



# AlphaXD Administrator's Manual

Effective: March 2019

The screenshot shows the AlphaXD web interface. On the left, there is a logo consisting of a square with a stylized 'X' inside, followed by the text "ALPHA XD" in large, bold, white letters. Below this, the text "HFC ELEMENT MONITORING" is displayed in a smaller font. A paragraph of text describes the system's capabilities: "Alpha XD provides status monitoring to critical elements in the HFC network including power supplies, fiber nodes, headend optics, network trackers and AlphaGateways. Alpha XD supports XM3 firmware download and XM360 OSP PM certification reports." On the right side of the interface, there is a "Web Client Login" section with two input fields labeled "User Name" and "Password", and a "Login" button.

**ALPHA XD**  
HFC ELEMENT MONITORING

Alpha XD provides status monitoring to critical elements in the HFC network including power supplies, fiber nodes, headend optics, network trackers and AlphaGateways. Alpha XD supports XM3 firmware download and XM360 OSP PM certification reports.

**Web Client Login**

User Name

Password

Login

Alpha Technologies Inc. | 3767 Alpha Way | Bellingham, WA 98226 | Tel: (360) 392-2217 | Technical Support: (800) 863-3364 | [www.alpha.com](http://www.alpha.com)

## Safety Notes

Alpha considers customer safety and satisfaction its most important priority. To reduce the risk of injury or death and to ensure continual safe operation of this product, certain information is presented differently in this manual. Alpha tries to adhere to ANSI Z535 and encourages special attention and care to information presented in the following manner:



### **WARNING! GENERAL HAZARD**

GENERAL HAZARD WARNING provides safety information to PREVENT INJURY OR DEATH to the technician or user.



### **WARNING! ELECTRICAL HAZARD**

ELECTRICAL HAZARD WARNING provides electrical safety information to PREVENT INJURY OR DEATH to the technician or user.



### **WARNING! FUMES HAZARD**

FUMES HAZARD WARNING provides fumes safety information to PREVENT INJURY OR DEATH to the technician or user.



### **WARNING! FIRE HAZARD**

FIRE HAZARD WARNING provides flammability safety information to PREVENT INJURY OR DEATH to the technician or user.

There may be multiple warnings associated with the call out. Example:



### **WARNING! ELECTRICAL & FIRE HAZARD**

This WARNING provides safety information for both Electrical AND Fire Hazards.



### **CAUTION!**

CAUTION provides safety information intended to PREVENT DAMAGE to material or equipment.



### **NOTICE:**

NOTICE provides additional information to help complete a specific task or procedure.

### **ATTENTION:**

ATTENTION provides specific regulatory/code requirements that may affect the placement of equipment and /or installation procedures.

# AlphaXD

## Administrator's Manual

035-511-B0-001, Rev. A4

Effective Date: March 2019

© 2019 by Alpha Technologies Services, Inc.

### Disclaimer

Images contained in this manual are for illustrative purposes only. These images may not match your installation.

Operator is cautioned to review the drawings and illustrations contained in this manual before proceeding. If there are questions regarding the proper operation of this software, please contact Alpha Technologies or your nearest Alpha representative.

Alpha shall not be held liable for any damage or injury involving its enclosures, power supplies, generators, batteries, other hardware, or software if used or operated in any manner or subject to any condition not consistent with its intended purpose or is installed or operated in an unapproved manner or improperly maintained.

### Contact Information

Sales information and customer service in USA  
(7AM to 5PM, Pacific Time):

360 392 2217

Complete technical support in USA  
(7AM to 5PM, Pacific Time or 24/7 emergency support):

800 863 3364

Website:

[www.alpha.com](http://www.alpha.com)

# Table of Contents

1.0 Introduction . . . . .	11
1.1 AlphaXD Features . . . . .	11
1.2 AlphaXD System Architecture . . . . .	12
1.3 AlphaXD Components . . . . .	13
1.4 AlphaXD System Deployment . . . . .	13
2.0 Getting Started . . . . .	14
2.1 Log In to AlphaXD . . . . .	14
2.2 AlphaXD Tab . . . . .	14
2.3 Basic Account Actions . . . . .	15
Changing the Account Password . . . . .	15
Log Out of AlphaXD . . . . .	15
3.0 Starting and Stopping AlphaXD . . . . .	16
3.1 Starting / Restarting AlphaXD on a Solaris Server . . . . .	16
Manually Starting AlphaXD on a Headless or Non-Headless Solaris Server . . . . .	16
3.2 Stopping AlphaXD on a Solaris Server . . . . .	17
Manually Shutting Down the AlphaXD Software on a Solaris Server . . . . .	17
Shutting Down the AlphaXD Software on a Solaris Server using a Web Browser . . . . .	17
Forcing Shut Down of AlphaXD Software . . . . .	17
3.3 Initial Launch of AlphaXD on a Windows Server . . . . .	18
3.4 Stopping AlphaXD on a Windows Server . . . . .	18
Stopping AlphaXD on a Windows Server . . . . .	18
Shutting Down the AlphaXD Software from a Client Machine . . . . .	19
3.5 Restarting AlphaXD on a Windows Server . . . . .	19
3.6 Authenticating Users Against an External LDAP Directory . . . . .	19
To Specify an External LDAP Directory for Authenticating Users . . . . .	20
4.0 POM Dashboard Setup . . . . .	21
5.0 Scheduler Reports . . . . .	23
6.0 System Setup . . . . .	24
6.1 Security Administration . . . . .	24
6.2 Groups . . . . .	25
Creating and Removing Groups . . . . .	25
Modifying Groups . . . . .	26
Adding or Modifying Members (Users) from a Group . . . . .	26
Changing Group Operation Settings . . . . .	26
Scopes . . . . .	27
6.3 Users . . . . .	28
Creating Users . . . . .	28
Modifying Users . . . . .	30
Deleting Users . . . . .	30
Changing User Status . . . . .	31
Terminating User Sessions . . . . .	31
6.4 Discovery Admin . . . . .	33
Discovery Configurator . . . . .	33
Specifying a Single Node for Discovery (IPv4 Only) . . . . .	36
Specifying Networks for Discovery . . . . .	37
Configuring Discovery of Remote Networks . . . . .	37
Discovering a Range of Network IP Addresses . . . . .	37
Discovering a Range of Node IP Addresses . . . . .	38

# Table of Contents, Continued

Performing Network-Specific Discovery of SNMP Devices . . . . .	38
Preventing Network Discovery . . . . .	39
Deleting Network Entries . . . . .	39
Forcing Rediscovery. . . . .	39
IPv6 Discovery . . . . .	40
Discovery Queue . . . . .	41
Automatic Template Downloads. . . . .	41
6.5 Alert Filtering and Suppression . . . . .	41
Alert Filters . . . . .	41
Filter Rules . . . . .	42
Device Status in Trees . . . . .	42
To Setup an Alert Filter . . . . .	42
JMX ALERT Forward Filtering – Northbound SNMP Traps . . . . .	44
Alert Forwarding Process . . . . .	44
Steps to Setup JMX Filtering . . . . .	45
JmxAlertFilters.xml File . . . . .	46
6.6 Device Configuration and User-Defined Configuration Fields . . . . .	47
6.7 Specifying Parameters for Power Outage Monitoring (POM) . . . . .	48
7.0 System Administration . . . . .	51
7.1 Administration - XM360 Configuration . . . . .	52
7.2 Using the Bulk Task Status Page. . . . .	53
7.3 See Devices in the Discovery Queue. . . . .	54
7.4 Using the Database Backup Page . . . . .	54
Restoring a Database . . . . .	54
7.5 Using the System Performance Page . . . . .	55
Server Details Tab. . . . .	55
Client Details Tab . . . . .	55
7.6 Using the Log Entries Page . . . . .	56
7.7 Using the Log Configuration Page . . . . .	56
Open the Logging Configuration Page . . . . .	56
Editing the Log Settings . . . . .	56
7.8 Using the Logs Monitor Page. . . . .	57
7.9 Setting the Automatic LogOut Time Duration. . . . .	57
8.0 Displaying Data . . . . .	58
8.1 Launching AlphaXD Data Display . . . . .	58
8.2 Categories of Displayable Data. . . . .	59
8.3 Data Display Options . . . . .	60
8.4 Legacy (CheetahNet) Devices Data Display . . . . .	60
8.5 Alpha XD Mobile Page . . . . .	61
9.0 Testing Power Supplies . . . . .	63
9.1 Creating Test Groups or Test Regions . . . . .	64
9.2 Setting Parameters for the Power Supply . . . . .	65
9.3 Power Supply Pre-Tests . . . . .	65
9.4 Background (Automatic) Power Supply Testing . . . . .	65
Creating a Background (Automatic) Power Supply Test . . . . .	66
Removing a Power Supply Test Group . . . . .	68
9.5 On-Demand Power Supply Testing. . . . .	68
Battery Analyst Test . . . . .	69

# Table of Contents, Continued

Inverter Test . . . . .	72
Deep-Drain Test . . . . .	72
Predictive Test. . . . .	73
9.6 Viewing Background (Automatic) Results for Completed Tests . . . . .	74
Viewing Background Testing Power Supply Groupings . . . . .	74
9.7 Viewing Status, Details and Results of On-Demand Tests . . . . .	75
Viewing On-Demand Test Status . . . . .	75
9.8 Excluding a Power Supply from Testing . . . . .	76
10.0 Email Alerts . . . . .	77
10.1 Setting up Emailing . . . . .	77
Configuring Email . . . . .	77
Creating Technicians . . . . .	78
Viewing, Creating, Deleting Technician Schedules . . . . .	79
10.2 Activating Technicians. . . . .	80
10.3 Update the Email Server . . . . .	81
10.4 Edit Technician Information . . . . .	82
10.5 Deleting Technicians . . . . .	82
10.6 Security Permissions . . . . .	82
10.7 Emailing Technicians Using Device Groups. . . . .	83
11.0 Forwarding Notifications to Third-Party Applications . . . . .	84
11.1 Editing the AlphaXD Trap Forwarding Table. . . . .	84
11.2 Trap Message Example . . . . .	86
11.3 Notification Formats . . . . .	87
Managed Object Notifications . . . . .	87
Alert Notifications . . . . .	88
12.0 Downloading Firmware . . . . .	89
12.1 Downloading Generic Firmware. . . . .	89
Setup . . . . .	89
Downloading Generic Firmware to One Device . . . . .	90
Downloading Generic Firmware to Multiple Devices . . . . .	90
12.2 Downloading to Motorola GX-2 Chassis Modules. . . . .	91
Downloading GX-2 Module Firmware to One Module. . . . .	92
Downloading GX-2 Module Firmware to Multiple Modules . . . . .	92
Downloading GX-2 Module Firmware to Like Modules (GX-2 Chassis). . . . .	93
Troubleshooting . . . . .	93
13.0 AlphaXD Utilities . . . . .	94
13.1 Send Event . . . . .	94
13.2 Importing HFC Manager Events into AlphaXD . . . . .	95
Procedure for Windows . . . . .	95
Procedure for Unix . . . . .	97
13.3 Multiple Device/AlarmDynamic Mapping and Route Calculation . . . . .	99
14.0 QAM Constellation Display . . . . .	102
14.1 The QAM Constellation Interface . . . . .	102
14.2 QAM Interface Variables and Parameters. . . . .	103
Device Details . . . . .	100
Configuration Settings. . . . .	100
Downstream (256 QAM) Frequency and Power . . . . .	104
Upstream Frequency and Power . . . . .	104

# Table of Contents, Continued

Downstream Signal Quality . . . . .	104
Codeword Error Rate . . . . .	104
14.3 Interpreting QAM Constellation Map Data by Visual Inspection . . . . .	105
15.0 System Recommendations and Troubleshooting . . . . .	106
15.1 New AlphaXD Installations . . . . .	106
Configuring AlphaXD to Discover DOCSIS-Based Elements . . . . .	106
15.2 Fine-Tuning AlphaXD Parameters . . . . .	107
System Verification . . . . .	107
Performance Tuning and Configuration . . . . .	107
15.3 AlphaXD Bandwidth Information . . . . .	108
15.4 Supported Headend Optical Modules . . . . .	109
15.5 Supported HMTS Devices . . . . .	110
15.6 Troubleshooting . . . . .	111
AlphaXD Startup Issues . . . . .	111
Errors Running Reports . . . . .	113
Database Backup Failures . . . . .	113

# Figures

Fig. 1-1, AlphaXD System Architecture - Typical HFC Installation . . . . .	12
Fig. 2-1, AlphaXD Login Page . . . . .	14
Fig. 2-2, AlphaXD Page . . . . .	14
Fig. 2-3, Basic Account Actions . . . . .	15
Fig. 3-1, Shutdown Server Link . . . . .	17
Fig. 4-1, POM Tree. . . . .	21
Fig. 4-2, Device Configuration - Property - Hub Container. . . . .	21
Fig. 4-3, Access POM Dashboard . . . . .	22
Fig. 5-1, Scheduler Reports Management . . . . .	23
Fig. 5-2, Create Scheduler Report . . . . .	23
Fig. 6-1, Administration Tab . . . . .	24
Fig. 6-2, Group Configuration Window . . . . .	25
Fig. 6-3, Operations Tree Window . . . . .	26
Fig. 6-4, Modify Profile Window . . . . .	27
Fig. 6-5, User Configuration Page . . . . .	28
Fig. 6-6, Add User Page . . . . .	29
Fig. 6-7, Add Multiple Users Page . . . . .	29
Fig. 6-8, Modify User Page - Edit Link . . . . .	30
Fig. 6-9, User Configuration Page - Change Status Menu. . . . .	31
Fig. 6-10, User Configuration Page . . . . .	31
Fig. 6-11, New User in Database. . . . .	32
Fig. 6-12, Terminating a User Session . . . . .	32
Fig. 6-13, Administration Page - Discover Admin Section . . . . .	33
Fig. 6-14, Discovery Configurator - General Tab. . . . .	34
Fig. 6-15, Initial Parameters Window. . . . .	35
Fig. 6-16, Discover Configurator - Network Discovery Tab. . . . .	36
Fig. 6-17, Discovery Queue Page . . . . .	41
Fig. 6-18, Alert Filters . . . . .	41
Fig. 6-19, Alert Filters Page . . . . .	42
Fig. 6-20, Filter Actions Buttons . . . . .	43
Fig. 6-21, New Alert Filter Page . . . . .	43
Fig. 6-22, EnglishToNative.properties . . . . .	47
Fig. 7-1, Administration Page . . . . .	51
Fig. 7-2, Location of XM360 Configuration via Administration Button . . . . .	52
Fig. 7-3, Configure XM360 Integration Window . . . . .	52
Fig. 7-4, Bulk Task Status Page . . . . .	53
Fig. 7-5, Database Backup Page. . . . .	54
Fig. 7-6, System Performance Page . . . . .	55
Fig. 8-1, Parameter Links . . . . .	59
Fig. 8-2, Data Display Table Headings . . . . .	60
Fig. 8-3, Set Data Display Options Page. . . . .	60
Fig. 8-4, Search Options Screen Page. . . . .	61
Fig. 8-5, Devices Selection Screen . . . . .	61
Fig. 8-6, Modify Transponder Screen . . . . .	61
Fig. 8-7, Group Configuration Screen . . . . .	62
Fig. 9-1, Battery Analysis Admin Tool Page . . . . .	67
Fig. 9-2, Battery Test Setup Page . . . . .	68
Fig. 9-3, Battery Analyst Page . . . . .	69



# Figures, Continued

Fig. 9-4, On Demand Inverter Test Page . . . . .	72
Fig. 9-5, Deep Drain Test Page . . . . .	72
Fig. 9-6, Predictive Test Page . . . . .	73
Fig. 9-7, Device Configuration Page . . . . .	76
Fig. 10-1, Email Setup Page . . . . .	77
Fig. 10-2, Notification Page . . . . .	78
Fig. 10-3, Category/Group Setup Tab . . . . .	78
Fig. 10-4, Schedules Page . . . . .	79
Fig. 10-5, Common Tab . . . . .	81
Fig. 13-1, Send Event Utility Page . . . . .	94
Fig. 13-2, HFC Migration Utility . . . . .	95
Fig. 13-3, HFC Migration Utility – Detailed Help with Descriptions. . . . .	96
Fig. 13-4, HFC Mgr Migration Complete . . . . .	96
Fig. 13-5, HFC Migration Utility on UNIX. . . . .	97
Fig. 13-6, Migration Complete on UNIX . . . . .	98
Fig. 13-7, Map Alert from Notifier – Menu Option . . . . .	100
Fig. 13-8, Location Map . . . . .	101
Fig. 13-9, Map with Routes. . . . .	101
Fig. 14-1, QAM Constellation Interface . . . . .	102
Fig. 14-2, Zoom Level of 1 (Left) and Zoom Level of 4 (Right). . . . .	103
Fig. 15-1, Oracle Database Errors . . . . .	111
Fig. 15-2, Successful AlphaXD Restart . . . . .	113

# Tables

Table 6-1, Initial Parameters - Discovery Configurator. . . . .	35
Table 6-2, JmxAlertFilters.xml Parameters. . . . .	46
Table 6-3, POM Configuration Parameters. . . . .	50
Table 9-1, Test Configuration Parameters . . . . .	66
Table 9-2, CAST Setting Parameters . . . . .	67
Table 9-3, Battery Analyst Q&A . . . . .	70
Table 9-4, Battery Analyst Testing Status Results . . . . .	71
Table 11-1, Variable Binding . . . . .	88
Table 13-1, HFC Manager Field / AlphaXD Field. . . . .	98
Table 14-1, QAM Constellation Map Data . . . . .	105
Table 15-1, Status Poll Interval Setup Matrix. . . . .	107
Table 15-2, UI Load Up Time. . . . .	108
Table 15-3, Supported Headend Optical Modules . . . . .	110
Table 15-4, Supported HMTS Devices . . . . .	111

# AlphaXD™ 6.5

AlphaXD™ is a trademark of Alpha Technologies, Inc.

DOCSIS® is a registered trademark of Cable Television Laboratories, Inc.

Solaris® and Oracle® are registered trademarks of Oracle Corporation and/or its affiliates.

Windows® is a registered trademark of Microsoft Corporation.

Chrome™ is a trademark of Google, Inc.

Firefox® is a registered trademark of Mozilla Organization.

All other trademarks and registered trademarks are the property of their respective owners.

The copyright and trade secret laws of the United States and other countries protect this material. It may not be reproduced, distributed, or altered in any fashion by any entity without the expressed written consent of Alpha Technologies, Inc.

This document contains proprietary information that shall be distributed or routed only within Alpha Technologies, Inc. and to its authorized clients, except with written permission from Alpha. Information contained within this document is subject to change without notice. The appearance of some of the graphics in the examples presented in this manual may vary slightly to the actual GUI in the software application.

©2018 Alpha Technologies, Inc. All Rights Reserved. Proprietary - Alpha Technologies, Inc. and Authorized Clients Only

AlphaXD Related Documentation:

- AlphaXD Administrator's Manual (*Alpha p/n 035-511-B0-001*)
- AlphaXD User's Manual (*Alpha p/n 035-512-B0-001*)
- AlphaXD Installation Manual (*Alpha p/n 035-513-C0-001*)

# 1.0 Introduction

AlphaXD™ Multi-Layered Network Assurance Software is a software suite with a complete set of applications for delivering element/network management system (EMS/NMS) solutions. The system is accessible through standard Web browsers on Windows and Solaris machines.

AlphaXD monitors, manages, and tests Hybrid Management Sub-layer (HMS), Data Over Cable Service Interface Specification (DOCSIS®), and legacy devices in Broadband Hybrid Fiber/Coax (HFC) distribution systems. Using embedded and external HMS and DOCSIS® transponders communicating with headend controllers or Cable Modem Termination Systems (CMTS), AlphaXD monitors and tests network devices such as:

- Nodes
- Generators
- Amplifiers
- Power Supplies
- End-of-Line (EL) devices
- Headend Optical Equipment
- AlphaGateways

AlphaXD also provides up-to-date status information, such as:

- On-demand testing
- Call Scheduler

## 1.1 AlphaXD Features

AlphaXD offers the following features:

- An industrial database utilizing Oracle® version 12cR1
- Scalability from dozens to thousands of monitored devices
- An easy-to-use and intuitive graphical interface
- Customizable user accounts with multiple levels of accessibility and privileges
- Auto-Discovery of transponders added to the network (IPv4 and IPv6)
- The ability to create groups for and manage the organization of all network elements
- Support of HMS, Alpha, and other vendor's MIBs for enhanced alarm processing
- Battery analysis that reveals battery trends and enables targeted maintenance repairs
- Integration of CheetahLight, DOCSIS and CheetahNet systems
- Keyboard localization
- Power outage monitoring
- Trap and alarm forwarding northbound to other systems
- Internationalized and currently available in English and Spanish

## 1.0 Introduction, continued

### 1.2 AlphaXD System Architecture

The AlphaXD system design is based on the distributed architecture of a server and intelligent transponders to reduce communications traffic. The distributed architecture allows for better speed, reliability and scalability of the system.

Alpha transponders retain, in flash memory, all information (alarm limits) needed to determine whether a power supply (or other monitored device) is operating within normal ranges. Detailed alarm information is reported immediately to AlphaXD via Simple Network Management Protocol (SNMP) traps in cases where alarms exist. Since SNMP traps do not guarantee delivery, AlphaXD uses a background synchronization process that continuously checks for lost traps and, if needed, takes remedial action to synchronize the data.

Messages sent to AlphaXD are error messages or responses to an operator's request to view an individual transponder element. All messages sent between the AlphaXD software and managed elements are SNMP messages.

Since the transponders send only alarm messages or data requested by an operator, the amount of traffic on the network connecting the transponders and AlphaXD is greatly reduced. This limited traffic allows for a faster and more robust platform. A single AlphaXD server can manage over 20,000 elements in the network via the latest Windows and Solaris platforms.

Since all communications between the AlphaXD software and transponders are SNMP messages, the architecture is open and standardized. This communications scheme makes all of the plant status and alarm information available for integration into a higher-level Operations Support System (OSS).

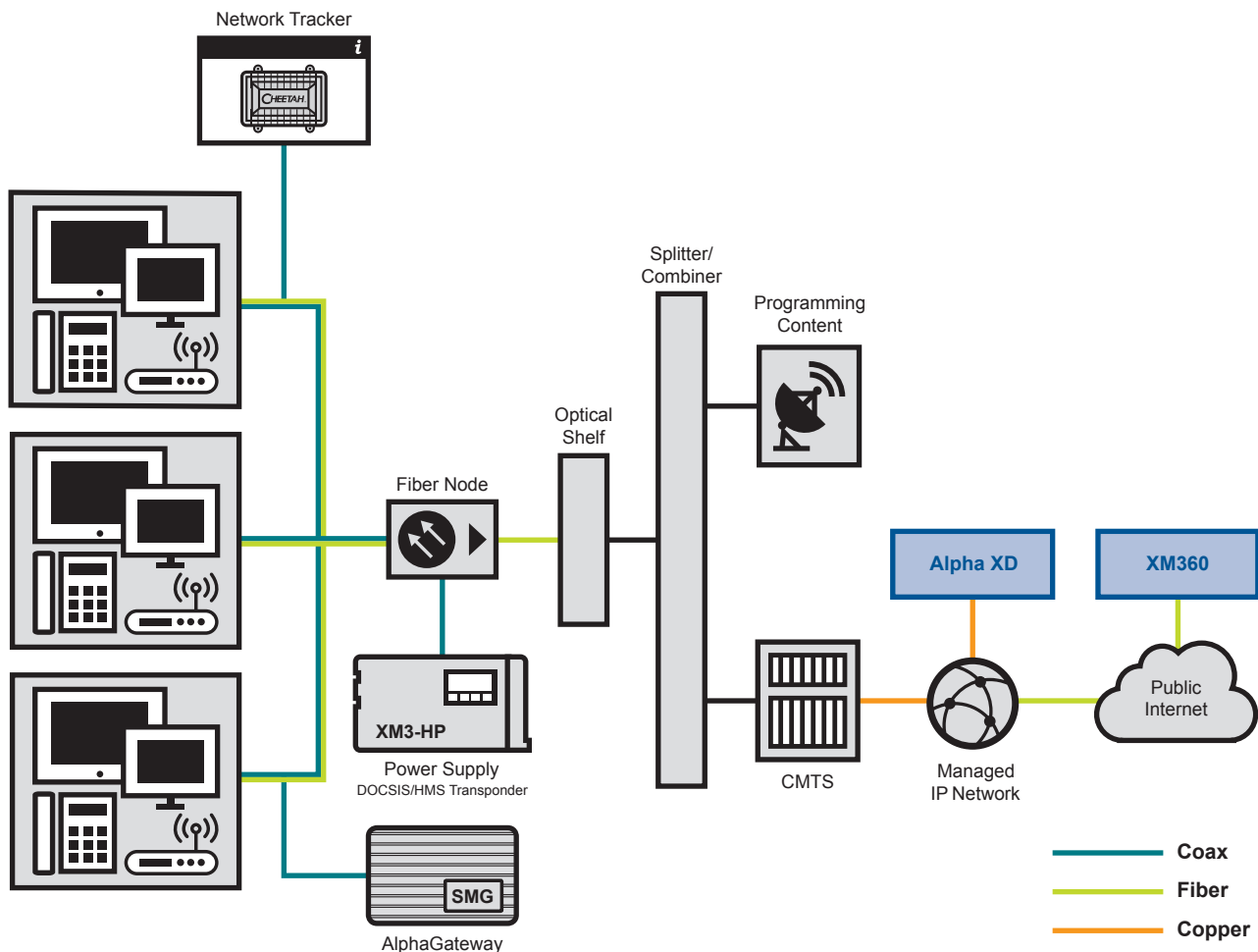


Fig. 1-1, AlphaXD System Architecture - Typical HFC Installation

## 1.0 Introduction, continued

### 1.3 AlphaXD Components

AlphaXD consists of the following five components:

- Oracle® Software
- Oracle® Database
- AlphaXD Database
- AlphaXD Application
- PCs running a Web browser

These components work together to allow the user to manage the cable system. They provide notification of problems reported by transponders, headend controllers, and inside plant equipment.

Database tables store the following information:

- Configuration data – Contains network element (NE) data, alarm limits and the current status of specified devices.
- Alarm data – Lists current alarms of all or selected devices and provides a historical listing of all alarms.
- Audit data – Tracks changes to parameters and user activity.
- Security system data – Establishes user name, password and privilege data for all users.

### 1.4 AlphaXD System Deployment

A system could be viewed as a single software server accessed by Web browsers on multiple PCs, with the software monitoring devices deployed throughout the physical network. Each AlphaXD server allows up to 25 simultaneous client connections. The only limiting factor is whether the capacity of the database will enable the total number of elements to be supported. While there is no hard limit on this, performance slowly decreases as database size increases. Server database capacity has been tested and performed well with up to 20,000 transponders. AlphaXD also supports up to 25 network trackers. For networks that have the potential to grow much larger than this, multiple separate systems should be considered. AlphaXD servers communicate using standard protocols such as Simple Network Management Protocol (SNMP), and Transmission Control Protocol/Internet Protocol (TCP/IP). This provides a flexible architecture for deployment.

# 2.0 Getting Started

## 2.1 Log In to AlphaXD

Open a supported Web browser (Chrome or Firefox) and enter http://AlphaXD:9090 (server name) or http://172.16.0.1:9090 (IP address).

On the AlphaXD Login page, enter a user name and password and click **Login** (Default Username: root) (Default Password: public).

