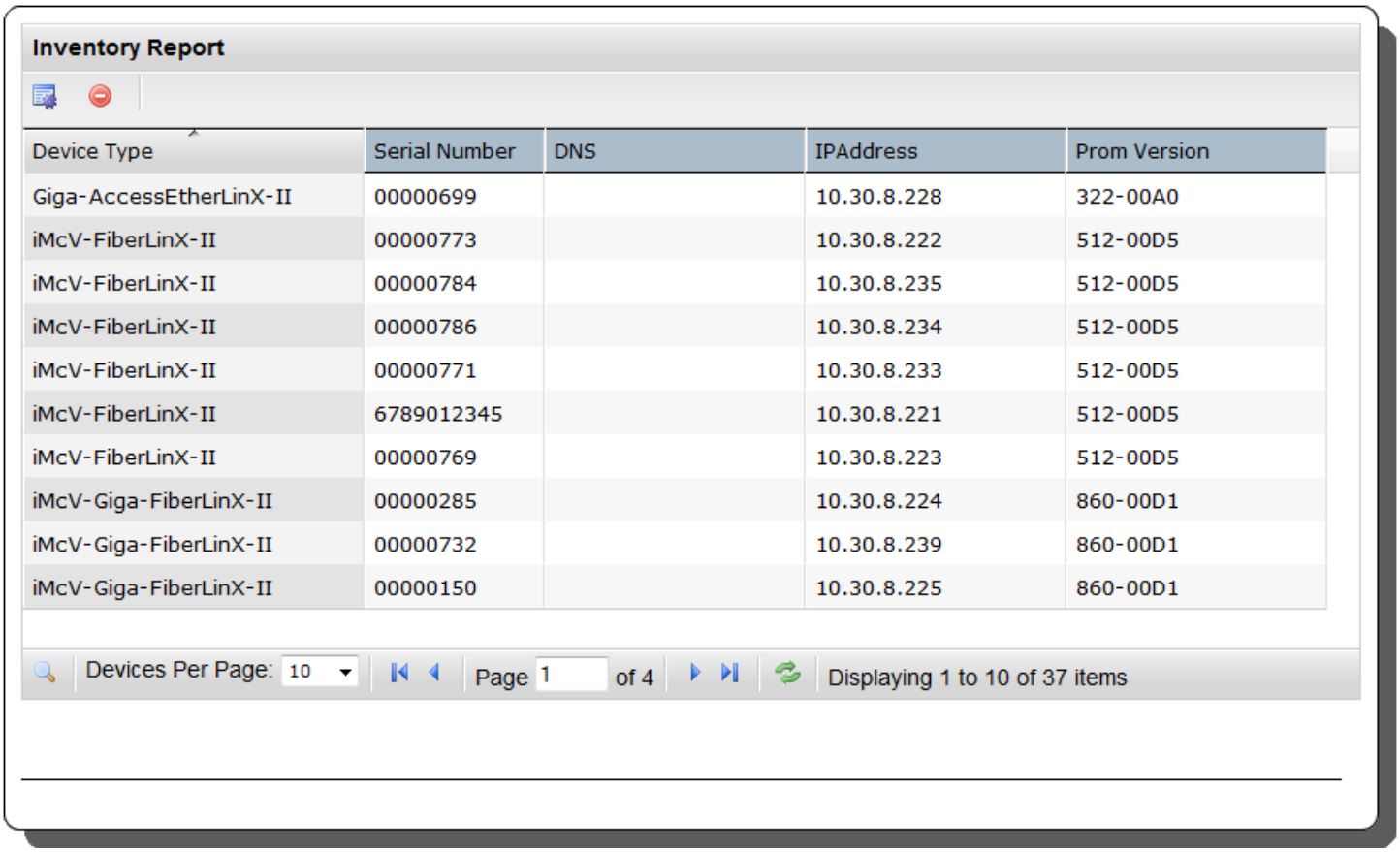


Figure 3.1 – Inventory Report Command



Inventory Report

Device Type	Serial Number	DNS	IPAddress	Prom Version
Giga-AccessEtherLinX-II	00000699		10.30.8.228	322-00A0
iMcV-FiberLinX-II	00000773		10.30.8.222	512-00D5
iMcV-FiberLinX-II	00000784		10.30.8.235	512-00D5
iMcV-FiberLinX-II	00000786		10.30.8.234	512-00D5
iMcV-FiberLinX-II	00000771		10.30.8.233	512-00D5
iMcV-FiberLinX-II	6789012345		10.30.8.221	512-00D5
iMcV-FiberLinX-II	00000769		10.30.8.223	512-00D5
iMcV-Giga-FiberLinX-II	00000285		10.30.8.224	860-00D1
iMcV-Giga-FiberLinX-II	00000732		10.30.8.239	860-00D1
iMcV-Giga-FiberLinX-II	00000150		10.30.8.225	860-00D1

Devices Per Page: 10 Page 1 of 4 Displaying 1 to 10 of 37 items

Figure 3.2 Inventory Report Example Display

Inventory Report Controls Icons

- Export Inventory Report to file

- Close Inventory Report dialog

- Display Inventory Search

- Refresh Inventory Report display

- Page Control, go to first page

- Page Control, go to last page

- Page Control, go to previous page

- Page Control, go to next page

Export Inventory Report

This allows the user to export the rows of data in an Inventory Report list. Access to this functionality is controlled through the "Export Control Icon" . When the user selects the "Export Control Icon" the "Export Format" dialog will be displayed as shown in Figure 3.3. Here the user can change the output filename or choose column options. The columns listed in the "Column Options" are associated with Inventory Report list. Pressing the "Export" control button will cause the system to create the file and store it to the "Exports Files Path" contained in the iView[2] "System Settings".

The default "Filename" displayed includes the text "Inventory_Export_" followed by the month, day, and year with a ".csv" filename extension. To change the default "Filename", click on the default filename with the mouse, an input element will display with a blue outline, enter the new filename, and then click on the input element with the mouse to close it. This will remove the blue outline around the input element and display the new filename.

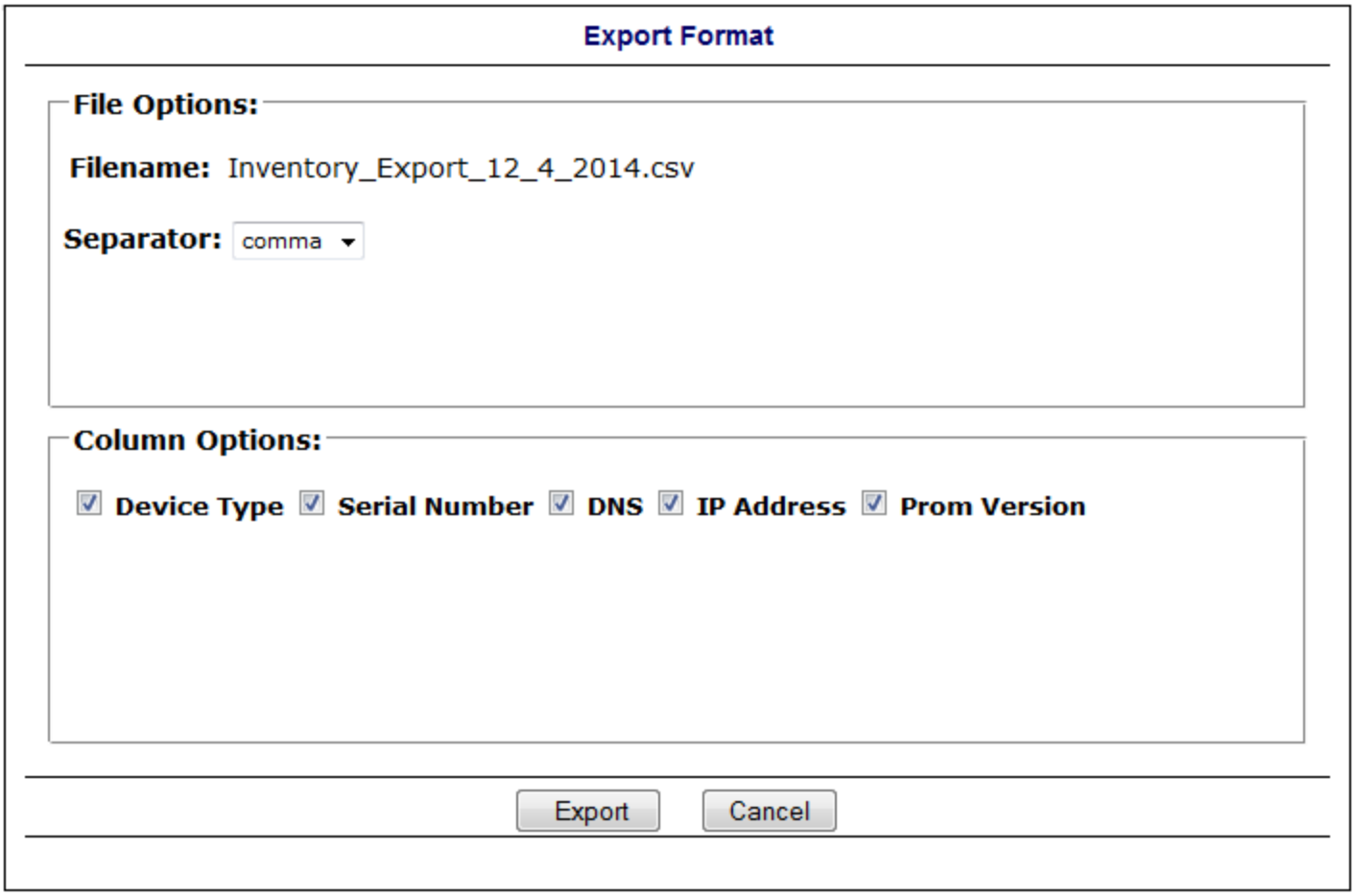


Figure 3.3 – Export Format dialog

Search Inventory Report

To access the search functionality in the Inventory Report display, press the icon in the lower left of the Inventory Report dialog.

To perform a search, enter the search term in the “Find” input area, select the column to search on from the drop down, and press the enter key. To clear the search criteria press the Clear command button.

To close the search display, press the icon.

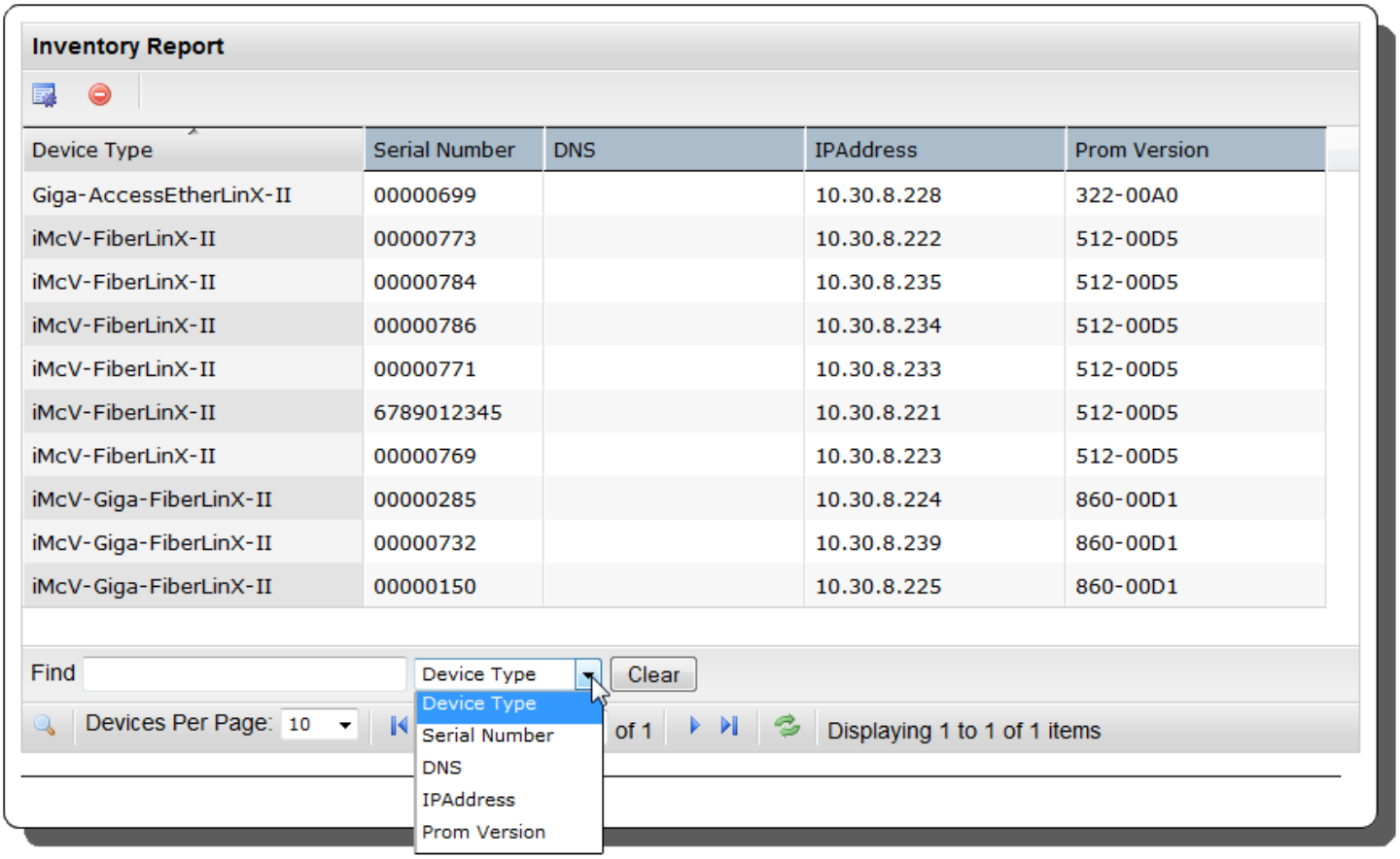


Figure 3.4 – Search Inventory Report

PS Inventory Report

The “PS Inventory Report” menu selection is located in the “Tools” menu commands. This command will display a list of manually entered Power Supply identification information for iMediaChassis 3/6/20. The devices are displayed in a paged manner. The size of the page is determined by the “Devices Per Page” setting as shown in Figure 3.5. The user can page forward and backwards to view the device specific information.

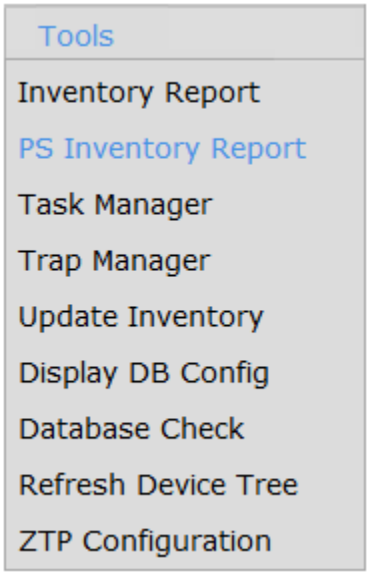
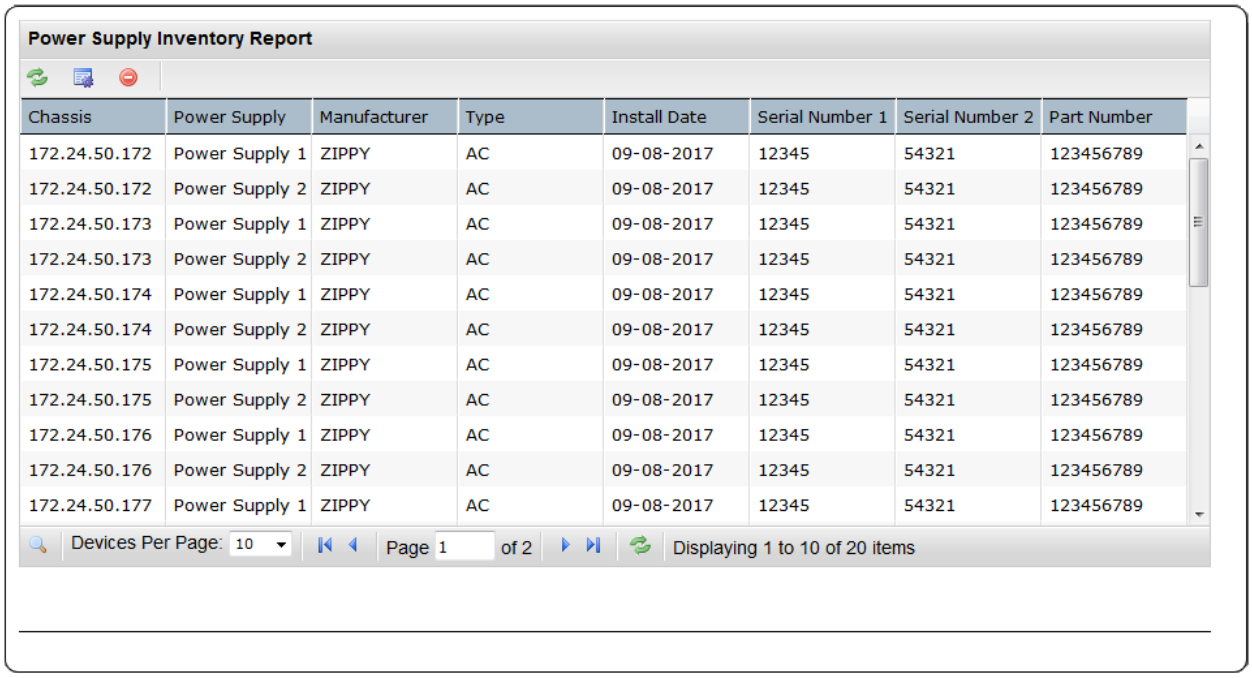


Figure 3.5 – PS Inventory Report Command



Power Supply Inventory Report

Chassis	Power Supply	Manufacturer	Type	Install Date	Serial Number 1	Serial Number 2	Part Number
172.24.50.172	Power Supply 1	ZIPPY	AC	09-08-2017	12345	54321	123456789
172.24.50.172	Power Supply 2	ZIPPY	AC	09-08-2017	12345	54321	123456789
172.24.50.173	Power Supply 1	ZIPPY	AC	09-08-2017	12345	54321	123456789
172.24.50.173	Power Supply 2	ZIPPY	AC	09-08-2017	12345	54321	123456789
172.24.50.174	Power Supply 1	ZIPPY	AC	09-08-2017	12345	54321	123456789
172.24.50.174	Power Supply 2	ZIPPY	AC	09-08-2017	12345	54321	123456789
172.24.50.175	Power Supply 1	ZIPPY	AC	09-08-2017	12345	54321	123456789
172.24.50.175	Power Supply 2	ZIPPY	AC	09-08-2017	12345	54321	123456789
172.24.50.176	Power Supply 1	ZIPPY	AC	09-08-2017	12345	54321	123456789
172.24.50.176	Power Supply 2	ZIPPY	AC	09-08-2017	12345	54321	123456789
172.24.50.177	Power Supply 1	ZIPPY	AC	09-08-2017	12345	54321	123456789

Devices Per Page: 10 Page 1 of 2 Displaying 1 to 10 of 20 items

Figure 3.6 – iView^2 Power Supply Inventory Report

PS Inventory Report Controls Icons

- Export PS Inventory Report to file

- Close PS Inventory Report dialog

- Display PS Inventory Search

- Refresh PS Inventory Report display

- Page Control, go to first page

- Page Control, go to last page

- Page Control, go to previous page

- Page Control, go to next page

NOTE: PS Inventory controls function as described in the “Inventory Report” section.

Task Manager

The Task Manager is used to control PROM Firmware Updates, Configuration Backups, and Configuration Restores to multiple SNMP agent-based devices. The Task Manager is accessed through the "Tools" top level menu as shown in Figure 3.7.

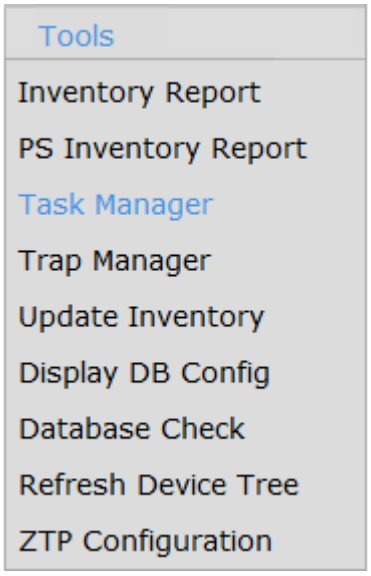


Figure 3.7 – Tools top level menu option for Task Manager

The Task Manager menu selection will display the "Task Manager" report display as shown in Figure 3.8. This report display will contain the list of tasks that have been created. The user can scroll through the list of tasks. The user can choose to archive tasks that have completed The user can add a PROM Firmware Update, Configuration Backup, or Configuration Restore task, export the list of tasks, print the list of tasks, or manually refresh the list of tasks.

Figure 3.8 – Task Manager Report Display

Task Manager Control Icons

- Add Task Control Icon: This control icon will allow the user to create a PROM firmware Update Task.

- Export Control Icon: This control icon will allow the user to export the data in the Report Display list to a comma separated file.

- Print Control Icon: This control icon will allow the user to print the data in the Report Display list.

- Refresh Control Icon: This control icon will allow the user to update the data in the Report Display list.

- Previous Report Control Icon: This control icon will allow the user to return to the previous report.

- Column Sort Ascending Control Icon: This control icon will allow the user to sort the data in the Report Display list from low to high.

- Column Sort Descending Control Icon: This control icon will allow the user to sort the data in the Report Display list from high to low.

- Cancel Control Icon: This control icon will allow the user to cancel pending tasks or task items.

- Polling Control Icon: This control icon signals to the user that the “Task Manager” or “Task Manager – Task Details” display is being updated.

Export Report Display

This allows the user to export the rows of data in a Report Display list. Access to this functionality is controlled through the "Export Control Icon" . When the user selects the "Export Control Icon" the "Export Format" dialog will be displayed as shown in Figure 3.9. Here the user can change the output filename, select a data separator, or choose column options. The columns listed in the "Column Options" are associated with the individual Report Display list. Pressing the "Export" control button will cause the system to create the file and store it to the "Exports Files Path" contained in the iView[2] "System Settings".