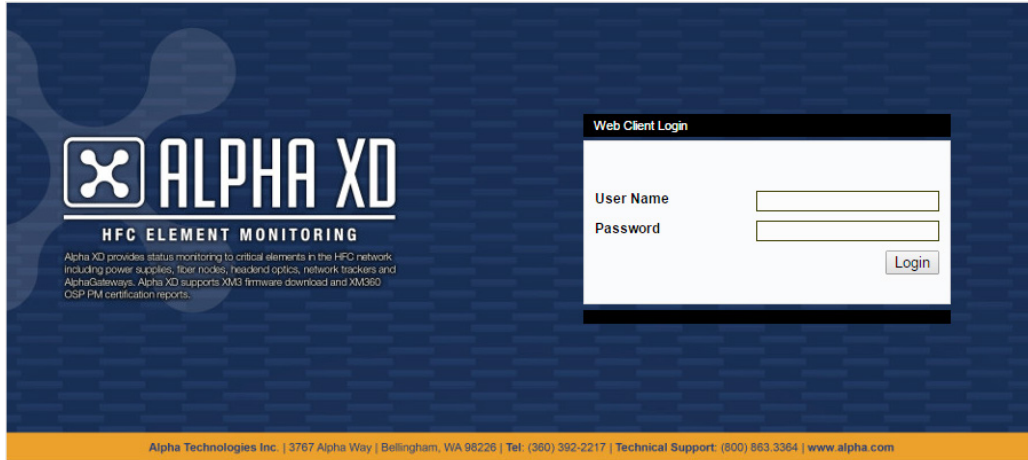


Fig. 2-1, AlphaXD Login Page

## 2.2 AlphaXD Tab

After logging in for the first time, AlphaXD will display the Faults page by default. Subsequent logins will display the last page where the user logged out. The AlphaXD page (accessed by the AlphaXD tab, see Fig. 2-2) provides an overview of the network, its elements and the overall status of the elements. This page is seen whenever an upper level container is selected in the tree such as, the root node of the tree, regions and groups. Selecting Alpha XD Mobile from this tab will open a dialog box to select a search option for Power supplies, Transponder MAC addresses or Nodes.

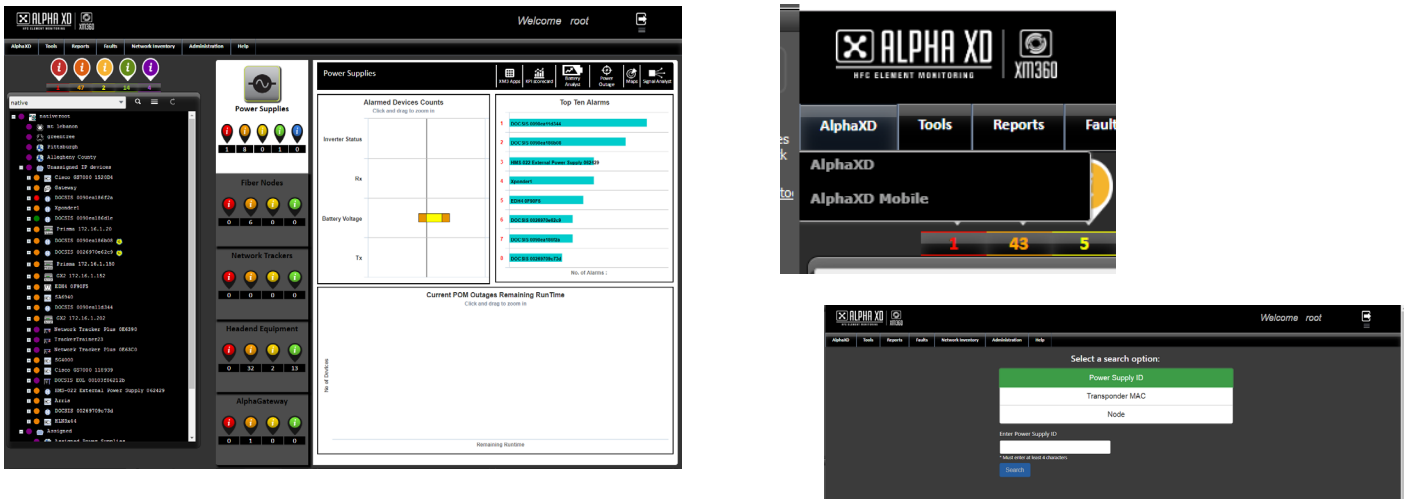


Fig. 2-2, AlphaXD Page

## 2.0 Getting Started, continued

### 2.3 Basic Account Actions

#### Changing the Account Password



#### **NOTICE:**

Usernames and Passwords are case-sensitive.

1. In the top right corner of any AlphaXD page, hover over the **List** icon.
2. Click **Change Password**.
3. In the pop-up **Browser Window**, enter the proper information.
4. Click **Submit**.

#### Log Out of AlphaXD

In the top right corner of any AlphaXD page, click on the **Logout** icon.



Fig. 2-3, Basic Account Actions

## 3.0 Starting and Stopping AlphaXD

Properly starting and stopping the AlphaXD software avoids potential problems. These problems can arise from open ports, commands and processes pointing to windows and other processes in unexpected states, and other miscommunications. Always start and stop the AlphaXD software according to the procedures in this section.

AlphaXD runs as a service on both Windows and Solaris systems. However, AlphaXD must be run manually the first time, so that the license key can be provided.

For details on installing the AlphaXD software and required licenses, please refer to the latest version of the AlphaXD Installation Guide (*Alpha p/n 050-0096*).

### 3.1 Starting / Restarting AlphaXD on a Solaris Server

The AlphaXD software running on a Solaris server may be restarted by rebooting the server itself as long as the software has been initially started, and the license information has been correctly entered. However, the Sentinel license service and the AlphaXD service can be manually restarted as well. The procedure in this section provides information on how to conduct a manual restart.



#### **NOTICE:**

---

The configuration of a Solaris Server is dependent upon the hardware and operating system settings. If the Solaris Operating System is configured to reboot automatically after a power failure, AlphaXD processes will start after the OS is running; no special setting is required for AlphaXD.

Some Solaris systems may be “headless”. The term headless typically refers to a system without graphics capability (i.e., no monitor) and generally no console or keyboard interface.



#### **NOTICE:**

---

On headless servers that have video cards, Alpha recommends installing a mouse, keyboard, and monitor prior to installing the AlphaXD software. These devices can be removed after the software is successfully installed. For servers without video cards, it is necessary to have an X-terminal application, such as Exceed, installed and running on a separate machine to access the AlphaXD server for installation. Also, the DISPLAY environment variable may need to be set before starting the actual installation to direct the launched GUI onto the X-window client. In csh (C Shell), use the command listed below. The x.x.x.x portion of the command is the IP address of the X-window client.

```
# setenv DISPLAY x.x.x.x:0.0
```

### Manually Starting AlphaXD on a Headless or Non-Headless Solaris Server

1. Change the directory to match the location of the AlphaXD installation.
2. Enter the following path: AlphaXD/lm720/bin
3. Type the command shown to start the license server: `#!/lserv &`
4. If desired, confirm that the license server is running by entering the following command: `ps -ef | grep lserv`
5. Next, enter the path shown in the following example: `opt/AlphaXD/bin`
6. Type the following command to start the AlphaXD software: `#!/startAlphaXD.sh &`
7. If desired, confirm that the AlphaXD software is running by entering the following command: `ps -ef | grep XD`



### 3.0 Starting and Stopping AlphaXD, continued

## 3.2 Stopping AlphaXD on a Solaris Server

The AlphaXD software can be shut down in one of two ways: manually at the server, or through a client machine using a Web browser interface. It may take several minutes for the AlphaXD shutdown to complete.

### Manually Shutting Down the AlphaXD Software on a Solaris Server

1. Enter the path shown in the following example: `/opt/AlphaXD/bin`.
2. Change to a super-user status.
3. Run the shutdown script by typing the following command. (Note the leading decimal point.): `./Shutdown.sh`
4. When the User Name and Password prompts appear, enter the appropriate User Name and Password information.

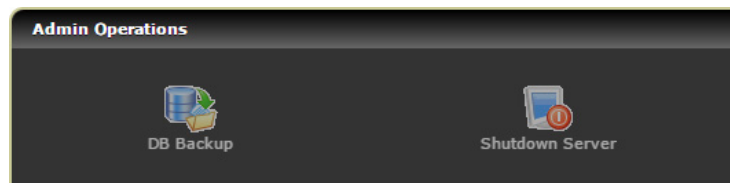
### Shutting Down the AlphaXD Software on a Solaris Server using a Web Browser

1. Connect to the server running the AlphaXD software using a client machine with a Web browser installed, and log into the AlphaXD system as a user with Admin privileges.

#### **NOTICE:**

To shut down AlphaXD, the operator must log into the system as a user with an Admin user privilege.

2. Select the **Administration tab**.
3. From the Admin Operations panel, select **Shutdown Server**.



**Fig. 3-1, Shutdown Server Link**

4. When the shutdown window displays, click **Yes**.

### Forcing Shut Down of AlphaXD Software

Forcing an AlphaXD shut down should only be done if other attempts to shut down AlphaXD have failed.

1. Enter `ps -ef |grep AlphaXD` to see the XD processes. Example: `# ps -ef |grep AlphaXD`

```
root 26598 26548 0 Aug 07 pts/5 0:00 /bin/sh ./startAlphaXD.sh
root 26599 26598 0 Aug 07 pts/5 106:15 ./jre/bin/java -cp ../classes
s:./classes/WebNMS_jars.jar:./classes/AlphaXD_ja
root 28755 28730 0 11:20:52 pts/7 0:00 grep AlphaXD
```

2. Enter `kill -9` and the process numbers. Examples:

```
# kill -9 26598
# kill -9 26599
# ps -ef |grep AlphaXD
```

## 3.0 Starting and Stopping AlphaXD, continued

### 3.3 Initial Launch of AlphaXD on a Windows Server

1. Using the Services feature in Windows, verify that the Sentinel license service is running.
2. Select **Start > All Programs > AlphaXD > Start AlphaXD**. The License Agreement window displays.
  - On Windows Server 2012, access AlphaXD by selecting **All Apps > Start AlphaXD**.
3. Click the **License Acceptance Checkbox**, then click **Next**. The Licensee Details window displays.
4. Click **Browse**. The Select License File window displays.
5. Navigate to the folder containing the AlphaXD license file. Select the file and then click **Open**.
6. Click the **Next** button in the Licensee Details window. Each license contains a list of authorized user names. The User Name field displays the default user name from the list. The user whose name appears in the User Name field will become the registered user assigned to this installation. To assign a different user name to the field, select the new user name from the drop-down list.
7. Select a new **User Name**, if desired.
8. Click **Finish**. A DOS (command) window appears and lists the AlphaXD primary modules as they start. After AlphaXD starts successfully, the DOS window displays a line of information containing a server port number.



#### CAUTION!

DO NOT close the DOS window. Closing the DOS window will cause the AlphaXD services to terminate. If desired, minimize the DOS window.

The server port number is used by client machines for communications. Once communications have been established between the server and client(s), operators can begin accessing the AlphaXD software through Web browsers installed on the client machine(s).

### 3.4 Stopping AlphaXD on a Windows Server

AlphaXD software must be shut down before the server is shut down, upgraded, or has other software installed. AlphaXD software that resides on a Windows system can be shut down locally, on the server where the software resides, or remotely through a client machine's Web browser.

#### Stopping AlphaXD on a Windows Server

1. On the Start Menu, navigate to the AlphaXD folder and select Shutdown AlphaXD. Select **Start > All Programs > AlphaXD > Shutdown AlphaXD**. The Shutdown AlphaXD Server window appears. If the port information does not need to be changed, proceed to Step 3.
  - On Windows Server 2012, access AlphaXD by selecting **All Apps > Shutdown AlphaXD**.



#### NOTICE:

If the AlphaXD default port information has not changed, it is not necessary to change the port information.

2. Click **Settings** to change the shutdown type or port number. Clicking Settings opens the Mode of Shutdown window. If desired, select the shutdown mode, enter the new port number, and click **OK** to save the changes or **Cancel** to close the window without saving the changes.
3. On the Shutdown AlphaXD Server window, enter a password and click **OK**. A DOS window will appear and display the AlphaXD processes as they are stopped.
4. When the processes have stopped, the Shutdown Status window is displayed. Click **OK**. AlphaXD is now shut down.

### 3.0 Starting and Stopping AlphaXD, continued

#### Shutting Down the AlphaXD Software from a Client Machine

1. Log into AlphaXD using a Web browser on a client machine.
2. On the AlphaXD main page, select the **Administration tab**.
3. In the Admin Operations panel, select **Shutdown Server**.
4. After the confirmation window, click **Yes** to shut down the server.

### 3.5 Restarting AlphaXD on a Windows Server



#### **NOTICE:**

If the AlphaXD default port information has not changed, it is not necessary to change the port information.

To restart AlphaXD on a Windows server, navigate to Start > All Programs > AlphaXD and select Start AlphaXD. A DOS window appears and lists the AlphaXD primary modules as they start.



#### **CAUTION!**

**DO NOT** close the DOS window. Closing the DOS window will cause the AlphaXD services to terminate. If desired, minimize the DOS window.

After AlphaXD starts successfully, the DOS window displays a line of information containing a server port number.

This port number is used by the client machines for communications. Once communications have been established between the server and client(s), operators can begin accessing the AlphaXD software through Web browsers installed on the client machine(s).

### 3.6 Authenticating Users Against an External LDAP Directory

AlphaXD supports two schemes of binding to an LDAP server: User Bind and Anonymous Bind. User binding requires the creation of a LDAP user account (typically a restricted, read-only account) with an associated user name and password. The user name and password need to be configured in AlphaXD (please refer to the ldap.conf example in this section). Anonymous binding does not require a login and/or password. Authentication via LDAP is a three-step process:

1. Bind to an LDAP account to be used for the AlphaXD application.
2. Issue an LDAP search to retrieve the DN to use for AlphaXD user level authentication.
3. Bind to the AlphaXD login name's account.

If the bind in Step 3 succeeds, the AlphaXD user authentication is deemed successful. If any step fails, the AlphaXD user authentication is deemed unsuccessful.



#### **NOTICE:**

The length for all AlphaXD passwords is limited to 8 characters. The LDAP user account password cannot be longer than 8 characters.

### 3.0 Starting and Stopping AlphaXD, continued

#### To Specify an External LDAP Directory for Authenticating Users

1. Add the file CTLdapAuthentication.jar to the CLASS\_PATH of the following files (depending on the platform). This jar file resides in the <AlphaXD-Home>/classes directory.
2. In the <AlphaXD-Home>/conf directory, edit the following files:

Edit the Following Files	
File Name	Changes
NmsProcessBE.conf	Provide an ARGS entry for the LDAP authentication class under the parameter PROCESS com.adventnet.nms.security.authentication.NmsAuthenticationManager ARGS AuthenticationImpl com.Cheetah.cable.ccms.authentication.CTLdapAuthenticationImpl maximum_allowed_login_failed_count 0
clientparameters.conf	Add the following entry to the end of the ARCHIVE parameter: ../classes/CTLdapAuthentication.jar
Serverparameters.conf	Add the following entry: #Added for LDAP Authentication CRYPTO_CLASS com.Cheetah.cable.ccms.authentication.CTLdapEncryption
ldap.conf	This file is referenced by AlphaXD's LDAP authentication mechanism. Of the ten attributes defined in this file, seven must be customized. The seven attributes are listed below with a short description following each.  MY_SERVICE="ldap://localhost:389" This is the host name and port number of the LDAP server, (default LDAP server port number is usually 389.)  MGR_DN="cn=Manager,dc=tollgrade,dc=com" The DN (Distinguished Name) for the directory manager entry.  MGR_PW="secret" The password for the manager DN.  SECURITY_AUTHENTICATION="simple" The authentication mechanism used to encrypt passwords stored in the attribute defined in PWD_ATTRIBUTE(see below).  USER_BASE="ou=people,dc=tollgrade,dc=com" The starting point for searching the ldap directory.  UID_ATTRIBUTE="cn" The name of the attribute for user login name.  PWD_ATTRIBUTE="userPassword" The name of the attribute for the password entry.

3. Navigate to the <AlphaXD-Home>/bin directory.
4. Shut down AlphaXD using the following command: shutdown.bat/.sh
5. Start AlphaXD for the first time using the following command: startAlphaXD.bat/.sh

# 4.0 POM Dashboard Setup

Follow the steps outlined below for setting up POM Dashboard.

## 1. Create POM Structure:

- Create Regions, Areas and Hubs that will be used to create the POM Dashboard hierarchy in the Native tree. Note that there is no specific device type for Area, use either the region type (Region -- Region -- None) or the hub type (Hub -- Hub -- None).
- Create the POM Tree with the name "POM" and copy element to the tree.
- Arrange the hierarchy of the in the POM Tree. The first level of the hierarchy is Region, the second level is Area, and the third level is Hub.

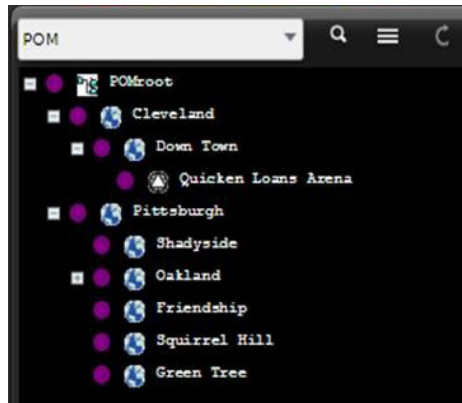


Fig. 4-1, POM Tree

## 2. Update Device Location and Hub Containers:

- Open the Device Configuration page of each device and access the **Property** tab. Expand the Parent device. In the *Location* field enter the address or GPS coordinates and in the *Hub Container* field enter the exact name of the Hub. Click the **Save** button. Note: The POM Dashboard does not map devices with no location, even if it is assigned to a hub. Also, The *Hub Container* entry is case sensitive. The hub name needs to be entered exactly as it appears in the POM tree. If the *Hub Container* name is not an exact match of what appears in the POM tree then it will not appear in the POM Dashboard.

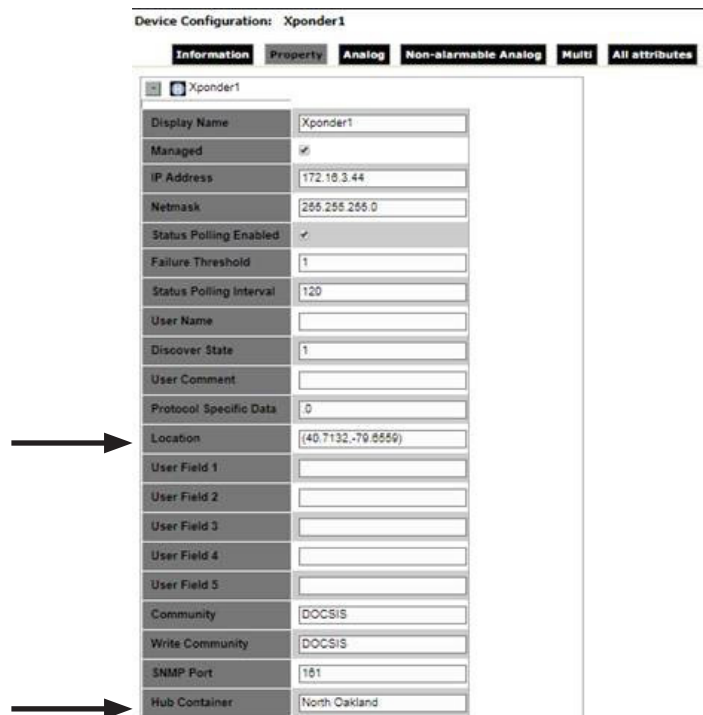


Fig. 4-2, Device Configuration - Property - Hub Container

## 6.0 System Setup, continued

3. To set a *Hub Container* for multiple devices select the desired devices in the tree. Right click on one of the highlighted devices and select **Bulk Property Update**. When the Bulk Property Update Dialog box appears select *Hub Container* from the **Properties** drop down menu. In the **Value** field enter the exact name of the Hub the devices should be assigned. Click the **Update** button. The Bulk Task Status page will appear. The current update will appear in the **Active Bulk Tasks** section until it complete. Once completed it will be moved to the **Completed Bulk Tasks** section of the page.
4. To access the POM Dashboard select **Faults** and then **POM Dashboard** from the menu bar.

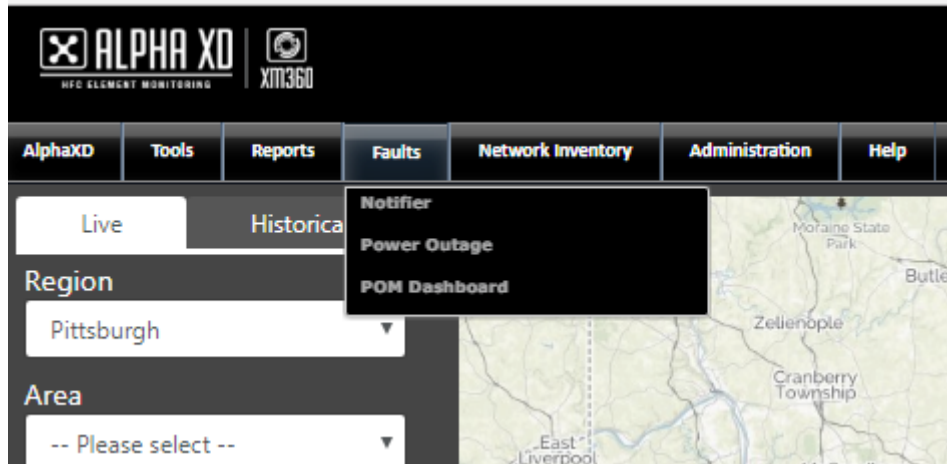


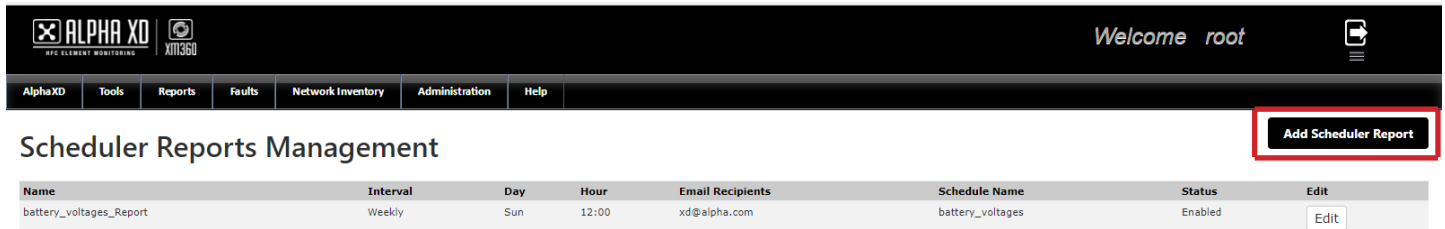
Fig. 4-3, Access POM Dashboard

## 5.0 Scheduler Reports

The Scheduler Reports is a licensed feature that allows the user to setup AlphaXD to generate scheduled reports from the Schedules in Schedule Management. These reports can be generated on a daily or weekly basis and can be setup to be e-mailed automatically. These generated reports are stored on the AlphaXD server in the following path: \\AlphaXD\webclient\reporting\schedulerReports.

To purchase the license for the Scheduler Reports option contact your Alpha sales representative.

Any Schedule in Schedule Management can be setup in Scheduler Reports. Once one of the Schedules in Schedule Management is setup in Scheduler Reports, it cannot be selected again (it is removed from the Schedules dropdown on the Create Scheduler Reports page).

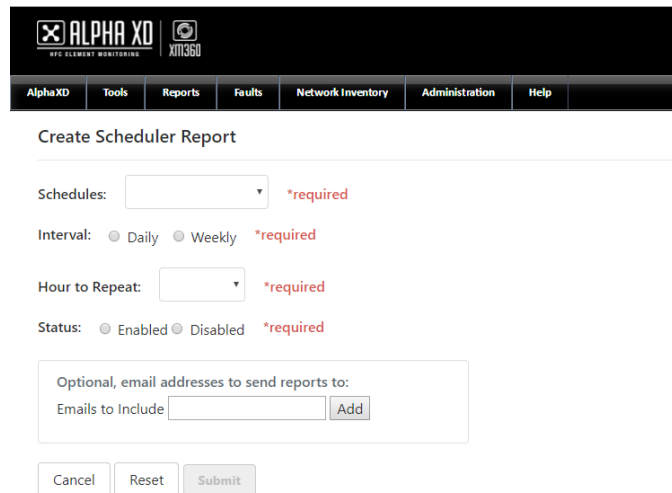


The screenshot shows the 'Scheduler Reports Management' page. At the top, there is a navigation bar with the AlphaXD logo and 'Welcome root'. Below the navigation bar, there is a table of reports. The table has columns for Name, Interval, Day, Hour, Email Recipients, Schedule Name, Status, and Edit. One report is listed: 'battery\_voltages\_Report' with a Weekly interval on Sunday at 12:00, email recipients 'xd@alpha.com', and a status of 'Enabled'. An 'Add Scheduler Report' button is highlighted with a red box in the top right corner.

Name	Interval	Day	Hour	Email Recipients	Schedule Name	Status	Edit
battery_voltages_Report	Weekly	Sun	12:00	xd@alpha.com	battery_voltages	Enabled	Edit

Fig. 5-1, Scheduler Reports Management

To add a Scheduler Report, click **Add Scheduler Report**. This will open the Create Scheduler Reports page.



The screenshot shows the 'Create Scheduler Report' page. It has a navigation bar at the top with the AlphaXD logo and 'Welcome root'. Below the navigation bar, there is a form with the following fields: 'Schedules:' with a dropdown menu and a '\*required' label; 'Interval:' with radio buttons for 'Daily' and 'Weekly' and a '\*required' label; 'Hour to Repeat:' with a dropdown menu and a '\*required' label; 'Status:' with radio buttons for 'Enabled' and 'Disabled' and a '\*required' label; and an optional section for 'Optional, email addresses to send reports to:' with a text box for 'Emails to Include' and an 'Add' button. At the bottom of the form, there are 'Cancel', 'Reset', and 'Submit' buttons.

Fig. 5-2, Create Scheduler Report

In the Create Scheduler Report page click the *Schedules* drop down box to select one of the Schedules from Schedule Management. If there are no Schedules setup in Schedule Management nothing will appear in this drop down box. Also, the Schedule in Schedule Management needs to be Enabled and had run at least once for there to be data in the Scheduler Report.

Select the *Interval* in which it is desired to generate the report, Daily or Weekly. A Weekly report will retrieve one week's worth of data and a Daily report will retrieve 24 hours worth of data.

Select the *Hour to Repeat*, 0:00 - 23:00.

Select the *Status* of the Report Generation. This needs to be Enabled for the report to be generated.

If it is desired to have the report e-mailed when generated enter an e-mail address in the *Emails to include* text box and then click the **Add** button. Additional e-mail addresses can be added after each click of the **Add** button.

Click the **Submit** button to save the settings for the Scheduler Report.

Once a Scheduler Report is created it can be deleted or edited by clicking the **Edit** button for the item.

## 6.0 System Setup

A typical AlphaXD system setup includes creating users, groups, and permissions, as well as configuring the discovery and auto-discovery parameters. These operations can be completed on the Administration page (Fig. 6-1). They can also be accessed via the dropdown menu of the Administration tab.

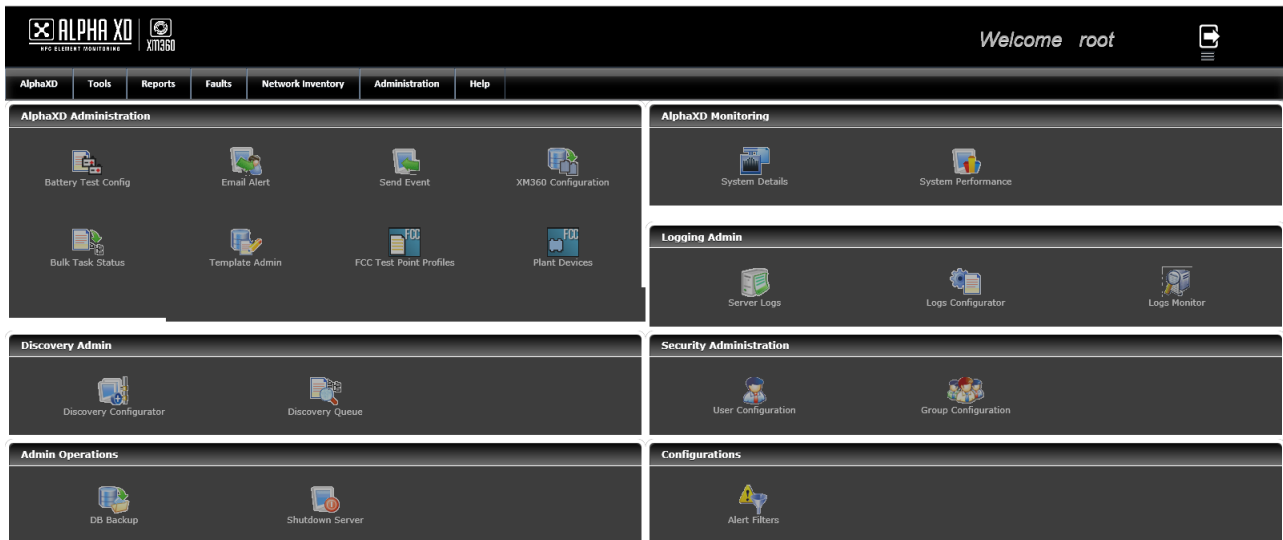


Fig. 6-1, Administration Tab

### Security Administration Panel

- User Configuration - Create and maintain user information
- Group Configuration - Create and maintain group information

### Discovery Admin Panel

- Discovery Configurator - Configure the discovery and auto-discovery parameters
- Discovery Queue - Display all of the active discoveries, the discoveries currently in the queue, and the discoveries on the waiting list

## 6.1 Security Administration

System Security consists of specifying the following:

- Groups - Where the administrator specifies permissions
- Scopes - Where the administrator limits permissions to specific tree views
- Users - Where the administrator creates login names and passwords for authorized users

Managing these aspects in combination allows administrators to ensure that access to AlphaXD is controlled, data integrity is assured and system use is properly logged.

The administrator should set up the system security in the following order:

1. Create groups
2. Apply scopes to groups
3. Create users (including specifying the groups to which they belong)



## 6.0 System Setup, continued

### 6.2 Groups

A group is a collection of access and function permissions. Creating a group means selecting from a list of specific permissions that are granted or denied to the group. The group(s) associated with a user name is the mechanism that determines a user's privileges.

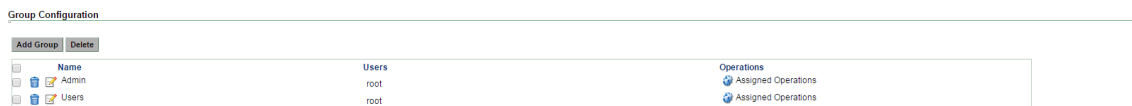
To decide what kinds of groups to create, define the types of users according to the functions they will perform. Create a group for each set of functions. For example:

- Administrative or root-level users have full permissions.
- Department heads have permission to create users, perform database backups and configure power supply testing schedules.
- General users can interact with devices, acknowledge and clear alarms, and run reports.

### Creating and Removing Groups

#### Create a group to define a set of permissions:

1. From the Security Administration panel, click the **Group Configuration** link. The Group Configuration window displays, as shown in Fig. 6-2.



**Fig. 6-2, Group Configuration Window**

2. Click **Add Group**.
3. Enter the group name. Group names should not contain spaces.
4. Expand the **AlphaXD** set and choose the desired operations and permissions by selecting the applicable checkboxes. Select the checkbox for the overall AlphaXD set to assign all of the permissions and operations for the set. Selecting any checkbox multiple times toggles the state of the permission among these three options:
  - First Click – A checkmark is placed in the checkbox to indicate the function is permitted.
  - Second Click – An X is placed in the checkbox to indicate the function is not permitted.
  - Third Click – The checkbox is cleared. Functions with cleared checkboxes are considered denied functions, and will not be permitted for the group.
5. When finished applying operations and permissions, click **Save**.

#### Deleting Groups:

Delete an individual group by selecting the **Trashcan** icon in front of the group name.

Delete multiple groups by selecting the checkboxes in front of each desired group name and clicking the **Delete** button.



#### **CAUTION!**

Do not attempt to delete all of the groups at one time.

## 6.0 System Setup, continued

### Modifying Groups

Click the **Group Configuration** icon from the Security Administration panel on the Administration tab to complete any of the following actions:

- Add and remove users from a group
- Add, modify, or remove operations and permissions
- Assign or remove custom view scopes

### Adding or Modifying Members (Users) from a Group

1. Select the **Group Configuration** icon from the Security Administration panel on the Administration tab.
2. On the Group Configuration screen, click on the name of the group being modified.
3. Select the **Members** header, expanding the Members section.
4. Click **Assign User**.
5. Highlight one or more user names in the Available Users field. Click the **Right-Facing Arrow** to add the name(s) into the Enrolled Users field.
  - If removing a user: highlight one or more names in the Enrolled Users field and click the **Left-Facing Arrow** to move the name(s) into the Available Users field.
6. Click **Submit** to update the group.

### Changing Group Operation Settings

Use the Group Configuration page to change the privileges of a user by changing the operation and privilege configuration of the group assigned to the user.

1. On the Group Configuration page, select a group name to modify.
2. Click on the Operation Settings header to expand the section.
3. Click Configure. The Operations Tree window displays, as shown in Fig. 6-3.

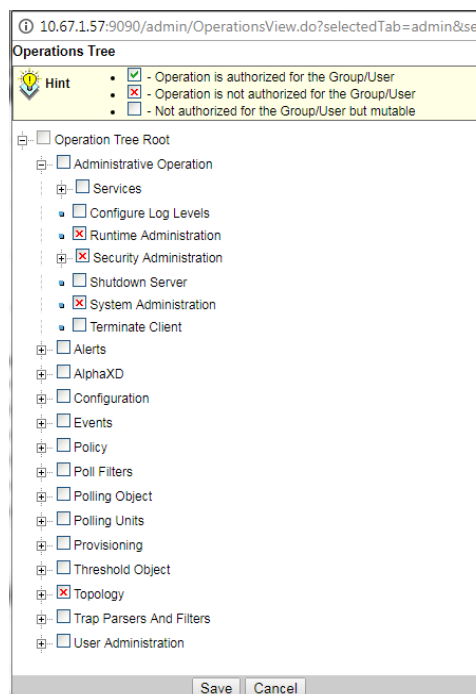


Fig. 6-3, Operations Tree Window

## 6.0 System Setup, continued

4. In the Operations Tree window, adjust the operations and privileges as desired. To save the changes press the Save button, or press the Cancel button to start over. Refer to the Creating and Removing Groups section for details on assigning operations.

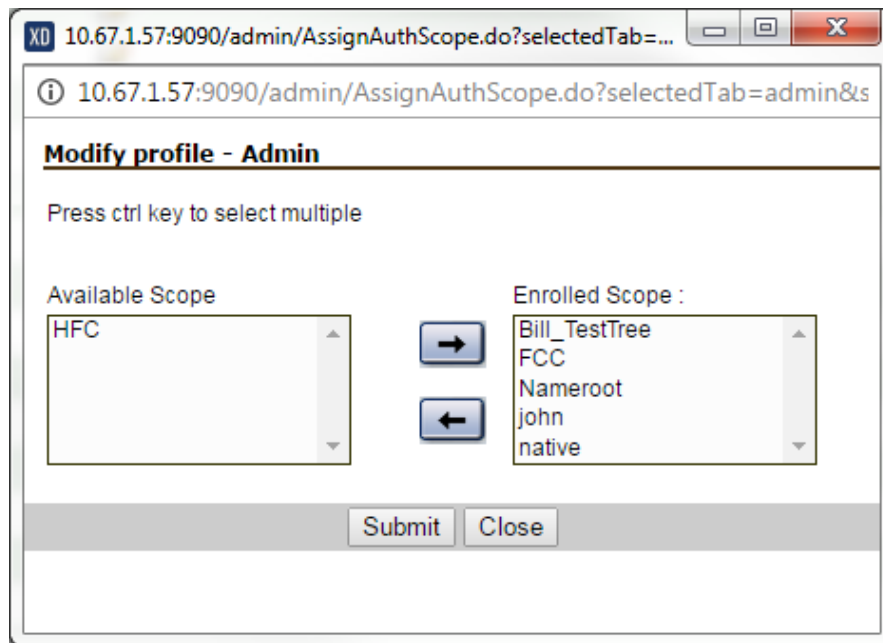
### Scopes

Scopes provide or limit access to specific tree views. Users must be given explicit permission to view these trees by being assigned to groups that have access to the tree(s). In addition, trees created by the user “root” are not automatically visible to all users.

Because the function of a scope is to limit a group’s permission, assign and remove scopes when creating or modifying groups.

Additional device tree names can be added (“enrolled”) to the Device Trees scope by assigning or removing the scope:

1. On the Modify Group page, click on the Custom View Scope section header to expand the section.
2. Select the Device Trees options from the Scope Name drop-down list to view the tree names currently assigned to the group. The enrolled tree names will appear in the Authorized Scopes list.
3. To enroll further tree names to the Device Trees scope, click Assign Scope. The Modify profile window, as shown in Fig. 6-4, will open and display the device tree names available to the scope and already enrolled to the scope.



**Fig. 6-4, Modify Profile Window**

4. To add a scope, select the desired Available Scope and click the right-facing arrow.
5. To remove a scope, select the desired Enrolled Scope and click the left-facing arrow.
6. Click Submit to save the changes, or Cancel to close the window without saving the changes.

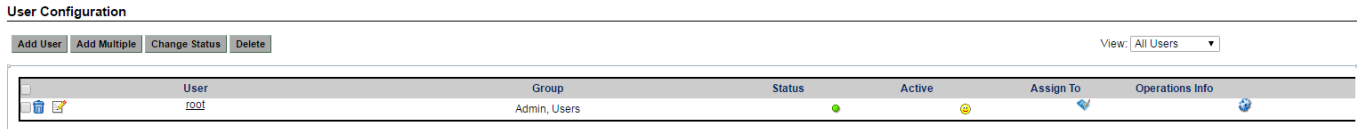
## 6.0 System Setup, continued

### 6.3 Users

#### Creating Users

AlphaXD user accounts are highly configurable. Permissions may be assigned or denied to users to limit or enable their exposure to a variety of features and functions on AlphaXD. These permissions are typically assigned when the user is created, but can also be changed at a later time.

Click the User Configuration icon to access the User Configuration page, as shown in Fig. 6-5.



**Fig. 6-5, User Configuration Page**

- Add User button – Use this button to create individual users.
- Add Multiple button – Use this button to create multiple (12 maximum) users at one time.
- Change Status dropdown menu – Use this button to change the status of one or more users.
- Delete button – Used in conjunction with the checkboxes in the front of the user names, this button is used to delete users from the system.
- Status column – Indicates the status of the user. A green icon indicates enabled, a gray icon indicates disabled.
- Active column – Indicates the active state of the user. A yellow icon indicates active, a gray icon indicates inactive.
- Assign To column – Provides access to the function for assigning/removing groups to/from a user.

## 6.0 System Setup, continued

### Create a Single User

1. On the Administration page, from the Security Administration panel, click **User Configuration**.
2. On the User Configuration page, click **Add User**.

**Add User**

User name

Password (Max. 8 characters)

Re-type Password

Available group names

Press ctrl key to select multiple

Add this user to a new group

Password expires in  days

Account expires in  days

Fig. 6-6, Add User Page

3. Enter the **User name** and **Password** (8 characters or less) information into the appropriate fields.
4. Select a **group name** from the Available group names section, or create a new group name by selecting the **Add this user to a new group checkbox**, and then entering the name in the adjacent field.
5. If necessary, select the **Password expires in** and/or the **Account expires in** checkboxes and enter the time, in days, into the adjacent field(s).
6. Click **Save**.

### Create Multiple Users

Up to 12 unique users may be created using this feature. When users are created using this feature, the password for each user will be the same as the user name. Changing each user's password requires editing each user account.

1. On the Administration page, from the Security Administration panel, click **User Configuration**.
2. On the User Configuration page, click **Add Multiple**.
3. Enter unique names into each user field (i.e., User 1, User 2, etc.). The user name can contain letters, numbers, underscores and hyphens. Spaces are not allowed.
4. Select one or more groups to assign to each user. Each user must have at least one group assigned. To assign the same group(s) to each user, select the "Apply selected group to all users" checkbox, as shown in Fig. 6-7.
5. Click **Save** to add the users to the system.

**Add Multiple Users**

A maximum of 12 users can be added in this page.

UserName	Selected Group
User 1: <input type="text"/>	<input type="checkbox"/> Admin <input type="checkbox"/> Users <input type="checkbox"/> Apply selected group to all users
User 2: <input type="text"/>	<input type="checkbox"/> Admin <input type="checkbox"/> Users
User 3: <input type="text"/>	<input type="checkbox"/> Admin <input type="checkbox"/> Users
User 4: <input type="text"/>	<input type="checkbox"/> Admin <input type="checkbox"/> Users
User 5: <input type="text"/>	<input type="checkbox"/> Admin <input type="checkbox"/> Users
User 6: <input type="text"/>	<input type="checkbox"/> Admin <input type="checkbox"/> Users
User 7: <input type="text"/>	<input type="checkbox"/> Admin <input type="checkbox"/> Users
User 8: <input type="text"/>	<input type="checkbox"/> Admin <input type="checkbox"/> Users
User 9: <input type="text"/>	<input type="checkbox"/> Admin <input type="checkbox"/> Users
User 10: <input type="text"/>	<input type="checkbox"/> Admin <input type="checkbox"/> Users
User 11: <input type="text"/>	<input type="checkbox"/> Admin <input type="checkbox"/> Users
User 12: <input type="text"/>	<input type="checkbox"/> Admin <input type="checkbox"/> Users

Fig. 6-7, Add Multiple Users Page


## 6.0 System Setup, continued

### Modifying Users

Modify a user to change associated groups, passwords and expiration dates.

1. On the Administration page, from the Security Administration panel, click **User Configuration**.
2. Click a **User name**.
3. To change the user profile information, click the **Edit** link, as shown in Fig. 6-8.

Modify profile - root

User Information:		Edit 
User name	root	
User Current Status	enabled	
Modify password expiration	0 days	
Modify account expiration	0 days	

**Fig. 6-8, Modify User Page - Edit Link**

4. Update user profile information and click **Submit** to save the changes.
5. Change the groups associated with the user, if desired.
  - Expand the **Associated Groups** section.
  - Click **Configure Group**. This opens the Modify profile window.
  - Highlight one or more user names in the Available Groups field. Press the **right-facing arrow** to add the name(s) into the Enrolled Groups field. If removing a group, highlight one or more names in the Enrolled Users window and press the **left-facing arrow** to move the name(s) into the Available Groups window. After making the desired change(s), press the **Submit** button to make the change.
6. Choose Permitted Operations to change the permissions and operations assigned to a user.

### Deleting Users

1. On the Administration page, from the Security Administration panel, click **User Configuration**.



#### CAUTION!

Do not delete all of the users at one time.

2. To delete a single user, click the **Trash Can** icon in front of the user name.
3. Delete multiple users by selecting the checkboxes in front of the desired user names, then clicking the **Delete** button.

## Changing User Status



### CAUTION!

Do not change the state of all users to *Disable* at one time.

1. On the Administration page, from the Security Administration panel, click **User Configuration**.
2. To change the status of a single user, select the **checkbox** in front of the user name.
3. Click the **Change Status** button and select the desired state.
4. To change the status of multiple users, select each **checkbox** in front of the desired user names.
5. Click the **Change Status** button and select the desired state.

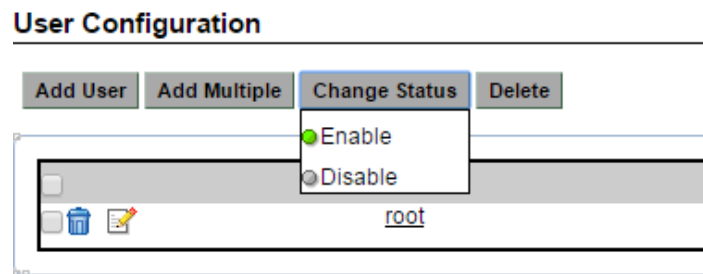


Fig. 6-9, User Configuration Page - Change Status Menu

## Terminating User Sessions

With the addition of the CheetahKillUser role, administrators now can terminate a session when the upper limit of licensed users (according to the license key) is met.



### NOTICE:

Only one CheetahKillUser role is allowed to be assigned in the database.

1. Logged in as administrator, on the Administration page, from the Security Administration panel, click **User**
2. Click **Add User**.

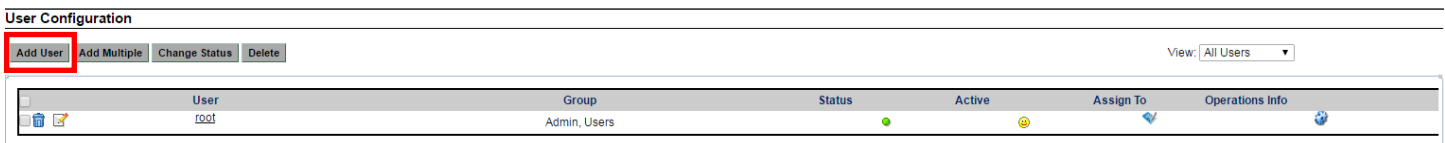


Fig. 6-10, User Configuration Page

## 6.0 System Setup, continued

3. Name the user **CheetahKillUser** and assign it to the **Admin** group.

USERNAME	GROUPNAME	OWNERNAME
CheetahKillUser	Admin	NULL
CheetahKillUser	default CheetahKillUser Group	NULL
root	Admin	NULL
root	Users	NULL

Fig. 6-11, New User in Database

4. When the upper limit of users is met, CheetahKillUser can log into AlphaXD and terminate any user session and change the user's status to Disable.

User Configuration

✔ User profile successfully modified

Add User Add Multiple Change Status Delete View: All Users

	Group	Status	Active	Assign To	Operations Info	
<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	Cheetah1	Technicians	●	☹	✔	🔄
	Cheetah2	BATechs	●	☹	✔	🔄
	Cheetah3	Users	●	☹	✔	🔄
	root	Admin, Users	●	☹	✔	🔄
	CheetahKillUser	Admin	●	☹	✔	🔄
	adminuser	Admin	●	☹	✔	🔄

Fig. 6-12, Terminating a User Session

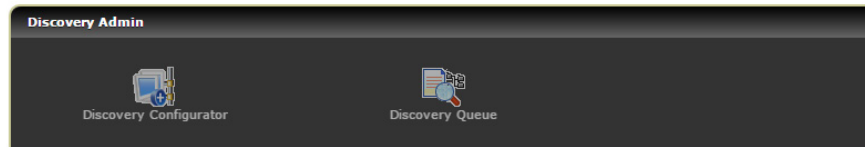


## 6.0 System Setup, continued

### 6.4 Discovery Admin

The Discovery Admin panel gives access to:

- The Discovery Configurator—used to configure the discovery and auto-discovery parameters.
- Discovery Queue—displays all of the active discoveries, the discoveries currently in the queue and the discoveries on the waiting list.



**Fig. 6-13, Administration Page - Discover Admin Section**

The Discovery Configurator is the tool used to specify the parameters for AlphaXD's auto-discovery process.

AlphaXD can discover devices:

- Added to its own (native) network.
- Added to CheetahNet, CheetahLight, and Cheetah DOCSIS networks when AlphaXD is properly integrated with these systems (see the chapter titled Integrating AlphaXD with Existing Cheetah Systems).

The AlphaXD discovery process consists of:

- "Seeing" a device in the network that is not in the AlphaXD database (or is in the database, but has been specified to be rediscovered).
- Obtaining the device's MAC or IP address.
- Determining the type of device (transponder, battery, optical node, etc.).
- Selecting the appropriate configuration template for the device type.
- Writing the device information into the AlphaXD database along with the name of the configuration template.
- Displaying the device in the AlphaXD Native view (if auto download of the template is used), and in the Not Provisioned column in the Network Inventory page.

After devices are discovered, the user must provision them by either downloading the appropriate template or by accessing the Device Configuration option.

#### Discovery Configurator

The Discovery Admin panel on the Administration page contains the Discovery Configurator link to specify the parameters for AlphaXD's initial auto-discovery process and ongoing rediscovery process.



**NOTICE:**

The Discovery Configurator acts as a medium to put the entries in the seed file, which is the file AlphaXD uses to perform auto-discovery and rediscovery. All modifications done using the Discovery Configurator affect only the seed file. There is no impact on the database.

## 6.0 System Setup, continued

Parameters in the Discovery Configurator allow AlphaXD to discover:

- A single IP Address
- A single network
- A range of network or node IP addresses

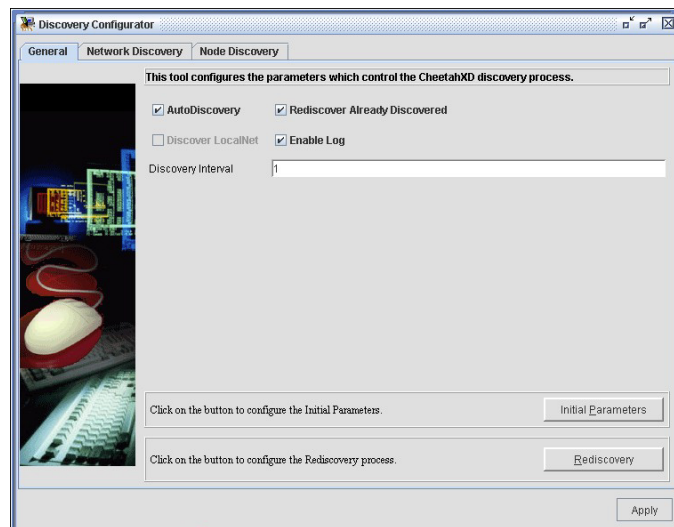
Additionally, the Discovery Configurator can prevent discovery of specific networks.

To set initial, general auto-discovery parameters:

1. On the Administration page, click the **Discovery Configurator** icon.
2. Log into the Discovery Configurator. Enter the appropriate user ID and password, and then click **Connect**.

### ✓ **NOTICE:**

After making any changes in the Discovery Configurator page, the changes must be applied to the AlphaXD server before they can take effect. Some of the configuration windows include a Reload button to apply changes. The bottom of the Discovery Configurator page includes an Apply button for applying changes.

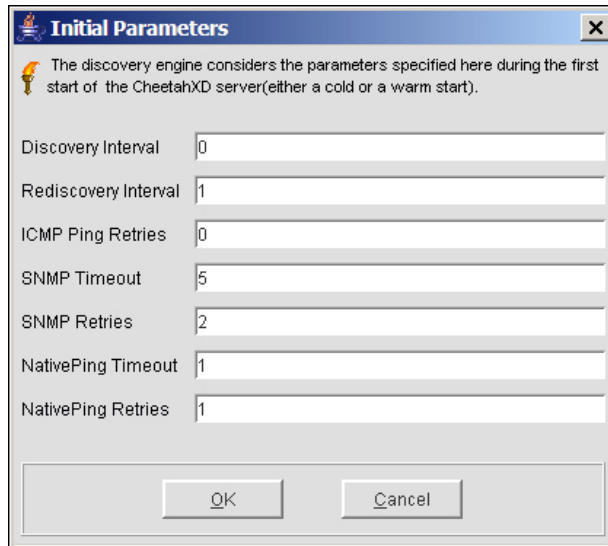


**Fig. 6-14, Discovery Configurator - General Tab**

3. Set the options on the General tab as desired.
  - Auto Discovery – This checkbox turns sweep-based discovery on and off. (Trap-based discovery still occurs based on the IP ranges setup.)
  - Rediscover Already Discovered – Checking this checkbox causes AlphaXD to discover all network elements, even those already discovered. Enable this checkbox when discovered devices need to be restored to default parameters. Disable this checkbox to improve system performance by discovering only those devices that have not yet been discovered.
  - Discover Local Net – Includes the local network and all of its nodes in the auto-discovery process.
  - Enable Log – AlphaXD will store detailed debug messages related to auto-discovery in “discoveryLogs.txt”.
  - Discovery Interval – Controls the interval (in minutes) between discovery of networks. The value set for this parameter affects the performance (CPU utilization and network traffic) of the discovery process.
4. Click **Initial Parameters** to specify the initial auto-discovery parameters. The values set here determine the speed of the initial discovery process. If no parameters are set in the Initial Parameters page, AlphaXD uses the values set for the parameters in the General tab.



**NOTICE:** None of the values are utilized until a change is made. Once a change is made, all of the field values are applied.



**Fig. 6-15, Initial Parameters Window**

5. Specify the values for the options on the Initial Parameters page. The following table describes each parameter:

Initial Parameters	
Parameter	Description
Discovery Interval	Interval (in seconds) between the discovery of any two devices in the network. The default value is 1 second. When initially deploying AlphaXD set this value low. Afterwards, during normal operations, this value can be changed to a higher number so that AlphaXD resources are applied to auto-discovery operations less often. This leaves AlphaXD resources free for other daily operations.
Rediscovery Interval	Interval (in hours) between polling sweeps of the discovered network(s). Default is 24 hours. If a negative value is specified, it is replaced by 24.
ICMP Ping Retries	Number of times AlphaXD pings ICMP (Internet Control Message Protocol) devices. Default is 0 (i.e., retry is performed only once), a setting of 1 causes a retry to be performed twice. Set this value as low as possible for optimum system performance.
SNMP Timeout	The maximum time, in seconds, that AlphaXD waits for a response from SNMP devices, before attempting a retransmission. Default is 1. Raise this value when auto-discovery is discovering a remote network where the response time could be more. This value is doubled for each retry, as specified in the SNMP Retries setting. For example, if SNMP Timeout is set to 5 seconds and SNMP Retries is set to 3, the first retry will occur in 5 seconds. The second retry will occur in 10 seconds, the third retry in 20 seconds and so on.
SNMP Retries	Number of times AlphaXD pings an SNMP device. Default is 0 (i.e., retry is performed only once), a setting of 1 causes a retry to be performed twice. Set this value as low as possible for optimum system performance.
NativePing Timeout	The maximum time, in seconds, that AlphaXD waits for a response from native devices, before attempting a retransmission. Default is 1 second.
NativePing Retries	Number of times AlphaXD pings native devices. Default is 1 retry.

**Table 6-1, Initial Parameters - Discovery Configurator**

## 6.0 System Setup, continued

### Specifying a Single Node for Discovery (IPv4 Only)

Alpha recommends using the Network Discovery page because AlphaXD uses the values specified on this page when performing both auto-discovery and rediscovery. Values specified in the Node Discovery page are used during initial auto-discovery only.

1. In the Administration page, click the **Discovery Configurator** icon.
2. Click the **Network Discovery** tab (to specify a node for both initial auto-discovery and ongoing rediscovery) or the Node Discovery tab (to verify the Discover checkbox is checked and to specify a node for initial auto-discovery only).
3. Select the **Set of Nodes** radio button.

Discover	IP Address	NetMask	StartIP	EndIP	DHCP
<input checked="" type="checkbox"/>	172.16.1.0	255.255.255.0	172.16.1.60	172.16.1.100	<input type="checkbox"/>
<input checked="" type="checkbox"/>	172.16.3.0	255.255.255.0	172.16.3.80	172.16.3.100	<input type="checkbox"/>
<input checked="" type="checkbox"/>	172.16.4.0	255.255.255.0	172.16.4.80	172.16.4.100	<input type="checkbox"/>
<input checked="" type="checkbox"/>	10.1.13.0	255.255.255.0	10.1.13.100	10.1.13.110	<input type="checkbox"/>
<input checked="" type="checkbox"/>	10.3.33.0	255.255.255.0	10.3.33.22	10.3.33.22	<input type="checkbox"/>

Fig. 6-16, Discover Configurator - Network Discovery Tab

4. Enter the **IP Address**.
5. Enter the **NetMask**.
6. (Optional) Enter the **starting IP Address**.
7. (Optional) Enter the **ending IP Address**.
8. Click **Add**. The selected node is added to the scrollable list at the top of the tab.
9. Click **Apply**. The node is included when auto-discovery and/or rediscovery executes.

## 6.0 System Setup, continued

### Specifying Networks for Discovery

Multiple networks can be included in the AlphaXD discovery process.

1. In the Administration page, click the **Discovery Configurator** icon.
2. Click the **Network Discovery** tab.
3. As described in the following sections, set the parameters in this tab to the network discovery behavior desired.

### Configuring Discovery of Remote Networks

By default, AlphaXD discovers all networks to which the server running the AlphaXD server is connected. It also adds any other network that it finds through the router to the topology, but designates that network object as unmanaged, meaning no discovery will occur.

1. Click the **Network Discovery** tab in the Discovery Configurator and verify it is checked.
2. Select **Discover**.
3. Select **Entire Network**.
4. Enter the **IP Address** of the network.
5. Enter the **NetMask** of the network.
6. Click **Add**. The IP Address and NetMask values are added to the screen with the Discover column enabled (checked). Discovery of those remote networks is enabled. Multiple networks can be configured by adding more IP Address and NetMask values.