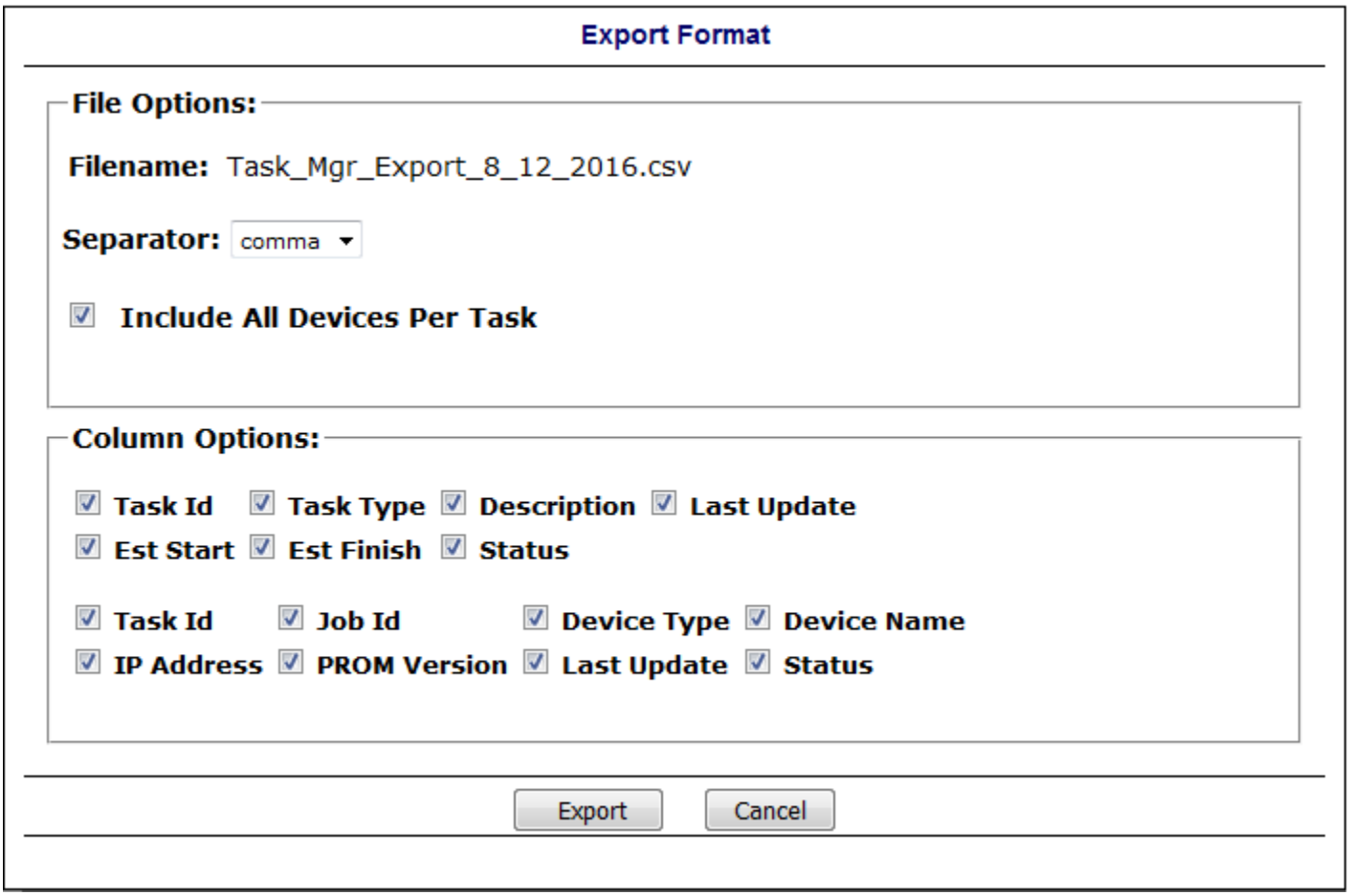


Figure 3.9 – Export Format Dialog

Print Report Display

This allows the user to print the rows of data in a Report Display list. Access to this functionality is controlled through the "Print Control Icon" . When the user selects the "Print Control Icon" a system print dialog will display allowing the user to select the printer where the document will be printed.

Task Id	Job Id	Device Type	Device Name	IP Address	PROM Version	Last Update	Status
8	49	17	FiberLinX-II - 192.168.10.223	192.168.10.223	89_2013-04-01-16-32-04.cfg	2013-04-12 13:56:38	Cancelled
8	50	17	FiberLinX-II - 192.168.10.216	192.168.10.216	82_2013-04-01-16-32-04.cfg	2013-04-12 13:56:38	Cancelled
8	51	17	FiberLinX-II - 192.168.10.221	192.168.10.221	87_2013-04-01-16-32-04.cfg	2013-04-12 13:56:38	Cancelled

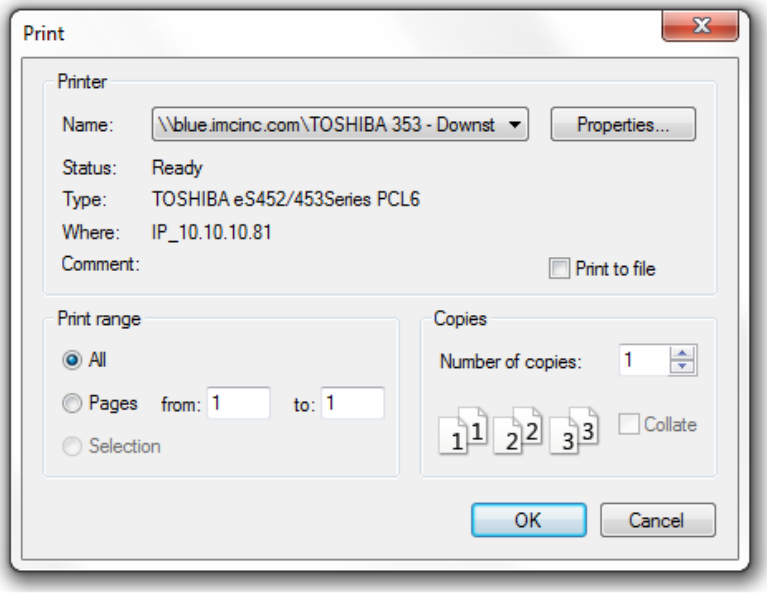


Figure 3.10 – Example System Print Dialog

Task Manager - Report Display

The “Task Manager” report display contains the list of tasks that have been created. This page will automatically refresh every 5 seconds. The user can access the “Task Manager Control Icons” in the upper left of the report display to perform operation on the displayed rows of data. By default this report display will hide tasks that have been archived. To display archived tasks uncheck the “Hide Archive Items” checkbox.

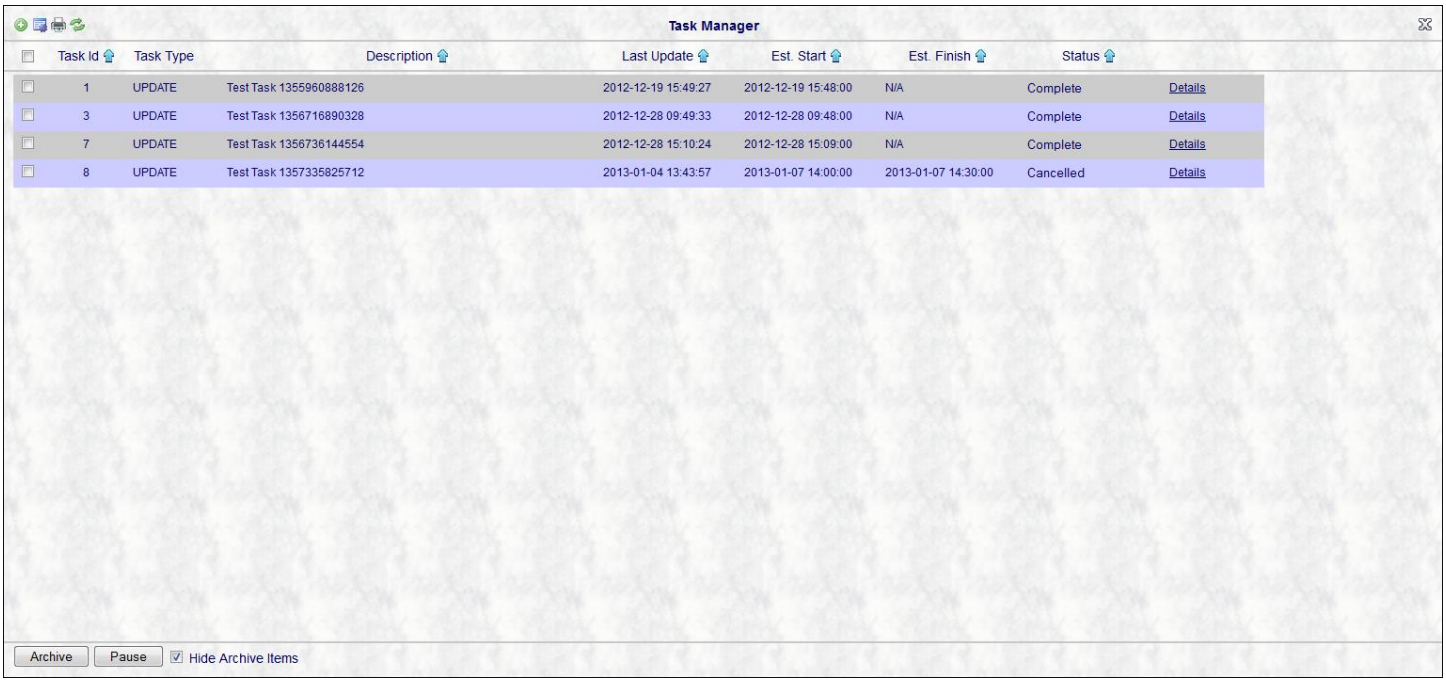


Figure 3.11 - Task Manager Report Display

Task Manager – Task Details Report Display

The "Task Manager – Task Details" report display contains the list of individual task items associated with a task. The user can access this report display by selecting the Details control in a task row in the "Task Manager" report display.

Figure 3.12 – "Task Manager – Task Details" Report Display

The “Task Manager – Task Details” report display contains an additional control selection which allows the user to display or hide the scheduling information associated with a Task. The ☑ Hide Task Schedule selection is checked by default which hides the scheduling information. Use the mouse to uncheck the “Hide Task Schedule” to display the scheduling information.

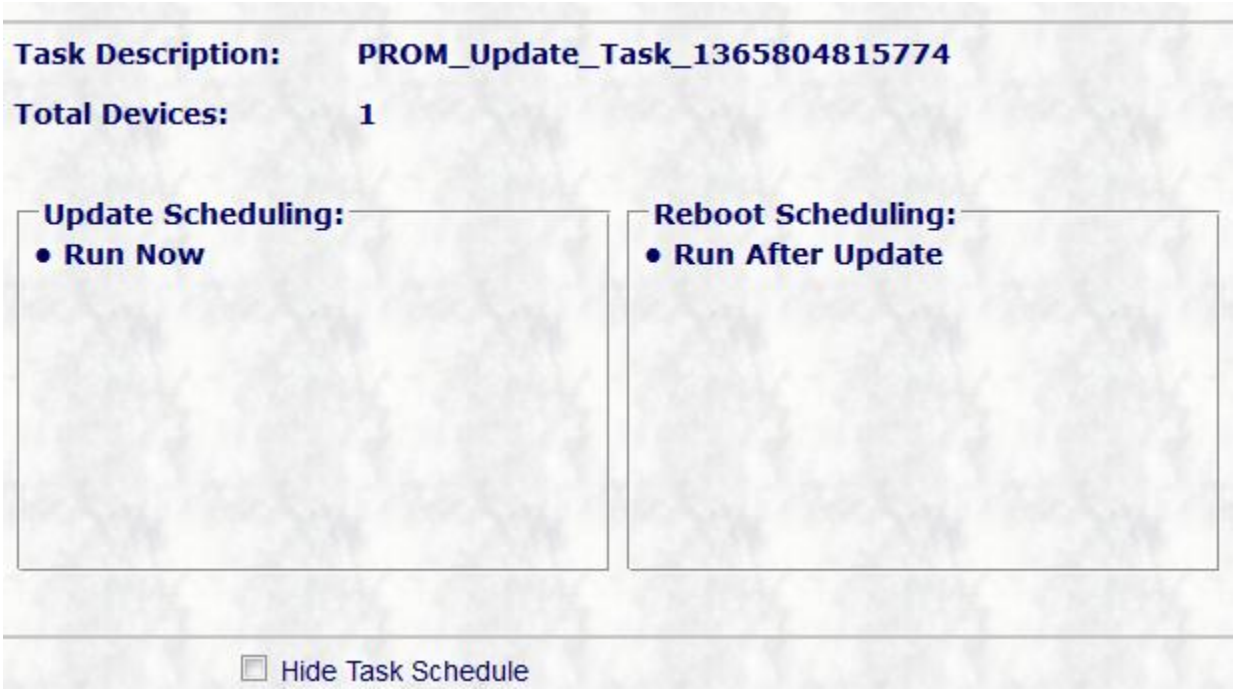


Figure 3.13 – “Task Manager – Task Details” Task Schedule display

Cancel Task

Tasks that have a status of “Scheduled” or “In Progress will display a “Cancel Task” control icon . This “Cancel Task” control icon allows the user to cancel the task. If the user presses the “Cancel Task” control icon, task items that are currently processing will be allowed to complete. All other task items in the task will receive a status of “Cancelled” and will not be run by iView[2].

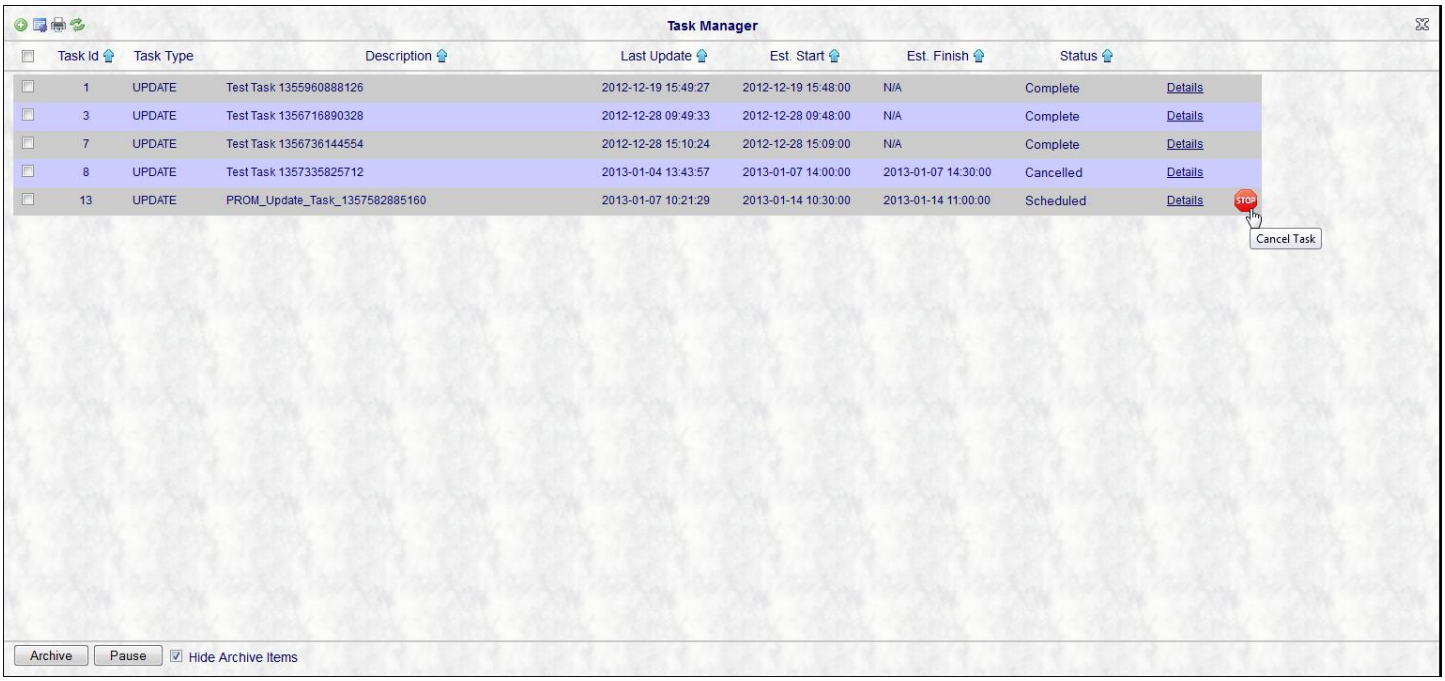


Figure 3.14 – Example Cancel Task Control Icon Display

Cancel Task Item

Task Items that have a status of “Scheduled” will display a “Cancel Task Item” control icon . This “Cancel Task Item” icon allows the user to cancel the specific task item. If the user presses the “Cancel Task Item” control icon iView[2] will cancel that task item from the running task and change the task item “Status” to “Cancelled”.

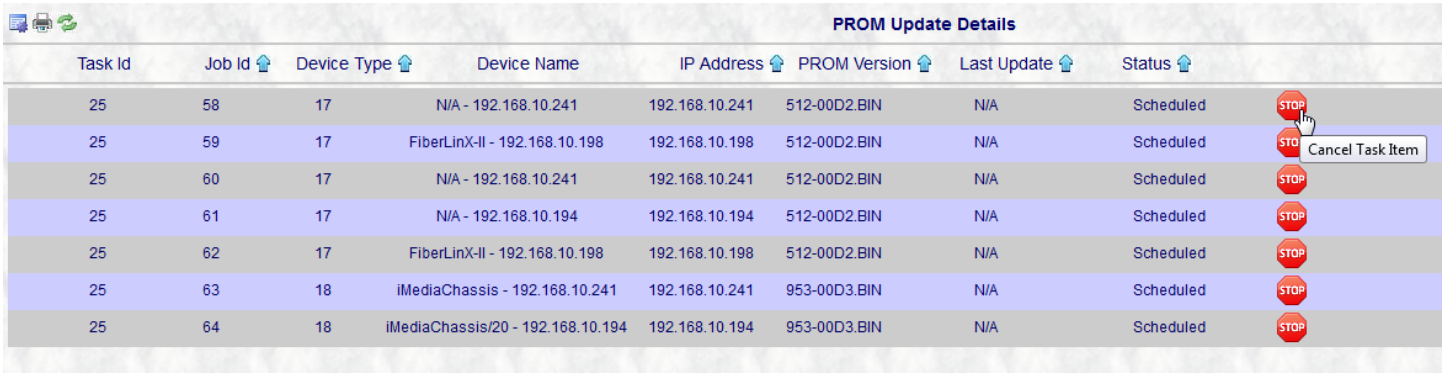


Figure 3.15 – Cancel Update Task Item Report Display

Create PROM Update Task

Step 1)

Adding a task for automated PROM updates to multiple SNMP agent-based devices is controlled through the "Add Task" control icon and the "Add Task" selection menu. The "Add Task" control icon is located in the top left corner of the Task Manager Report Display. Figure 3.16 shows the control icon display for the Task Manager Report Display. Move the mouse over the "Add Task" control icon until the cursor changes to the pointer and click on the control icon. This will display the "Add Task" selection menu as shown in Figure 3.17. From the "Add Task" selection menu choose "PROM Update" with the mouse and click the selection to display the devices available for update.

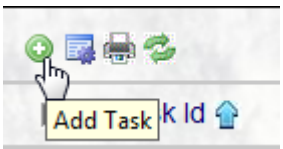


Figure 3.16 – "Add Task" Control Icon

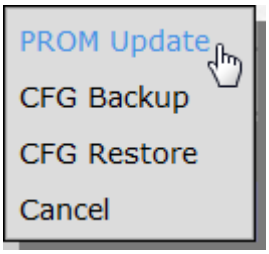


Figure 3.17 – "Add Task" Selection Menu

Step 2) – Display the Task Editor

The "PROM Update" selection from the "Add Task" Selection Menu will display the "Task Editor" dialog. The "Task Editor" is where the "Task Description" can be set, devices can be added or removed from a task, the task schedule can be set, and the task can be submitted for processing. For new tasks, the "Task Editor" will not contain any devices in the task. Devices are added to a task using the "Add Device(s)" command button. Press the "Add Device(s)" command button to display the list of available devices.