### Discovering a Range of Network IP Addresses

Specify one or more ranges of network IP addresses to be included in auto-discovery and rediscovery.

1. Click the **Network Discovery** tab in the Discovery Configurator.
2. Verify the **Discover** checkbox is checked.
3. Select **Set of Nodes**.
4. Enter the **IP Address** of the network.
5. Enter the **NetMask** of the network.
6. Enter the **starting IP address** (of the range of IP addresses to be discovered).
7. Enter the **ending IP address** (of the range of IP addresses to be discovered).
8. Click **Add**. Multiple Range of IP addresses in a single network can also be configured.



---

**NOTICE:**

The range of IP addresses specified here will not be discovered and added if any of the node properties are specified in the Disallow Criteria. Ensure that the properties of the IP addresses specified here are not specified in the Disallow Criteria.

### Discovering a Range of Node IP Addresses

The Discovery Configurator offers two places to specify a range of nodes for discovery:

- The Network Discovery page
- The Node Discovery page

Alpha recommends using the Network Discovery page because AlphaXD uses the values specified on this page when performing both auto-discovery and rediscovery. Values specified in the Node Discovery page are used during initial auto-discovery only.

Specify one or more ranges of node IP addresses to be included in auto-discovery and rediscovery.



#### **NOTICE:**

---

Select DHCP: Only when the Start IP and the End IP are given with the DHCP option disabled, will that particular range of network get discovered. But if Start IP and End IP are specified with DHCP enabled, then the nodes in that particular range will be discovered as DHCP nodes, and other nodes will also be discovered as Non-DHCP nodes.

1. Click the **Network Discovery** tab in the Discovery Configurator.
2. Verify **Discover** is checked.
3. Select **Set of Nodes**.
4. Enter the **IP Address** of the network.
5. Enter the **NetMask** of the network.
6. Enter the **starting IP Address** (of the range of IP addresses to be discovered).
7. Enter the **ending IP Address** (of the range of IP addresses to be discovered).
8. Click **Add**. A multiple range of IP addresses in a single network can also be configured.

### Performing Network-Specific Discovery of SNMP Devices

The AlphaXD discovery module facilitates discovering SNMP V1 or V2 devices in a specific network or a range of devices in a network. By default, the discovery engine uses the community string public and the agent port 161 while discovering SNMP devices. But some devices in the network could use a different port and community.

These procedures cause the discovery engine to discover those SNMP devices in the specified network with the configured community and port.

To discover SNMP (V1 or V2) devices in a particular network:



#### **NOTICE:**

---

This option can also be set in the Initial Parameters page. When the options are different, the settings specified here in the SNMP Properties page prevail.

1. Click the **Network Discovery** tab in the Discovery Configurator.
2. Select **SNMP**.
3. Click **SNMP Properties**.
4. Click the **V1** or **V2** radio button as required.
5. Enter the **Community of the Node** in the Community field.
6. Enter the **Port** in the SNMP Agent Port field.
7. Click **OK**.

## 6.0 System Setup, continued

### Preventing Network Discovery

This procedure prevents a network from being discovered and added to the topology database. Multiple networks can be prevented by adding more IP addresses and Netmasks.

1. Click the **Network Discovery** tab in the Discovery Configurator.
2. Deselect (uncheck) the **Discover** option.
3. Click **Apply**.

### Deleting Network Entries

Delete a network from the auto-discovery and rediscovery processes by selecting it in the Network Discovery tab of the Discovery Configurator, and clicking the Delete button. Deleting an entry in the Discovery Configurator does not delete the network from the database. The network is deleted from the file "seed.file". This file stores the auto-discovery and rediscovery parameters defined using the Discovery Configurator. The deleted network will not be discovered. The deleted network will not be rediscovered unless the database has been re-initialized.

### Forcing Rediscovery

When necessary, the operator can force the system to perform a rediscovery.

1. Click the **Network Discovery** tab of the Discovery Configurator.
1. Select the desired network in the network list.
2. Click **Force Discover**.

## 6.0 System Setup, continued

### IPv6 Discovery

The Discovery Configurator does not support IPv6 entries. However, if IPv6 discovery is needed, the “seed.file” file can be edited.

1. Navigate to the **AlphaXD\conf** directory on the server.
2. Open **seed.file**.
3. At the end of the file (before the “</SEED>” entry) enter the following: where the “2001:100:8f45:3::/64” entry would enable discovery of all transponders with the prefix length of 2001:100:8f45:3:: and the “2001:100:8f45:1::8f2” entry would enable discovery of a transponder with a specific IPv6 address. Users can create as many prefix length and/or specific IPv6 address entries as needed.

Example Seed File with IPv6 entries in **Bold**:

```
<DISCOVERY DAY_OF_THE_MONTH="-1" DAY_OF_THE_WEEK="MON,TUE" DISCOVER="true"
DISCOVERY_INTERVAL="1" DISCOVER_LOCALNET="false" ENABLE_DHCP_DISCOVERY="false" ENABLE_
ICMP_DISCOVERY="false" ENABLE_LOG="true" ENABLE_SNMPV3_DISCOVERY="false" ENABLE_SNMP_
DISCOVERY="true" HOUR="17,9" PING_RETRIES="0" PING_TIMEOUT="1" READ_COMMUNITY="DOCSIS"
REDISCOVER_ALREADY_DISCOVERED="true" REDISCOVER_INTERVAL="24" SNMP_RETRIES="0" SNMP_
TIMEOUT="2" WRITE_COMMUNITY="DOCSIS"/>
<NATIVE_PING ICMP_DEBUG_LEVEL="1" ICMP_RETRIES="2" ICMP_SWEEP_PACKETS="10" ICMP_SWEEP_
SLEEP_INTERVAL="2" ICMP_TIMEOUT="2" PING_SWEEP="false"/>
<TO_DISCOVER>
<net END_IP="172.16.1.250" NETMASK="255.255.255.0" NETWORK_ID="172.16.1.0" READ_COMMUNITY="public"
SNMPAGENTPORTS="161" SNMP_VERSION="V2" START_IP="172.16.1.1"/>
</TO_DISCOVER>
<TO_DISCOVERIPV6>
<UNICAST ADDRESS="fd8b:d464:8237:3::/64"/>
<UNICAST ADDRESS="fd8b:d464:8237:3::8f2"/>
</TO_DISCOVERIPV6>
</SEED>
```

4. Save and close the file.
5. Restart the AlphaXD server.



#### **NOTICE:**

---

IPv6 discovery is TRAP-based. Sweep discovery CANNOT be performed on IPv6 devices.



## 6.0 System Setup, continued

### Discovery Queue

The Discovery Queue displays devices in various stages of auto-discovery. Both the queue and the devices on the wait list can be cleared.

Active Discoveries												
Description	Class	Priority	Attempt	Max. Attempts	Last Attempt	Next Attempt	Id	Invoked From Event	Invoked From seed	Timeout(ms)	Retries(ms)	Extended Props.
Discoveries In Queue (First 100 Shown): 0												
Description	Class	Priority	Attempt	Max. Attempts	Last Attempt	Next Attempt	Id	Invoked From Event	Invoked From seed	Timeout(ms)	Retries(ms)	Extended Props.
Discoveries In Wait List (First 100 Shown): 0												
Description	Class	Priority	Attempt	Max. Attempts	Last Attempt	Next Attempt	Id	Invoked From Event	Invoked From seed	Timeout(ms)	Retries(ms)	Extended Props.

Fig. 6-17, Discovery Queue Page

### Automatic Template Downloads

The automatic download template feature can be configured to automatically download alarm limits to CL legacy transponders and HMS/DOCSIS transponders at the time the transponder is discovered. The procedure for enabling this feature is different for each system. Contact Alpha Technical Support for details on how to enable this feature.

## 6.5 Alert Filtering and Suppression

AlphaXD provides the user the ability to suppress alerts. Suppression of alerts can be managed using one of two different methods:

1. Configure AlphaXD to suppress Alerts from being displayed in Notifier using the Alert Filter feature.
2. Users licensed for the JMXAgent (Northbound traps) can suppress targeted alerts at the AlphaXD server.

### Alert Filters

AlphaXD provides operators the ability to suppress Alerts from showing up in the Fault Views. This operation has security permissions which provide the XD Administrator the ability to enable/disable this feature for specific users.

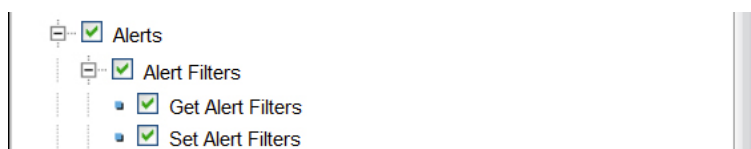


Fig. 6-18, Alert Filters

- Get Alert Filters - user can launch the Alert Filter GUI but the Load Filter link on the page has been removed.
- Set Alert Filters - user can launch the Alert Filter GUI but the Add Filter and Save Filter links on the page have been removed.
- Alert Filter - user does not have the ability to open up the Alert Filter GUI.

For users to have all access to the Alert Filter Function, all three permissions must be on.

## 6.0 System Setup, continued

### Filter Rules

Alerts can be filtered by any and all of the fields displayed on the page. This includes Source, Severity, Message, Category and Entity.

As data is entered into each field, the entries are logically “AND”-ed together to create the filter. To set up an OR scenario, enter two separate filters.

A wildcard in the form of an asterisk (\*) is utilized. The asterisk (\*) can signify one or many characters and can be used at any point in the string. For example, these are all valid uses of the wildcard:

- Source: = DOCSIS\_00103f\*
- Source: = \*0966\*
- Source: = DOCSIS\*aabbcc

#### **NOTICE:**

- AlphaXD **MUST BE RESTARTED** for any new filter modifications to take effect. BLANK filters cannot be used. If there is a filter with a name and none of the five attribute fields are filled in ALL alerts coming into the system will be suppressed.
- Not all fields need to be utilized; a filter can be set up using only a single field.
- New filters have no effect on existing alerts being viewed. Just because a filter is created does not mean it will clear existing alerts; the new filter will only affect those alerts generated after the XD system has been restarted.
- POM alerts are also suppressed if a criterion is met.

### Device Status in Trees

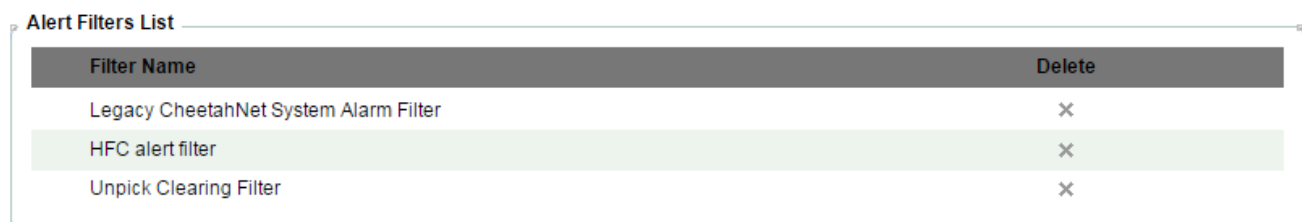
GX2 – Each module will show the active status even though alerts are suppressed.

Transponders – Show up as green in the tree view if the source is to be suppressed, otherwise it will show whatever status the highest alert severity is.

### To Setup an Alert Filter

Navigate to the Administration page and click the Alert Filters icon. (AlphaXD includes a default policy configuration that should not be altered.)

#### Alert Filters



The screenshot shows a table titled "Alert Filters List" with two columns: "Filter Name" and "Delete". There are three rows of filter entries. The second row, "HFC alert filter", is highlighted in light green.

Filter Name	Delete
Legacy CheetahNet System Alarm Filter	×
HFC alert filter	×
Unpick Clearing Filter	×

Fig. 6-19, Alert Filters Page

## 6.0 System Setup, continued

There is a default set of filters that are utilized by AlphaXD (at upper right).

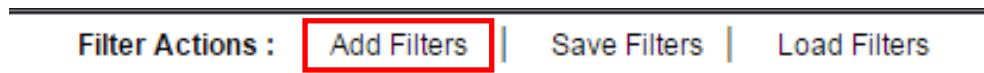


Fig. 6-20, Filter Actions Buttons



### CAUTION!

Do not delete any of these filters. Normal alert processing will be affected.

To add a filter, click Add Filter.

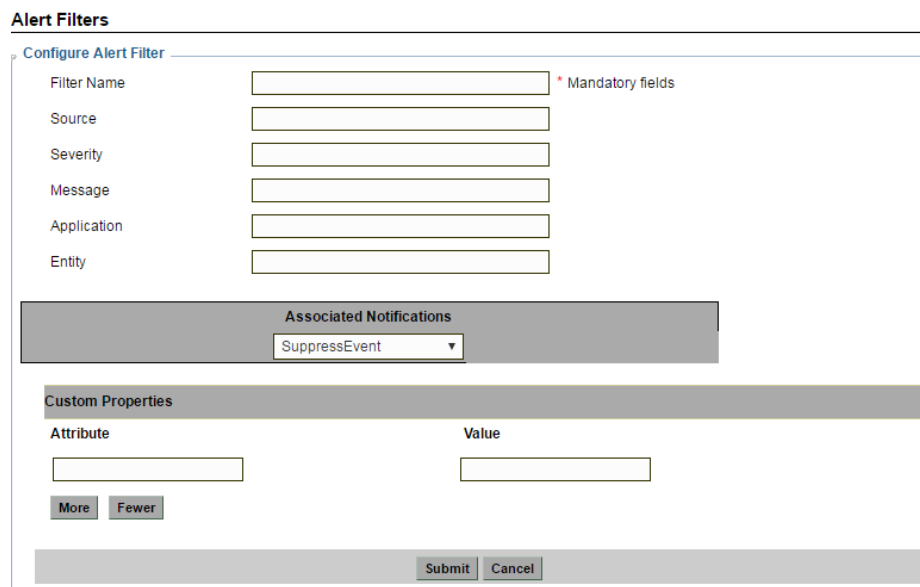
The screenshot shows a web interface titled "Alert Filters". Below the title is a section "Configure Alert Filter" with several input fields: "Filter Name" (with a red asterisk and "Mandatory fields" label), "Source", "Severity", "Message", "Application", and "Entity". Below these fields is a section "Associated Notifications" with a dropdown menu showing "SuppressEvent". Below that is a section "Custom Properties" with a table for "Attribute" and "Value". At the bottom of the form are "More" and "Fewer" buttons, and at the very bottom are "Submit" and "Cancel" buttons.

Fig. 6-21, New Alert Filter Page

The data entered here will be the criteria used to suppress alerts from showing up in the Faults view.

- Filter Name – Each filter must be given a name. Any combination of Numbers, Letters and spaces can be utilized to create the filter name.
- Source – This is the AXD system name of the device. This is not the Display Name. The Source name on this page corresponds to the NAME property for any device in the system.
  - Used to filter alerts from a single device (DOCSIS\_00103faabbcc)
  - Used to filter alerts for all like devices (DOCSIS\_00103f\*)
- Severity – This is related to the severity value for alerts such as Major, Minor Critical, etc.
  - Used to filter out all Critical alerts
- Message – This relates to the message column displayed for each alert within the Faults view.
  - Used to suppress alerts with targeted text in the Message column
- Category – Really means Application
  - Example, HFC, IP, etc.
- Entity – This relates to the Entity field in an alert.
  - Use this filter if a targeting Entity string needs to be suppressed from Notifier.

## 6.0 System Setup, continued

### JMX ALERT Forward Filtering – Northbound SNMP Traps

Utilizing JMX ALERT Forward Filtering is a three-step process.

1. The JMX agent must first be licensed. To verify if the Northbound SNMP traps feature has been licensed, open the AlphaXD\_License.xml file and look for this entry:

```
<Component Name="NorthBound">
<Properties Name="CORBANorthBound" Value="true"/>
<Properties Name="JMXAgent" Value="true"/>
</Component>
```

2. The V1V2TrapForwardingTable.xml file must be pointing to the third part trap listener. The file is located in AlphaXD\conf\jmx\_agent\conf. For more details refer to the section titled Utilizing the SNMP Agent to Forward Notifications to Third Party Applications in the User Guide.
3. The filters need to be setup properly for the environment.

Setting up the filters is done using the JmxAlertsFilters\_Example.xml file. This file is located in AlphaXD\conf. The forward filter feature was introduced to suppress ALERTS (not EVENTS) at the AlphaXD server before they can be forwarded to the 3rd Party Trap listener. There are two types of filters that can be used:

- Include Filter – This filter is inclusive and only those devices or attributes in the filter will be forwarded. Users would invoke this filter when only concerned about a few devices and would like to filter out everything else. Example – I only want to see Standby Alerts forwarded.
- Exclude Filter – This filter is exclusive and only those devices or attributes in the filter will NOT be forwarded. Users would invoke this filter when all Alerts should be forwarded with the exception of some specific device or attribute. Example – I want to see all Alerts except for a select set of devices.

### Alert Forwarding Process

Each Alert generated by AlphaXD follows the same filtering process on its way to the third-party listener. The Alert is first evaluated by the Include criteria portion of the filter and then passed onto the Exclude criteria portion of the filter to be evaluated. If the Alert matches any of the Exclude criteria, it is dropped and not forwarded.

### Steps to Setup JMX Filtering

1. Make a copy of the example file. The new file must be called JmxAlertFilters.xml.
2. Open the file for editing. The example file below is a filter that says:
  - Include only those alerts from the device DOCSIS\_00103fe2a829 but exclude Alerts from the device if they are for the Return Laser 4 attribute.

```
<com.tollgrade.cable.ccms.jmxagentutil.CTJMXAlertFilter>
  <includeAlertCriteria class="vector">
    <com.tollgrade.cable.ccms.devicemodel.hfcccommon.CTHFCAlert>
      <source>DOCSIS_00103fe2a829</source>
    </com.tollgrade.cable.ccms.devicemodel.hfcccommon.CTHFCAlert>
  </includeAlertCriteria>
  <excludeAlertCriteria class="vector">
    <com.tollgrade.cable.ccms.devicemodel.hfcccommon.CTHFCAlert>
      <source>DOCSIS_00103fe2a829</source>
      <alarmingAttachment>Return Laser 4</alarmingAttachment>
    </com.tollgrade.cable.ccms.devicemodel.hfcccommon.CTHFCAlert>
  </excludeAlertCriteria>
</com.tollgrade.cable.ccms.jmxagentutil.CTJMXAlertFilter>
```



---

**NOTICE:**

Any entry, even a NULL entry, in either section of the filter gets evaluated. If a filter type is not needed, it is best to completely remove those entries from the active file. For example, to exclude alerts from a device with the source name of DOCSIS\_00103f112233, the JmxAlertFilters.xml file would look like the following:

```
<com.tollgrade.cable.ccms.jmxagentutil.CTJMXAlertFilter>
  <excludeAlertCriteria class="vector">
    <com.tollgrade.cable.ccms.devicemodel.hfcccommon.CTHFCAlert>
      <source>DOCSIS_00103f112233</source>
    </com.tollgrade.cable.ccms.devicemodel.hfcccommon.CTHFCAlert>
  </excludeAlertCriteria>
</com.tollgrade.cable.ccms.jmxagentutil.CTJMXAlertFilter>
```



---

**NOTICE:**

The JMX Forward Filter features is for Alerts only. System Change Notification will still be forwarded. For example, if a device is added to the exclude portion of the Filter goes into a Time Out state, the Critical Alert will not be forwarded but the moChangeNotification message will be forwarded.

## 6.0 System Setup, continued

### JmxAlertFilters.xml File

The following parameters can be used in the JmxAlertFilters.xml file:

JmxAlertFilters.xml Parameters	
Parameter	Field
id	alarmField1
gatewayPar (Display Name)	alarmField2
modTime	alarmField3
severity	alarmField4
priority	alarmField5
createTime	alarmField6
category	alarmField7
who	alarmField8
attributeName	alarmField9
webNMS	alarmField10
webNMS	stateChangeCount
entity	
groupName	
source	
topLevel Par	
deviceCategory	
currentValue	
limitViolated	
alarmingAttachment	

Table 6-2, JmxAlertFilters.xml Parameters

## 6.0 System Setup, continued

### 6.6 Device Configuration and User-Defined Configuration Fields

The Property tab of the Device (and Template) Configurator includes five generic fields for capturing additional device information such as physical location, manufacturer information, installation dates, or other user-specific information. When CheetahNet devices are imported into AlphaXD, AlphaXD uses some of these fields to store device configuration information that was defined in CheetahNet, but is not represented in the default CheetahNet configuration parameters.

By default, these fields are named User Field 1 through User Field 5, but AlphaXD offers a way to change the field labels to reflect the information captured.

#### To Access the User-Defined Configuration Fields:

1. Access the Device Configuration or Template Configuration module.
2. Click the Property tab.
3. Scroll down to view the user-defined fields at the bottom of the page.

#### To Change the Labels on User-Defined Fields:

1. Open the text file EnglishToNative.properties in text editor. The default path for this file is c:\AlphaXD\html\.
2. Scroll to the lines depicted by the highlighted areas in the figure below.

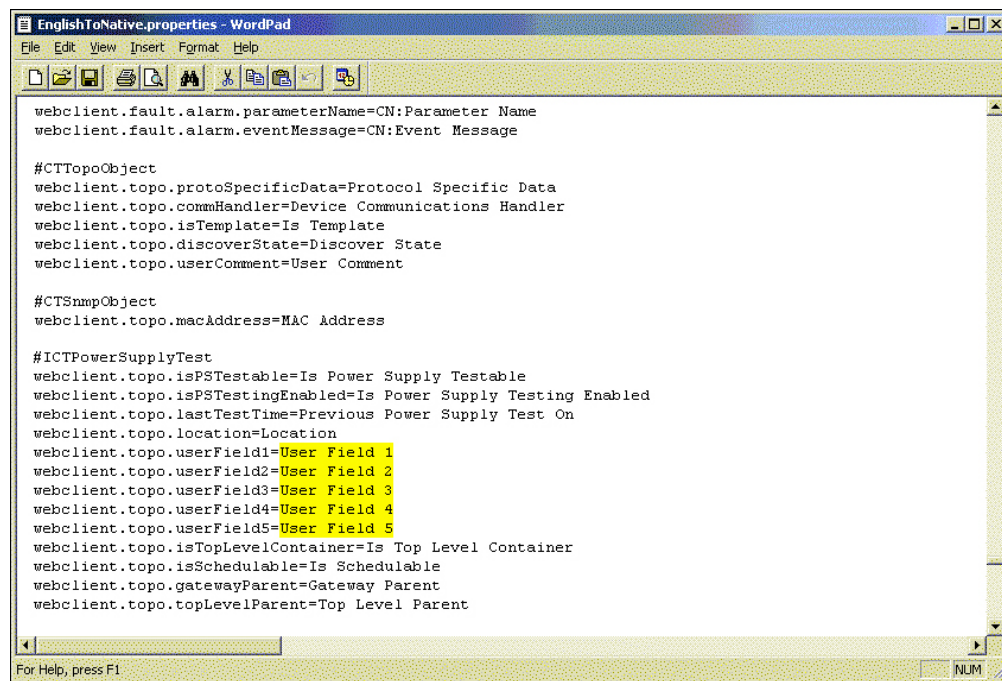


Fig. 6-22, EnglishToNative.properties

3. Edit the text depicted by the highlighted areas to change the labels of the user-defined fields, obeying the following conventions:
  - Create names with a maximum of 32 characters, including spaces.
  - Only use printable ASCII characters in these field names (no control characters).
4. Save the file and close it.
5. Restart the server for the label changes to take effect.

## 6.7 Specifying Parameters for Power Outage Monitoring (POM)

For an accurate computation of the standby estimate during a commercial outage, it is necessary that the PowerOutageMonitoring configuration file (under the AlphaXD/conf folder) be configured with the information about the power supplies and batteries.

There are two types of algorithms that are used for the computation of the standby capacity during commercial power outage conditions:

1. Predictive Computation (PKC): This is more accurate than the LSS method below, and uses detailed information about the power supply and its batteries. This computation is used for all of the HMS and DOCSIS® HMS devices.
2. Least Squared Method (LSS): This is used for all non-HMS power supply types, and as a fallback when PKC cannot be used.

User field 2 in the POM alert shows the type of algorithm (PKC or LSS) that is being used for the computation of the standby capacity. User field 3 in the POM alert provides an indication of the reliability of the standby estimate. For example, if the slope drops off too steeply or too soon, the batteries may not be fully-charged, and it will be indicated in this field that the standby estimate is unreliable.

The POM algorithm has been updated to provide its first Standby Remaining value as close to 10 minutes as possible based upon the user defined <pomRefreshInterval> value set in the powerOutageMonitoring\_Parameters.xml file. Once the initial value is displayed, the algorithm is then updated based on the <pomRefreshInterval> going forward.

The following table defines the various POM configuration parameters and their description. Open the file AlphaXD\conf\PowerOutageMonitoring\_Parameter.xml in Notepad or a similar editor to customize the parameters in the following table. Restart AlphaXD for parameter changes to take effect.

POM Configuration Parameters		
Parameter Name	Default Value	Parameter Description
pomAnalysisCutoffBiasInSeconds	0	Additional time in seconds to subtract from actual standby time computed in POM Notifier. Should be zero by default.
pomCriticalVoltageDifferential	3.0	If voltage gets within 3 volts of the cutoff voltage, the POM shifts to a smaller window size for the Least Squares calculation (if being used). This makes it quicker to pick up changes in the slope of the voltage drop off.
pomCutoffVoltage12VoltBattery	10.5	Unused but needs to be here for backwards compatibility.
pomCutoffVoltage6VoltBattery	5.3	Unused but needs to be here for backwards compatibility.
pomCutoffVoltageTable		This is the top level element, below which the various configurations of power supply types are defined.
entry		The <entry> and </entry> tags hold all information about a particular power supply modifier. A separate entry is required for each personality type.
String	Standard	Personality of power supply. Standard is used as default.
CTPomCutoffVoltages		Element that holds the power supply and battery specific information for a particular personality.
battAge	Unknown	Age of oldest battery in string. Possible choices are: Unknown, New, 6 Months, 1 year, 1 ½ years, 2 years, 2 ½ years, 3 years, 3 ½ years, 4 years, 4 ½ years, 5 years, More than 5 years



## 6.0 System Setup, continued

POM Configuration Parameters		
Parameter Name	Default Value	Parameter Description
battAmpHrRating	70	Defines the Amp Hr rating of power supply.
battChem	Unknown	Holds the battery chemistry information. Choices are: Lead, Acid, Gel, Cell, APC, P, Other
cutoffVoltage12VoltBattery	10.5	12 volt battery cutoff value. This is the finish line on which the calculations will be based.
cutoffVoltage6VoltBattery	5.3	6 volt battery cutoff value. This is the finish line on which the calculations will be based.
max2Battery12VLifetimeInHours	1.5	Max lifetime for 2 batteries, 12 volts. Calculation for this configuration will not exceed this value.
max2Battery6VLifetimeInHours	1.0	Max lifetime for 2 batteries, 6 volts. Calculation for this configuration will not exceed this value.
max3Battery12VLifetimeInHours	3.0	Max lifetime for 3 Batteries, 12 volts. Calculation for this configuration will not exceed this value.
max3Battery6VLifetimeInHours	2.0	Max lifetime for 3 batteries, 6 volts. Calculations for this configuration will not exceed this value.
max4Battery12VLifetimeInHours	4.0	Max lifetime for 4 batteries, 12 volts. Calculation for this configuration will not exceed this value.
max4Battery6VLifetimeInHours	3.0	Max lifetime for 4 batteries, 6 volts. Calculation for this configuration will not exceed this value.
maxNBattery12VLifetimeInHours	5.0	Max generic lifetime catch-all for all other 12V battery configurations.
maxNBattery6VLifetimeInHours	4.0	Max generic lifetime catch-all for all other 6V battery configurations.
powerSupplyType	Unknown	PS Type. Choices are: Unknown, Alpha AM, Alpha AM2, Alpha XM, Alpha XM2, Alpha XM3, Alpha/Lectro ZTT , Alpha/Lectro ZTT+, Alpha/Lectro SS, Alpha/Lectro CPR, APC, TSP, Antec/PG, Slug Equisil
pomDefaultDispatchLeadTimeInMinutes	5	Subtract this from standby estimate for dispatching tech.
pomDeltaSlope	-0.015	Change in slope by this much triggers smaller window size for least squares calculation.
pomInputVoltagePowerOutageThreshold	0.0	Input Voltage must drop below this value to trigger POM Calculation.
pomMessageTimeToLiveInHours	8	POM alert will be deleted from the system after this number of hours (after restoration of commercial power).
pomMinWindowSize	20	Minimum window size (number of samples) for calculations.
pomSeasonalAdjustmentInMinutes	0	A seasonal or other situational time adjustment that the application will add to determine a truck roll. A positive number reduces the dispatch time, while a negative number increases the time to dispatch.
pomRefreshInterval	180000	Interval the page refreshes.
pomFailureTimeInHours	2	Time in hours that indicates a failure for expected battery runtime. If there is an outage and the power supply transponder loses communications with the server prior to the indicated amount of time it will be considered a failure.