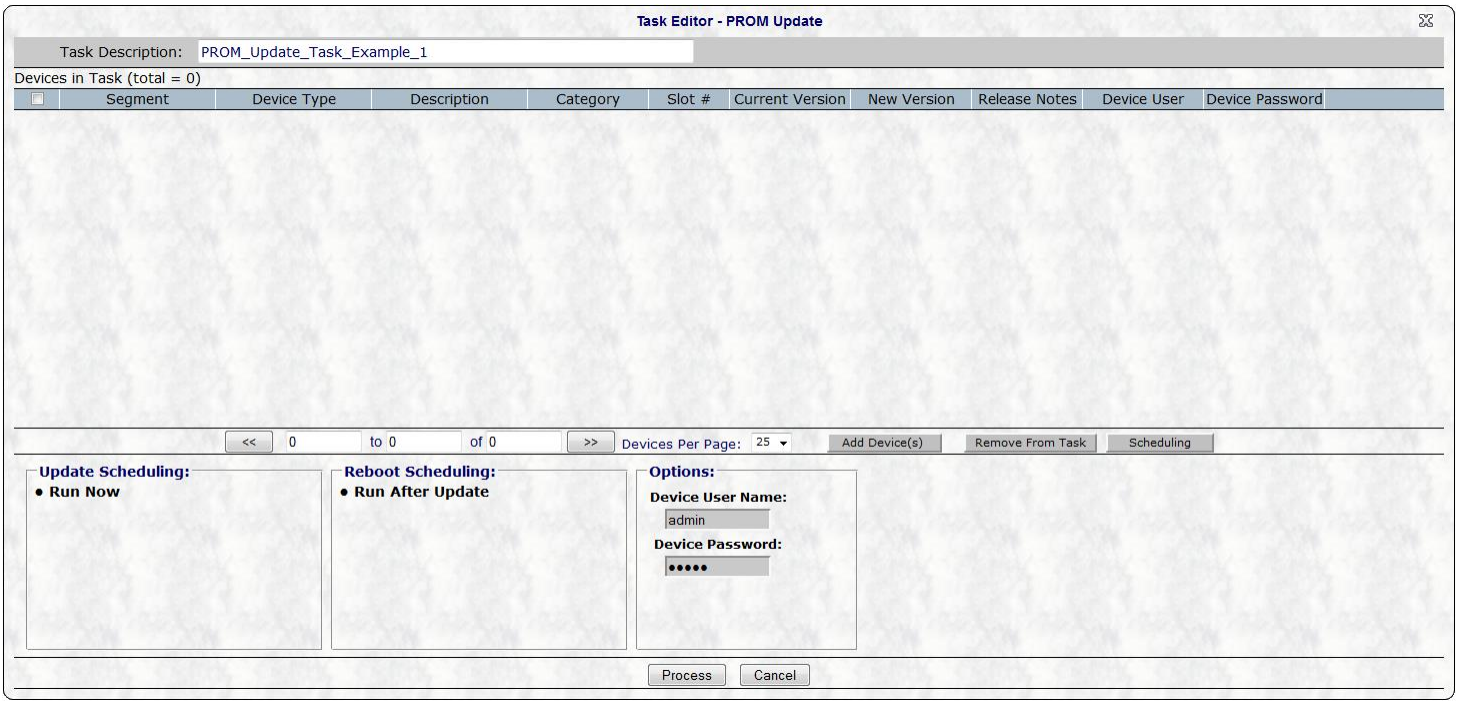


Figure 3.18 – Task Editor Dialog for PROM Update

Step 3) – Select Devices to Add to the Task

The "Add Device(s)" command button will display the "Task Editor – Device Search Results" dialog. This is where devices are selected for the task. To add a device to the task, select the checkbox to the left of the device you want to add and then press the "Save To Task" command button. You selection will be removed from the Task Editor – Device Search Results" dialog and added to the task. Now press the "Cancel" command button.

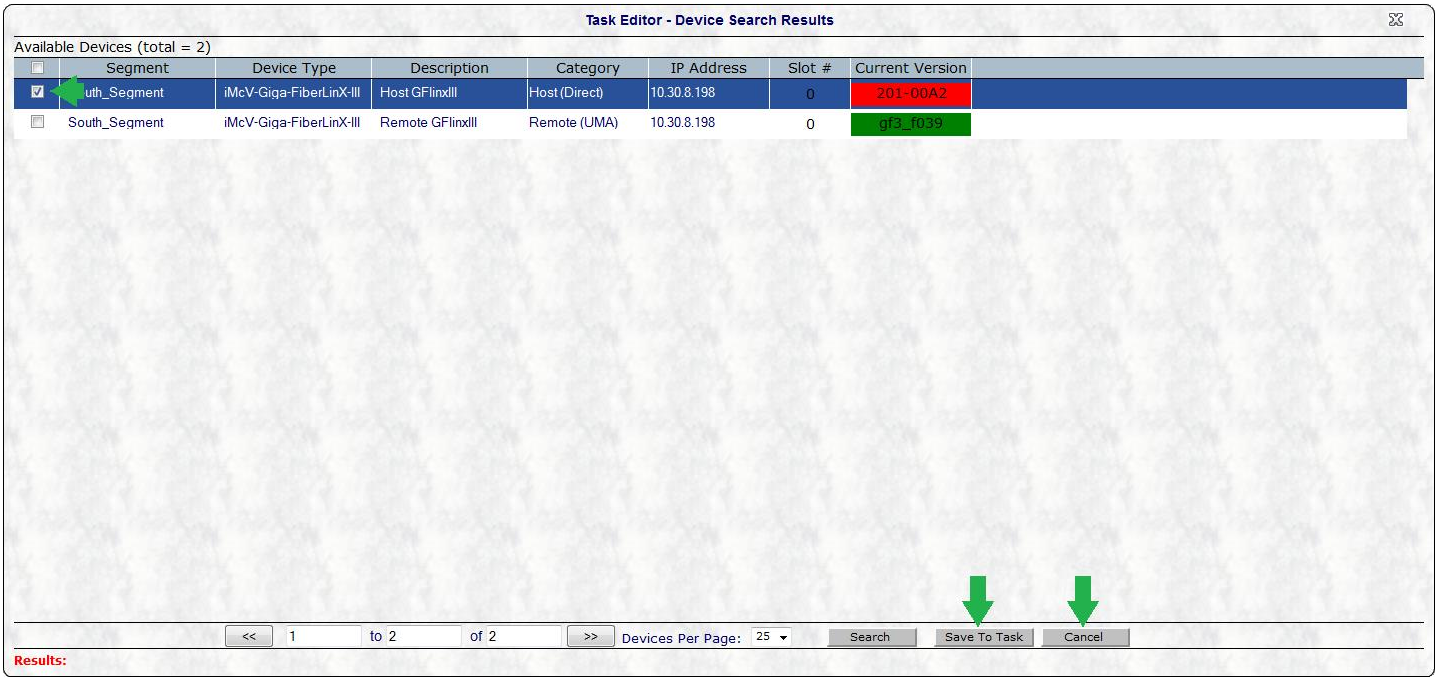


Figure 3.19 – "Task Editor – Device Search Results" dialog

Step 4) – Set the Scheduling

Pressing the “Cancel” command button will close the “Task Editor – Device Search Results” dialog and re-display the “Task Editor”. The device(s) you selected will now be displayed. By default, the scheduling is set to run immediately. Scheduling is controlled through the “Scheduling” command button. Press the “Scheduling” command button to display the “PROM Update Task Scheduling Settings” dialog. Refer to the “Task Scheduling Options” for more detailed information about task scheduling.

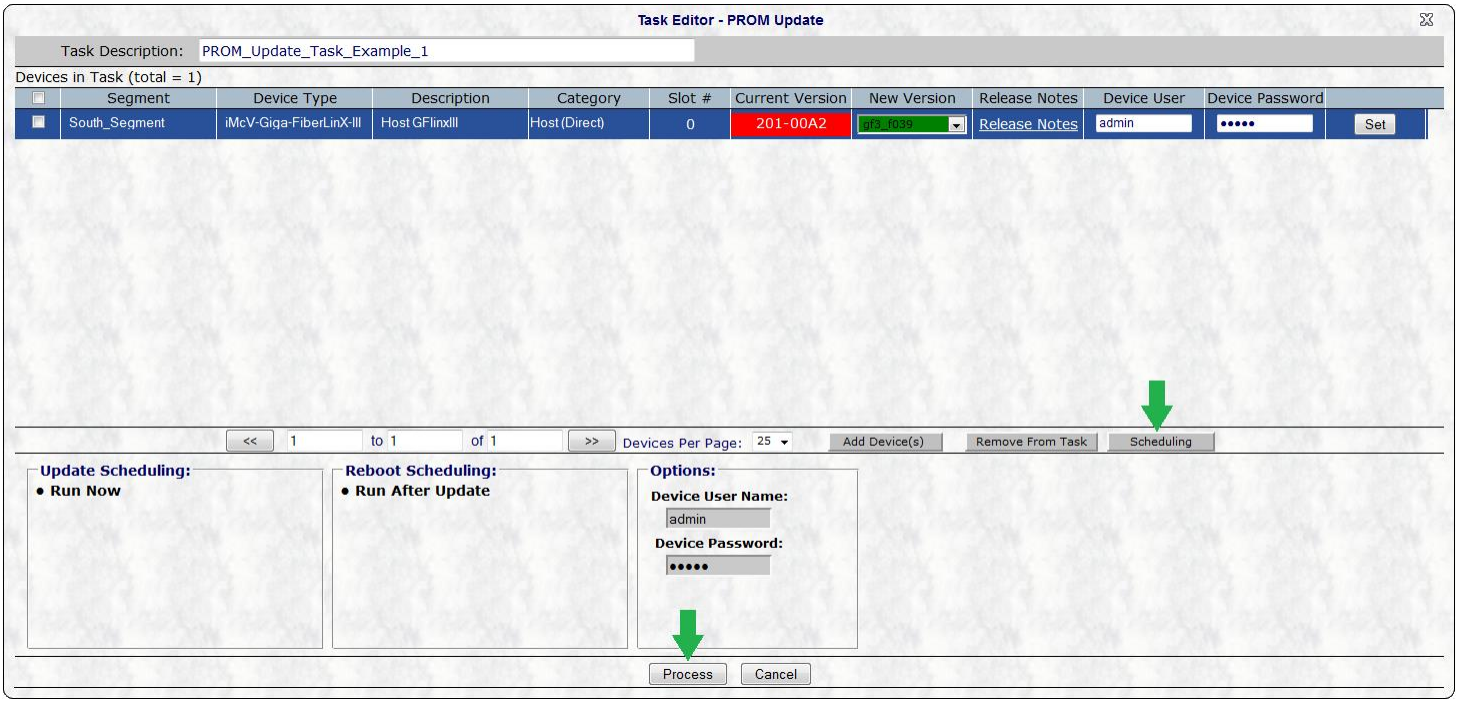


Figure 3.20 – “Task Editor - PROM Update” - Scheduling

Step 5) – Process the Task

Once the devices have been added and the scheduling set it is now time to submit the task for processing. This is controlled by the “Process” command button located at the bottom of the “Task Editor – PROM Update” dialog. Press the “Process” command button to complete the task creation and submit the task for processing. The “Task Editor - PROM Update” dialog will be closed and the new task will display in the “Task Editor” as shown in figure 3.21.

Figure 3.21 – Task Editor with new task

Once the user has made their selections and set the “Scheduling” options they will press the “Next” control button in the lower left corner of the Report Display as shown in Figure 3.22.

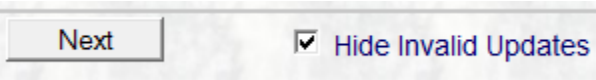


Figure 3.22 – Next Control Button

Trap Manager

Users can configure their trap functionality by choosing the “Trap Manager” menu item under the “Tools” menu category.

NOTE: The “Trap Manager” menu is only for “B&B Devices”.

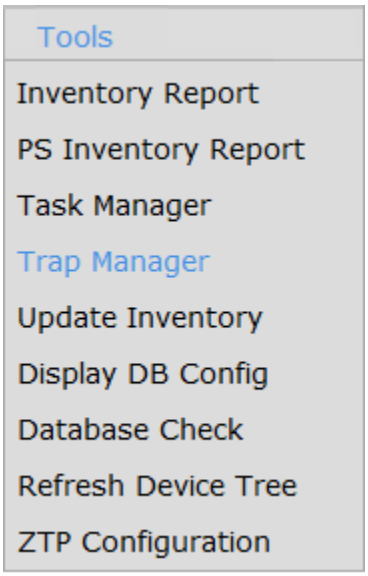


Figure 3.23 – Trap Manager Menu Item

The “Trap Manager” allows a user to Enable or Disable trap listening and to choose the types of traps they want to receive. The user can navigate through their various network segments by using the “Segment” dropdown list. When a different network segment is selected the “Devices” dropdown list will also update. Figure 3.24 shows the default user interface.

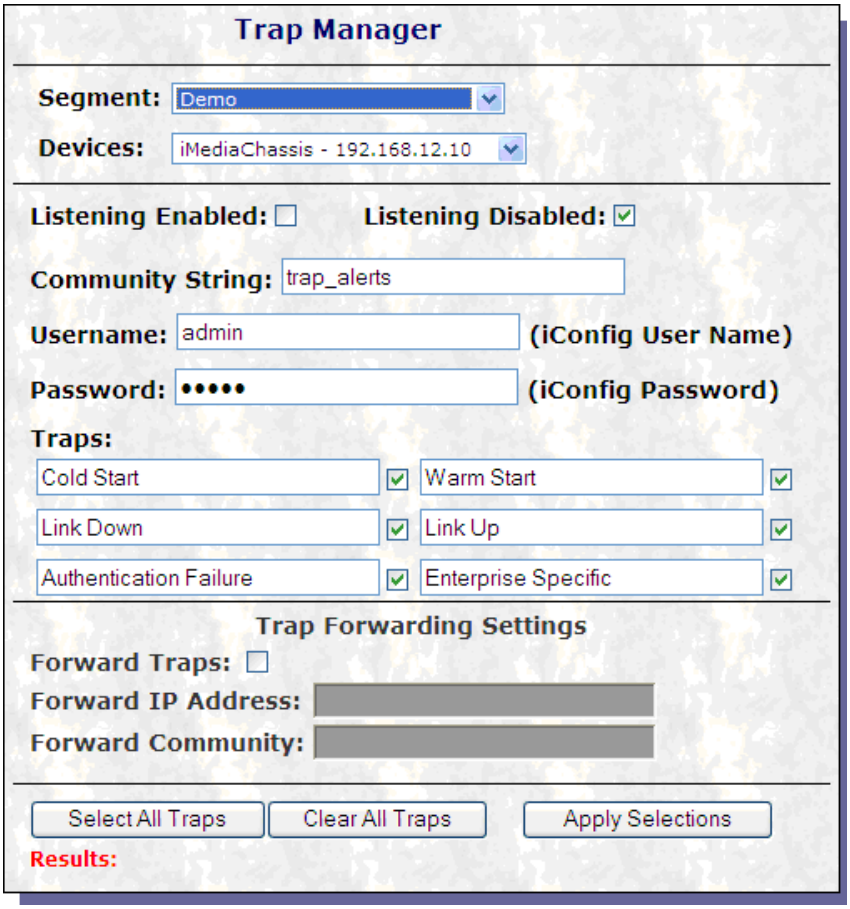


Figure 3.24 – Default Trap Manager User Interface

Trap Forwarding

The iView^2 also allows a user to forward traps received from IMC Networks devices to another IP Address. To enable Trap Forwarding the user will first click the "Forward Traps:" checkbox. Next the user will enter a "Forward IP Address" and a "Forward Community" name. To save the settings the user will click the "Apply Selections" command button. Once the user clicks the "Apply Selections" command button iView^2 will attempt to save the configuration values. The results of the "Apply Selections" operation will be displayed in the "Results:" section of the Trap Manager User Interface.

Once iView^2 is able to successfully store the trap forwarding configuration values every trap received by iView^2 from the configuration device will be forwarded to the configured "Forward IP Address". All forwarded traps will include 2 additional binding fields "Original Host Name" and "Original Source IP Address". The "Original Host Name" field will contain the device naming information that identifies the particular device in the "iView Network Segment List". The "Original Source IP Address" contains the IP Address of the device that originally generated the trap.

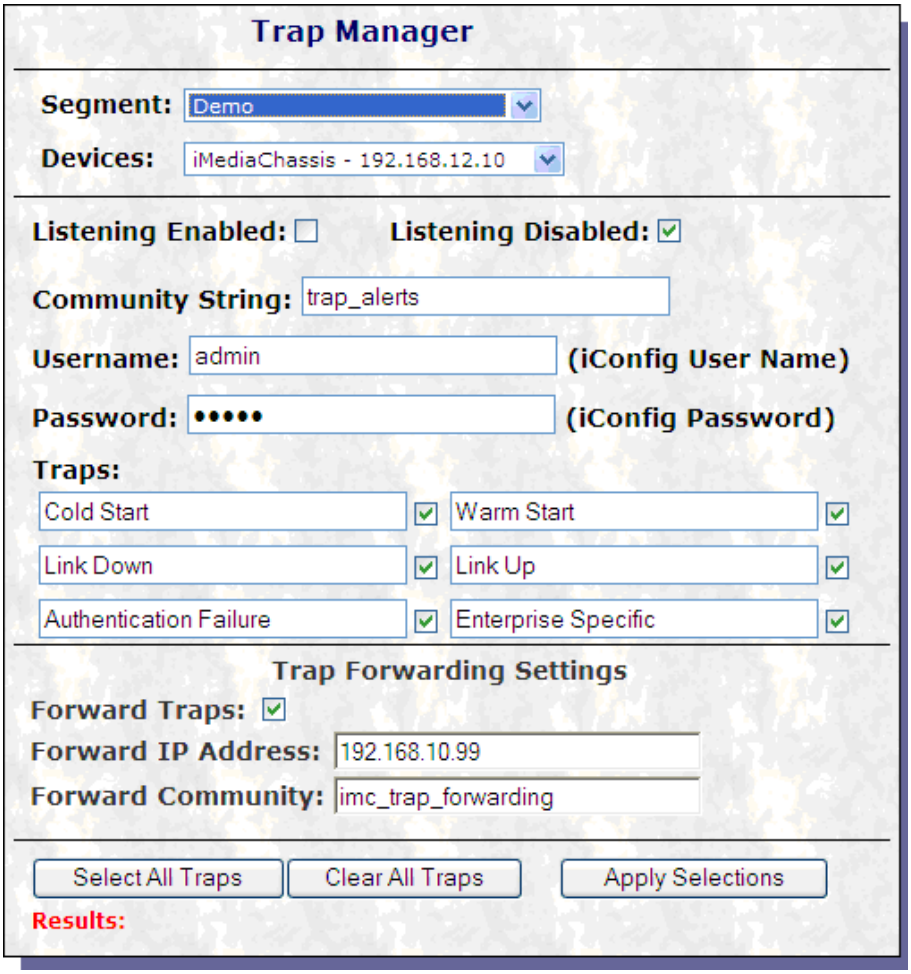


Figure 3.25 – Example Trap Forwarding Settings

Trap Management Reporting

Once a user has configured the trap management they can view received trap information using the trap reporting functionality. The trap reporting functionality is accessed by clicking on the “Alerts” image, which is located in the header area as shown in figure 3.26.

Figure 3.26– Default “Alerts” image

When traps are reported on an active device the “Alerts” image will flash.

Figure 3.27 – Example “Alerts” flash image

Using the mouse to click on the “Alerts” image will display the trap reporting dialog. The standard trap information displayed for an individual trap includes the received date and time, the host sending the trap information, and a description of the trap. Users can use the checkbox at the beginning of each trap row to select that trap for archiving. Users can use the “Select All” option to select all the listed traps for archiving. NOTE: Choosing to archive a trap does not remove it from the database it will only cause the trap information not to be displayed.

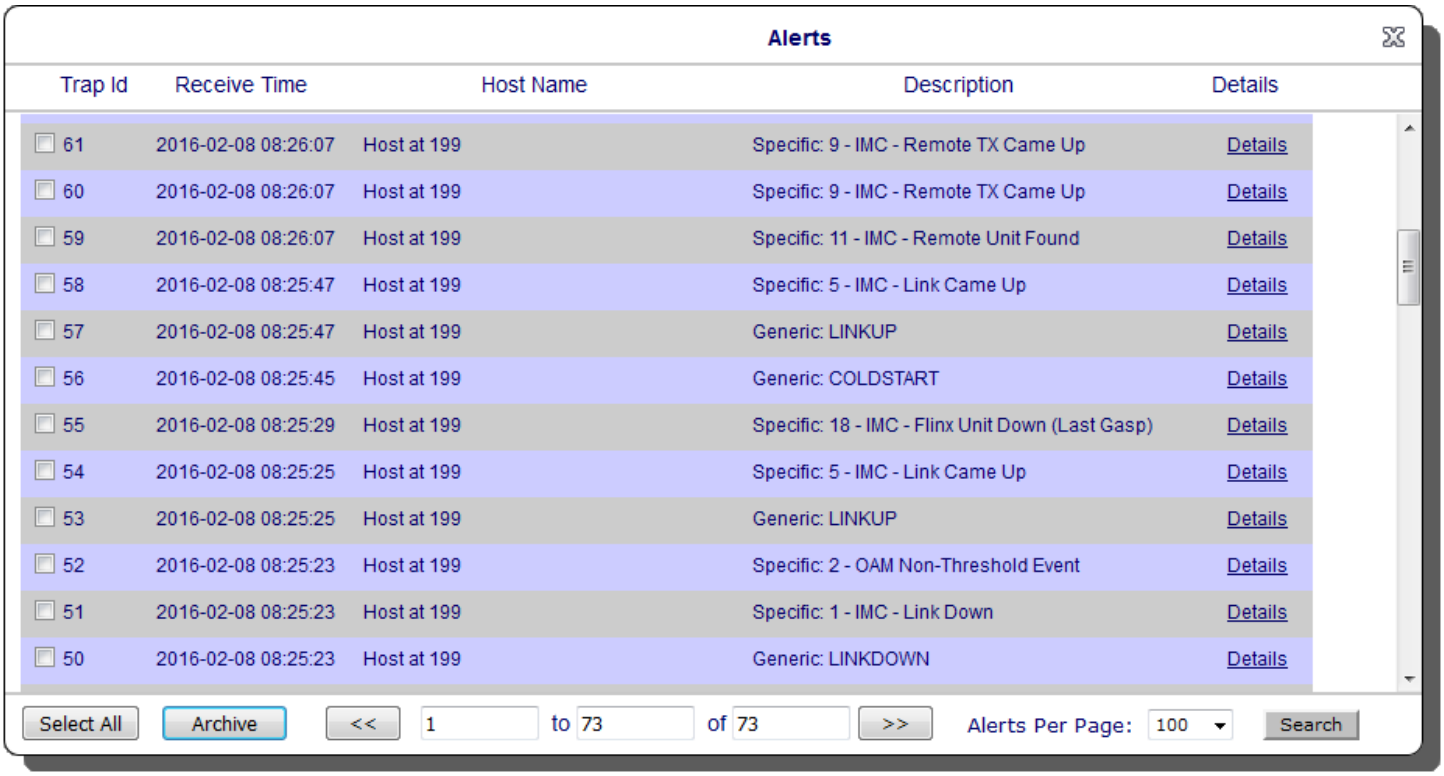


Figure 3.28 – Trap Reporting dialog with example trap information

Display Trap Details:

Selecting the “Details” option for a particular trap will display the “Variable Bindings” details for a trap as shown in figure 3.29.

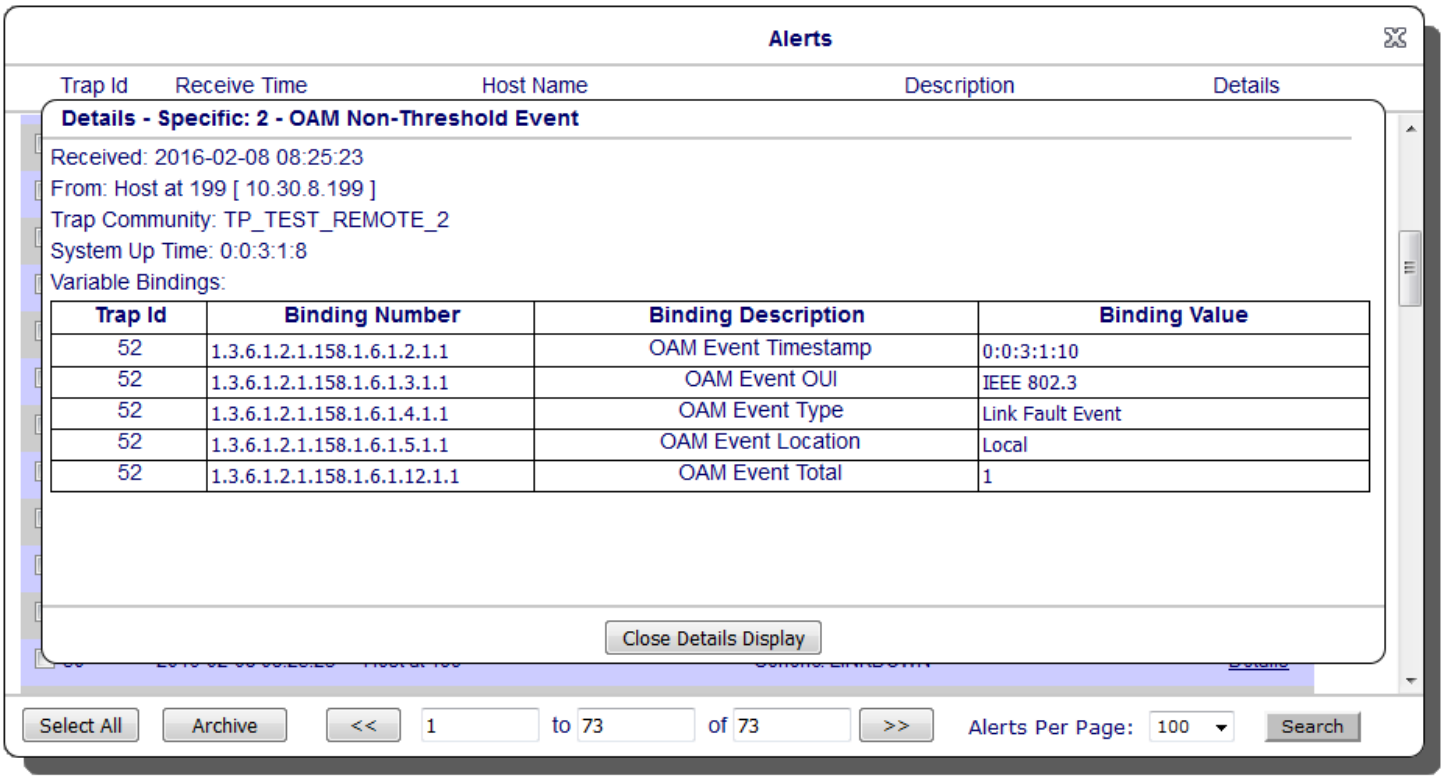


Figure 3.29 – Trap Bindings Reporting

Paging Through Traps:

Users can navigate through their trap listings using the Page Previous [<<] and Page Next [>>] buttons. Press either of these navigation buttons will display the next or previous page of alert data.

Archive Traps:

Users can use the [Archive] command button to remove traps from being displayed in the "Alerts" dialog box.
To select a trap for archiving the user can either individually choose the traps by clicking the checkbox to the left of the "Trap Id" or they can press the [Select All] command button to choose all the traps in the current display. A trap that has been selected for archiving will have a green checkmark ☑ in the trap checkbox. Once they have selected the traps they want to archive they will press the [Archive] command button and the system will update the database to mark those traps are archived. Archived traps will no longer be displayed in the "Alerts" dialog box but will remain in the database.

Setting Alerts Per Page:

Users can change the number of traps that are displayed per page using the "Alerts Per Page" dropdown selector as shown in Figure 3.30. Available selections are 10, 100, 500, and 1000. Changing the default selection will cause the list to be refreshed.

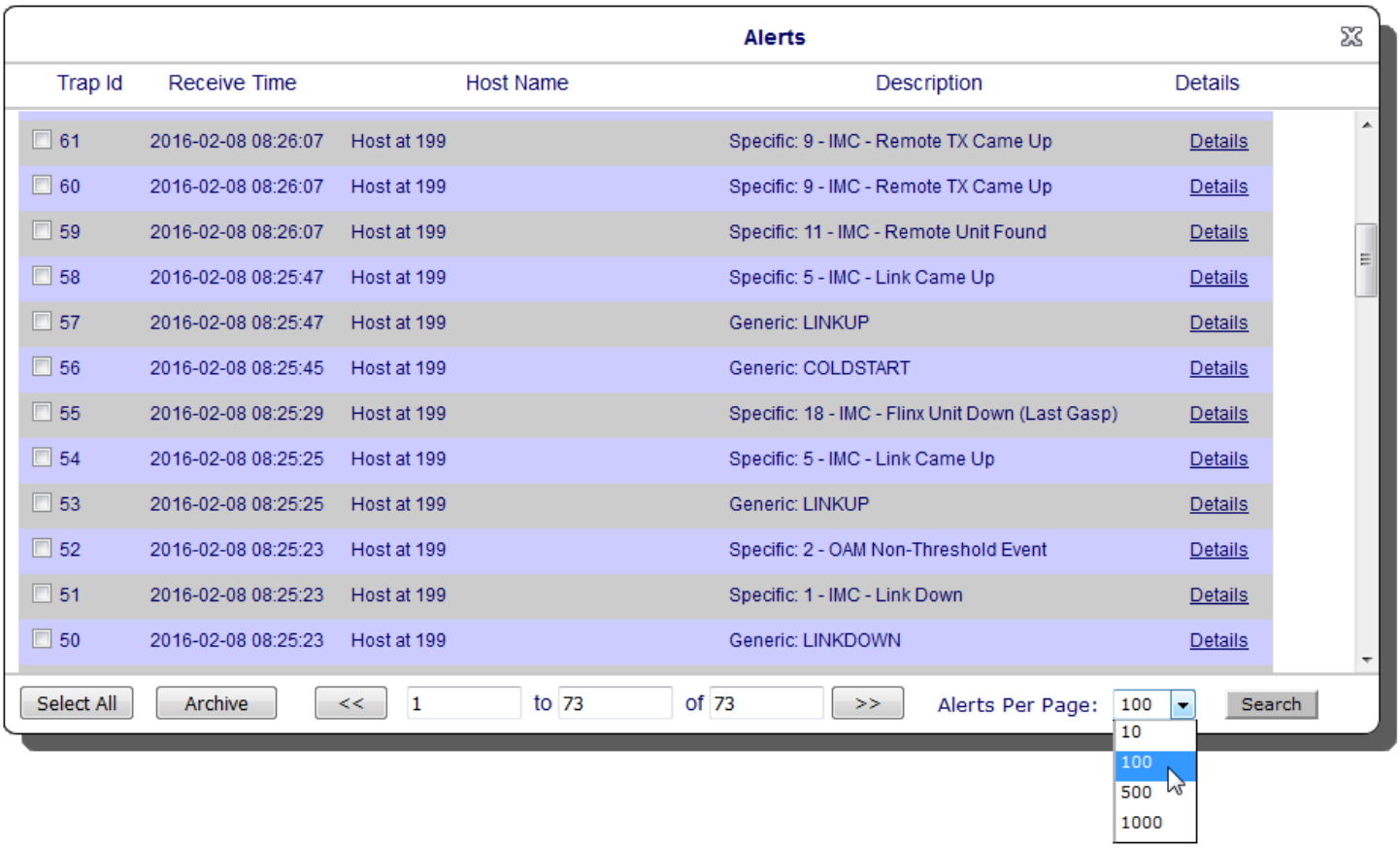


Figure 3.30 – Alerts Per Page Display

Trap Search:

Using the Trap Search functionality the user can refine the number of traps that are displayed. To access the Trap Search functionality press the Search command button. This will display the "Alerts Search Settings" dialog as shown in Figure 3.31. Here the user can enter information that will refine the default search algorithm. For example, enter a "Host Name" to see the traps associated with only that host.

Host Name – Entering a host name will cause the search to only return traps generated by that particular host.
Trap Id – Entering a trap id will cause the search to only return that particular trap.
Description – Selecting a trap description will cause the search to return traps that have that trap description.
Date From – Selecting a "Date From" will cause the search to return traps that were received from that date forward.
Date To – Selecting a "Date To" along with a "Date From" will cause the search to return traps that were received during that time period.

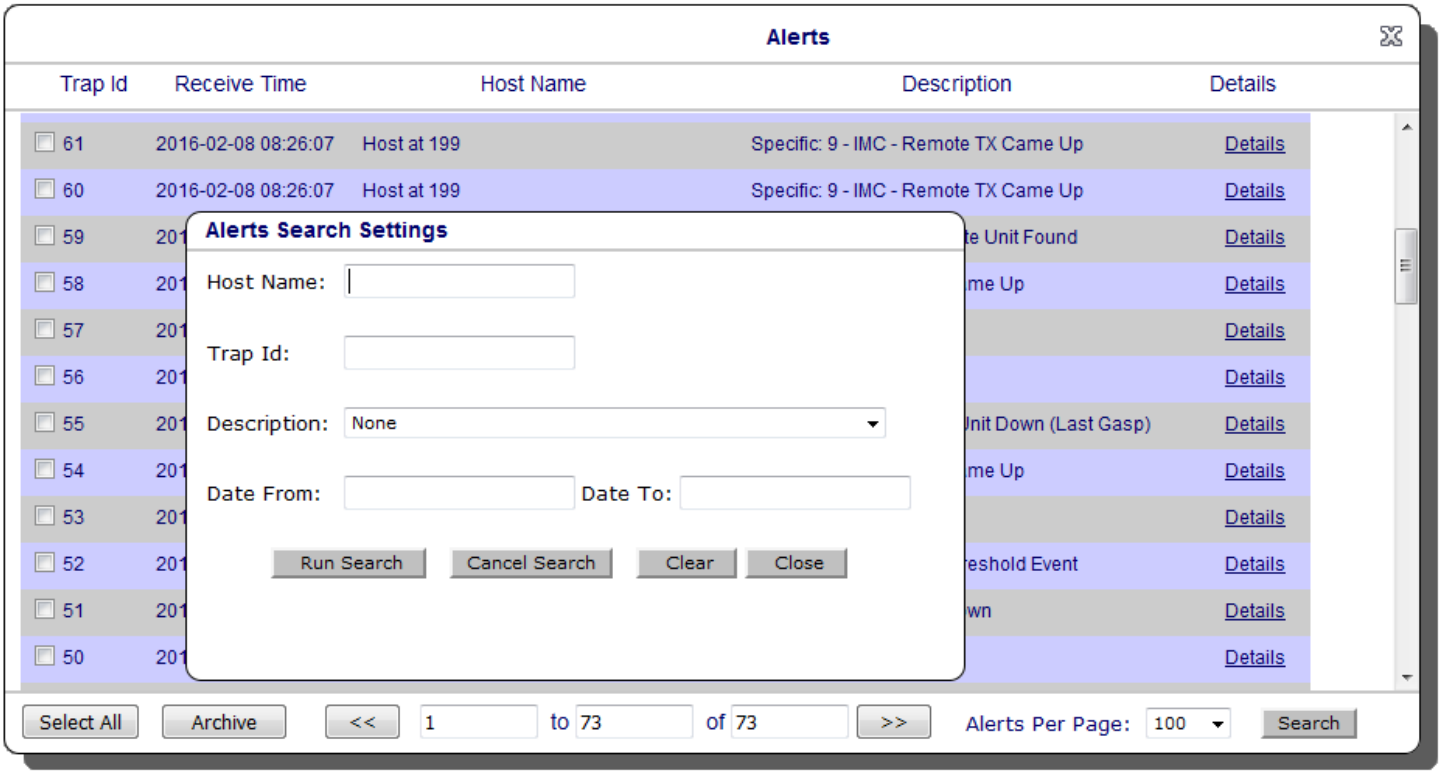


Figure 3.31 – Trap Search Display

Once the user has entered their search criteria, press the Run Search command button to execute the search.
Pressing the Cancel Search command button will cancel the search and refresh the display using the default search algorithm.
Pressing the Clear command button will clear the current search criteria.
Pressing the Close command button will close the "Alerts Search Settings" dialog without running the search.

Update Inventory

The iView "Update Inventory" is the list of all available PROM firmware devices including UMA and Remote devices. The iView "Update Inventory" functionality was added as port of the "Task Manager" process update. When a new device is added to the "iView Network Segment List" iView^2 will determine whether the device is a chassis, host, or standalone and check to see if there are UMA devices (in the case of a chassis) or Remote devices. Any found UMA or Remote PROM firmware devices will be added to the "Update Inventory" database tables and included in any Task Manager PROM firmware update report display.

The "Update Inventory" function should be manually run for all iView^2 configuration that are Version 3.0.55 or earlier prior to performing any Task Manager PROM firmware update processing. This will insure iView^2 has the most current configuration information. The average running time to check the inventory of a single 20-slot iMediaChassis is 8 seconds.

To manually run the "Update Inventory" function, select the "Update Inventory" menu selection in the "Tools" menu as shown in Figure 3.32.

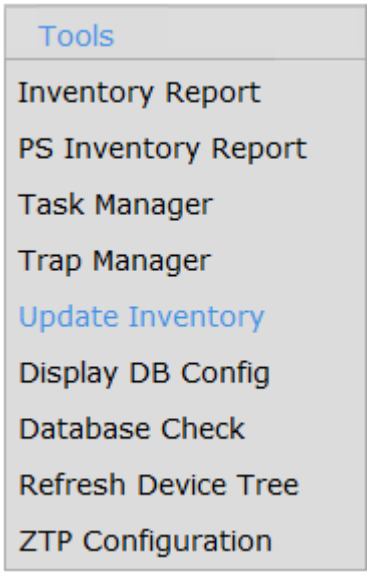


Figure 3.32 – "Update Inventory" menu selection

While the "Update Inventory" function is running iView^2 will display a "polling" icon in the upper left corner of the iView^2 display as shown in Figure 3.33. The "Update Inventory" function runs on the server and is not affected if the user closes their browser window. The "Update Inventory" polling icon will continue to display until the "Update Inventory" function is complete.

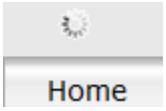


Figure 3.33 – Update Inventory polling display

Display DB Config

The “Display DB Config” menu selection located in the “Tools” menu commands will display a list of the current tables in the database and their associated version numbers.

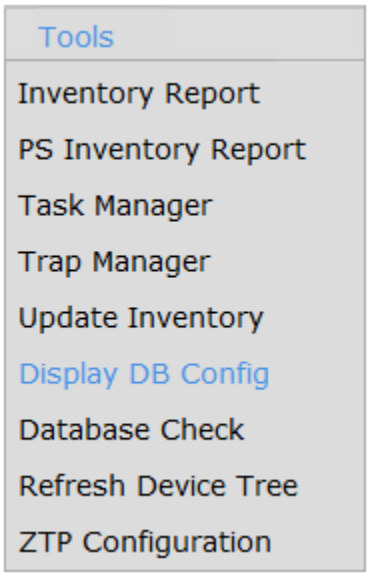


Figure 3.34 – Display Database Configuration Menu Command

The “iView DB Table Configuration” dialog is included as a diagnostics tool in the event a Support Engineer needs to verify the installation configuration.

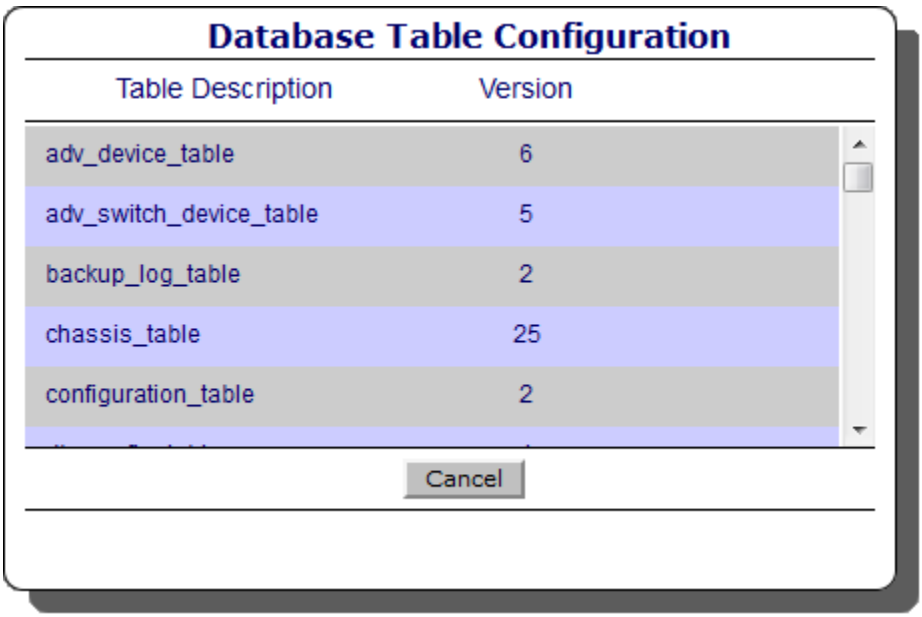


Figure 3.35 – iView DB Table Configuration Dialog

Database Check

The “Database Check” menu selection located in the “Tools” menu commands will display the status of the current tables in the database.

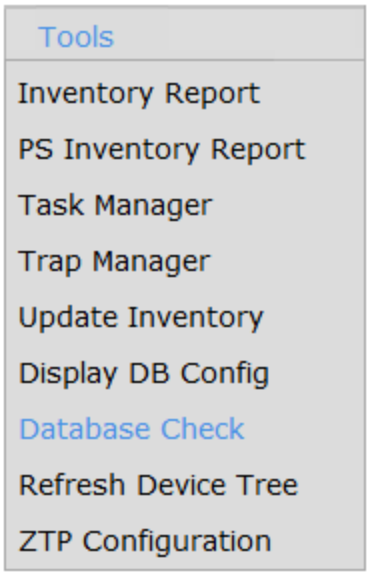


Figure 3.36 – Display Database Check Menu Command

The “Database Check” report is included as a diagnostics tool in the event a Support Engineer identifies a problem associated with the iView^2 database (iview). It lists all the tables in the iView^2 database (iview) as well as the current status of each table. A “Msg Text” of “OK” indicates the particular table is operating correctly.

Database Table Status

Table	Operation	Msg Type	Msg Text
adv_device_table	check	status	OK
adv_switch_device_table	check	status	OK
backup_log_table	check	status	OK
chassis_table	check	status	OK
configuration_table	check	status	OK
db_config_table	check	status	OK
device_search_table	check	status	OK
device_tree_table	check	status	OK
device_type_table	check	status	OK
device_uma_table	check	status	OK
h_chassis_images_table	check	status	OK
iconfig_login_table	check	status	OK

Figure 3.37 – Database Check current state report display

Refresh Device Tree

The “Refresh Device Tree” menu selection will re-display the “iView Network Segment List” by retrieving the current list of devices from the iView[2] database.

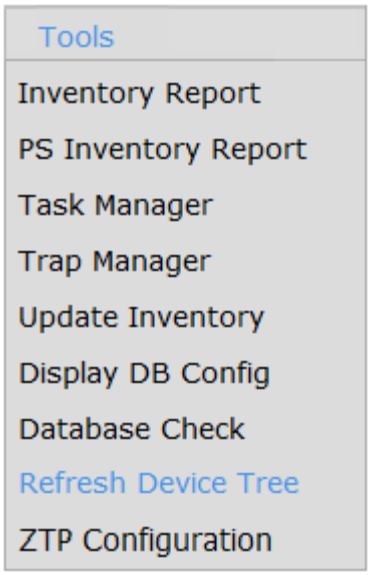


Figure 3.38 – Refresh Device Tree Menu Command

ZTP Configuration

The “ZTP Configuration” menu selection will display the “ZTP Configuration” dialog. This allows the user to create zero-touch provisioning (ZTP) configuration files for B&B Electronics devices that provide support for this functionality.

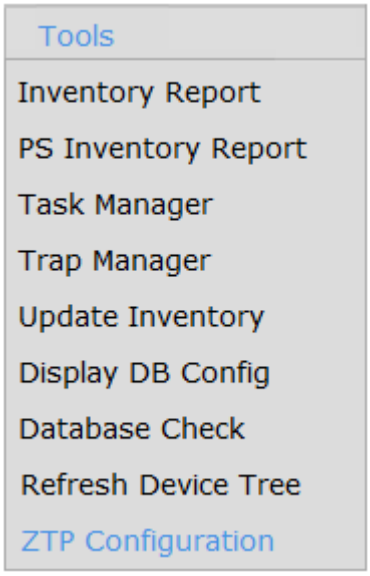


Figure 3.39 – ZTP Configuration Menu Command

Figure 3.40 – ZTP Configuration Dialog

ZTP Configuration Control Icons

- Add Configuration Icon: This control icon will allow the user to create a ZTP configuration file.

- Delete Configuration Icon: This control icon will allow the user to delete a ZTP configuration file.

- Edit Attributes Icon: This control icon will allow the user to edit the attributes associated with a ZTP configuration file.

- Search Icon: This control icon will allow the user to search for a ZTP configuration file.

Administration Menu Items

Add iView² User

For users with an "Administrator" user access level, the "Add User" command is available under the "Administration" menu command (figure 4.1). Selecting the "Add User" command will display the dialog as shown in figure 4.2.