## 6.0 System Setup, continued

POM Configuration Parameters		
Parameter Name	Default Value	Parameter Description
pomGenRefuelAlarmTimeInMinutes	45	Lead time in minutes for an alarm to be generated to indicate a generator needs to be refueled.
pomGenExcessiveRuntimeInHours	24	Amount of time in hours that a generator can run prior to an alarm being generated.

**Table 6-3, POM Configuration Parameters**

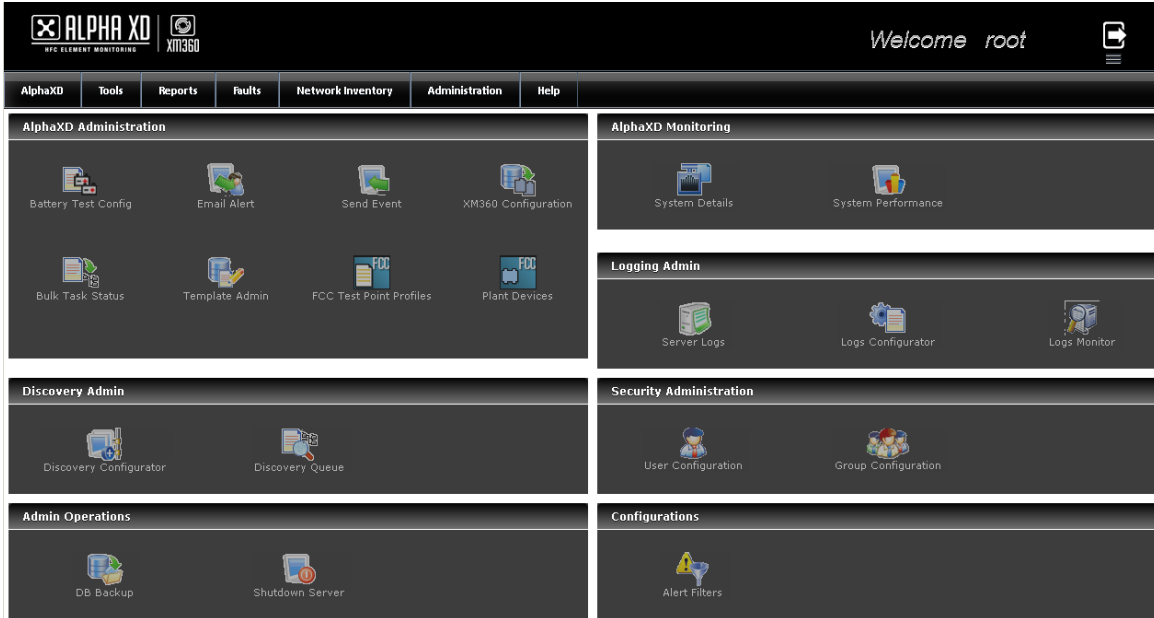


**NOTICE:**

By using the Device Config application, an operator can set an individual power supply's type, the battery chemistry, the battery age, its Ampere hr rating, and its dispatch lead time. These parameters, when set, will override the default configurations set in the POM XML file for this particular power supply device. The Device Config override is only available for HMS Power Supplies.

# 7.0 System Administration

The Administration page offers access to the AlphaXD administrative and system setup functions. To access the Administration page, click the Administration tab.



**Fig. 7-1, Administration Page**

The functions on the Administration tab page are arranged in six groups which are also accessible by the links in the AlphaXD Administration tab at the top of the page.

- Battery Test Config - A tool to configure the parameters of automatic background power supply testing.
- Email Alert - A page to set up technician email parameters.
- XM360 Configuration - A page to configure the XM3 Integration and displays last polling as well as scheduled polling.
- Send Event - A tool to test that devices are properly sending events to the AlphaXD server.
- Bulk Task Status - A page that displays the items in the active, waiting and completed bulk task queues.
- Template Administration - A page to review, administer, and apply templates and alert profiles.
- FCC Test Point Profiles - A page to assign HFC Plant devices from the Plant Devices page to their relative point of impact on the Network Tracker FCC proof measurements.
- Plant Devices - A page to model the RF characteristics of HFC plant devices used in FCC proof of performance measurement calculations with the Network Tracker.
- Discovery Configurator - A page to view and modify auto-discovery configuration settings.
- Discovery Queue - A tool that displays devices in various stages of auto-discovery and allows the operator to clear the queue or clear devices still waiting to be auto-discovered.
- DB Backup - A page to specify database backup parameters and perform manual backups.
- Shutdown Server - A page for proper and controlled shutdown of the server.
- System Details - A page showing summarized data of various aspects of the system.
- System Performance - A page showing the status of server resources to be used for system diagnostics.
- Server Logs - A page where the operator can view information about log entries.
- Logs Configurator - A page where the operator specifies how events are logged and retained.
- Logs Monitor - A page where the operator can view a snapshot of a log file in real time. The Log Viewer provides tools for searching through the file and for searching for specific data.
- User Configuration - A tool used to create and maintain user information.
- Group Configuration - A tool to create and maintain group information.
- Alert Filters - A page to configure the details of low level alarm information processing through AlphaXD.

## 7.0 System Administration, continued

### 7.1 Administration — XM360 Configuration

To Configure the XM360 Integration, select the **Administration** button on the XD Tab bar. From the drop down window, select **Alpha XD Admin**. From the next window, select **XM360 Configuration**. The Configure XM360 Integration page will appear allowing the operator to enable the configuration, log in, name and set a start time and date for the polling run. Additionally, the operator may force a polling run from this window. This page also displays the last time the polling ran and when the next poll is scheduled to run.

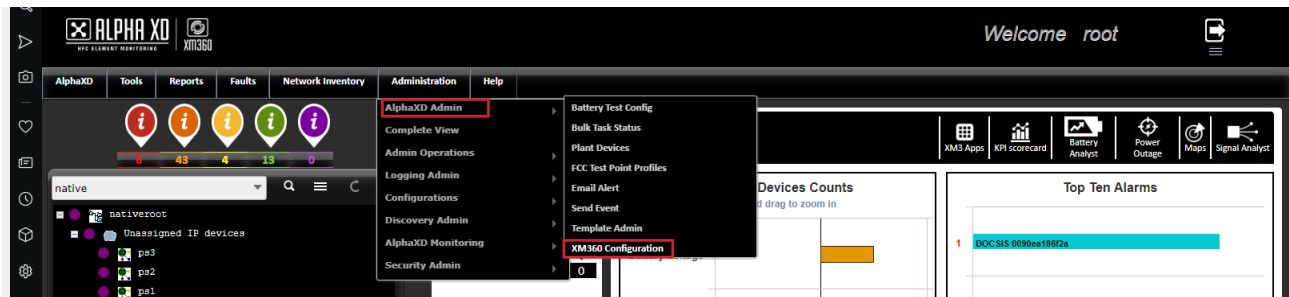


Fig. 7-2, Location of XM360 Configuration via Administration Button

A screenshot of the 'Configure XM360 Integration' window in the Alpha XD interface. The window title is 'Configure XM360 Integration' and it features a 'Force Polling Run' button in the top right. The configuration options are as follows:

- Status:  Enabled  Disabled
- User Name:
- Password:
- Report Name:
- Start Date:  (with a calendar icon)
- Hour:  (with a dropdown arrow)
- Last Run: Tue Dec 04 2018 12:33:25 GMT-0800 (Pacific Standard Time)
- Next Run: Wed Dec 05 2018 12:17:42 GMT-0800 (Pacific Standard Time)

At the bottom, there are 'Update' and 'Back' buttons.

Fig. 7-3, Configure XM360 Integration Window

## 7.2 Using the Bulk Task Status Page

The Bulk Task Status page displays the items in the active, waiting and completed bulk task queues. The items displayed here have either had the Download All or Download Changes options selected when provisioned. This page also displays manual transponder resets, alert profile downloads and generic firmware downloads.

Bulk Task Status										
Refresh In <input type="text" value="2"/> Seconds <input type="button" value="Refresh"/> <input type="button" value="Pause"/> <input type="button" value="Options"/>										
Active Bulk Tasks										
	Id	User	Device Count	Task Type	Task State	Time Started	% Complete	Estimated Completion Time	Actions	
<input type="button" value="+"/>	4	root	1	Device Download (All)	Running	11-09-2016 15:18:01	0 %	Unknown	<input type="button" value="Cancel"/>	
Waiting Bulk Tasks										
	Id	User	Device Count	Task Type	Time Submitted	Priority	Actions			
Completed Bulk Tasks										
	Id	User	Device Count	Task Type	Task State	Time Started	Time Completed	Actions		
<input type="button" value="+"/>	3	root	1	Profile Download (*_T_Transponder_CL_Legacy_Transponder_3000)	Finished with errors	11-09-2016 12:36:38	11-09-2016 12:37:28	<input type="button" value="Restart"/>	<input type="button" value="Remove"/>	
<input type="button" value="+"/>	2	root	1	Profile Download (*_T_Transponder_CL_Legacy_Transponder_3000)	Finished with errors	11-09-2016 11:52:33	11-09-2016 11:53:24	<input type="button" value="Restart"/>	<input type="button" value="Remove"/>	
<input type="button" value="+"/>	1	root	1	Profile Download (*_T_Transponder_CL_Legacy_Transponder_3000)	Finished	11-09-2016 11:39:29	11-09-2016 11:40:39	<input type="button" value="Restart"/>	<input type="button" value="Remove"/>	
<input type="button" value="+"/>	0	root	1	Device Download (All)	Finished	11-08-2016 10:32:35	11-08-2016 10:32:44	<input type="button" value="Restart"/>	<input type="button" value="Remove"/>	
<input type="button" value="Clear Completed Tasks"/>										

Fig. 7-4, Bulk Task Status Page

- Id – The ID of the task.
- User – The name of the user that initiated the task.
- Device Count – The number of devices that the task is acting upon.
- Task Type – The type of task being executed.
- Task State – The current state of the task.
- Time Started – The time that the task started.
- Time Submitted – The time that the task in the waiting queue was submitted.
- Priority – The priority of the task in the waiting queue. Priorities can be adjusted by the operator.
- % Complete – The percentage of the task that is complete. This applies only to tasks in the active queue.
- Estimated Completion Time – The estimated completion time for the task in the active queue.
- Time Completed – The completion time for the task. This applies only to tasks in the completed queue.
- Actions – The type of actions associated with a particular task that are available.

The Active Bulk Tasks queue displays currently active tasks. This queue holds a maximum of five tasks.

The Waiting Bulk Tasks queue displays the tasks that are in the queue but are not yet running. When a task is completed, the task with the highest priority in the Waiting Bulk Tasks queue is moved into the Active Bulk Tasks queue (A priority number of 1 is a higher priority than a priority number of 5). When two or more tasks in the Waiting Bulk Tasks queue have the same priority level, the system will give a higher priority to the task with the earliest task submission time.

The tasks in the Completed Bulk Tasks queue display the finished status of the task in the Task State parameter. Each task can be removed or restarted individually, or all of the tasks can be removed at once by clicking Clear Completed Tasks. This queue holds a maximum of 25 tasks.

Task details can be viewed by clicking on the button next to the task ID number.

### 7.3 See Devices in the Discovery Queue

1. In the AlphaXD Administration section of the Administration tab page, click **Discovery Queue**.
2. To clear the queue, click **Clear Queue**.
  - To clear just the devices still waiting to be auto-discovered, click **Clear Wait List**.



#### **NOTICE:**

Clearing the Discovery Queue will cause trap-based discoveries to be lost. The device will need to be rediscovered or reset.

### 7.4 Using the Database Backup Page

The Database Backup page allows the operator to specify database backup parameters and perform manual backups.

**Fig. 7-5, Database Backup Page**

- Refresh Field – The amount of time (in seconds) before the page is refreshed.
- Manual Refresh – Manually refreshes the page.
- Daily Backup Enabled – When enabled, the system will perform a daily system backup at the predetermined time.
- Database Backup Execution Hour – Specifies when the daily system backup will begin.
- Number of Backups to Archive – Specifies the maximum number of backup files to save. After reaching the limit, the system automatically overwrites the oldest file.
- Save – Saves the changes made to the database backup parameters.
- Backup Status – Information pertinent to the database backup.
- Execute Backup Now – Performs a manual database backup.

These backup procedures only save the application data necessary to restore the database. Backup procedures can be scheduled through another custom or operating system scheduling mechanism. Ensure there is enough disk space, as well as a cleanup method, in the location, drive or partition before scheduling a regular backup.



#### **NOTICE:**

Alpha recommends copying backup files to a separate directory or drive.

## 7.0 System Administration, continued

### Restoring a Database

#### Windows:

1. Shutdown AlphaXD.
2. Open a DOS window with Administrator privileges on the server where the database is installed.
3. Change to the directory AlphaXD\_HOME\conf\ccms\_database\Windows
4. Run the following command: “cheetahxd\_dbimport Auto\_CheetahXD\_11\_22\_2015 00\_05\_05”
  - “Auto\_CheetahXD\_11\_22\_2015 00\_05\_05” is the name of the backup file without the .tar.bz2 extension.
  - Messages will display on the screen as the database is being restored.
  - The backup file is located in AlphaXD\backup.

#### Solaris:

Use the following steps to run the database restore utility for AlphaXD on a UNIX system:

1. Shutdown AlphaXD.
2. Navigate to: cd AlphaXD\_HOME/conf/ccms\_database/Unix
3. Run the following command: “./cheetahxd\_dbimport.sh Auto\_CheetahXD\_11\_22\_2010 00\_05\_05 ”
  - Auto\_CheetahXD\_11\_22\_2010 00\_05\_05 is the name of the backup archive without the .tar.bz2 extension.
  - Messages will display on the screen as the database is being restored.
  - The backup file is located in AlphaXD\_HOME/backup.

## 7.5 Using the System Performance Page

The System Performance page contains two tabs (Server Details and Client Details) that show the various details of the server. By default, the System Performance page opens to the Server Details tab.

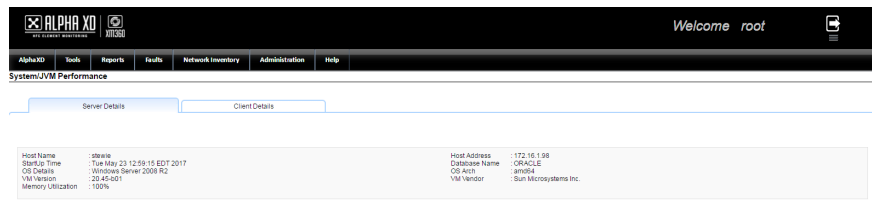


Fig. 7-6, System Performance Page

### Server Details Tab

The Server Details tab contains system level information pertaining to the server. The following details can be found on the Server Details page: Host Name, StartUp Time, OS Details, VM Version, Memory Utilization, Host Address, Database Name, OS Arch and VM Vendor.

### Client Details Tab

The Client Details Tab displays information about the machine on which this function is being executed, and the AlphaXD server with which it is communicating.

The Terminate Client feature is Security controlled. Only specified users are allowed to terminate others' sessions. A user cannot terminate his own session. To terminate a user's session, click on the “x” in the right-hand column.

### 7.6 Using the Log Entries Page

The Log Entries page lists logs for the AlphaXD system. Clicking on a log entry in the Name column displays a new browser window containing details about the log entry.

### 7.7 Using the Log Configuration Page

The Log Configuration page is used to specify how events are logged and retained. AlphaXD's capabilities include many text files for logging events within the various modules.

Each file can be configured to specify:

- The level of detail included in log entries.
- The maximum number of lines allowed in the file (after which the oldest entry is deleted to make room for the newest entry).
- The number of generations of the file that can exist.
- The maximum number of lines cached.

#### Open the Logging Configuration Page

1. In the Server Details panel in the Administration page, click the **Logs Configurator** icon.
2. Scroll the list to find the desired logging file and make any desired changes.
3. After making changes, scroll to the bottom of the list and click **Submit** to make the specified changes to the log files.
  - Click **Cancel** to return to the System Administration page without making the specified changes.
  - Click **Reset** to return all the log files to the default parameters.

#### Editing the Log Settings

The "Max Lines/File", "File Count" and "Max Lines Cached" log parameters can be edited through the associated XML file.

1. Navigate to the **Conf directory**.
2. Edit "**log4j.xml**".

Following is a sample log file entry:

```
<appender class="com.adventnet.management.log.NMSRollingFileAppender"
name="ctautodiscoverylog_file">
  <param name="File" value="logs/CTAutodiscoveryLog.txt"/>
  <param name="MaxFileSize" value="15MB"/>
  <param name="MaxBackupIndex" value="10"/>
  <layout class="org.apache.log4j.PatternLayout">
    <param name="ConversionPattern" value="[%d{dd MMM yyyy
HH:mm:ss:SSS}] %-5c{2}: %m%n"/>
  </layout>
</appender>
```



### 7.8 Using the Logs Monitor Page

The Logs Monitor page is used to view a snapshot of a log file in real time. The Log Viewer tab also provides tools for searching through the file and for searching for specific data within the file.

To view the logs in real-time:

1. In the Server Details panel in the Administration page, click the **Logs Monitor** icon.
2. Select the number of lines (at the end of the file) to be reviewed from the **Show Last** drop-down menu.
3. Select the name of the file to be reviewed from the **drop-down list**.
4. Click **View Logs** to view the lines of data within the file.
  - Search specific data by clicking the **Magnifying Glass** icon at the upper right corner of the window.
  - Open the viewer in a new window by clicking the **Maximize** icon at the upper right corner of the window.

### 7.9 Setting the Automatic LogOut Time Duration

To modify the length of time that a Client User can be logged into a session prior to being logged off, edit the file listed below, modify the numerical value in the highlighted line, whereas the numerical value will be an actual value in minutes to define the new desired logout duration.

AlphaXD/WEB-INF/web.xml

```
<!-- End XD servlet mappings -->
<welcome-file-list>
    <welcome-file>/webclient/common/html/Login.html</welcome-file>
</welcome-file-list>
<session-config>
    <session-timeout>30</session-timeout>
</session-config
```

## 8.0 Displaying Data

The AlphaXD Data Display feature displays real-time data from managed devices and the database. Analog information can be displayed as text or in graphical gauge and chart displays. Data can be displayed through:

- A device's local context menu accessed through:
  - A tree view
  - A notifier alarm
  - A device inventory list
  - The Alarm Template device list

Real-time data represents the actual values collected by AlphaXD at intervals specified in the Data Display Options. Devices or device attributes can also be excluded from the Data Display.

Displayable data include alarm data, as well as operational, download and configuration status. Data can be displayed for:

- All managed attributes of HMS and DOCSIS top-level devices (such as a transponder, a HEC, a CMTS, Network Trackers, AlphaGateways, GX2 headend equipment, Prisma headend equipment, or a power supply)
- One attribute of an HMS or DOCSIS device.
- CheetahNet devices, if CheetahNet is installed and integrated with AlphaXD.

Within AlphaXD, users can elect to display specific categories of data for multiple devices simultaneously by launching multiple instances of the Data Display. Because displaying data is resource-intensive, Alpha recommends using Data Display judiciously to minimize impact on overall system performance.

### 8.1 Launching AlphaXD Data Display



**NOTICE:**

---

Browser pop-up blockers must be disabled in order to see a device's Data Display.

To Launch AlphaXD Data Display, right-click on an element in the tree and then select the Data Display option from the local menu. This display can remain open and refresh automatically every thirty seconds, or at a user-specified interval.



**NOTICE:**

---

This is the local menu option for HMS and DOCSIS devices. The local menu for CheetahNet devices includes an option to launch CheetahNet's Data Display. (CheetahNet must be installed in order to run CheetahNet Data Display for CheetahNet devices.)

### 8.2 Categories of Displayable Data

When selecting Data Display from a managed object's local menu, a Data Display page for that object appears. Links at the top of the page offer different types of data to display, but not all categories apply to all devices. Different device types are monitored for different attributes. The links located in the middle of the page are used to display various groups of parameters.



**Fig. 8-1, Parameter Links**

- Analog – Displays the value of an attribute that is required to operate within a predetermined range as set in the device's configuration, and which causes an alarm when the value is out of range (i.e. battery voltage). Analog data display consists of the analog attribute name, the actual measurement value and the limit values set for the device, and can display in text or graphic format. If the attribute value is in an alarm state, it will be highlighted in the appropriate alarm-severity color.
- Non-Alarmable Analog – Displays the value of an attribute as set in the device's configuration, but which does not cause an alarm when the value is out of range (i.e. Battery Temperature Compensation, High Water Mark).
- Controls – Displays the actual state of discrete parameters and equipment functions. Also allows control of equipment functions (i.e. placing a power supply into standby mode). The control name describes the operation of the control. Most controls are based on a 2-step process: Set the value, then enable the control.
- Multi – Displays multi-valued device parameters. Each value can be independently configured to be either in a disabled state or an alarm state. An enumerated parameter generates an alarm if its current value is configured to be an alarm condition. If the value changes to another value that is also configured to be an alarm, another alarm is generated. A return (normal or clear) occurs when the value changes to one that has its associated alarm disabled.
- Misc – Displays miscellaneous data specific only to the selected device type. An example of Misc data is information retrieved directly from a transponder (such as model or serial number), instead of from the database.
- DeviceCfg – Launches the device configuration page, allowing a privileged operator to review and modify the device configuration (name, address, alarm limits, etc.)

Additional items at the top of the digital display page are:

- Stop – stops AlphaXD from gathering data and stops the session on the selected device.
- Refresh – forces an immediate data collection and resets the automatic data collection interval.
- Options – click this link to access configurable options for the current data display session. See the following section, Data Display Options, for more information.
- Refresh in...Seconds – this value counts down the seconds between each instance of AlphaXD performing a data collection. The default interval is thirty seconds, but can be reset for the current data display session using Data Display's Options link.

Real-time data represents the actual values obtained by AlphaXD at intervals specified in the Data Display Options.

## 8.0 Displaying Data, continued

The table headings describe the values that were measured in detail:

Attribute Name	Actual	Units	LoLo	Lo	Nominal	Hi	HiHi
----------------	--------	-------	------	----	---------	----	------

**Fig. 8-2, Data Display Table Headings**

- Attribute Name – The name of the property that was measured.
- Actual – The actual value of the measured property.
- Units – The type of units used to measure the property (i.e. volts, watts, percent, dBmV).
- LoLo, Lo, Nominal, Hi, HiHi – Used as a frame of reference for what is considered very low, low, normal, hi, or very high for the measured property.

## 8.3 Data Display Options

Click the Options link at the top of any Data Display page to specify how data is displayed.

Set DataDisplay Options:

text	▼
15	▼
30	▼

Select Analog Measurement Display Format  
Set Refresh Interval In Seconds.  
Set Pagination Count.

**Fig. 8-3, Set Data Display Options Page**

The drop-down menus provide different Data Display options.

- Select Analog Measurement Display Format – Specifies how the data is to be displayed. Available options are Text (default), Roundgauge, and Trendchart.
- Set Refresh Interval in Seconds for Current Session Only – The interval (in seconds) at which AlphaXD will collect data during the current data display session: 15, 30 (default), 45, 60.
- Set Pagination Count for Current Session Only – The number of desired pages for the current data display session: 10, 12 (default), 14, 16, 18, 20, 22, 24, 26, 28, 30.

## 8.4 Legacy (CheetahNet) Devices Data Display

Selecting a legacy (non-HMS) transponder launches the CheetahNet application displaying data using the CheetahNet Data Display feature. The CheetahNet client must be installed for this feature to operate. Also, if the operator has Battery Admin privileges and the VHEC proxy is running, the operator will be able to select the native AlphaXD Data Display.

## 8.0 Displaying Data, continued

### 8.5 Alpha XD Mobile Page

Selecting Alpha XD Mobile from this tab will open a dialog box to select a search option for Power supplies, Transponder MAC addresses or Nodes. Select the desired search option. Once the search option is selected a search text box for that option will appear. Begin to enter the search criteria in the text box. Once the minimum character limit is reached, the Search button becomes active and can be clicked (*data from a sample Transponder MAC search is shown below*).

Once the Search button is clicked the Device Selection page appears.

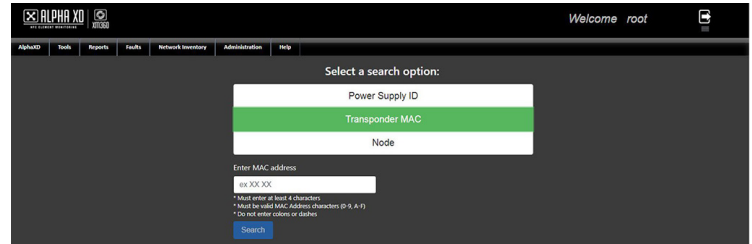


Fig. 8-4, Search Options Screen Page

Select the device to edit from the list and click the **Get Transponder** button.

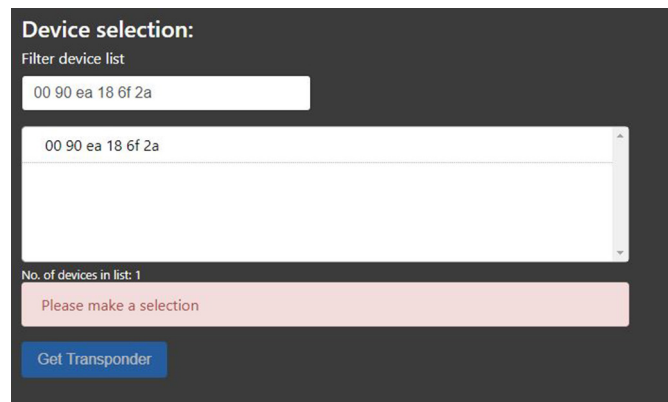


Fig. 8-5, Device Selection Screen

After the **Get Transponder** button is clicked the Modify Transponder page is displayed. From here the following fields can be changed.

- Display Name
- Node
- Power Supply Model
- Oldest Battery Date
- Battery Chemistry
- Battery Amp Hr Rating
- Tamper Polarity

If using a mobile device, an option to update the device location to the user's position is available. Select **Update Location** to do so. Once the fields are changed click the Update Transponder button. After this the information will be saved to the database. To remove the device from the system, click the **Remove Device** button on this page.

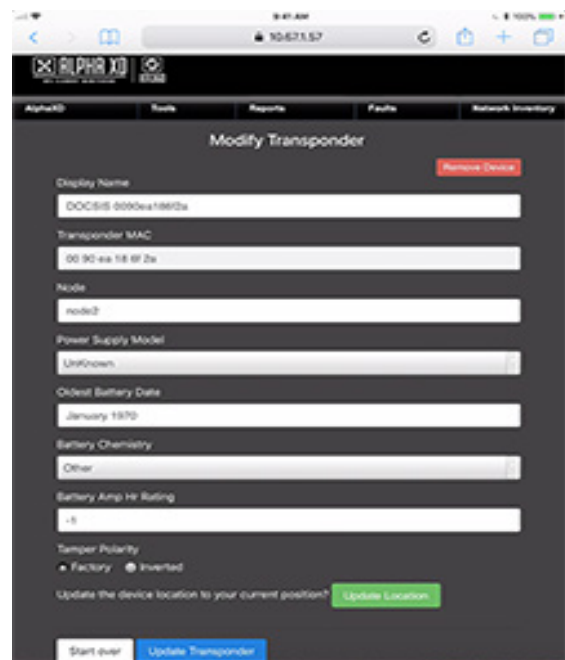


Fig. 8-6, Modify Transponder Screen

#### **NOTICE:**

Once the **Update Transponder** button is clicked, the data is saved so the data entered will also appear in the Device Configuration page for the device.

## 8.0 Displaying Data, continued

### Alpha Mobile Screen:

Customizing the character limit for the search filter can be done by editing entries in the EnglishToNative.properties and/or EnglishToNativeSpanish.properties files. The entries for each option are listed below.