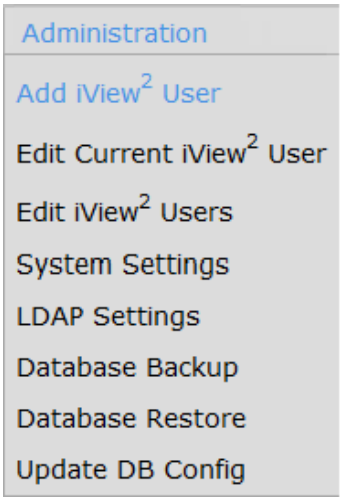


Figure 4.1 – Add iView² User menu command

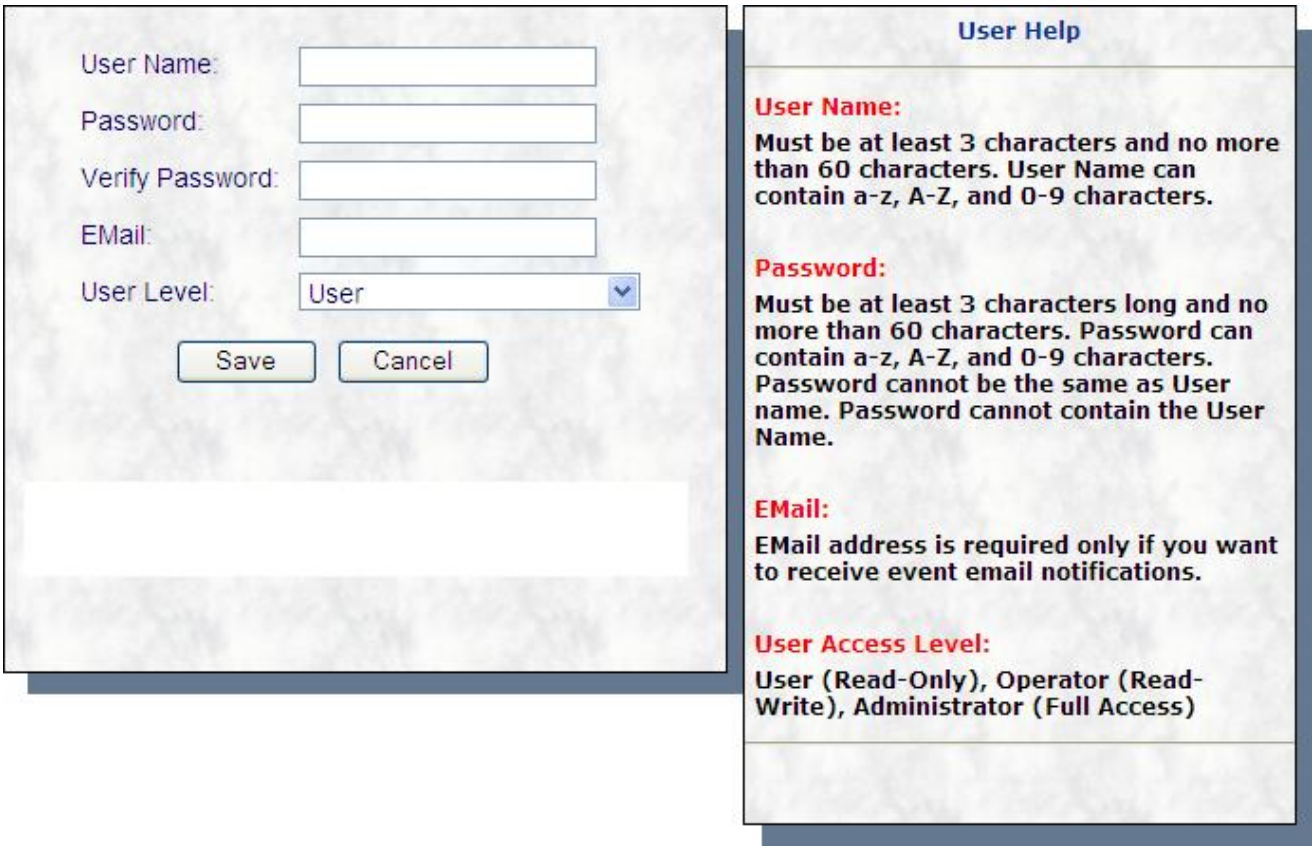


Figure 4.2 – Add iView² User display

Edit Current iView² User

For users with an "Administrator" user access level, the "Edit Current User" command is available under the "Administration" menu command (figure 4.3). Selecting the "Edit Current User" command will display the dialog as shown in figure 4.4.

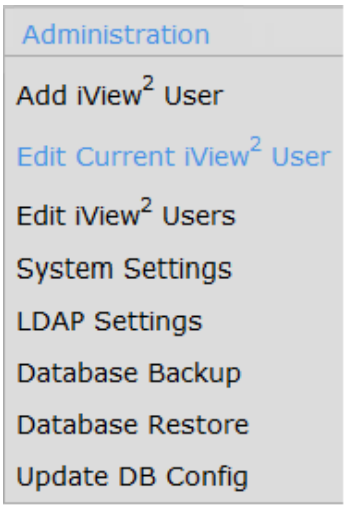


Figure 4.3 – Edit Current iView² User menu command

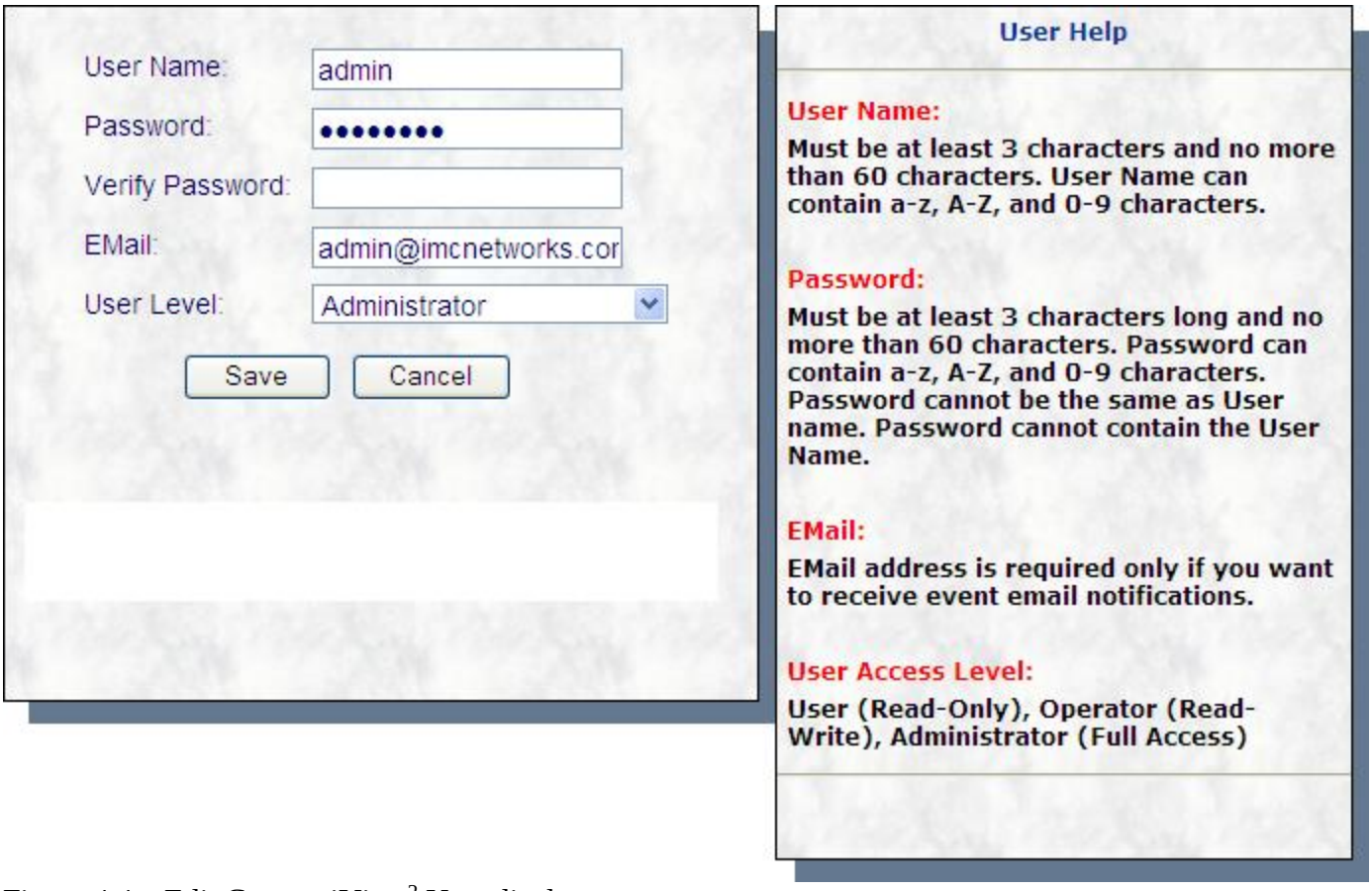


Figure 4.4 – Edit Current iView² User display

Edit iView² Users

For users with an "Administrator" user access level, the "Edit Users" command is available under the "Administration" menu command (figure 4.5). Selecting the "Edit Users" command will display the dialog as shown in figure 4.6.

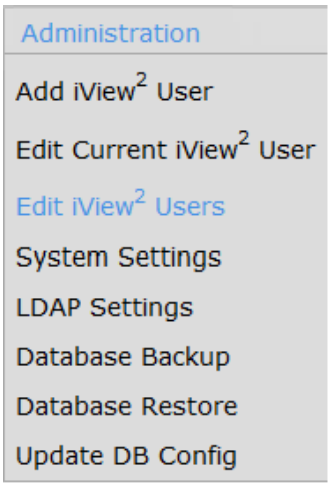


Figure 4.5 – Add iView² Users menu command

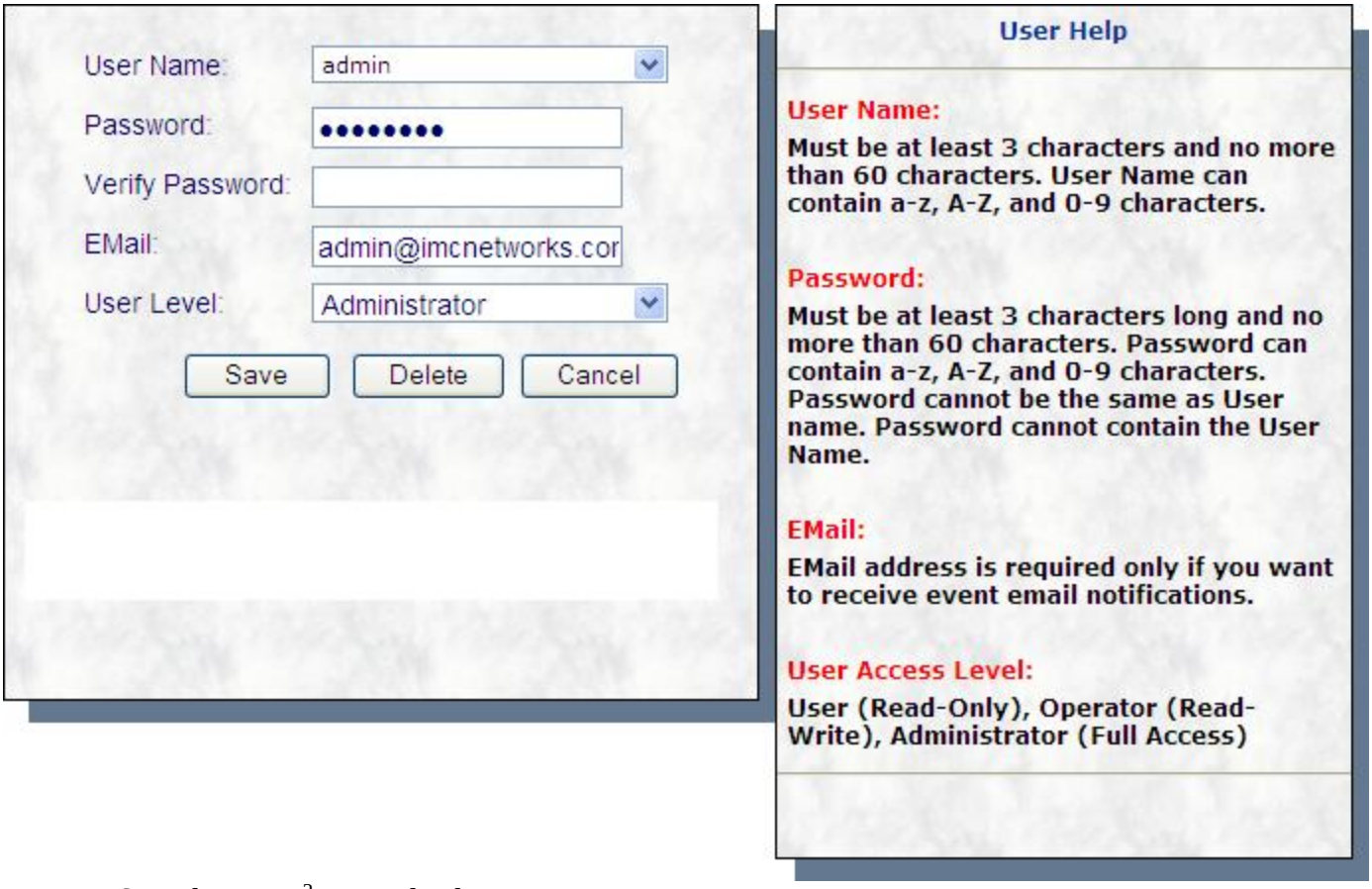


Figure 4.6 – Edit iView² Users display

System Settings

Global options associated with the iView^2 server system are controlled through the "System Settings" menu item in the "Administration" menu as shown in Figure 4.7.

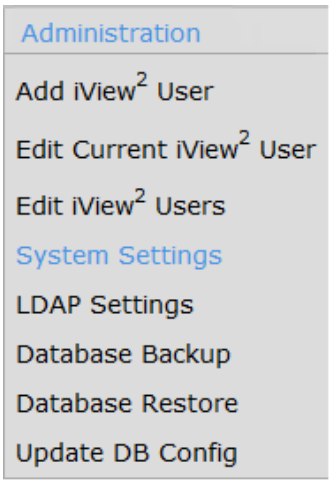


Figure 4.7 – System Settings Menu Selection

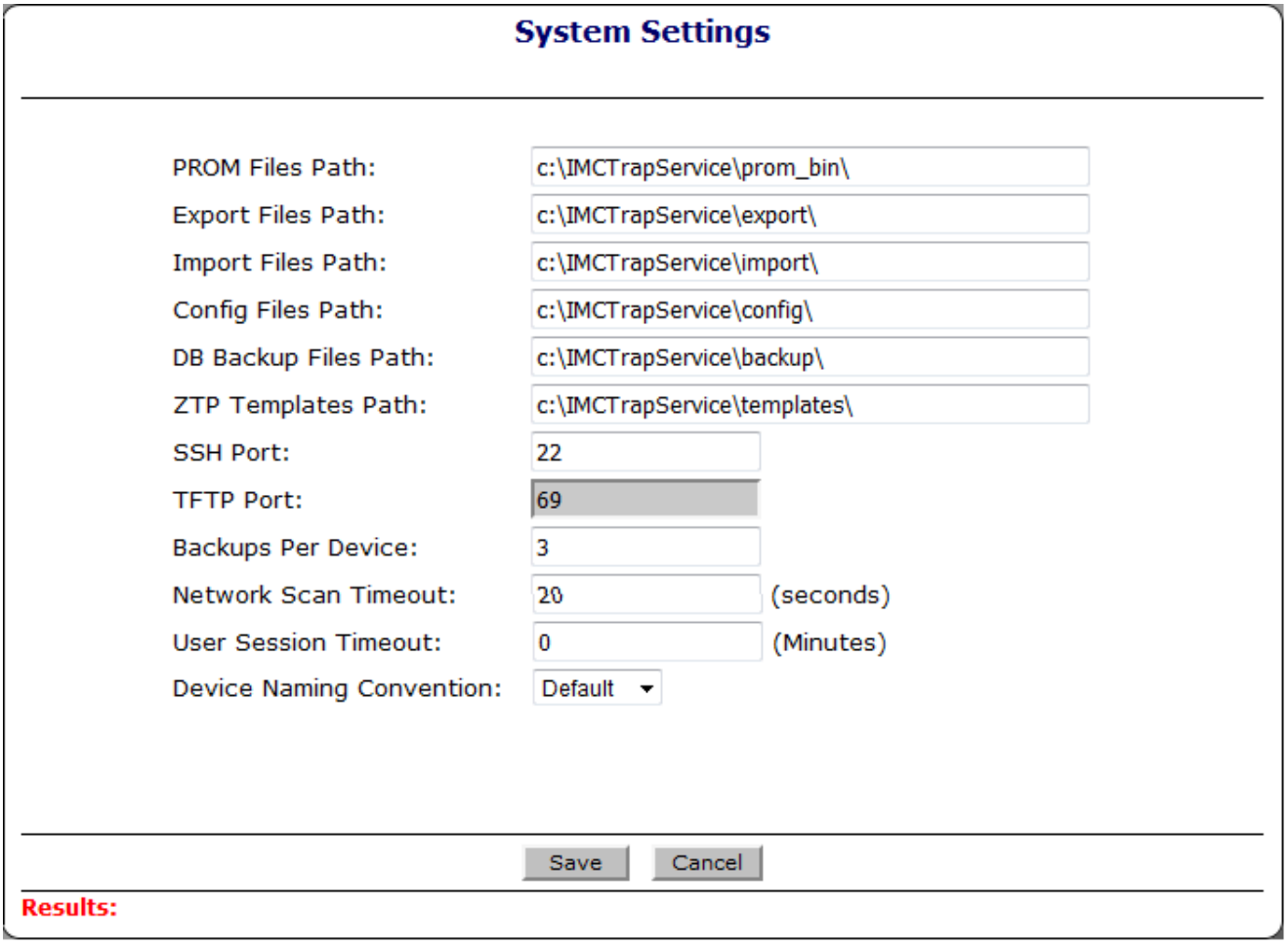


Figure 4.8 – System Settings Dialog Box

PROM Files Path – Identifies the location of the device PROM firmware binary files.

Export Files Path – Identifies the location of the delimited files exported from iView^2.

Import Files Path – Identifies the location of the delimited files for import to iView^2.

Config Files Path – Identifies the location of the device configuration backup files.

DB Backup Files Path – Identifies the location of iView^2 database backup files.

ZTP Templates Path – Identifies the location of Zero-Touch Provisioning templates.

SSH Port – Identifies the port for SSH device access.

TFTP Port – Identifies the TFTP port used by iView^2.

Backups Per Device – Identifies the max number of configuration backup files per device.

Network Scan Timeout – Identifies the amount of time iView^2 will wait for device communications.

User Session Timeout – Identifies the amount of time iView^2 will wait for user activity.

Device Naming Convention – Identifies the type of device naming used by iView2.

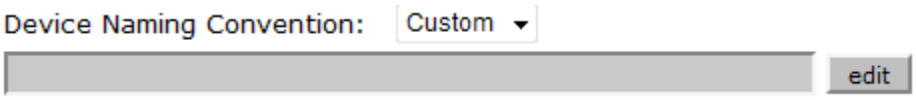
User Session Timeout

The "User Session Timeout" field in the System Settings dialog provides the ability to close a user session when no activity has been performed. For example, if the "User Session Timeout" is set for 10 minutes, if the user has not worked in the iView^2 browser application for 10 minutes, the user session will be closed and the user will need to re-login to iView^2 if they want to perform further work.

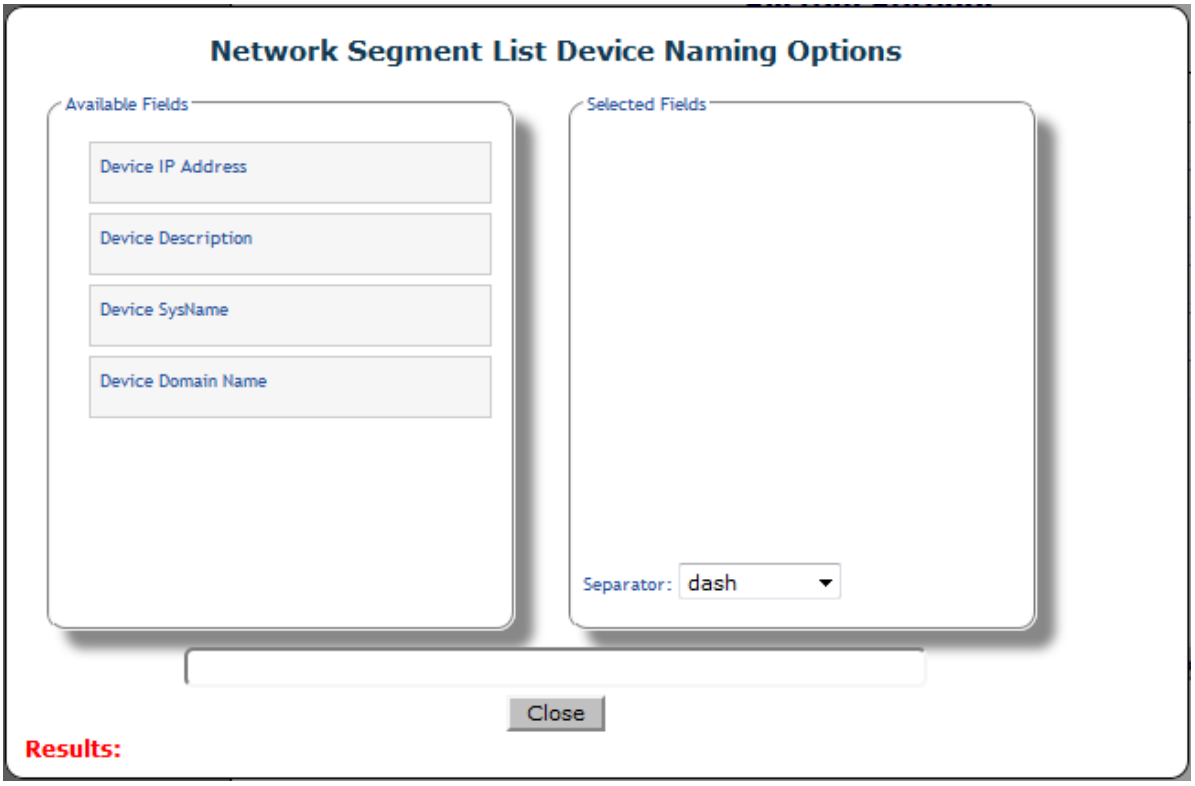
Device Naming Convention

The "Device Naming Convention" option can be used to change the default device naming mechanism used by iView^2. By default, iView^2 will attempt to use the unit description setting as the device name displayed in the "iView Network Segment List". If the unit description is not available, iView^2 will use the unit sysname followed by a dash (-) followed by the unit ip address. If the "Device Naming Convention" is set to "Custom", iView^2 will use the identified custom naming convention.