Power Supply ID abmDashboard.config.minPSCharSearchSize=4

Transponder Mac abmDashboard.config.minMacCharSearchSize=4

Node abmDashboard.config.minNodeCharSearchSize=4

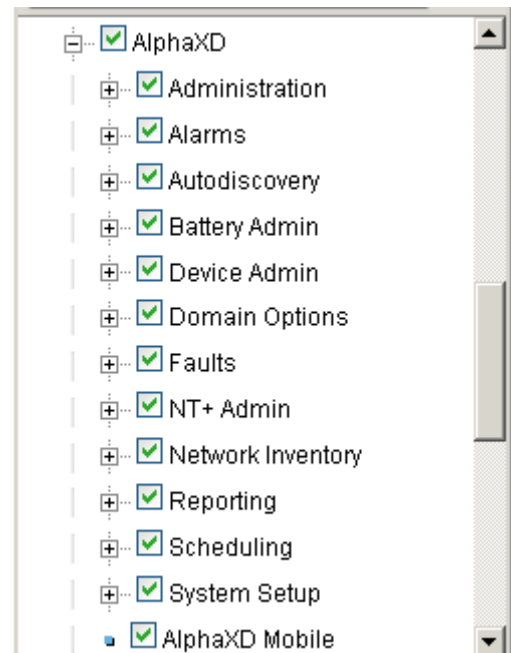


#### **NOTICE:**

The values set to 4 by default and cannot be set lower than 4 for performance purposes. If a user enters a value lower than 4, it will disregard the change.

### Group Configuration:

Access to the Alpha Mobile screens can be controlled via the Group configuration screen. A new option for 'AlphaXD Mobile' has been added under 'AlphaXD'.



**Fig. 8-7, Group Configuration Screen**

## 9.0 Testing Power Supplies

Testing the power supplies in the network on a regular basis ensures their capacity to support their associated network devices for the expected length of time during a power interruption. Only users with administrative level privileges can set up power supply testing parameters. In addition, users must have Battery Analyst Administrator privileges to access the Battery Global Admin Parameters page, enable and disable the associated functions, set default test parameters and run tests on demand. Users with Battery Admin User privileges can access the battery test results and can run tests on demand, but cannot access the Battery Admin Test Configuration information.

AlphaXD offers two ways to test power supplies:

- Automatically – Testing all power supplies on an on-going schedule (also called background testing).
- On-demand – selecting one power supply for one of the following immediate tests:
  - Battery Analyst Test – the same type of test as the automatic (background) test, which determines the general status of power supplies. This test can be run on more than one power supply simultaneously.
  - Inverter Test – to determine whether a power supply inverter is operational.
  - Deep Drain Test – to determine the amount of time the power supply can provide power during an actual outage, and to “exercise” the batteries for maintenance purposes by fully discharging and then recharging them.
  - Predictive Test – to determine the amount of time the power supply can provide power during an actual outage (the same as a Deep Drain Test), but without performing an actual deep drain on the power supply.

Run automatic and on-demand testing separately or simultaneously.

Power supplies are factory-defined as testable or not. The power supplies must be provisioned and downloaded in the AlphaXD software to be considered testable. If they are testable, the user can override the device’s configuration and exclude the power supply from automatic testing. See Excluding a Power Supply from Testing later in this chapter.

AlphaXD power supply testing primarily involves voltage testing. When available on power supplies, current and temperature readings are taken as well, depending on the type of power supply test being run.

Battery voltage tests place the power supply into a standby state (simulating an actual power outage) for the duration specified in the testing schedule. The following is a list of issues to consider when specifying the testing parameters.

- Power supplies in standby state are having their batteries drained. Ensure testing times, durations and intervals do not deplete the power supply’s batteries, with the exception of deep drain testing.
- Some power supplies are designed to stay in standby mode for a set amount of time, which may be shorter than the duration specified in the testing schedule. During battery testing, a power supply’s test will terminate according to the power supply’s design and settings. AlphaXD will display error messages for power supply attributes that did not yield enough samples (as defined in the Battery Admin testing configuration). An example would be a testing configuration that specifies taking three voltage measurements during standby, but only two measurements were completed before the power supply came out of standby. This can be overridden during an on-demand deep drain test. Alpha recommends becoming familiar with the parameters of each type of power supply before designing test schedules and performing on-demand tests.
- Ensure that test schedules allow batteries ample time to recharge between tests.
- By default, power supplies are tested one at a time, but a maximum of sixteen power supplies can be tested simultaneously.
- Non-provisioned power supplies and transponders set to Not Testable will not be tested.
- Make sure the supply’s “In Standby Limit” is set to a time value that is greater (longer) than the length of the test time.
- Power supplies in the Broadband Power System (BPS) or Unity Wave cannot be tested.
- Power supplies can be grouped to better facilitate the testing process. By placing power supplies into test groups (regions), the testing process can be distributed throughout the network, thereby preventing large sections of one portion of the network from being tested at one time.

## 9.0 Testing Power Supplies, continued

### 9.1 Creating Test Groups or Test Regions

Testing a power supply usually requires placing the supply into standby. Many operators consider it undesirable to simultaneously place several power supplies that are within close proximity to each other or located on the same portion of the network into standby mode. A more desirable approach is to distribute the testing of the supplies more evenly across the entire network. Placing power supplies into Test Groups provides an operator with the ability to distribute the testing over the entire network because the background testing algorithm will only test one supply from each region at one time. Placing groups of supplies into regions prevents the entire group from being tested at the same time.

To group power supplies, create trees specifically for power supply testing.

1. Navigate to the **AlphaXD** tab.
2. Hover over the **List** icon in the tree menu and click **Editing Tree Panel**.
3. In the right pane of the Tree Editing Panel, click the **Drop-Down Menu** and select the **Native Tree**.
4. Click the **nativeroot** item on the top of the tree view to highlight it.
5. Hover over the **List** icon and click **Add New Element**.
6. In the **Category Drop-Down Menu**, select **Device Group -- PS Test Group -- None**.
7. Enter the device name in the **Name** field.
8. Click **OK**. Repeat these steps for any additional power supply test groups.
9. In the Tree Editing Panel, hover over the **List** icon and click **Add Tree**.
10. Enter a **Name** and **Description** for the tree and click **New**.
11. Open the **Native** tree or **HFC** tree in the left pane of the Tree Editing Panel.
12. In the left pane of the Tree Editing Panel, select a power supply (select multiple using Ctrl-click).
13. Hover over the **List** icon in the left pane, then select **Copy Node** (Alone / With Children) to copy the selected power supplies.
14. Select the desired location to paste the copied devices to the tree in the right pane.
15. Hover over the **List** icon in the right pane and click **Paste**. Repeat as necessary.

Once the power supplies have been moved into various groups, the testing process can be distributed throughout the network, preventing large sections of one portion of the network from being tested at the same time.



## 9.0 Testing Power Supplies, continued

### 9.2 Setting Parameters for the Power Supply

To set the parameters for the power supply:

1. Right-click on the power supply device in the primary tree view and select Device Configuration.
2. On the Device Configuration page, select the Property tab.
3. Select the expand button to the left of the device name.
4. Edit the Power Supply Type, Battery Chemistry Type, Oldest Battery Type, Oldest Battery Age, and Battery Amp Hr Rating, as needed.

These parameters, when set, will override the default configurations set in the POM XML file for a particular power supply. Note: The Device Config override is only available for HMS power supplies. Please refer to Chapter 11: Fault Views – Power Outage Monitoring for details on customizing the Power Outage Monitoring application.

### 9.3 Power Supply Pre-Tests

Before any power supply test executes, the power supply is tested to ensure that the following conditions are met:

- The power supply has been provisioned.
- Commercial power must be present. If there is an actual power outage and no commercial power is present, the test will not execute.
- The tamper status indicates the housing is closed. In the event the power supply tamper status is disabled or otherwise not present, this pre-test will not occur and the power supply test will not commence. The tamper status verification can be disabled during setup.

Power supplies that were not tested due to a failure in one of these pre-tests will not be tested again until the automatic testing schedule reaches them again, or until another on-demand test is executed and they pass the pre-test.

### 9.4 Background (Automatic) Power Supply Testing

Automatic power supply tests run in the background according to the parameters specified in the Battery Analysis Admin Tool. Create a power supply testing schedule based on one of the following:

- Testing all power supplies in the network, regardless of how long it takes.
- Specifying the time when the tests should be run, regardless of how many power supplies are tested within that time frame. Repeat the test at regular intervals to meet the ongoing testing requirements.

Automatic testing can be enabled and disabled using the Battery Test Config option in the Administration page. Power supplies that are added, auto-discovered, or deleted after the testing parameters are specified are automatically included or excluded from subsequent testing, depending on the supply's "testability", and/or whether or not they have been explicitly excluded from testing. For more information on excluding power supplies, refer to Excluding a Power Supply from Testing later in this chapter.

## 9.0 Testing Power Supplies, continued

### Creating a Background (Automatic) Power Supply Test

#### To Specify Power Supply Testing Parameters:

1. Click the Administration tab page.
2. Click Battery Test Config. The Battery Analysis Admin Tool displays.
3. Set the following parameters as desired.

Test Configuration Parameters	
Parameter	Description
Battery Analysis Server	Click the button to select Enabled (to enable testing to occur) or Disabled (to prevent testing from occurring). This must be enabled to allow automatic download and on-demand power supply testing.
Check Tamper Switch	Status of the tamper switch. The following conditions apply: <ul style="list-style-type: none"><li>• Enabled: The Battery Analyst process will not run if the tamper switch is open.</li><li>• Disabled: The Battery Analyst process will run regardless of the tamper switch state.</li></ul>
Testing Time Period	The testing start and stop time. Click the Run Tests From radio button and click the two drop-down menus to select a start time and a duration. If all power supplies are not tested during the allotted time, the testing begins the next time with the first untested power supply.
Do Not Run On	Specify the dates and/or days of the week that will be exceptions to the schedule being created. On these dates and/or days, testing will not take place. Type one or more dates in mm/dd/yyyy format, multiple dates separated by commas, and/or check one or more boxes next to the days of the week. These days and dates will be exempt from the testing schedule.
Test Start Date (mm/dd/yyyy)	Click the calendar icon and select a date for the testing to begin.
Run Test Every	If testing on an ongoing basis, select a testing interval from 7 to 365 days.
Number of Parallel Tests	The number of power supplies to be tested simultaneously, from one to eight power supplies. This parameter can be used in conjunction with test regions, so that only one supply per region is tested each time the background test is performed.
Purge Data After	The length of time to retain power supply test results, up to a maximum of one year. Results can be exported to other formats, via the Battery Analyst Reports feature, for saving data beyond one year.
* The maximum time for a test is 60 minutes.	

**Table 9-1, Test Configuration Parameters**

## 9.0 Testing Power Supplies, continued

- In the Test Configuration Parameters section, select a Power Supply Test Group from the pulldown menu of existing Power Supply Test Groups. Selecting a new Test Group will only display the saved configuration parameters for that Test Group.

The screenshot displays the 'Battery Analysis Admin Tool' interface. At the top, it shows the user 'root' and the save time '02:09 03/25/13'. The main section is titled 'Battery Analysis Global Parameters' and includes:
 

- Battery Analysis Server:** Enabled (green button)
- Check Tamper Switch:** Disabled (grey button)
- Run Tests From:** 1:00 AM for 6 hours
- Do Not Run On:** A text field for dates with a note '\*Dates should be separated by commas.' and a 'Days' section with checkboxes for Mon, Tue, Wed, Thu, Fri, Sat, and Sun.

 Below this is the 'Schedule Configuration Parameters' section:
 

- Test Start Date:** 10/24/2016
- Run Test Every:** 180 days
- Num of Parallel Tests:** 8
- Purge Data After:** 180 days

 The 'Test Configuration Parameters' section is currently set to 'CAST Criteria' (checkbox checked) and 'PS Test Group: Default'. It includes:
 

- Number of Pre-Test Samples:** 2
- Test Duration (minutes):** 5
- Number of Post-Test Samples:** 2
- Seconds between Measurements:** 60
- A 'Configured PS Test Group' dropdown menu.

 At the bottom, there are buttons for 'Add/Modify PS Test Group', 'Remove PS Test Group', and 'Setup Admin Schedule'.

**Fig. 9-1, Battery Analysis Admin Tool Page**

- From here, the parameters are defaulted to CAST Criteria, defined as:
  - A 10 Minute Test
  - 1 Pre-Test Measurement Collection
  - 1 Post-Test Measurement Collection
  - Data Collected Every 15 seconds During Test for 10 Minutes
- Or, set the following parameters as desired by unchecking the CAST Criteria checkbox (See the table below).

CAST Setting Parameters	
Parameter	Description
Number of Pre-Test Samples	The number of measurements (from one to five) to take before a test cycle.
Test Duration (minutes)	How long the test will run (not including the pre-test and post-test measuring). <ul style="list-style-type: none"> <li>A minimum of 10 measurements are required to determine the battery runtime capacity in the final report. The power supply's internal testing duration configuration should be taken into account as this will override external commands and can cause the Battery Analyst test to fail.</li> </ul>
Number of Post-Test Samples	The number of measurements (from one to five) to take after the test cycle.
Seconds Between Measurements	The number of seconds between each measurement.

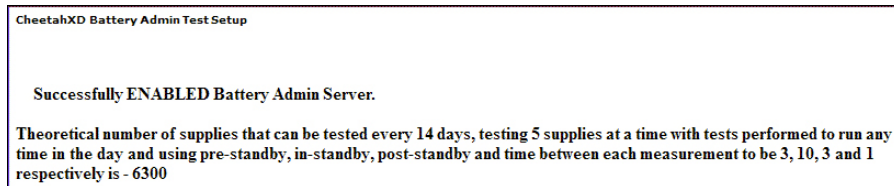
**Table 9-2, CAST Setting Parameters**

## 9.0 Testing Power Supplies, continued

7. If active, click the Add/Modify PS Test Group Button.
8. Click the Setup Admin Schedule button. AlphaXD displays a page showing the parameters of the test schedule, and the estimated number of testable power supplies that will be tested.

### **NOTICE:**

When Power Supply Test Groups are involved, no more than one power supply will ever be in standby at the same time within a given group. The exception to the rule is Unassigned Groups. If no groups are defined, the number of power supplies that will be in standby at the same time is determined by the value given in the Number of Parallel Tests drop-down box (found on the Battery Analysis Admin Tool page).



**Fig. 9-2, Battery Test Setup Page**

Once the schedule is completed, the Battery Analysis Server Button (on the Battery Admin page) can be clicked at any time to enable and disable the automatic testing as desired. The Setup Admin Schedule button must be clicked to save any changes, including the Battery Analysis Server button.

## Removing a Power Supply Test Group

1. In the “Test Configuration Parameters”, select a Power Supply Test Group from the “PS Test Group” list.
2. Click Remove PS Test Group.
3. Click Setup Admin Schedule.
4. When removed, power supplies in the associated test group will return to the default settings.

## 9.5 On-Demand Power Supply Testing

An on-demand power supply test executes immediately. By default, the tests will be run via CAST Criteria parameters, unless the CAST Criteria checkbox is de-selected. Results of on-demand tests are available through the on-demand test page and by running the Battery Analyst Report. To execute an on-demand test without the background processes, enable the Battery Analyst server, then select all of the days in the “Do Not Run” section.

### **NOTICE:**

CAST (AlphaXD Analytics Self-Test) Criteria is a default 10 minute self-test. The Testing Parameters consist of:

- 1 Pre-Test Measurement
- 1 Post-Test Measurement
- Data Collection in 15 second intervals for 10 minutes

### **Run an On-Demand Power Supply Test:**

1. Ensure that the Battery Analysis Server option is enabled. See Creating a Background (Automatic) Power Supply Test for information on enabling the Battery Analysis Server option.
2. Display the power supply to be tested in the Tree Viewer (expand the view one level, if necessary, to expose the icon).
3. Right-click on the power supply to display the local menu.
4. Select the desired on-demand test from the local menu: Battery Analyst, Battery Tests (Inverter Test, Deep Drain Test, or Predictive Test).

## 9.0 Testing Power Supplies, continued

### Select Multiple Power Supplies to Run an On Demand Test:

1. Ensure that the Battery Analysis Server option is enabled. See Creating a Background (Automatic) Power Supply Test for information on enabling the Battery Analysis Server option.
2. Display the power supplies to be tested in the Tree Viewer (expand the view one level, if necessary, to expose the icon).
3. Control-click on the power supplies to be tested.
4. Right click on any of the selected power supplies and select Battery Analyst from the local menu.

### To Run an On Demand Test on Multiple Power Supplies in a Container:

1. Ensure that the Battery Analysis Server option is enabled. See Creating a Background (Automatic) Power Supply Test for information on enabling the Battery Analysis Server option.
2. Right-click on the container that includes the desired power supplies (Supported containers are: The root of a tree, ps test group container, hub container, headend container, region container, Unassigned IP Device container).
3. Right click on the container and select Battery Analyst from the local menu.



#### **NOTICE:**

Only the Battery Analyst test can be performed when executing an On Demand test for multiple power supplies.

## Battery Analyst Test



#### **NOTICE:**

All Battery Analyst tests offer an option to perform the test in the next 1-24 hours

This test is the same test that is executed when the background automatic testing is run, except that this test is created and run on an on-demand basis with a user configured test name. The test also allows the user to override some of the default admin configured parameters.

The following page displays when the Battery Analyst test is selected from the local menu of a testable power supply in a tree.

On Demand Battery Test

Device Name	DOCSIS 0090ea04b2d9 Power Supply 1
Create Battery Test Name	

Current Test Configuration Parameters

<input checked="" type="checkbox"/> CAST Criteria	
Delay (in hours)	0
Number of Pre-Test Samples	1
Test Duration (minutes)	10
Number of Post-Test Samples	1
Seconds between Measurements	15

Create BA Test

Fig. 9-3, Battery Analyst Page



#### **NOTICE:**

The maximum time for a test is 60 minutes.

## 9.0 Testing Power Supplies, continued

1. Enter a name for the test in the **Create Battery Test Name** text box (up to 200 characters, no special characters or spaces and cannot start with a numeric value). This name will appear in the Battery Analyst Report. It is helpful to make this name meaningful, perhaps including the test type and/or date the test is run. Note that the power supply to be tested is displayed in the Device Name text field.
2. Accept the displayed test configuration parameters, or click the drop-down menus and change them.
3. Click **Create BA Test** to run the test.

### General Q&A on Battery Analyst

Battery Analyst Q&A	
Question	Answer
What constitutes a failure of the BA report?	A failure is reported in Battery Analyst if during the discharge part of the test one of the batteries is outside the Discharge Variance value set by the user during the report creation. This indicates the battery did not trend with the other batteries and the battery string impedance normalcy is outside the user set criteria.
Will Lectro CPR Power Supplies run in Battery Analyst?	Yes, given that the test is set to a 1 minute time limit. However, CPR standby time limitations could create false failures.
What if Standby Test Time in the device is set to a shorter time frame than the BA test?	The power supply will be removed from standby based on the Standby Test time in the device and would cause a false failure. The test time in the device must be more than the test time set for the BA test..
What happens when On Demand BA test is run for a dead device?	The test will take a long time to load and will fail after loading. No data is reported.
If the On Demand Tests from the Battery Test Page are deleted, do the results get removed from the database?	Yes
Are standby counters triggered with BA Tests?	Yes
If polling is OFF, does a BA Test still run?	Yes
Is POM triggered with BA Tests?	No, because a loss of Input Voltage threshold has not been violated.
Will test run if Output Current reads 0.00?	Yes
If the fuse is missing or bad, will a BA Test run?	No, because that generates an Output Voltage alert, which stops the test from running.
If a test starts and then fails, is the test time updated?	Yes. The failed transponders will not test again until it is time to do so.
Can a currently running Background BA test be stopped?	Yes, by setting the schedule to Disable, there will be a database error in the BattAdmin log file when there is an attempt to write data to the database.
Will tests run if BA Schedule is changed?	Yes
If a test cannot start because of a Comms issue, tamper issue, Output Voltage issue, or In Standby issue, does the Test Time get deleted?	Yes
What constitutes a started test?	If any Pre Standby measurement is recorded
Will the test run if the Input Voltage is in a Lo or LoLo alert?	No. The Input Voltage needs to be over 95 Volts.
Will tests run if the Tamper Switch is open?	It depends on the Tamper Switch setting on the BA Admin Page. If it is set to Enabled, then if a Tamper Switch alert is present, a test will not run. If this setting is set to disabled, then the test will run.
Will the standby test run if a power supply is incorrectly configured?	Yes, and if all else is OK, the test will complete.

**Table 9-3, Battery Analyst Q&A**

## 9.0 Testing Power Supplies, continued

### Battery Analyst Testing Status Results

Battery Analyst Testing Status Results				
Value	MIB Definition	Meaning	Possible Cause	Remedy
1	The test is idle	No test has been run on this device since the last time it was reset or since it was installed.	Newly installed or a reset transponder.	N/A
2	In Progress	When the test is running normally, this value is in the In Standby portion of the data grid.	Test is running.	N/A
4	Complete	Post test value showing the device made it into and out of standby.	Successful Test	N/A
7	Abort Standby from Host	This indicates that the Power Supply was taken out of standby.	Power supply taken out of standby physically or remotely.	N/A.
8	Abort - AC Output Voltage Alarm	There is a Lo or LoLo Output Voltage Alert or a fuse may be bad/missing.	There is a Lo or LoLo Output Voltage Alert.	Correct the Output Voltage alert.
			Fuse may be bad, missing or loose.	Fix or replace the fuse.
9	Abort - Power supply took itself out of standby	The power supply came out of standby mode. This could be caused by several things.	Weak batteries	Verify batteries with a load tester. May need to be replaced.
			Inverter failure	Replace the inverter.
			Battery breaker open	Reset the breaker.
			Loose battery connections/corroded connections	Clean and/or tighten terminal connections.
9	Abort - Power supply took itself out of standby	The power supply came out of standby mode. This could be caused by several things.	Excess load	Check Output Current reading. If high, reduce the load.
10	Abort - Power supply already in standby	The power supply was already in a standby state.	Power supply was in standby.	Take the power supply out of standby.
11	Abort - Output alarm	Power supply output failure (Alpha related).	Power supply output has failed.	N/A
91	None	Backend Test Failure - No Communication	Loss of RF to transponder.	Restore RF communications.
92	None	Backend Test Failure - Already in Standby	Power Supply was in standby.	Take the power supply out of standby.
93	None	Backend Test Failure - Tamper Switch Open	Battery Admin Setup has enabled the Tamper Switch check.	Disable the check from the Battery Admin page.
				Keep the Tamper check active, but resolve issue at the power supply.
94	None	Backend Test Failure - Input Voltage too low	Input Voltage is below 95 Volts.	Minimum Voltage of 95 required to run test.

**Table 9-4, Battery Analyst Testing Status Results**

## 9.0 Testing Power Supplies, continued

### Inverter Test

The Inverter Test initiates the power supply inverter, placing the power supply in standby for approximately 60 seconds.

In tree view, click to select a battery/power source, right-click to view the Common menu and select Battery Tests > Inverter Test.

#### On Demand Inverter Test

Device Name	DOCSIS 0090ea0d74f9 Power Supply 1
Create Inverter Test Name	

Create Inverter Test

**Fig. 9-4, On Demand Inverter Test Page**

1. Type a name for the test in the Create Inverter Test Name text box (up to 200 characters, with no special characters or spaces and cannot start with a numerical value). This is the name that will appear in the Battery Analyst Report. It is helpful to make this name meaningful, perhaps including the test type and/or date the test is run.
2. Note that the power supply to be tested is displayed in the Device Name text field.
3. Click Create Inverter Test to begin the test.

Battery voltages, output currents and temperature readings are collected at the start of the test, and again just before the inverter is switched back off. The results are stored in the database.

### Deep-Drain Test

The deep drain test simulates an actual power outage to determine the length of time the power supply can remain in standby. This test performs a deep discharge until one of the following user-specified conditions is met:

- A user-configurable minimum battery voltage is reached, generally 10.5 V for a 12 V battery.
- A user-configurable minimum input voltage is reached.
- A user-configurable maximum test time limit is reached.

#### On Demand Deep Drain Test

Device Name	DOCSIS 0090ea0d74f9 Power Supply 1
Create Battery Test Name	

#### Deep Drain Test Parameters

Max Test Time (min)	60
Data Collection Interval (min)	5
Reset Standby Interval (in min)	11
Min. Input Voltage Limit(V)	
Min. Battery Voltage Limit(V)	

Create Deep Drain Test

**Fig. 9-5, Deep Drain Test Page**



## 9.0 Testing Power Supplies, continued

1. Type a name for the test in the Create Inverter Test Name text box (up to 200 characters, with no special characters or spaces and cannot start with a numerical value). This is the name that will appear in the Battery Analyst Report. It is helpful to make this name meaningful, perhaps including the test type and/or date the test is run.
2. Note that the power supply to be tested is displayed in the Device Name text field.
3. Specify (or accept) the following testing parameters:
  - Max Test Time (min) - The deep drain test will terminate if it is still running when the specified number of minutes has been reached.
  - Data Collection Interval (min) - How often (in minutes) battery measurements will be taken during the test.
  - Reset Stand by Interval (min) - Power supplies are designed to remain in standby for a specific amount of time when commercial power is present. See the power supply manufacturer's documentation for the maximum test time value. To keep these power supplies in standby for longer, specify a time here, in minutes, which is less than the power supply's maximum test time value. The test will briefly bring the power supply out of standby and immediately return it to standby, resetting the power supply testing time.
  - Min. Input Voltage Limit (V) - The minimum limit for the input voltage at which the test will terminate.
  - Min. Battery Voltage Limit (V) - The minimum limit for the battery voltage at which the test will terminate.
4. Click Create Deep Drain Test to begin the test.

## Predictive Test

The predictive test estimates the standby capacity of a power supply during an actual power outage. It predicts the likely results of the Deep Drain Test, but without draining the batteries. This test requires the following parameters:

- Power supply type
- Battery technology
- Battery age
- Battery Amp-Hr rating

The accuracy of the test is heavily dependent on the values specified; entering incorrect values will likely produce an inaccurate estimate.

Select Predictive Test from the local menu of a testable power supply in a tree.

On Demand Predictive Test

Device Name	DOCSIS 0090ea0d74f9 Power Supply 1
Create Predictive Test Name	

Predictive Test Parameters

Power Supply Type	UnKnown ▾
Battery Amp-Hour Rating (Ah)	120 ▾
Battery Type/Technology	Gel Cell ▾
Battery Age	UnKnown ▾

Test Criteria (if applicable)

Max Test Time (min)	Not Applicable ▾
Reset Standby Interval (in min)	Not Applicable ▾
Min. Battery Voltage Limit (V)	Not Applicable ▾

Create Predictive Test

Fig. 9-6, Predictive Test Page

## 9.0 Testing Power Supplies, continued

1. Type a name for the test in the Create Inverter Test Name text box (up to 200 characters, with no special characters or spaces and cannot start with a numerical value). This is the name that will appear in the Battery Analyst Report. It is helpful to make this name meaningful, perhaps including the test type and/or date the test is run.
2. Note that the power supply to be tested is displayed in the Device Name text field.
3. Specify (or accept) the following testing parameters. The more specific and accurate the parameters, the more realistic the results of the Predictive test will be.
  - Power Supply Type - XM, XM2, XM3, Lectro ZZT, etc.
  - Battery Amp – Hour Rating (Ah) – see the power supply manufacturer’s documentation for this value.
  - Battery Type / Technology – usually “lead-acid” but can be “gel cell” or other type of technology.
  - Battery Age – how long the battery has been installed and operational.
  - Max Test Time (min) – specify how long the test will run and collect sample. The test will terminate when it has been running for this number of minutes. The default is ten minutes.
  - Reset Standby Interval (min) – Many power supplies are designed to remain in standby for a specific amount of time, when commercial power is present. See the power supply manufacturer’s documentation for the maximum test time value. To keep these power supplies in standby for longer, specify a time, in minutes, that is less than the power supply’s maximum test time value. The test will briefly bring the power supply out of standby when the specified time is reached and immediately return it to standby, thereby resetting the power supply testing time. For example, for a power supply that remains in standby for thirty minutes, set the Reset Standby Interval to 25. In 25 minutes, while the power supply is still in standby, the test brings the power supply out of standby. After approximately five seconds, the test puts the power supply back into standby, where it will begin counting its thirty minute standby limit again, or until another 25 minutes has elapsed, when the test will again briefly bring it out of standby. It is important to know the standby limits of the power supply being tested to effectively run the Predictive Test.
  - Min. Battery Voltage Limit (V) – During the test, if the battery voltage reaches this limit, the test will terminate.
4. Click Create Predictive Test to begin the test.