To set the custom naming convention, change the "Device Naming Convention" from "Default" to "Custom". A new input box will appear with an "edit" command button.



Press the "edit" command button to display the "Network Segment List Device Naming Options" dialog. Click on each desired entry in the "Available Fields" section to move the selection to the "Selected Fields" section. Press the "Close" command button when done.



Verify the settings are correct in the "System Settings" dialog and press the "Save" command button to store your selections to the database. When done select the "Tools" -> "Refresh Device Tree" menu selection to refresh the Network Segment List.

LDAP Settings

Overview:

The iView^2 LDAP functionality uses the Java Naming and Directory Interface (JNDI) API to communicate with the user LDAP server. The JNDI implementation supports LDAP Version 3. The iView^2 LDAP implementation is a 2-step process of authentication and authorization. The authentication step determines if the user has LDAP access and is a group member of the domain. The authorization step determines if the user has an identified iView^2 role level. An iView^2 user with an "administrator" role level must set the values in the "LDAP Settings" dialog before iView^2 will attempt to perform LDAP authentication and authorization.

At login, the user will enter their LDAP User Name, LDAP Password, and check the "Use LDAP" checkbox in the iView^2 login dialog box. During the authentication step, iView^2 will attempt to bind to the user LDAP server using the "LDAP Server", "LDAP Port", "LDAP Authentication", and "User Custom Format" settings in addition to the entered LDAP User Name and LDAP Password. Once the LDAP server connection is established, iView^2 will authenticate a user by performing a search of the SAM-Account-Name against the entered LDAP User Name using the "LDAP Base DN". If the LDAP User Name is not found, the error message "ERROR: LDAP Authentication: FAILED" will be displayed in the iView^2 login dialog box. If the LDAP User Name is found, the authentication process is successfully completed and iView^2 moves on to the authorization step.

If the "LDAP Authorization" settings are configured, the iView^2 authorization process will attempt to search for inclusion of the user login for each of the entered user role distinguished names. The iView^2 authorization process will search each of the entered authorization DNs starting with the "Administrator DN", then the "Operator DN", and finally the "User DN". The first match found will associate the user login with the user functionality level.

NOTE: If the "LDAP Authorization" setting is not checked, iView^2 will only perform the authentication step and if the user is successfully authenticated, a default role of "user" will be assigned to the login.

Configuration:

For users with an “administrator” user role, the “LDAP Settings” command is available under the “Administration” menu command (figure 4.9). This command will establish the LDAP connection requirements. Selecting the “LDAP Settings” command will display the “LDAP Settings” dialog as shown in figure 4.10.

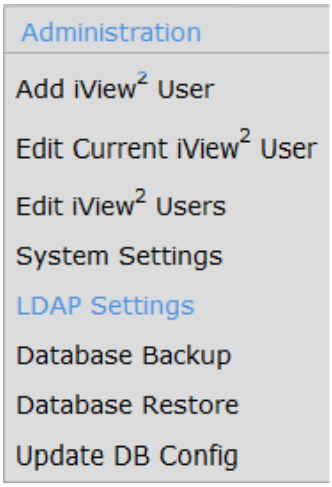


Figure 4.9 – LDAP Settings Menu Selection

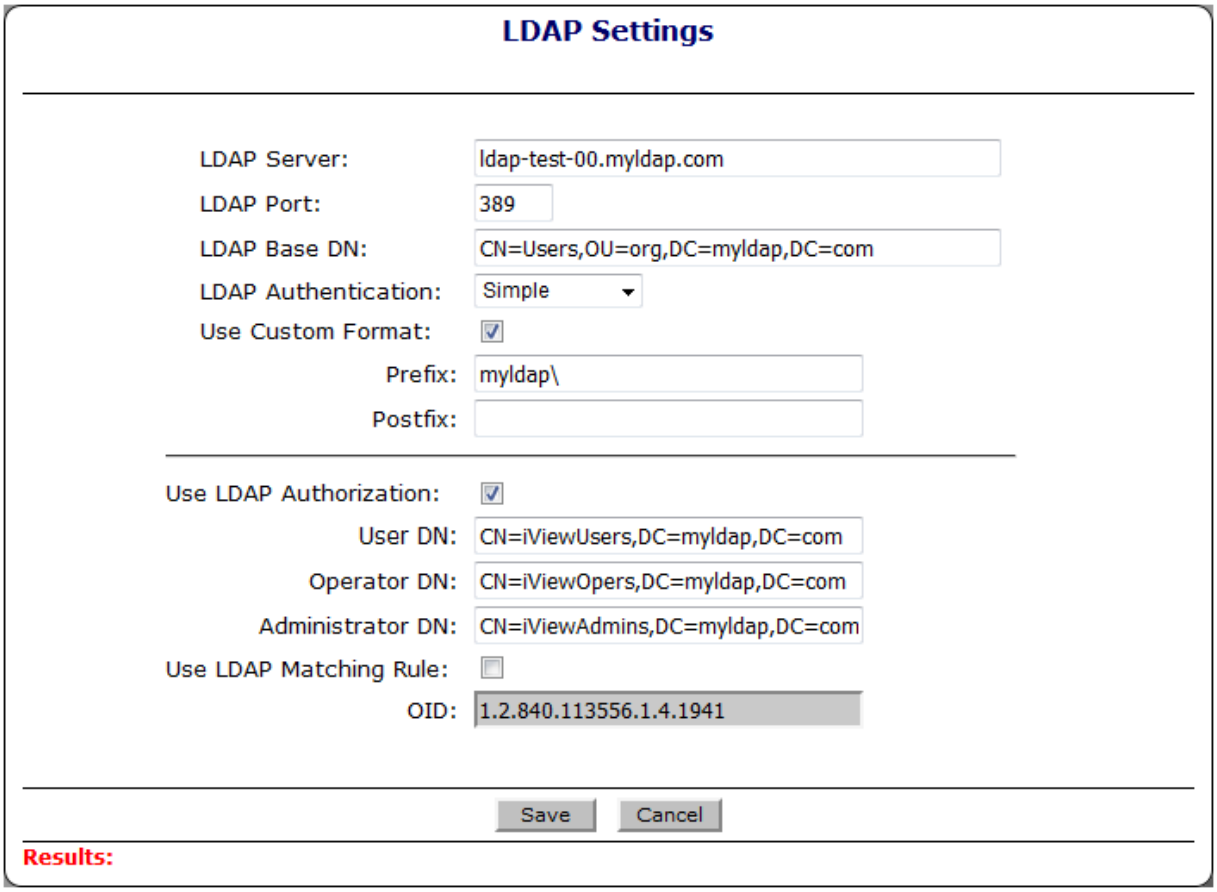


Figure 4.10 – LDAP Settings Dialog Box

Setting Name	Setting Description
LDAP Server	Identifies the LDAP server to use.
LDAP Port	Identifies the LDAP port number.
LDAP Base DN	Identifies the Distinguished Name (DN) to use for authentication.
LDAP Authentication	Identifies security level to use.
Use Custom Format	Identifies prefix and/or postfix information to add to login user name.
Prefix	Identifies the value to use before the login user name.
Postfix	Identifies the value to use after the login user name.
Use LDAP Authorization	Identifies the use of authorization during LDAP login.
User DN	Identifies the DN to use to authorize user level functionality.
Operator DN	Identifies the DN to use to authorize operator level functionality.
Administrator DN	Identifies the DN to use to authorize administrator level functionality.
Use LDAP Matching Rule	Identifies the use of the Active Directory Matching Rule Extension OID.
OID	Identifies the Object Identifier (OID) for the matching rule.

LDAP Settings used for authentication:
LDAP Server
LDAP Port
LDAP Base DN
LDAP Authentication
Use Custom Format

LDAP Settings used for authorization:
LDAP Server
LDAP Port
LDAP User DN
Use Custom Format
LDAP Authorization
LDAP Matching Rule OID

Use Custom Format:

Referring to figure 3.45, the "Use Custom Format" checkbox is used to enter prefix or postfix information that will be added to the entered user name during LDAP login. In the displayed example, the "Prefix" string "myldap\" will be added to every user name during LDAP login. For example, if the user name was "testUser", iView^2 will use "myldap\testUser" as the LDAP login user name.

LDAP Matching Rules:

The LDAP Matching Rules follow the Microsoft Windows Active Directory OID numbering associated with the LDAP Matching Rules extension in Active Directory. The LDAP Matching Rules provide additional criteria for how the iView^2 authorization search is performed. For example, the default "LDAP_MATCHING_RULE_TRANSITIVE_EVAL" OID of "1.2.840.113556.1.4.1941" , if checked will cause the iView^2 authorization search to be performed in a recursive manner against the "memberOf" LDAP attribute.

```
(&(objectClass=user)(sAMAccountName=testUser)(memberOf:1.2.840.113556.1.4.1941:=CN=IVIEW-
ADMINS,OU=IVIEW,OU=TEST,DC=myldap,DC=com))
```

Figure 4.11 – Example search filter string

Database Backup

For users with an “Administrator” user access level, the “Database Backup” command is available under the “Administration” menu command (figure 3.47). This command will create a complete copy of all the contents of the iView^2 database. Selecting the “Database Backup” command will display the “Database Backup” dialog as shown in figure 4.12.

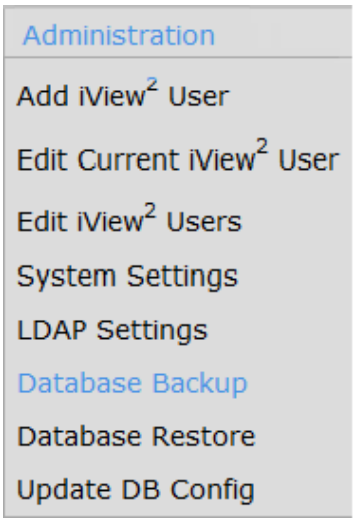


Figure 4.12 – Database Backup Menu Selection

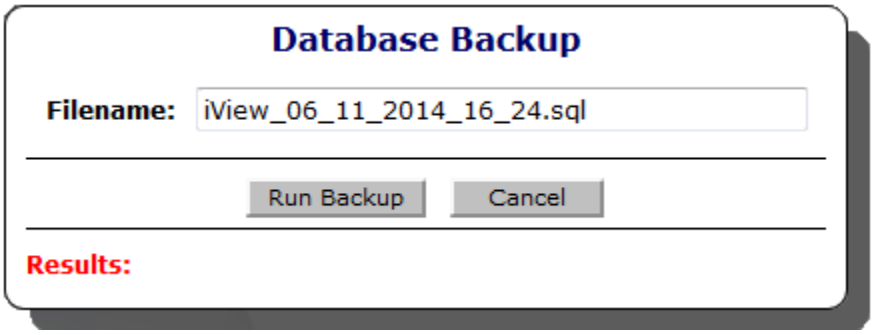


Figure 4.13 – Database Backup Dialog Box

The default filename can be changed by the user. The filename extension must be “.sql”.

Pressing the “Run Backup” command button will trigger the iView2 server to create a backup file of the entire contents of the iView2 database to the “DB Backup Files Path” identified in the iView^2 System Settings.

When complete, the results of the operation will be displayed in the “Results:” section of the Database Backup dialog box, as shown in figure 4.14.

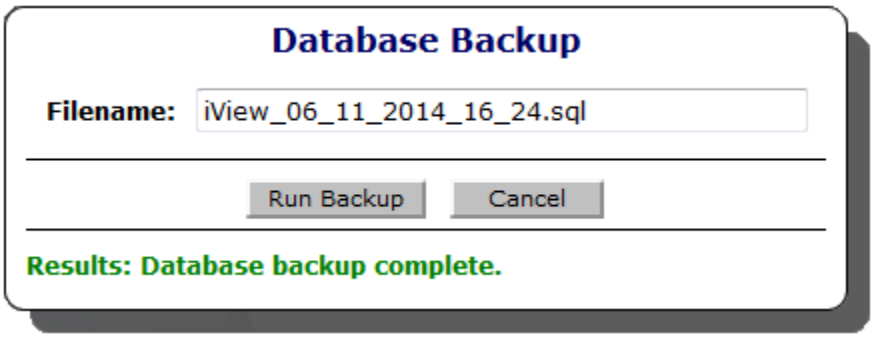


Figure 4.14 - Database Backup Dialog Box Results Display

Database Restore

For users with an "Administrator" user access level, the "Database Restore" command is available under the "Administration" menu command (figure 4.15). This command will restore a previously created iView^2 database backup file and overwrite the existing iView^2 database. Selecting the "Database Restore" command will display the "Database Restore" dialog as shown in figure 4.16.

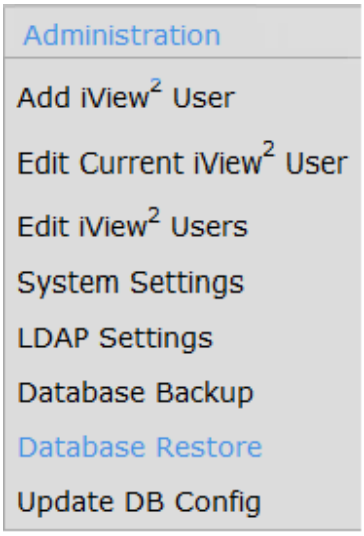


Figure 4.15 – Database Restore Menu Selection

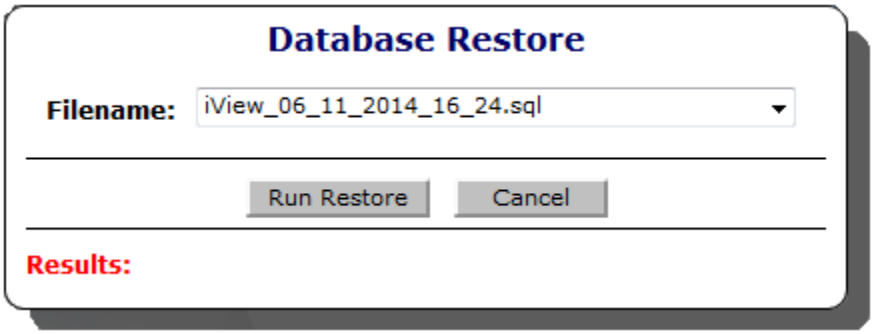


Figure 4.16 – Database Restore Dialog Box

The user will select a filename from the list and press the “Run Restore” command button. This will present a warning box to the user as shown in figure 4.17.

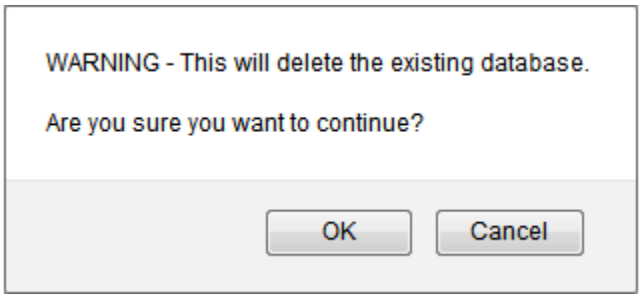


Figure 4.17 – Database Restore Warning

When the database restore operation is complete the results will display in the “Results” section of the Database Restore dialog box as shown in figure 4.18.

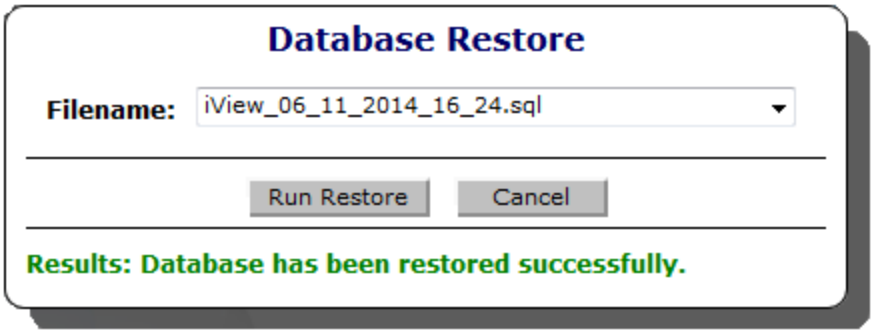


Figure 4.18 - Database Restore Dialog Box Results Display

Update DB Config

The "Update DB Config" menu selection located in the "Administration" menu commands and provides the ability to initialize and update the configuration tables in the iView^2 database on a manual basis.

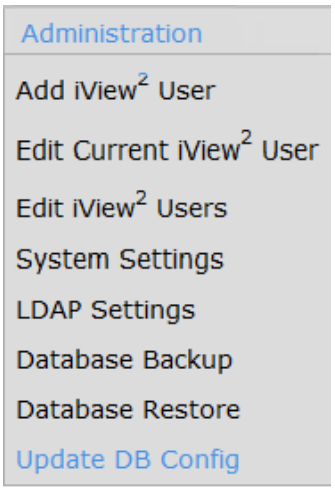


Figure 4.19 – Update Database Menu Command

When the database configuration is complete a results list will display the functions that were performed.

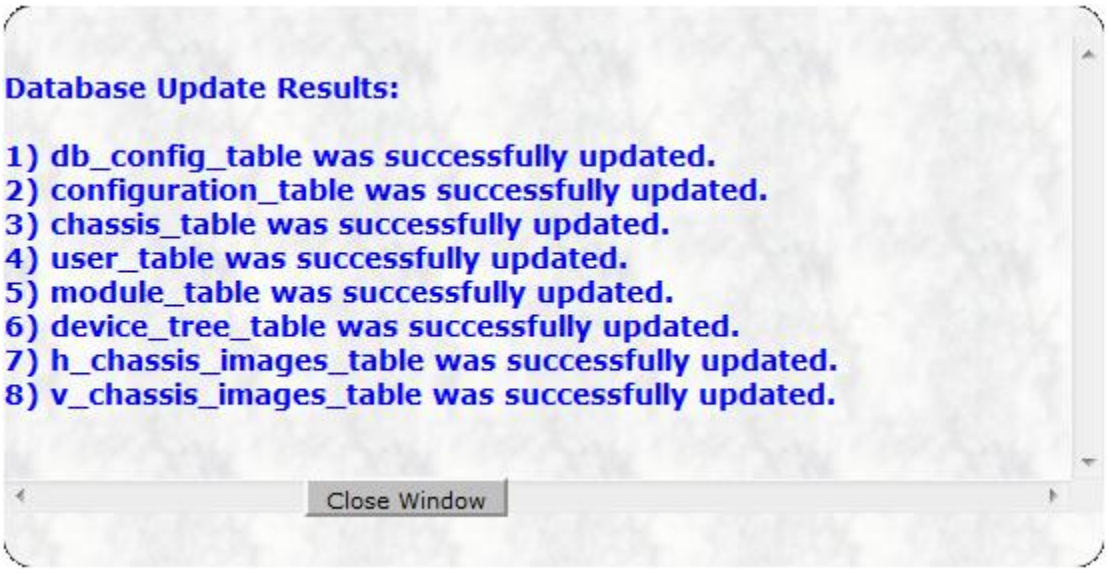


Figure 4.20 – Results Display

Appendix A

Task Scheduling Options

All task scheduling is controlled through the Task Scheduling Settings dialog as shown in figure 5.1.

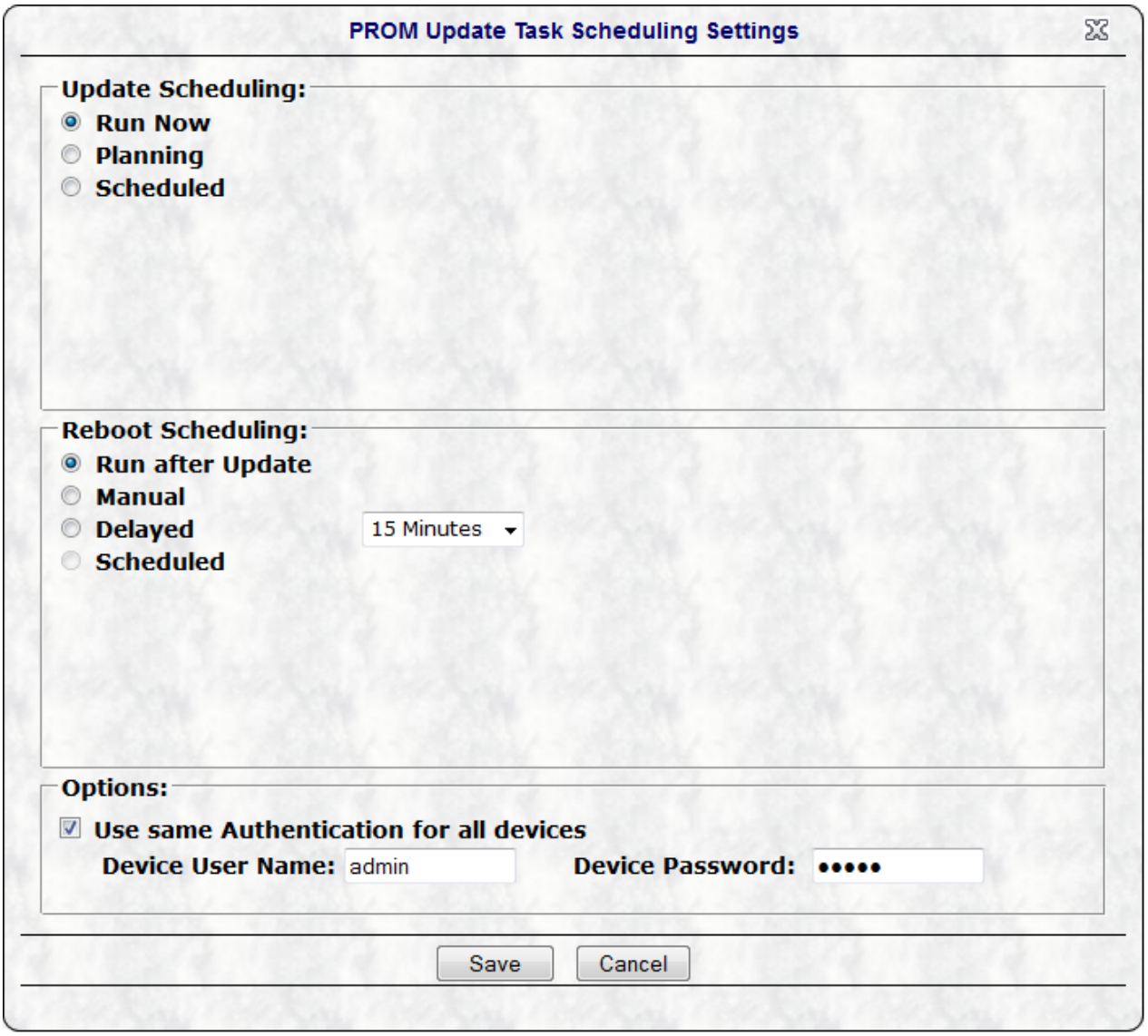


Figure 5.1 – Task Scheduling Settings Dialog

Update Scheduling:
Run Now – Task items will begin to execute as soon as iView^2 can begin processing the update.
Planning – Task items will be stored but not executed.
Scheduled – Task items will be scheduled to run no earlier than the date and time requested by the user.
Repeating – Task items will be scheduled to run on a repeating basis once a day or once a week.

NOTE:
The Update Scheduling "Start" and "Stop" time settings represent a window of available system processing time. If "Repeating" is set to "None" any task items that have not been processed within the time window will be cancelled. If "Repeating" is set to "Daily" or "Weekly" any task items that have not been processed within the time window will be rescheduled for the next time window.

Reboot Scheduling:
Run after Update – The task item will reboot each device when the firmware update to the device is complete.
Manual – The task item will not reboot each device when the firmware update to the device is complete.
Delayed – The task item will reboot each device after the firmware update to the device is complete and the delay selection time has passed.
Scheduled – The task item will be scheduled to reboot no earlier than the date and time requested by the user.

NOTE:
The Reboot Scheduling "Start" and "Stop" time settings represent a window of available system processing time. If "Repeating" is set to "None" any task items that have not been rebooted within the time window will be cancelled. If "Repeating" is set to "Daily" or "Weekly" any task items that have not been rebooted within the time window will be rescheduled for the next time window.

Scheduling Guidelines

● Avoid scheduling update or reboot tasks during daylight savings time change over. The update/reboot process scheduler is designed to run tasks at an exact millisecond time and repeat an exact millisecond apart, so there is a chance the tasks could run at an incorrect start time if they are scheduled to occur when the daylight savings time change over occurs.

● Repeating options for Update Scheduling and Reboot Scheduling should match. If the Update Scheduling option is set to “Scheduled” and the Update Scheduling “Repeating” option is set to “Daily” or “Weekly” and the Reboot Scheduling option is set to “Scheduled” then the Reboot Scheduling “Repeating” option should be set to match the Update Scheduling “Repeating” option.

● A maximum of 10 PROM Updates via unique IP Addresses will run simultaneously. UMA PROM Updates through a single IP Address will occur in a serial manner. To ensure the maximum number of devices getting updated in a given window of available system processing time, select a combination of devices such that the devices are accessible through as many different IP Addresses as possible. For example instead of updating multiple host/remote devices in a single chassis in a schedule, select multiple host/remote devices in different chassis or standalone host/remote pairs of devices.

● If a device is connected directly to the network (i.e. has a unique IP address) and also managed through the management chassis or host, DO NOT schedule the same device for updating through direct update (using the device IP Address) and UMA update (using the SNMP Management device IP Address). This will result in an update conflict and the PROM update will fail.