## 9.6 Viewing Background (Automatic) Results for Completed Tests

View results for background power supply testing by running a Battery Analyst Report through the **Reports** Page.

### Viewing Background Testing Power Supply Groupings

When background test schedules are created, a user with the appropriate permission can specify running one or up to sixteen tests simultaneously. For example, in a system with 100 power supplies, a testing schedule configured to run five tests in parallel will test 20 devices in each of the five threads created for the simultaneous testing.

AlphaXD offers three ways to view which power supplies are grouped for simultaneous testing, and which groups are currently being tested (on standby). Background testing must be enabled and running to view these groupings.

1. Through on-demand tests - when an on-demand test is successfully created, a confirmation screen will display.
2. Click the View All On Demand Tests Status link. To view all power supplies in the On Demand test click on View Schedule.
3. Click the Battery Tests link under Scheduling.

### 9.7 Viewing Status, Details and Results of On-Demand Tests

Viewable On-demand Test Information:

- Status
- Details
- Results
- Date and time of most recent test

#### Viewing On-Demand Test Status

View on-demand test status from the page that displays as soon as the newly-created test begins from the Reports menu bar option (click Scheduling, then Battery Tests) or from the Device Configuration module.

Click the View all on-demand tests status link. The on-demand test details that display include:

- Test Name – this is the name the user types in the Create [Test Name] field
- Test Type – this is the type of on-demand test (Battery Test, Inverter Test, Deep Drain Test, Predictive Test)
- Test Status – this column shows whether the test is running or has completed.

For completed tests, the Test Status column includes two links: View Results and Delete. Click the View Results link to see the results of the on-demand test.



---

**NOTICE:**

Test will remain on this page until they are deleted by clicking the Delete link. On-demand reports can also be viewed from the Battery Analyst Report link located under the Reports menu.

Test status can also be viewed through the Device Configuration Module. Click the power supply's local context menu in any tree view and select Device Configuration.

The Information tab page of the Device Configuration includes the following on-demand test parameters:

- Last date and time the Deep Drain test was run
- Status of the last Deep Drain Test
- Last date and time the Predictive test was run
- Status of the last Predictive test
- Last date and time the Inverter test was run
- Status of the last Inverter test.



---

**NOTICE:**

The Battery Analyst test can be run as an on-demand test and as a background, automatic test. This test's information in the Information tab page, shown in the following figure, is listed in the parameter Previous Power Supply Test On (directly above the highlighted parameters). This parameter displays the date and time of the most recent Battery Analyst test, whether it was run from the background process or an on-demand test request

## 9.0 Testing Power Supplies, continued

Device Configuration: DOCSIS 0090ea0a87ef Power Supply 1

Information Property Analog Multi All attributes

DOCSIS 0090ea0a87ef Power Supply 1	
Name	DOCSIS_0090ea0a87ef_Power_Supply_1
Type	Power Supply
Last Status Update Time	2004-05-18 11:02:17.94
Last Status Change Time	2004-05-18 11:02:17.94
Failure Count	0
Device Communications Handler	CTHMSCommHandler
CTopoObject Type	TCPO
Is Top Level Container	true
Is Schedulable	true
Top Level Parent	DOCSIS_0090ea0a87ef
Gateway Parent	DOCSIS_0090ea0a87ef
Last Update Time	2015-07-21 12:04:12.356
Last Download Time	2015-07-21 12:04:12.382
Status Poll Off Timer Remaining (mins)	0
MAC Address	00 90 ea 0a 87 ef
Is Power Supply Testable	true
Previous Power Supply Test On	1969-12-31 19:00:00.0
Last Deep Drain Test Time	1969-12-31 19:00:00.0
Last Deep Drain Test Status	none
Last Predictive Test Time	1969-12-31 19:00:00.0
Last Predictive Test Status	none
Last Inverter Test Time	1969-12-31 19:00:00.0
Last Inverter Test Status	none
Last POM Standby Time	1969-12-31 19:00:00.0
Monthly Input Power	-1.0
Latest Inverter Runtime	0
Category	Power Supply
Template Type	HMS Power Supply
Modifier	Standard_1 (Standard_1)
Group Name	HMS
Application	HFC
Active Template	*_T_Power_Supply_HMS_Power_Supply_Standard_1


 **NOTICE:**  
A test date of 1969-12-31 19:00:00.0 indicates that a test has never been completed.

Fig. 9-7, Device Configuration Page

## 9.8 Excluding a Power Supply from Testing

Both automatic and on-demand power supply tests normally test all applicable power supplies. The Device Configuration module allows exclusion of a specific power supply from testing.

1. Display the power supply in any tree view (expand the view by one level if necessary to expose the icon).
2. Left click on the device to display the local menu.
3. Select Device Configuration.
4. Click the Property tab.
5. Click on the button to the left of the device name.
6. Click the Is Power Supply Testing Enabled checkbox to remove the checkmark.
7. Click Save.

The power supply will not be included in either automatic or on-demand testing.

# 10.0 Email Alerts

AlphaXD's Emailing feature can forward alarms to a technician immediately via email.

## 10.1 Setting up Emailing

An email setup is created per technician, and includes:

- Device types for the technician
- The chosen alarm priority (set priority or greater) that will trigger a page to the technician
- The time period during which the technician is available
- Specifics of the technician's e-mail account

### To Begin Emailing Setup:

1. Click the **Administration** tab at the top of the page.
2. Click the **Email Alert** icon in the AlphaXD Administration menu.
3. Create an email setup by specifying the email parameters on the five tab pages in the following order:
  - Configure e-mail specifics
  - Create the technicians
  - Activate the technicians
  - Update the server

### **NOTICE:**

The Save button in each tab only saves the current information for that tab. It does not update the server. After making all changes to this and/or any other information in Email Admin, click the Common tab and click the button to Save/Update the Server.

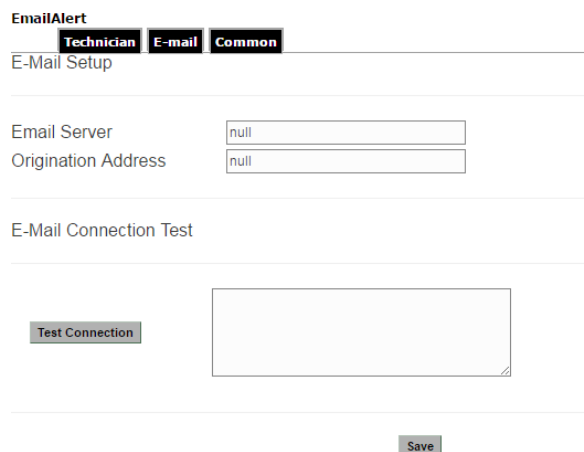
## Configuring Email

Click the email tab to open the Email Setup page.

- Email Server –type the name of the technician's or company's email server.
- Origination Address – type the email address from which the notification message originates. It represents the "from" address that appears in the header of an email message.
- Test Connection – click Save before clicking Test Connection. Test Connection tests the connection to the email server. After completing a test, the system displays a brief status message indicating the success or failure of the test.

### **NOTICE:**

- The email server may need to have an account that matches the AlphaXD origination address name.
- The TCP/IP ports associated with SMTP email must be open between the AlphaXD server and the target email server network.



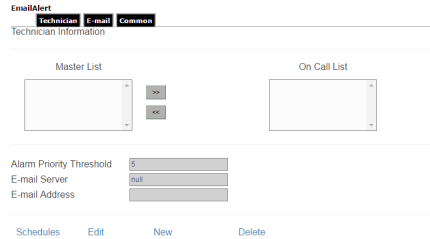
**Fig. 10-1, Email Setup Page**

## 10.0 Email Alerts, continued

### Creating Technicians

Creating technicians for emailing involves specifying the notification parameters for emailing, as well as the devices they support.

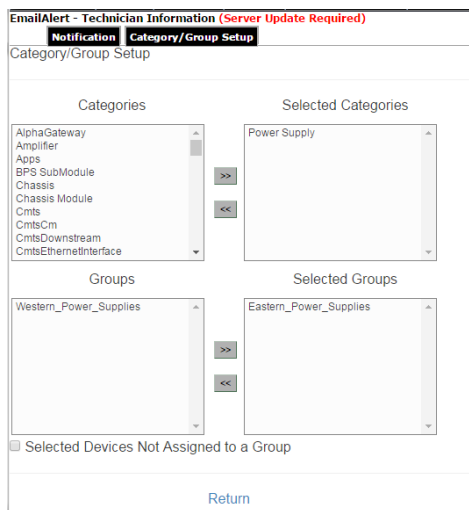
1. Click **New** on the Technician Information tab page.



The screenshot shows the 'EmailAlert' interface with the 'Technician Information' tab selected. It features two list boxes: 'Master List' and 'On Call List', each with '>>' and '<<' arrows between them. Below these are three text input fields: 'Alarm Priority Threshold' (containing '5'), 'E-mail Server' (containing 'null'), and 'E-mail Address'. At the bottom, there are four buttons: 'Schedules', 'Edit', 'New', and 'Delete'.

**Fig. 10-2, Notification Page**

2. Select the **Notification Type** for the technician.
3. Enter the technician's name in the Technician Name text box.
4. Click the drop-down box to select the **Alarm Priority Threshold**. The technician will be notified when an alarm occurs at this priority level or higher (1 being the highest, 99 being the lowest). An attribute's priority can be seen/set in Device Configuration.
5. Click the **Email Server** drop-down box and select the technician's email server.
6. Enter the technician's email address in the **Email Address** text box.
7. Click **Save**. (Use the Common tab and click the button to Save/Update the Server to save the changes.)
8. Click the **Category/Group Setup** tab.



The screenshot shows the 'EmailAlert - Technician Information (Server Update Required)' interface with the 'Category/Group Setup' tab selected. It features two main sections: 'Categories' and 'Groups'. The 'Categories' section has a list box on the left containing items like 'AlphaGateway', 'Amplifier', 'Apps', 'BPS SubModule', 'Chassis', 'Chassis Module', 'Cmts', 'CmtsCm', 'CmtsDownstream', and 'CmtsEthernetInterface'. A list box on the right, 'Selected Categories', contains 'Power Supply'. The 'Groups' section has a list box on the left containing 'Western\_Power\_Supplies' and a list box on the right, 'Selected Groups', containing 'Eastern\_Power\_Supplies'. Below these sections is a checkbox labeled 'Selected Devices Not Assigned to a Group' and a 'Return' button.

**Fig. 10-3, Category/Group Setup Tab**

9. Scroll through the **Categories** list and select one or more devices for the technician (Use Ctrl+Click for multiple selections).
10. When the desired devices are selected, click the **Arrow** icon to move them to the **Selected Categories** list.
11. If the desired devices to be emailed about belong to a certain group, select the group from the **Groups** list and click the **Arrow** icon to move the Group(s) to the **Selected Categories** list.
12. If desired devices to be emailed about do not belong to a group, check the **Selected Devices Not Assigned to a Group** checkbox.
13. Click **Return**. (Use the Common tab and click the button to Save/Update the server to save the changes to the server.)

## 10.0 Email Alerts, continued

### Viewing, Creating, Deleting Technician Schedules

View, create and delete technician schedules through the Technician Information tab page of the Email Alert module.

To View a Technician's Schedule:

1. With a technician selected in the Technician Information tab page, click Schedules.

The screenshot shows the 'EmailAlert - Technician Information' page with the 'Schedules' tab selected. A large text area at the top displays the schedule details: 'start date : 11/09/2016 at 05:00:00 EST, stop date : 11/09/2016 at 12:00:00 EST'. Below this is a form with the following fields and controls:

- Display Schedules For Date:** A text field containing '11/09/2016' with a calendar icon to its right.
- Display All Dates:** A checkbox that is currently unchecked.
- Technician Name:** A text field containing 'john'.
- Start Time:** A time selection field with dropdowns for '01', '00', and 'AM'.
- Start Date:** A text field containing '11/09/2016' with a calendar icon to its right.
- End Time:** A time selection field with dropdowns for '01', '00', and 'PM'.
- End Date:** A text field containing '11/09/2016' with a calendar icon to its right.
- List Schedules:** A dropdown menu currently showing 'List Schedules'.

At the bottom of the page, there are two buttons: a blue 'Return' link and a grey 'Update' button.

**Fig. 10-4, Schedules Page**

2. To view a technician's schedule, the start date of the schedule is required. Click the calendar icon below the Display Schedules for Date field and select the start date. If a technician's schedule with that start date exists, it displays in the large text box at the top of the page. A calendar for the current month opens.
3. Click a date to display existing schedules for that date. The four icons at the top of the calendar, on either side of the month and year display, allow selection of the previous year, the previous month, the next year and the next month.

To Create a Technician's Schedule:



#### **NOTICE:**

When selected, the Display All Dates option displays all of the schedules (both active and inactive) for a particular technician.

1. After selecting a technician on the Technician Information tab page, click Schedules. The Schedules page opens.
2. Click the List Schedules drop-down box and select Add Schedule.
3. Specify a start time and stop time using the drop-down boxes, and a start date and stop date using the calendar icons to the right of the Start Date and End Date fields.
4. Click the Update button to save the schedule.
5. Click the Return link.
6. Click to select a technician name. Press the arrow button. This will send an email to the technician.

## 10.0 Email Alerts, continued

The Update button saves the current information but does not update the server with the new information. After making all changes to this and/or any other tab page in Email Admin, click the Common tab and click the button to Save/Update the Server for the changes to take effect.

To Delete a Technician's Schedule:

1. With a technician selected in the Technician Information tab page, click Schedules.
2. The Schedules page opens.
3. Click the List Schedules drop-down box and select Delete Schedule.
4. Click the Update button to save the schedule.

The Update button saves the current information but does not update the paging server with the new information. After making all changes to this and/or any other tab page in Email Admin, click the Common tab and click the button to Save/Update the Server for the changes to take effect.

## 10.2 Activating Technicians

After a technician is created, devices are assigned, and a schedule is created, activate the technician on the Technician Information page.

To activate a technician:



**NOTICE:**

---

Before activating or moving a technician to the On Call List, the technician must already have a schedule and at least one device assigned.

1. Open the Technician Information tab page (this is the default page).
2. Scroll the Master List to find the technician name and single click it to select it.
3. Click the double right-facing arrows to move the selected technician from the Master List to the On Call List. The technician is now activated to begin receiving alarm notifications according to the technician's emailing setup.



**NOTICE:**

---

To move a technician to the On Call List, the technician must have a device and a schedule already assigned.

Similarly, to deactivate a technician, select the technician's name in the On Call List and click the double left facing arrows to move the technician to the Master List. The technician is now deactivated and will not receive alarm notifications.



### 10.3 Update the Email Server

Specify email server attributes using the Common tab in Email Administration. Email Server attributes include:

- Changes saved on any of the other Email Administration tab pages
- Starting and stopping the email server
- Alarm handling

To update the email server:

1. Click the Common tab in Email Administration.

The screenshot shows the 'PageAlert' configuration window with the 'Common' tab selected. The interface is divided into several sections: 'Notification System', 'Notification Limits', and 'Overflow Action'. In the 'Notification System' section, there are checkboxes for 'Enable' and 'Automatic Re-enable', and a text input field for 'Re-enable In Minutes' with the value '0'. A note states: 'An unchecked Enable box will stop the paging server.' The 'Notification Limits' section contains text input fields for 'E-mail Alarm Queue Size' and 'Pager Alarm Queue Size', both with the value '0', and a checkbox for 'Enable Notification for Clear Events'. The 'Overflow Action' section has a checkbox and a text input field for 'Automatically Stop Actions For' with the value '0' and the unit 'Minutes'. At the bottom, there is a link for 'Refresh Enable Checkbox' and a 'Save/Update Paging Server' button.

**Fig. 10-5, Common Tab**

2. Complete the following fields:

- Enable – Click this checkbox to start the email server and activate all email schedules and parameters.
- Automatic Re-enable – Click this checkbox to automatically re-enable the email server after it has been disabled due to the Enable checkbox being unchecked. The next option, Re-enable in Minutes, specifies how many minutes pass before the Enable checkbox is re-checked.
- Re-enable In Minutes – When the Automatic Re-enable checkbox is checked, specify the number of minutes to pause before re-enabling the email server. This is useful to allow time for other areas of the network to recover before email resumes.
- Email Alarm Queue Size – Type the number of alarms to hold in the queue for sending to email accounts. Any alarm that arrives after this number has been exceeded will not trigger a notification, but it will be written to the log file. The maximum number of alarms the queue will hold is 9999.
- Enable Notification for Clear Events – Click in the checkbox to activate. When activated, devices will send an alarm when the event clears (returns from an alarm state).

## 10.0 Email Alerts, continued

- Overflow Action – Click the checkbox to specify how to handle the notification queue when it is in overflow. Clicking this checkbox enables the next option.
- Automatically Stop Actions For ... Minutes – Check the checkbox to activate, and specify the number of minutes to suspend the alarming function when it is in an overflow condition. This prevents a device triggering numerous, similar alarms from overwhelming the notification system.
- Refresh Enable Checkbox – Use this link to refresh the page with the original values.
- Save/Update Paging Server – Click this button after making any changes on any of the tab pages in Email Administration. The Save button on the tab pages saves changes and allows the user to move to other tab pages, but the changes are not communicated to the email server until this button is clicked.

## 10.4 Edit Technician Information

As technicians, equipment and responsibilities change, edit the technician information to ensure the paging setup is always accurate, current, and covers the needed dates and times.

To Edit Technician Information:

1. Display the Email Alert menu's Technician Information page.
2. Scroll the Master List and select the name of the technician to edit.
3. Click the Edit link at the bottom of the Technician Information page.

## 10.5 Deleting Technicians

Delete a technician when the person will no longer be notified of alarms. When a technician is deleted, all of the schedules associated with that technician are deleted as well.

To Delete a Technician:

1. Display the Email Alert menu's Technician Information page.
2. Scroll the Master List and select the name of the technician to delete.
3. Click the Delete link at the bottom of the Technician Information page.

## 10.6 Security Permissions

Enabling the Email Admin permission allows the users within a group to access the Email Alert link and perform all of the tasks associated with emailing.

To enable the Email Admin permission:

1. Navigate to the Security Administration panel and click Group Configuration.
2. When the Group Configuration display opens, choose a group's Assigned Operations link. The Operations Tree displays.
3. From the Operations Tree, go to AlphaXD > Administration > AlphaXD Admin and click Paging Admin to enable it.

### 10.7 Emailing Technicians Using Device Groups

As its name implies, a Device Group allows operators to arrange devices (such as HECs, transponders, etc.) into groups. In systems that contain large numbers of devices, an operator can better organize the devices by grouping them into individual Device Groups. These groups are then moved to custom tree views to organize the system even further.

Perhaps one of the most significant features of Device Groups is the ability to page one or more technicians based on Device Groups. Once created, a Device Group can be assigned to one or more technicians within the system.

To add granularity, operators have the flexibility of being able to designate which device categories within the Device Group will page a particular technician.

To Email a Technician-Based on a Device Group:



**NOTICE:**

---

For information on creating and moving/assigning devices using the Tree Viewer, see the AlphaXD User's Manual (Alpha p/n 035-512-B0-001). Device Groups should be used from custom view trees.

1. From the View Editing panel in the Tree Viewer, create a custom view tree.
2. From the View Editing panel in the Tree Viewer, create a device with a Device Group type in the Native tree view.
3. Copy the Device Group from the Native view tree to the custom view tree.
4. Place devices into the Device Group by copying the devices from the Native view tree into the Device Group in the custom view tree. Refer to the Tree Viewer chapter in this manual for information on creating trees, creating elements and moving/copying devices to and from trees.
5. At this point, the Device Group exists and it has devices assigned to it. Assign the Device Group to one or more technicians. From the Administration page in the AlphaXD Administration panel, click the Page Alert icon.
6. Select a technician name from the Master List and click the Edit button.
7. In the Technician Information window, click on the Category/Group Setup tab.
8. Highlight one or more devices in the Categories window. Click the right-facing arrow to add the device(s) into the Selected Categories window. If removing a device, highlight one or more devices in the Selected Categories window and click the left-facing arrow to move the device(s) into the Categories window. The devices in the Selected Categories window will be the only devices within the selected Device Groups that will send pages to this technician.
9. Highlight one or more Device Group names in the Groups window. Click the right-facing arrow to add the group(s) into the Selected Groups window. If removing a group, highlight one or more groups in the Selected Groups window and click the left-facing arrow to move the group(s) into the Groups window.
10. If some of the devices had been overlooked during the configuration process or possibly added after this phase of the process, it's possible that some of the device's emailing may get overlooked. To ensure that all device emailing is accounted for, activate the Selected Devices Not Assigned to a Group option by clicking on the checkbox next to the option. Any device not assigned to a group will send its pages to this technician.

# 11.0 Forwarding Notifications to Third-Party Applications

The SNMP Agent application provides AlphaXD with the capability to forward alerts to one or more third party applications that can accept SNMP traps. The SNMP Agent is a separate application that requires the appropriate software license. For more information on obtaining an SNMP Agent license, please contact an Alpha sales representative.

The format of the SNMP trap messages are defined by data contained in MIB files that are stored on the AlphaXD server. The MIB files are not necessary for third party applications but can be referenced if desired. The following example provides the default installation location for the MIB files. Be certain to substitute the appropriate drive letter in the Drive portion in the following example.

C:\AlphaXD\mibs

AlphaXD provided the operator the ability to filter traps being forwarded to the third party application. Refer to Section 6.5, Alert Filtering and Suppression, for details on how to use the filtering feature.

## 11.1 Editing the AlphaXD Trap Forwarding Table

The trap forwarding table is an Extensible Markup Language (XML) file called V1V2 Trap Forwarding Table.xml. This file specifies the host IP addresses on the network that will receive trap messages. Alpha recommends making a backup of the default file before making edits to the file.

To edit the AlphaXD Trap Forwarding table:

1. On the AlphaXD server, navigate to the location of the V1V2TrapForwardingTable.xml file. The following examples list the default installation locations for the Windows and Solaris systems.
2. Open the file V1V2TrapForwardingTable.xml in a text editor. The file contains the following default data:

Windows: C:\CheetahXD\conf\jmx\_agent\conf

Solaris: /opt/CheetahXD/conf/jmx\_agent/conf

3. Change the value of the "managerHost" entry to the IP address of the targeted northbound machine. If more than

```
<?xml version="1.0" encoding="UTF-8" ?>
<Table>
  <row>
    <column name="managerHost" value="127.0.0.1" />
    <column name="managerPort" value="8003" />
    <column name="version" value="2" />
    <column name="community" value="public" />
    <column name="timeOut" value="3200" />
    <column name="retries" value="0" />
    <column name="rowStatus" value="1" />
  </row>
</Table>
```

## 11.0 Forwarding Notifications to Third-Party Applications, continued

one machine will be receiving traps, duplicate a “row block” (i.e.; all of the data between and including the <row> </row>) for each additional machine, as shown in the following example. Edit each row block as appropriate for each machine.

4. Change the value of the “managerPort” entry to that of the targeted machine’s SNMP port number. This entry

```
<?xml version="1.0" encoding="UTF-8" ?>
<Table>
  <row>
    <column name="managerHost" value="10.3.65.24" />
    <column name="managerPort" value="162" />
    <column name="version" value="2" />
    <column name="community" value="public" />
    <column name="timeOut" value="3200" />
    <column name="retries" value="0" />
    <column name="rowStatus" value="1" />
  </row>
  <row>
    <column name="managerHost" value="10.3.65.45" />
    <column name="managerPort" value="162" />
    <column name="version" value="2" />
    <column name="community" value="public" />
    <column name="timeOut" value="3200" />
    <column name="retries" value="0" />
    <column name="rowStatus" value="1" />
  </row>
</Table>
```

must match the port number defined on the targeted machine for receiving SNMP traps (usually port 162).

5. The default values of the remaining entries are generally sufficient for most cases, but can be changed as desired for the environment. The following is a brief definition of each value.
  - version – SNMP protocol version (must be set to the value of 2)
  - community – SNMP trap community string
  - timeOut – SNMP timeout in seconds
  - retries – Number of times to retry when communications fail
  - rowStatus – The status of this conceptual row. Until all instances of all the corresponding columns are appropriately configured, the value of the corresponding instance of the usmUserStatus column is “notReady” or zero (0).

Once all of the edits have been made, save the file. Do not rename the file.



### **NOTICE:**

---

This file is read only once at startup. Anytime this file is changed AlphaXD must be restarted.

## 11.0 Forwarding Notifications to Third-Party Applications, continued

### 11.2 Trap Message Example

The trap notification OIDs, as of AlphaXD v3.2, match the actual MIB definitions. There is a variation in the OID sent based on a V1 or a V2 trap. In the AlphaXD implementation the specific trap notification OIDs for V1 traps are:

Enterprise OID: .1.3.6.1.4.1.2082.3.2.3.8.2

Generic Type: 6

Specific Type: 1 -

Clear Specific Type: 2

- Warning Specific Type:

3 -

Minor Specific Type: 4

- Major Specific Type: 5

- Critical

For V2 traps are:

Trap OID: .1.3.6.1.4.1.2082.3.2.3.8.2.1 -

Clear Trap OID: .1.3.6.1.4.1.2082.3.2.3.8.2.2

- Warning Trap OID:

.1.3.6.1.4.1.2082.3.2.3.8.2.3 -

Minor Trap OID: .1.3.6.1.4.1.2082.3.2.3.8.2.4

- Major Trap OID:

.1.3.6.1.4.1.2082.3.2.3.8.2.5 -

Critical

For Notification Traps:

.1.3.6.1.4.1.2082.3.2.2.14.2.1.1 moEnrolNotification

.1.3.6.1.4.1.2082.3.2.2.14.2.2.2 moDeenrolNotification

.1.3.6.1.4.1.2082.3.2.2.14.2.3.3 moAttrChangeNotification

The specific varbinds for each trap are defined in the MIB properties for the trap notification prefix.

## 11.0 Forwarding Notifications to Third-Party Applications, continued

Below is an example of a typical trap message that will be forwarded. It provides a reference as to the type of bindings available for use with third-party applications.

```
Manager Address: 10.1.37.18 Port: 0
Community: public
Bindings (10)
    Binding #1: sysUpTime.0 *** (timeticks) 0 days
    00h:06m:17s.02th Binding #2: snmpTrapOID.0 *** (oid)
alertMajorNotification Binding #3: sequenceNum ***
(gauge32) 76
Binding #4: alertentity *** (octets)
DOCSIS_00269709c73d_Power_Supply_3:psTotalStringVoltage
[44.4F.43.53.49.53.5F.30.30.32.36.39.37.30.39.63.37.33.64.5F.50.6F.77.65.72.5F.53.
75.70.70.6C.79.5F.33.3A.70.73.54.6F.74.61.6C.53.74.72.69.6E.67.56.6F.6C.74. ...
Binding #5: alertownerName *** (octets) (zero-length) [
(hex)] Binding #6: alertDescription *** (octets) DOCSIS XM2
00269709c73d
Power Supply 3: Current Value = 58.00
Binding #7: alertTimeStamp *** (gauge32) 3227678312
Binding #8: alertNotificationId *** (int32) 252886
Binding #9: alertcategory *** (octets) Power Supply
[50.6F.77.65.72.20.53.75.70.70.6C.79 (hex)]
Binding #10: alertExtraProperties *** (octets)
GatewayDeviceName=DOCSIS XM2 00269709c73d,TopLevelDeviceName=DOCSIS XM2
00269709c73d Power Supply 3
[47.61.74.65.77.61.79.44.65.76.69.63.65.4E.61.6D.65.3D.44.4F.43.53.49.53.20.58.4D.
32.20.30.30.32.36.39. ...
```

## 11.3 Notification Formats

The AlphaXD SNMP Agent application forwards managed object notifications and alert notifications. These two types of notifications are discussed in more detail in the sections that follow.

### Managed Object Notifications

The three types of managed object notifications the SNMP Agent forwards on to other machines are listed below, along with a brief description of each type.