Scheduling Options Screenshots

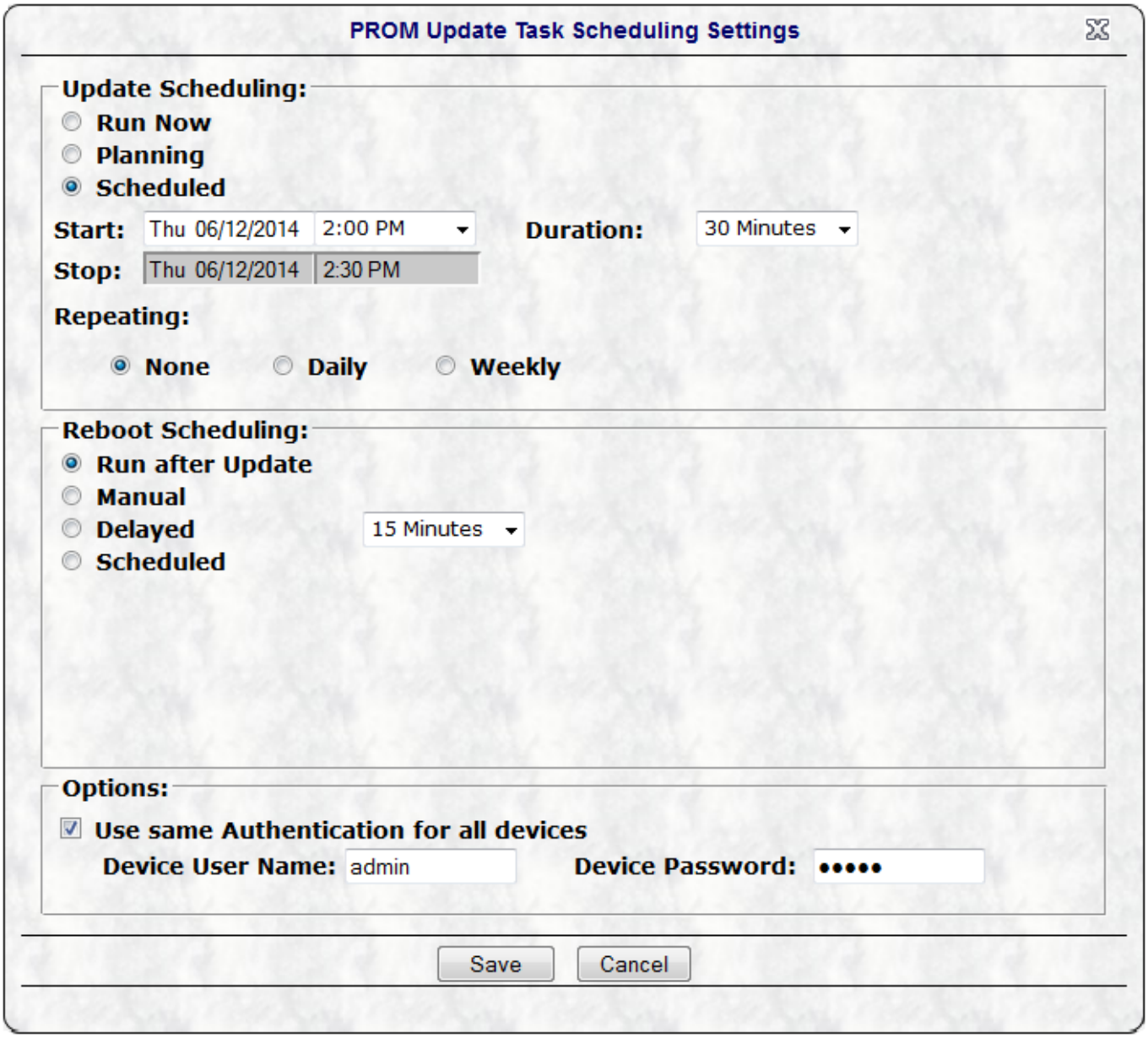


Figure 5.2 – Update Scheduling Display

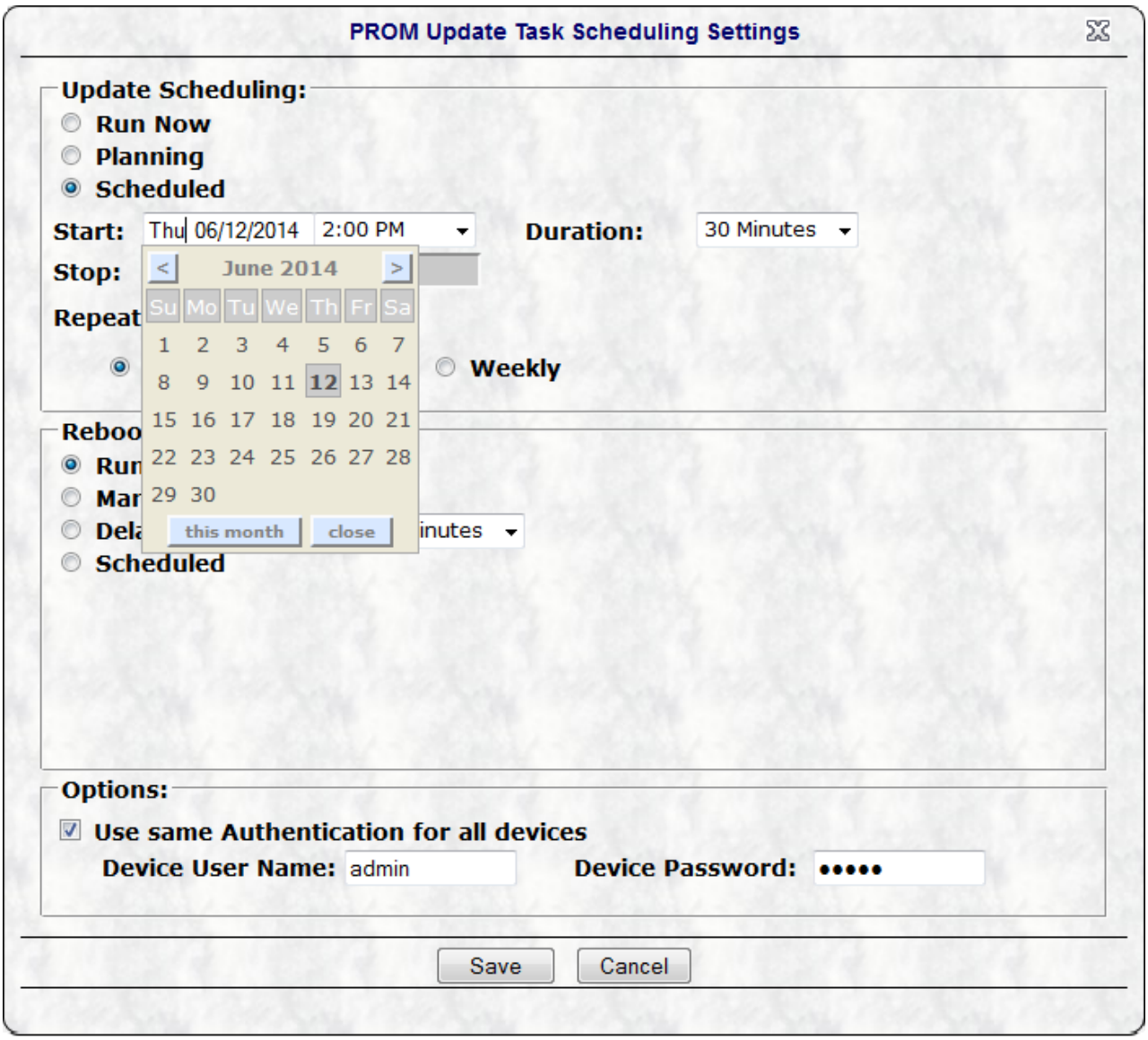


Figure 5.3 – Update Scheduling: Select a Start Date

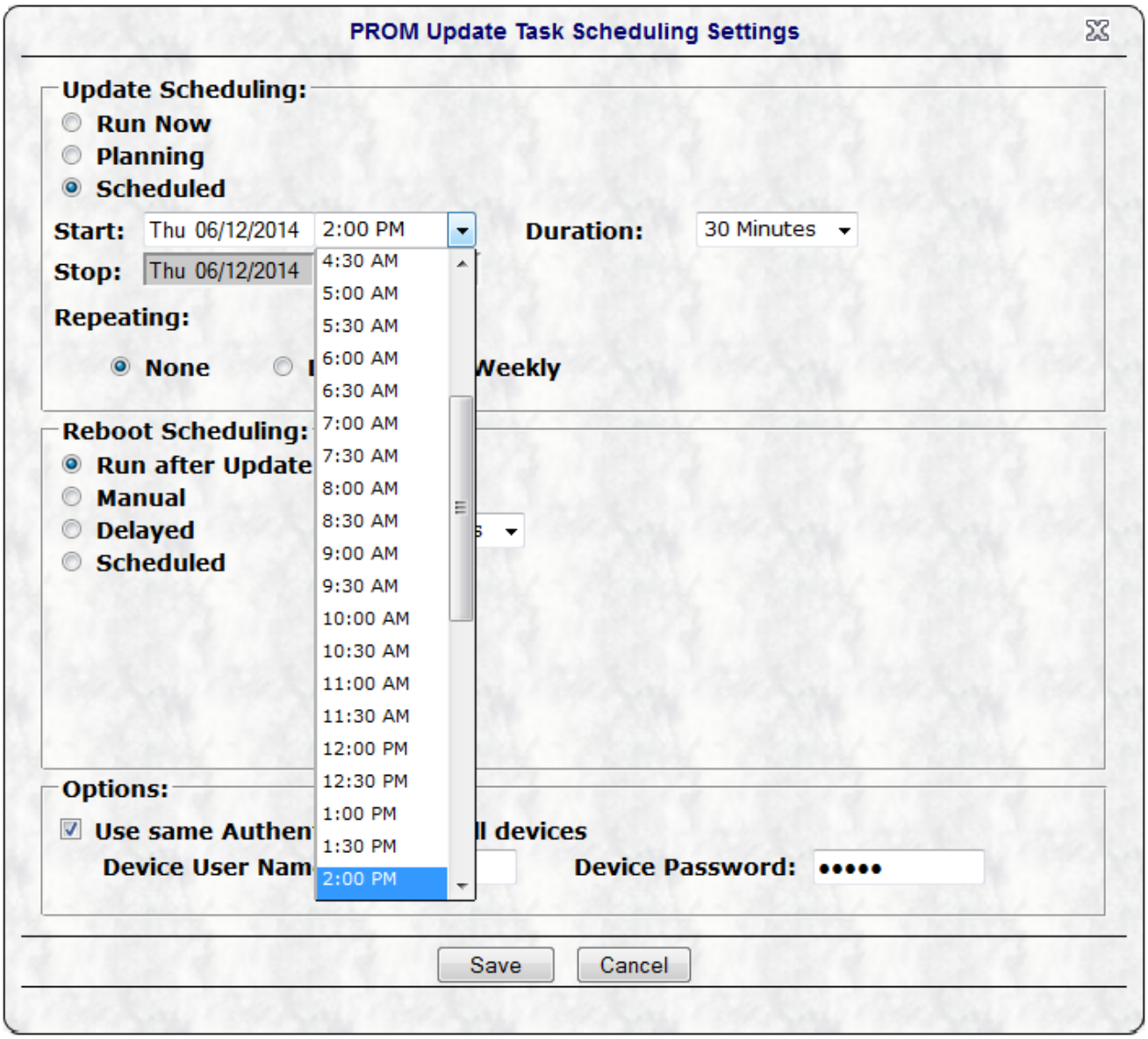


Figure 5.4 – Update Scheduling: Select a Start Time

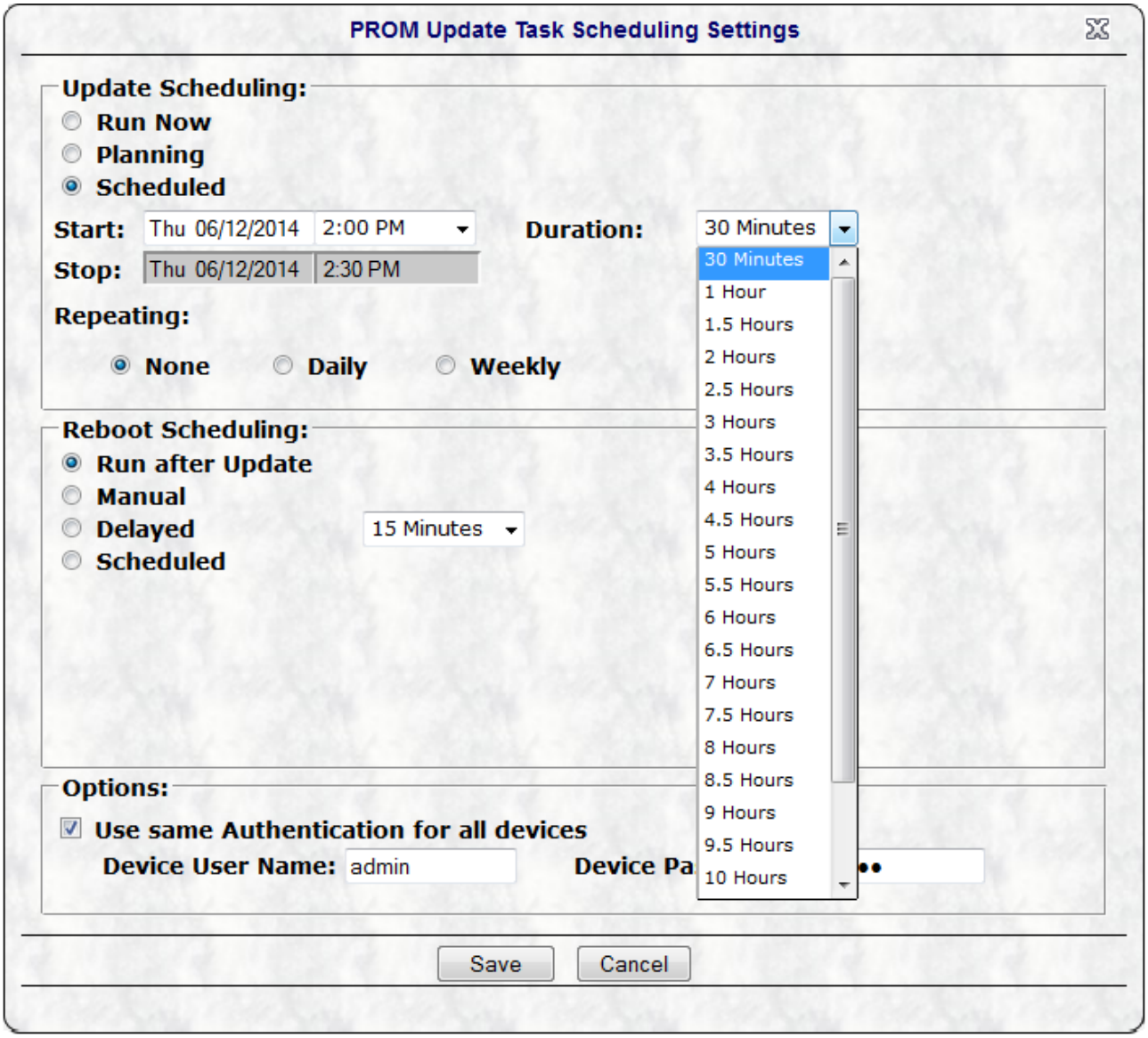


Figure 5.5 – Update Scheduling: Select a Duration

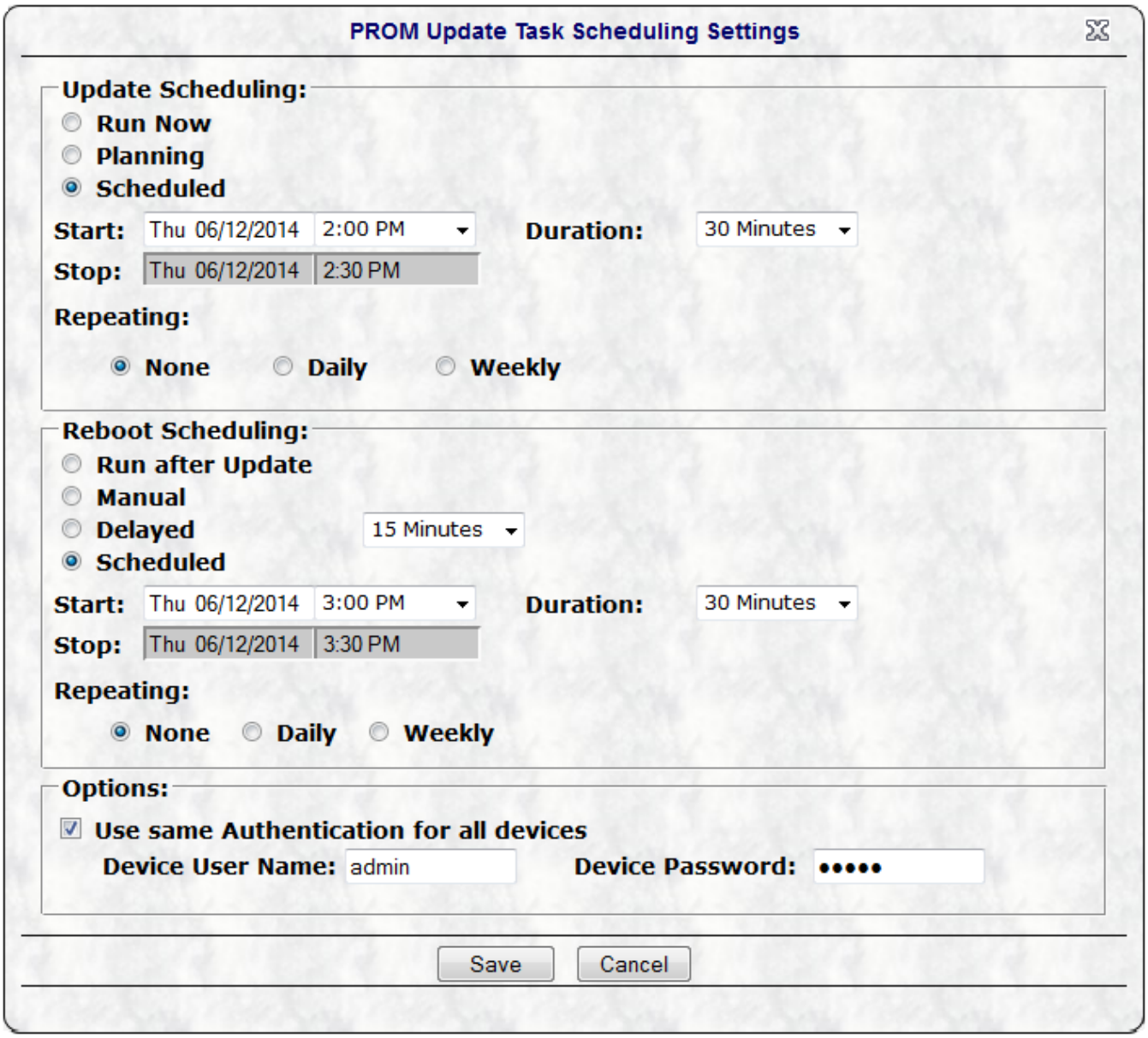
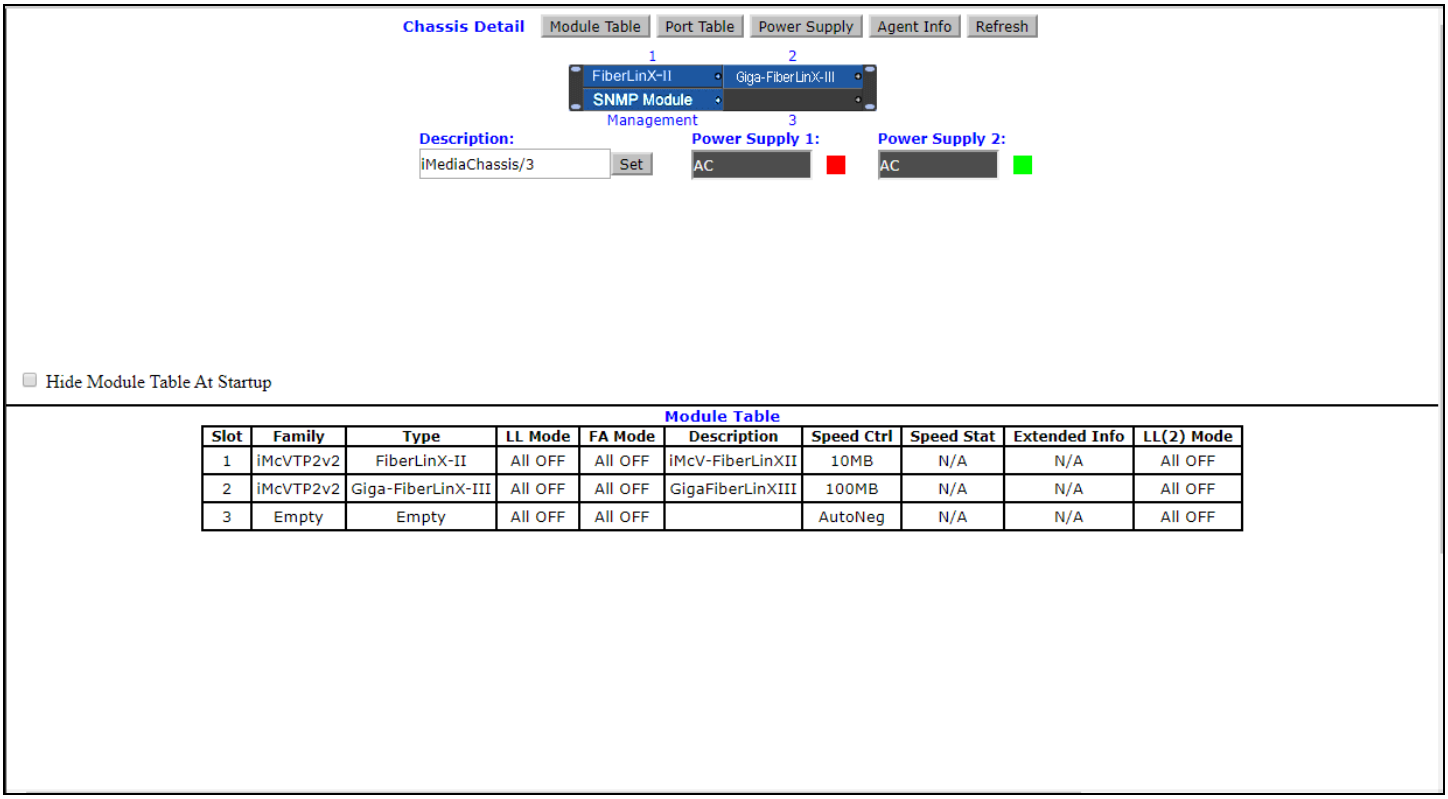


Figure 5.6 – Reboot Scheduling

Using the Chassis View

Selecting a chassis from the "IMC Network Tree" will display the default chassis view. The chassis view consists of 2 sections. The top section displays the "Chassis Detail" view and the bottom section displays the tables (i.e. Module Table, Port Table) associated with the chassis.



Slot	Family	Type	LL Mode	FA Mode	Description	Speed Ctrl	Speed Stat	Extended Info	LL(2) Mode
1	iMcVTP2v2	FiberLinX-II	All OFF	All OFF	iMcV-FiberLinXII	10MB	N/A	N/A	All OFF
2	iMcVTP2v2	Giga-FiberLinX-III	All OFF	All OFF	GigaFiberLinXIII	100MB	N/A	N/A	All OFF
3	Empty	Empty	All OFF	All OFF		AutoNeg	N/A	N/A	All OFF

Figure 5.7 – Default Chassis View

By default, the “Module Table” is displayed when a new chassis is displayed. To disable this feature, the “Chassis Detail” display also includes a configuration option “Hide Module Table At Startup”. If the user clicks to check the “Hide Module Table At Startup”, the “Module Table” will not be created and a splash screen will display instead.

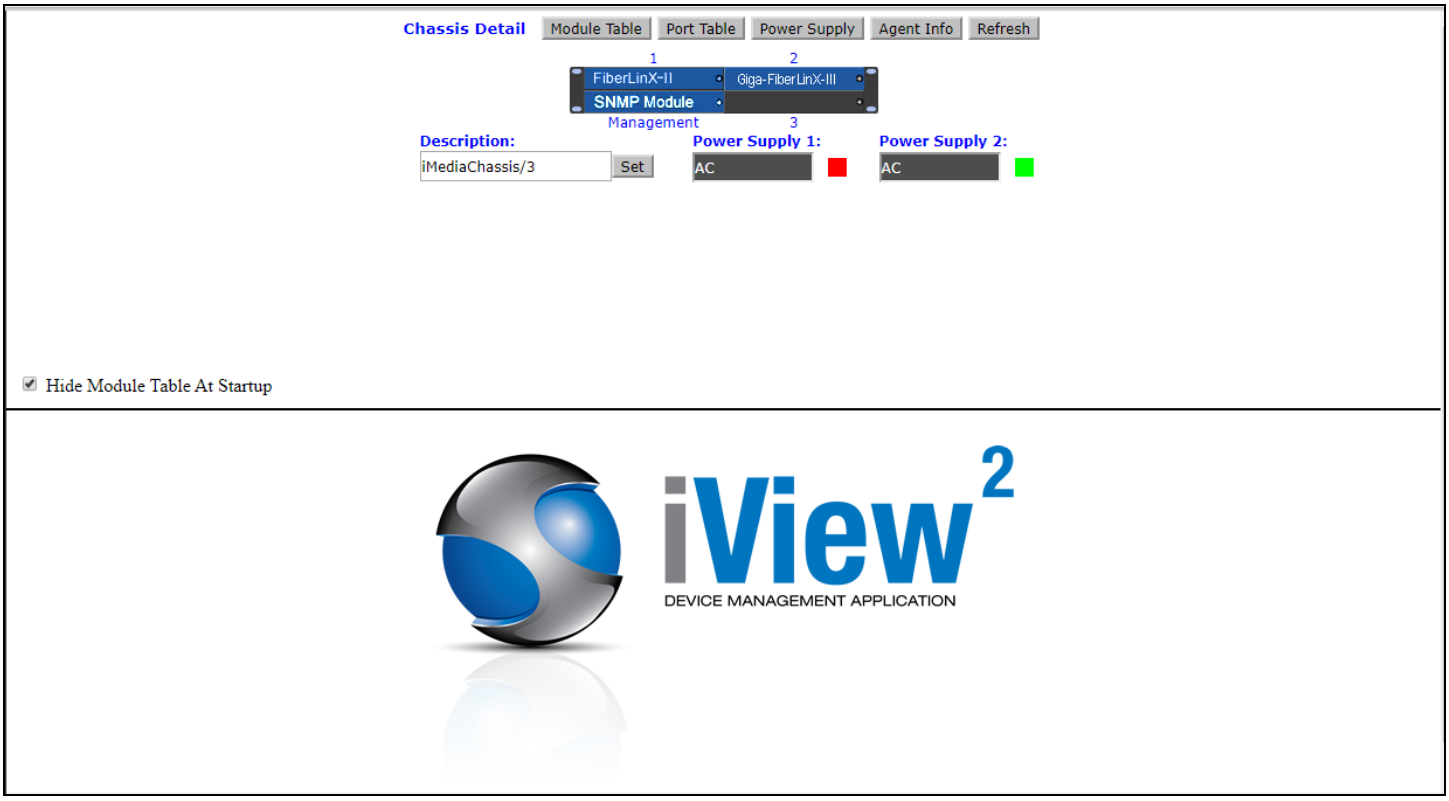


Figure 5.8 – Chassis View with “Hide Module Table At Startup” enabled.

Accessing the SNMP Module

Selecting the “SNMP Module” from the “Chassis Detail” view will replace the Chassis View with the SNMP Module view. To return to the Chassis View select the chassis from the “iView Network Segment List”.

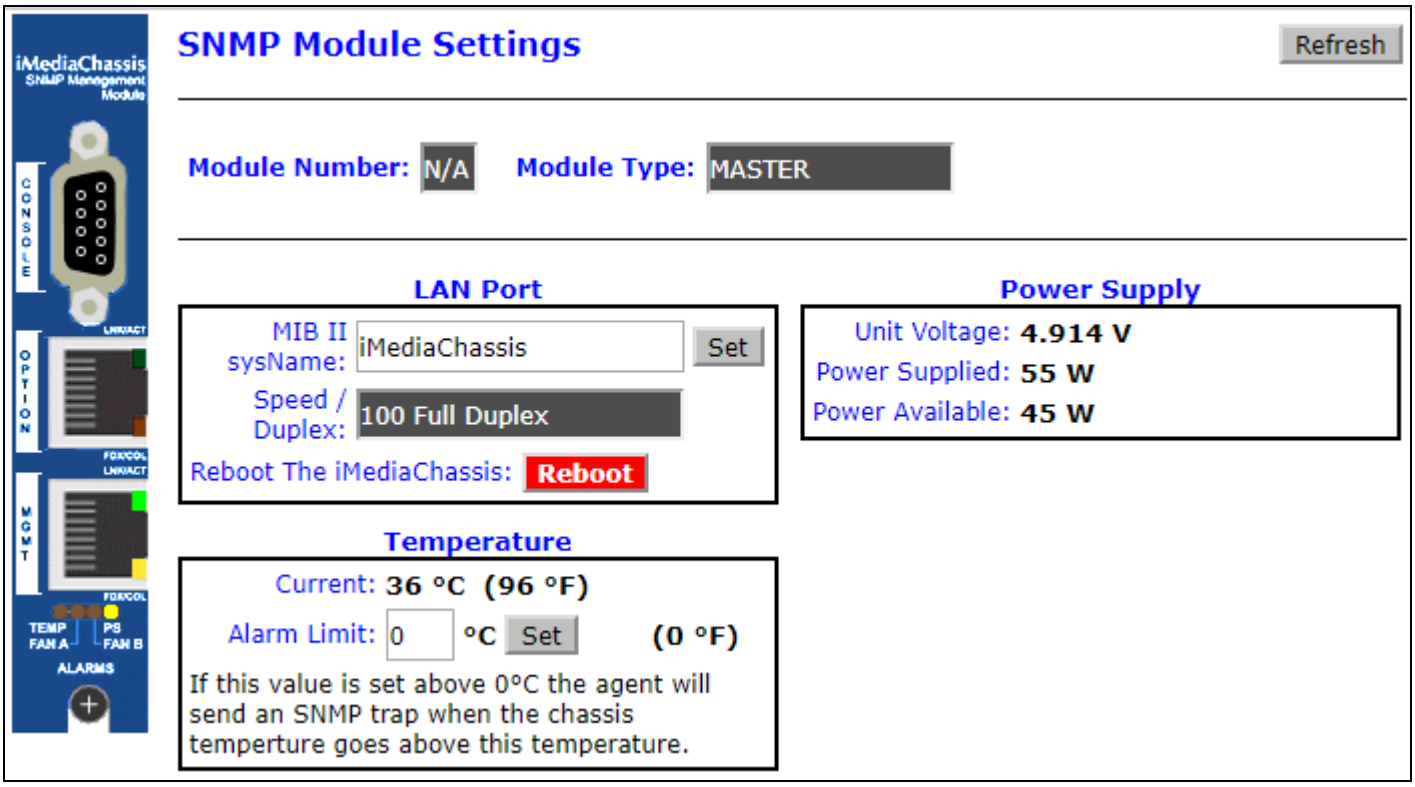


Figure 5.9 – SNMP Module View

iMediaChassis Power Supply Identification Information

There currently is no standard programmatic method to identify the type and manufacturer of power supplies that may be installed in iMediaChassis 3/6/20. iView[2] does allow a user to manually enter, store, and retrieve power supply identification information. Access to this functionality is through the iMediaChassis 3/6/20 Web Brower menu as shown in Figure 5.10.

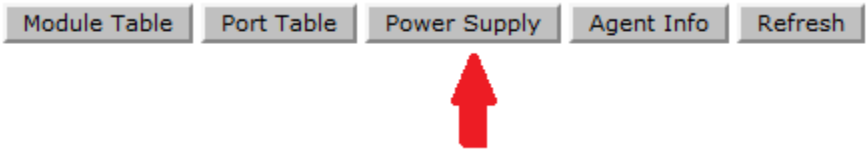


Figure 5.10 – iMediaChassis 3/6/20 Web Browser menu

Selecting the "Power Supply" command button from the menu will display the "Power Supply Information" dialog.

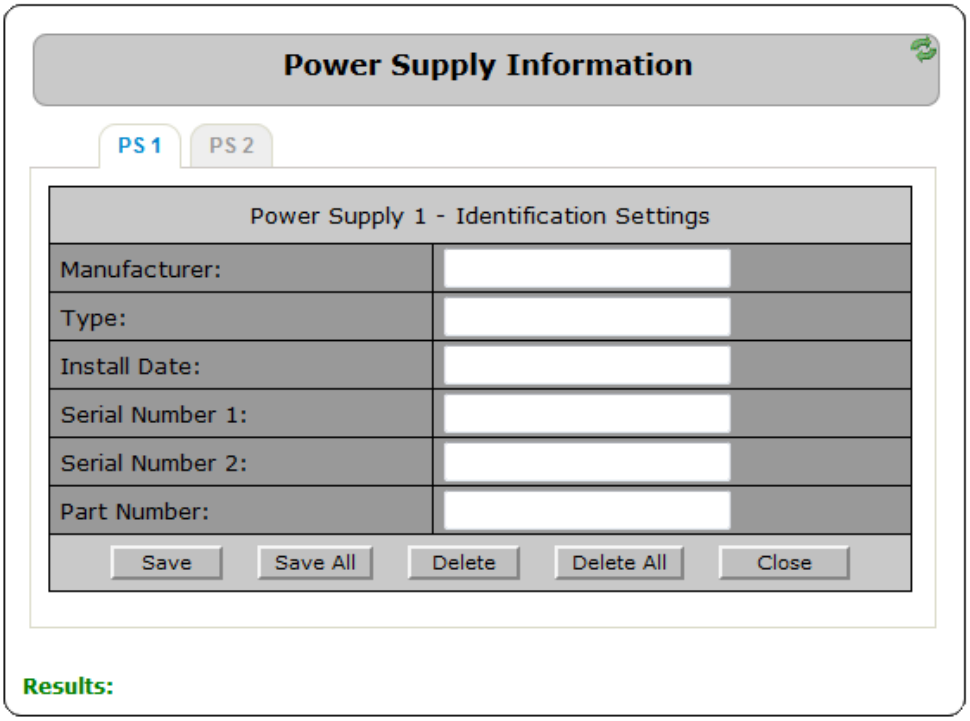


Figure 5.11 - iMediaChassis 3/6/20 "Power Supply Information" dialog

Command Button	*Functionality*
Save	*Save the current tab information to the database for that iMediaChassis.*
Save All	*Save all tabs information to the database for that iMediaChassis.*
Delete	*Delete the current tab information from the database for that iMediaChassis.*
Delete All	*Delete all the tabs information from the database for that iMediaChassis.*
Close	*Close the Power Supply Information dialog.*

Figure 5.12 – "Power Supply Information" command button functionality list

Manufacturer – This is a text field. It supports up to 255 characters using the ECMA-94 standard.
Type – This is a text field. It supports up to 255 characters using the ECMA-94 standard.
Install Date – This is a date field. It uses the format MM-DD-YYCC.
Serial Number 1 – This is a text field. It supports up to 255 characters using the ECMA-94 standard.
Serial Number 2 – This is a text field. It supports up to 255 characters using the ECMA-94 standard.
Part Number – This is a text field. It supports up to 255 characters using the ECMA-94 standard.

Figure 5.13 – “Power Supply Information” data types

Appendix B

B+B SmartWorx Supported Modules

Module Type Id	Module Description
1	iMcV-PIM
2	TP/BNC
3	BNC/FO
4	iMcV-LIM
5	1250-S2MM
9	Mode Converter
10	ATM
11	iMcV-LIM
17	TX/SX-10100
18	GigTXLX
19	FiberWay
21	BWMgr
24	GigTXLX-V2
25	T1/E1/J1
27	WDM
28	iMcV-LIM
29	iMcV-LIM 10/100
30	MediaLinX
31	FM-LIM
32	FT-MediaLinX
33	iMcV-FiberLinX
35	Mode Converter
36	Mode Converter
37	FT-MediaLinX-2TX
38	DS3/E3/STS-1
39	Giga-MediaLinX
41	VDSL-CPE
42	Gigabit
43	FT-ModeConverter
44	iMcV-PIM
45	iMcV-LIM
46	iMcV-Giga-FiberLinX
47	iMcV-FiberLinX
48	iMcV-Giga-FiberLinX
50	MidSpan
51	CCTV
52	iMcV-FiberLinX-II
53	Gigabit
54	Giga-MediaLinX
55	MediaLinX
56	iMcV-Mode Converter
57	T1/E1/J1 SFP
58	iMcV-Switch
59	T1/E1/J1 LT
60	DS3/E3/STS-1 L.T.
61	DS3/E3/STS-1 L.T. (Remote)
62	T1/E1/J1 L.T. (Remote)
63	E1-MUX/4+Eth
64	E1-MUX/4
65	E1-MUX/4+Eth Remote

66	E1-MUX/4 Remote
67	T1/E1/J1
68	IE-iMcV-MediaLinX
69	IE iMcV-VDSL2 Extender
70	IE-iMcV-Gigabit
71	iMcV-T1E1J1-LT
72	iMcV-LIM
73	IE-iMcV-T1-MUX/4
75	IE-iMcV-T1-MUX/4 Remote
77	iMcV-T1E1J1-LT Remote
78	IE-iMcV-2xLIM
79	DS3/E3/STS-1
80	IE-iMcV-MultiWay
81	iMcV-10G-Converter XFP/XFP
82	iMcV-10G-Converter SFP+/SFP+
83	IE-iMcV-MuxDemux
84	IE-iMcV-MuxDemux
85	IE-iMcV-E1-MUX4
87	IE-iMcV-E1-MUX4 Remote
89	iMcV-Giga-MediaLinX
90	iMcV-Giga-FiberLinX-III
100	iMcV-10G-Converter SFP+/UTP
281	T1/E1/J1-SSF
284	iMcV-LIM
286	MediaLinX-SSF
288	FT-MediaLinX-SSF
294	DS3/E3/STS-1-SSF
295	Giga-MediaLinX-SSF
296	VDSL-CO-SSF
298	Gigabit-SSF
13717	IMC-595MPI-A
13718	IMC-595MPI-PS-A

eWorx Supported Modules

Module Type Id	Module Description
23845	SE305-T
23848	SE308-T
23846	SE316-T
24357	SEG305-T
24360	SEG308-T
24358	SEG316-T
24105	SEC310-2SFP-T
24102	SEC318-2SFP-T
33480	SEC510-2SFP-T
33481	SECP510-2SFP-T
33484	SEGP510-2SFP-T
33487	SEG510-2SFP

Advantech Supported Modules

Module Type Id	Module Description
21780	EKI-5525S-SC
21779	EKI-5525S-ST
21778	EKI-5525M-SC
21777	EKI-5525M-ST
21796	EKI-5524SS-SC
21795	EKI-5524SS-ST
21794	EKI-5524MM-SC
21793	EKI-5524MM-ST
22309	EKI-5725
21797	EKI-5525
21800	EKI-5528
21798	EKI-5526
22312	EKI-5728
22313	EKI-5729F
22310	EKI-5726
22294	EKI-5726F
22057	EKI-5629C
22054	EKI-5626C
33482	EKI-7710E-2C
33482	EKI-7710E-2CI
33483	EKI-7710E-2CP
33483	EKI-7710E-2CPI
33485	EKI-7710G-2C
33485	EKI-7710G-2CI
33486	EKI-7710G-2CP
33486	EKI-7710G-2CPI