- moEnrolNotification – This notification is sent when an object has been discovered in a particular Management Domain.
- moDeenrolNotification – This notification is sent when an object has been deleted from a particular Management Domain.
- moAttrChangeNotification – This notification is sent when there is a change in the value of the Management Object.

## 11.0 Forwarding Notifications to Third-Party Applications, continued

### Alert Notifications

Alert notifications are synchronous messages sent from AlphaXD for various alarm severities. The five types of alert notifications are listed below, along with a brief description of each type.

- alertClearNotification – This notification states that one or more previous alerts have been cleared.
- alertWarningNotification – This notification states that an alert of severity “warning” has been raised on a Managed Object.
- alertMinorNotification – This notification states that an alert of severity “minor” has been raised on a Managed Object.
- alertMajorNotification – This notification states that an alert of severity “major” has been raised on a Managed Object.
- alertCriticalNotification – This notification states that an alert of severity “critical” has been raised on a Managed Object.

The following table lists the variable binding values and their descriptions that are used in the alert notification traps.

Variable Binding	
Variable Binding Number	Description
1	SysUpTime: This is the amount of time the SNMP Agent application has been running.
2	Notification type: This is the notification type (i.e., clear, warning, minor, major, or critical).
3	sequenceNum: Specifies the sequence number of the trap. This number starts from zero every time the SNMP Agent application is started.
4	alertEntity: This is a concatenation of the alarming device (Managed Object) followed by a colon (:), which is then followed by the name of the actual alarming parameter. Example: Managed Object Name:fnReturnLaserCurrent A managed object in the HFC domain may be a battery object, a power supply object or a transponder object.
5	alertOwnerName: Currently a value of Null (unused).
6	alertDescription: This defines the details of the alert message.
7	alertTimeStamp: Contains the time stamp of the time that this alert was modified.
8	alertNotificationId: This is a sequential ID number for each alert. AlphaXD stores this number.
9	alertCategory: Defines the category of the alert (i.e., power supply, fiber node, etc.).
10	alertExtraProperties: Contains the name value pair for the Gateway Parent and the TopLevel Parent of the managed object name in binding 4 (alertEntity). Please refer to Section 17.3.2.1 for details on the Gateway and Top Level Parent concepts.

**Table 11-1, Variable Binding**



# 12.0 Downloading Firmware

## 12.1 Downloading Generic Firmware

### Setup

1. Navigate to the AlphaXD installed directory.
2. Open the “backup” directory in the AlphaXD directory.
3. If it does not already exist, create a directory called “gx2FwFiles\genericFwFiles” in the “backup” directory.
4. Place all Firmware files in the genericFwFiles directory.



#### **NOTICE:**

---

- If the backup directory does not exist it will need to be created with the directory name “backup”.
  - If using a different TFTP server, the files must be in a genericFwFiles directory from the root of the TFTP server directory. The files also must exist in the AlphaXD genericFwFiles folder so they appear in the Firmware File list of the Generic Firmware Download page.
  - Ignore steps 5-10 if another TFTP Server is already configured. Copy the generic Firmware files to the default TFTP directory.
5. If running, shut down the AlphaXD server.
  6. Navigate to the “conf” directory in the AlphaXD installed directory.
  7. Open the file titled “NmsProcessesBE.conf” with a text editor.
  8. Remove the “#” from in front of the following lines to activate the TFTP process and to set the path of the generic firmware files.

```
PROCESS      com.adventnet.nms.tftp.NmsTftpServer
```

```
ARGS         TFTP_ROOT_DIRECTORY /AlphaXD/backup/gx2FwFiles/
```

- For example, In a Windows environment if the install path for AlphaXD is C:\Program Files\ then the path would display the following:

```
Program Files/AlphaXD/backup/gx2FwFiles/
```

- In a Unix environment if the install path for AlphaXD is /export/home then the path would display the following:

```
/export/home/AlphaXD/backup/gx2FwFiles/
```

9. Save the altered NmsProcessesBE.conf file.
10. Restart AlphaXD.

### Downloading Generic Firmware to One Device

1. Right click on the individual device to which the new firmware will be downloaded to and select **Download**, and then **Download Generic Firmware**.
2. When the Generic FW Download Page appears select the **Module Name** and the corresponding firmware file to be downloaded to the device.



---

**NOTICE:**

The Module Name section lists the devices or modules that will accept firmware downloads through AlphaXD and the Firmware File sections lists the files that have been placed in the genericFwFiles directory.

3. If an external TFTP server is used, enter the **IP address** of the external TFTP server in the **TFTP Server IP Address** field.
4. Click the **Download FW** button to begin the download.

After the **Download FW** button is clicked the Bulk Task Status page will appear. This page displays the firmware download progress. For more information on the Bulk Task Status page see the section titled, "Bulk Task Status". When the firmware download is complete it will be moved from the "Active Bulk Tasks" section of the page to the "Completed Bulk Tasks" section of the page.

### Downloading Generic Firmware to Multiple Devices

1. Select the desired devices for firmware download.
2. Right click on any of the selected devices and select **Download** and then **Download Generic Firmware**.
3. Repeat steps 2-4 of the section titled, "Downloading Generic Firmware to One Device".

### 12.2 Downloading to Motorola GX-2 Chassis Modules

1. If running, shutdown the AlphaXD server.
2. Navigate to the AlphaXD installed directory.
3. Open the “backup” directory in the AlphaXD directory.
4. Create a directory called “gx2FwFiles” in the “backup” directory.

**NOTICE:**

---

If the backup directory does not exist it will need to be created with the directory name “backup”.

5. Place all GX-2 Firmware files in the gx2FwFiles directory.
6. Navigate to the “conf” directory in the AlphaXD installed directory.
7. Open the file titled “NmsProcessesBE.conf” with a text editor.
8. Remove the “#” from in front of the following lines to activate the TFTP process and to set the path of the GX2 firmware files.

```
PROCESS      com.adventnet.nms.tftp.NmsTftpServer
```

```
ARGS         TFTP_ROOT_DIRECTORY /AlphaXD/backup/gx2FwFiles/
```

- For example, In a Windows environment if the install path for AlphaXD is C:\Program Files\ then the path would display the following:

```
Program Files/AlphaXD/backup/gx2FwFiles/
```

- In a Unix environment if the install path for AlphaXD is /export/home then the path would display the following:

```
/export/home/AlphaXD/backup/gx2FwFiles/
```

9. Save the altered NmsProcessesBE.conf file.
10. Restart AlphaXD.
11. Connect to the Server with a Web browser and navigate to a tree view where the GX-2 Chassis('s) are displayed.
12. Right click on the GX-2 chassis icon in the tree and select “Device Configuration”.
13. When the Device Configuration page opens click on the “Misc” tab.
14. When the page changes, find the Control Module and click the “+” to expand the options (The Control Module will be the only module with a “+” next to the icon).
15. Enter the IP address of the AlphaXD server in the TFTP Server text box.
16. Click the Save and Download button.

**NOTICE:**

---

If a TFTP Server IP address already exists in the GX-2 Control module, it will be overwritten if the Save and Download button are clicked.

17. Repeat Steps 12-15 for each additional GX-2 Chassis which will require new firmware updates.

## 12.0 Downloading Firmware, continued

### Downloading GX-2 Module Firmware to One Module

1. Right click on the individual GX-2 module to which the new firmware will be downloaded to and select “Download”, and then “Download GX2 Firmware”.
2. When the GX2 FW Download Page appears select the firmware file to be downloaded to the module.

 **NOTICE:**

---

If a firmware file(s) cannot be identified for the specific module type selected, all available firmware files will appear.

3. If it is desired to download firmware to the module’s inactive image but to continue operating on the current active image after the download operation has completed, select the “No Reset” radio button. If it is desired to download firmware to the module and to switch to the image that was downloaded after the download operation has completed, select the “Reset Module” radio button.
4. Click the “Download GX2 FW” button to begin the download.

After the “Download GX2 FW” button is clicked the Bulk Task Status page will appear. This page displays the firmware download progress. For more information on the Bulk Task Status page see the section titled, “Bulk Task Status”. When the firmware download is complete it will be moved from the “Active Bulk Tasks” section of the page to the “Completed Bulk Tasks” section of the page.

 **NOTICE:**

---


There is a timeout value of 15 minutes for the TFTP file transfer and a timeout value of 30 minutes for the firmware download to the module.

### Downloading GX-2 Module Firmware to Multiple Modules

Although multiple modules can be selected for the firmware download only one module is downloaded at a time. Once a module has been downloaded the next module in the Bulk Task List is then downloaded.

This continues until all selected modules of the same type have been downloaded.

1. Select the desired modules for firmware download.
2. Right click on any of the selected GX-2 modules and select “Download” and then “Download GX2 Firmware”.
3. Repeat steps 2-4 of the section titled, “Downloading GX-2 Module Firmware to One Module”.

 **NOTICE:**

---

If different module types are selected, all firmware files that are compatible with any of the selected module types will appear on the GX2 FW Download Page. If this occurs, select the firmware file that corresponds with the module type.

## 12.0 Downloading Firmware, continued

### Downloading GX-2 Module Firmware to Like Modules (GX-2 Chassis)

Although multiple modules can be selected for the firmware download only one module is downloaded at a time. Once one module has been downloaded the next module in the Bulk Task List is then downloaded. This continues until all selected modules of the same type have been downloaded.

1. Select one or more GX-2 Chassis in the tree.
2. Right click on any of the selected GX-2 Chassis and select “Download” and then “Download GX2 FW Chassis”.
3. When the GX2 FW Download Page appears, select the firmware file with the modules desired for download.



---

**NOTICE:**

In the Download GX2 FW Chassis mode, all available firmware files will appear.

4. If it is desired to download firmware to the module’s inactive image but to continue operating on the current active image after the download operation has completed, select the “No Reset” radio button. If it is desired to download firmware to the module and to switch to the image that was downloaded after the download operation has completed, select the “Reset Module” radio button.
5. Click the “Download GX2 FW” button to begin the download. After clicking the “Download GX2 FW” button the “Bulk Task Status” page displays. This page displays the firmware download progress. For more information on the Bulk Task Status page, see the section titled, “Bulk Task Status”. When the firmware download is complete, it will be moved from the “Active Bulk Tasks” section of the page to the “Completed Bulk Tasks” section of the page.



---

**NOTICE:**

There is a timeout value of 15 minutes for the TFTP file transfer and a timeout value of 30 minutes for the firmware download to the module.

## Troubleshooting

### Events

Traps are sent from the GX2 Chassis that detail the progress and status of the GX2 Firmware Download process. These traps are turned into AlphaXD Events by the Fault Processing subsystem and can be tracked through the Event Tab of the Notifier Faults Viewer application. The events will show up in the Event tab with a “Severity” field value of “Info” and can be identified by the “Gateway Parent” field value matching the GX2 Chassis Display Name. The “Message” field value will give the specific detailed information associated with each Event.

### Download Log File

The download log information is stored in two files inZ: <INSTALL\_DIR>/logs

AlphaXD creates 2 log files of a user specified length (the default is 10,000 lines) and names them CTNetworkInventoryAPIBE<index>.txt and CTNIBulkTaskManager<index>.txt where <index> is the number 1.

Each log file is appended with entries up to a user-specified number of lines. When that maximum is reached, a new log file is created and named appropriately where <index> is the number 2, and so on.

AlphaXD creates a user-specified number of log files (the default is 10). When the maximum number of files is reached, AlphaXD deletes the oldest file before creating the new one.

# 13.0 AlphaXD Utilities

## 13.1 Send Event

The Send Event utility is a way to:

- Populate the Custom Extensions menu
- Test the Notifier

The Send Event utility can also be accessed in the Administration tab page of AlphaXD.


Send an Event:

1. In the AlphaXD Administration section of the Administration tab page, click Send Event. The Send Event Utility opens.
2. Create the type of event to send through the AlphaXD system by specifying the following:
  - Severity – Click the drop-down menu and select the desired severity.
  - Source – Type the source name of the device from which the event will be sent.
  - Attribute – Select the device’s managed attribute generating this test event.
  - Application Category – Currently, only events from HFC devices are supported.
  - Device Category – Specify the type of device (power supply, fiber node, etc).
  - Message Text – Type a text message regarding the event.
  - Group Name – This text field is currently not used by AlphaXD.
  - Top-Level Parent – Type the IP address of the device’s top-level parent device, which reports to the transponder (example, for the temperature attribute of a battery, the top-level parent is the power supply).
  - Gateway Parent – Type the IP address of the transponder monitoring the device.
  - Alarming Attachment – Type the display name of the attribute triggering the alarm.
  - Entity – Type the unique alarm ID (default convention is managed object name:attribute name).
  - Repetitions – Type the number of times the event will be sent.
  - Interval – Type the number of milliseconds to wait between each send operation.
  - Alternate Severity – If yes, the Send Event operation will send both an alarm event and a clear event.
  - Increment Resource Name – If yes, when sending multiple repetitions, AlphaXD will display a serialized entry for each unique send in the form of: managed object name\_n where n is 1 for the first event send, 2 for the second event send, and so on.

**SendEvent Utility**

Severity	1 - Critical	
Source		(*)
Attribute		(*)
Application Category	HFC	(*)
Device Category		(*)
Message Text		
Group Name		
Top-Level Parent		
Gateway Parent		
Alarming Attachment		
Entity		
Repetitions	1	
Interval	0	
Alternate Severity	No	
Increment Resource Name	No	

**Fig. 13-1, Send Event Utility Page**

 **NOTICE:**  
Items marked with an asterisk (\*) in the above image must match the device entries in the AlphaXD database.

## 13.2 Importing HFC Manager Events into AlphaXD

Alarms/events can be imported from a Motorola HFC Manager system. Depending on date and time, the HFC Manager events will either be imported directly into the AlphaXD database or exported out to Comma Separated Values (CSV) files. If the events are exported to CSV files, they can always be viewed from within AlphaXD Notifier by applying a time filter for the time span desired. Then the CSV files can be imported. For more on creating filters in Notifier see the section titled, "Faults" in the User's Guide.

Prior to importing the HFC Manager Events into AlphaXD, the MySQL database on the HFC Manager server must be configured to allow remote access from the AlphaXD server. Log into the Windows HFC Manager Server, and open a terminal (cmd) window. Set the default directory to the location that contains the MySQL executables and enter the MySQL database as the root user.

```
C:> cd c:\HFCMgr\mysql\bin>mysql -u root
```

Then enter the following commands:

1. mysql>update mysql.db set Host='% ' where Db='webnmsdb';
2. mysql>update mysql.user set Host='% ' where user='root';
3. mysql>GRANT ALL ON WebNmsDb.\* TO root@'% ' IDENTIFIED BY "";
4. mysql>FLUSH PRIVILEGES;
5. mysql>exit

### Procedure for Windows

From the AlphaXD Server, open a Command Prompt window and navigate to the AlphaXD\bin directory (as shown below) to enter the command: "migrateHfcMgrUtil"



```
C:\AlphaXD\bin>migrateHfcMgrUtil
#####
AlphaXD : Motorola HFC Mgr Migration Utility
#####

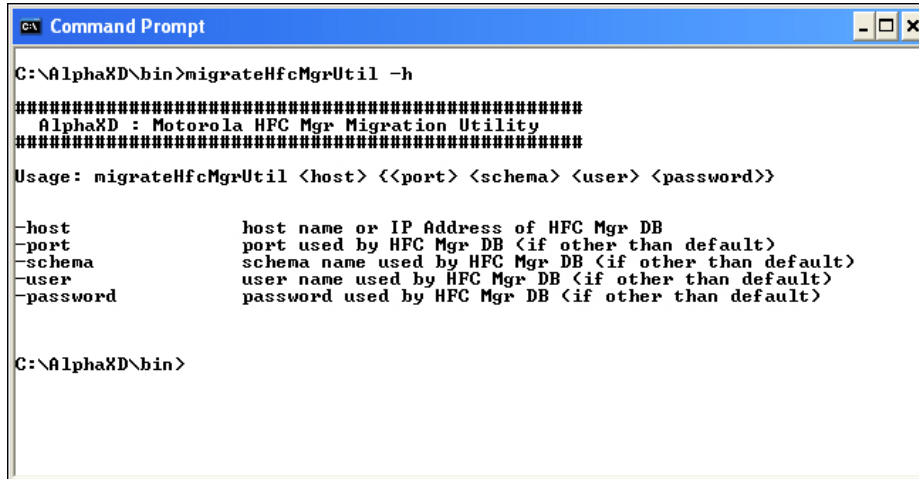
Valid Host/IP Address required as first option.
Use option: -host hfcMgrServer <or> -host 10.1.2.3
            -h to show help.

C:\AlphaXD\bin>_
```

Fig. 13-2, HFC Migration Utility

### 13.0 AlphaXD Utilities, continued

To display more detailed help with descriptions of available arguments, enter the command: “migrateHfcMgrUtil -h”



```
Command Prompt
C:\AlphaXD\bin>migrateHfcMgrUtil -h
#####
AlphaXD : Motorola HFC Mgr Migration Utility
#####
Usage: migrateHfcMgrUtil <host> <<port> <schema> <user> <password>>

-host          host name or IP Address of HFC Mgr DB
-port          port used by HFC Mgr DB <if other than default>
-schema        schema name used by HFC Mgr DB <if other than default>
-user          user name used by HFC Mgr DB <if other than default>
-password      password used by HFC Mgr DB <if other than default>

C:\AlphaXD\bin>
```

Fig. 13-3, HFC Migration Utility – Detailed Help with Descriptions

To begin the HFC Mgr Migration using the HFC Mgr defaults (port, schema, user, password) enter the following command: “migrateHfcMgrUtil -host <host>”, where <host> is the host name or IP address of the HFC Mgr database.

 **NOTICE:**

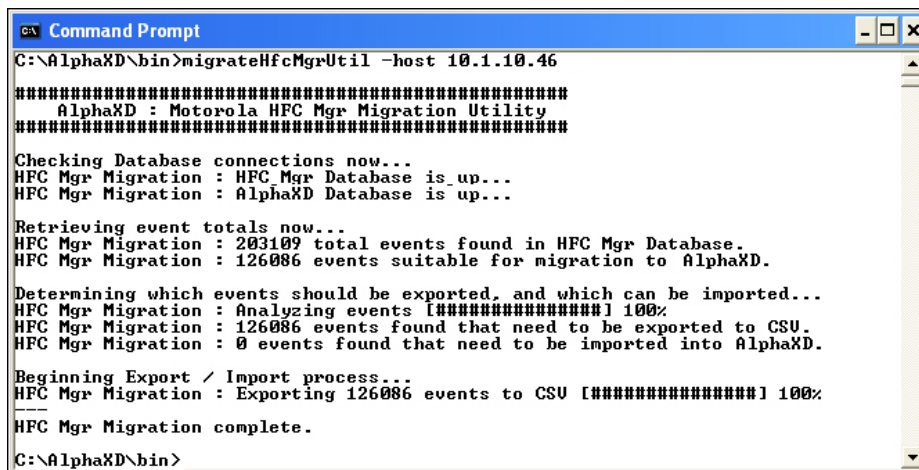
If not using HFC Mgr defaults, those values will need to be passed in as arguments.

“migrateHfcMgrUtil -host <host> -port xxx -schema xxx -user xxx -password xxx”, where <host> is the host name or IP address of the HFC Mgr database and each xxx represents the non- default value that needs to be passed in.

After the migration has started, it will first verify both the HFC Mgr and AlphaXD Databases are accessible.

It will then display status for the events that need to be migrated and how many of the events will be either imported into AlphaXD or exported to CSV files.

Once the preliminary tasks are complete the actual migration will begin. Status indicators will display the progress of the migration until complete.



```
Command Prompt
C:\AlphaXD\bin>migrateHfcMgrUtil -host 10.1.10.46
#####
AlphaXD : Motorola HFC Mgr Migration Utility
#####
Checking Database connections now...
HFC Mgr Migration : HFC Mgr Database is up...
HFC Mgr Migration : AlphaXD Database is up...

Retrieving event totals now...
HFC Mgr Migration : 203109 total events found in HFC Mgr Database.
HFC Mgr Migration : 126086 events suitable for migration to AlphaXD.

Determining which events should be exported, and which can be imported...
HFC Mgr Migration : Analyzing events [#####] 100%
HFC Mgr Migration : 126086 events found that need to be exported to CSU.
HFC Mgr Migration : 0 events found that need to be imported into AlphaXD.

Beginning Export / Import process...
HFC Mgr Migration : Exporting 126086 events to CSU [#####] 100%
HFC Mgr Migration complete.

C:\AlphaXD\bin>
```

Fig. 13-4, HFC Mgr Migration Complete



### 13.0 AlphaXD Utilities, continued

All events that have been exported to CSV files will be found in c:\AlphaXD\backup\events.

A separate file will be created with all of the events for each day.

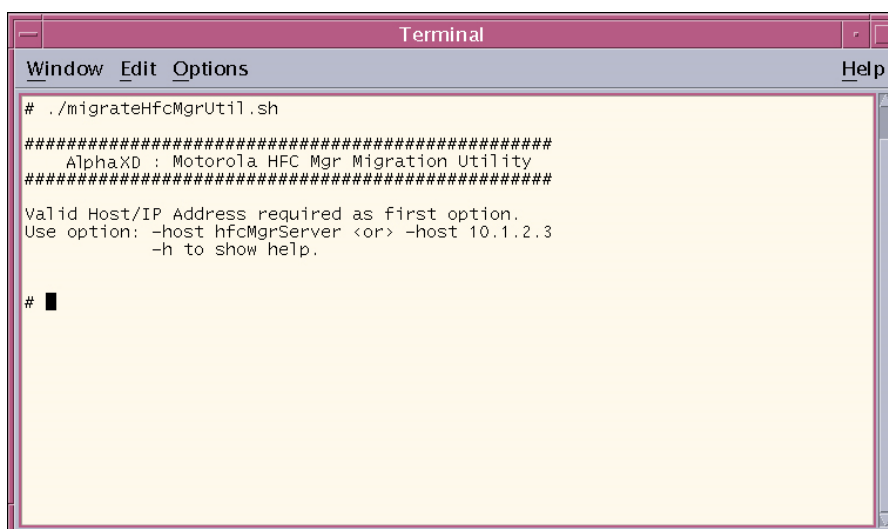
Events within CSV files can be viewed with a standard text editor or spreadsheet application that can recognize comma separated values (CSV) files.

They can also be viewed within AlphaXD Notifier by applying a Date and Time filter in the Events View. For more information on how to create filters in Notifier, please refer to the section titled “Faults” in the User’s Guide.

Once an HFC Manager device is discovered in AlphaXD, then those imported events associated with that device will now be visible for it.

### Procedure for Unix

From the AlphaXD Server, open a Terminal window and navigate to the AlphaXD/bin directory (as shown below) to enter the command: “./migrateHfcMgrUtil.sh”



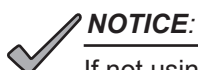
```
Terminal
Window Edit Options Help
# ./migrateHfcMgrUtil.sh
#####
AlphaXD : Motorola HFC Mgr Migration Utility
#####
Valid Host/IP Address required as first option.
Use option: -host hfcMgrServer <or> -host 10.1.2.3
            -h to show help.
# █
```

Fig. 13-5, HFC Migration Utility on UNIX

To display more detailed help with descriptions of available arguments, enter the command: “./migrateHfcMgrUtil.sh -h”

To begin the HFC Mgr Migration using the HFC Mgr defaults (port, schema, user, password) enter the following command: “./migrateHfcMgrUtil.sh -host <host>”, where <host> is the host name or IP address of the HFC Mgr database.

“migrateHfcMgrUtil.sh -host <host> -port xxx -schema xxx -user xxx -password xxx”, where <host> is the host name or IP address of the HFC Mgr database and each xxx represents the non- default value that needs to be passed in.



**NOTICE:**

If not using HFC Mgr defaults, those values will need to be passed in as arguments.

After the migration has started, it will first verify both the HFC Mgr and AlphaXD Databases are accessible. It will then display status for the events that need to be migrated, and how many of the events will be either imported into AlphaXD or exported to CSV files.

### 13.0 AlphaXD Utilities, continued

Once the preliminary tasks are complete the actual migration will begin. Status indicators will display the progress.

```

Terminal
Window Edit Options Help
# ./migrateHfcMgrUtil.sh -host 10.1.10.46
#####
AlphaXD : Motorola HFC Mgr Migration Utility
#####

Checking Database connections now...
HFC Mgr Migration : HFC Mgr Database is up...
HFC Mgr Migration : AlphaXD Database is up...

Retrieving event totals now...
HFC Mgr Migration : 203109 total events found in HFC Mgr Database.
HFC Mgr Migration : 126086 events suitable for migration to AlphaXD.

Determining which events should be exported, and which can be imported...
HFC Mgr Migration : Analyzing events [#####] 100%
HFC Mgr Migration : 126086 events found that need to be exported to CSV.
HFC Mgr Migration : 0 events found that need to be imported into AlphaXD.

Beginning Export / Import process...
HFC Mgr Migration : Exporting 126086 events to CSV [#####] 100%
--
HFC Mgr Migration complete.
#
    
```

**Fig. 13-6, Migration Complete on UNIX**

All events that have been exported to CSV files will be found in AlphaXD/backup/events. A separate file will be created with all of the events for each day. Events within CSV files can be viewed with a standard text editor or spreadsheet application that can recognize comma separated values (CSV) files. They can also be viewed within AlphaXD Notifier by applying a Date and Time filter in the Events View. For more information on how to create filters in Notifier, please refer to the section titled, “Faults” in the User’s Guide. Once an HFC Manager device is discovered in AlphaXD, then those imported events associated with that device will now be visible for it.

The following table displays how the HFC Manager fields are mapped to AlphaXD fields.

HFC Manager Field → AlphaXD Field	
HFC Manager Field	AlphaXD Field
Time	Created / Modified
Severity	Severity
Source	Source
failureObject	Attribute
Entity	Entity (Source + failureObject from HFC Mgr)
DeviceType	DeviceCategory
Text	Message
Node	Node
DeviceName	Userfield1
ModelNumber	Userfield2
SerialNumber	Userfield3
ChangedValue	Userfield4
TrapIdentifier	Userfield5
Card	Userfield6
Port	Userfield7

**Table 13-1, HFC Manager Field / AlphaXD Field**

### 13.3 Multiple Device/AlarmDynamic Mapping and Route Calculation

AlphaXD allows operators to identify and graph alarm clusters from Tree Views and Notifier by selecting elements which in turn visually depict alarming devices on a street map. This graphical functionality provides a view of the offending devices allowing users to quickly ascertain if a system problem is concentrated in a specific node or is more widespread. With the alarming devices depicted on a map, this new mapping functionality will calculate, for the Field Engineer, optimized street routes from a default Headend starting point through multiple device locations. This feature provides the most benefit for customers who have accurate depictions of their network topology within custom Tree Views. With a proper topology, all devices located under a single Region or Hub can be populated on a map from a single object in the tree.

The Google Maps API has been integrated for this feature. Google Maps requires the operator to purchase a Right-To-Use License from Google Inc.

To Activate/Update Mapping Software:



#### **NOTICE:**

---

The AlphaXD server will require TCP port 80 access to [www.google.com](http://www.google.com) to utilize some advanced features associated with the mapping tools.

1. Navigate to AlphaXD\_HOME\html\.
2. Open the EnglishToNative.properties file in a text editor
3. Search for the following string - Mapping messages and defaults. It is located near the bottom of the file.
4. Uncomment the line item to activate the target mapping application.
5. The EnglishToNative.properties file also allows for a default location to be set. To change the default location edit

```
#  
  
# Mapping messages and defaults  
  
#  
  
geomap_provider=Google
```

the “geomap\_headendLatLng=” line to reflect the latitude and longitude of the default starting location:

```
#default headend lat/lng is Pittsburgh  
  
geomap_headendLatLng=(40.44,-80.0)  
  
geomap_defaultZoom=11  
  
geomap_selectRoutePoints=Select Route Points:  
  
geomap_ctrlClick=(Ctrl-Click for multiple selection)  
  
geomap_quickestRoute=Quickest Route  
  
geomap_clearRoute=Clear Route
```

### 13.0 AlphaXD Utilities, continued

Use the Alert Mapping Feature:

Each device must have a valid address populated in the Location field found on the Property Tab. The format of the information required should be the following:

- Requires either a valid street address or Latitude/Longitude values
- Format
  - 381 Mansfield Ave, Pittsburgh PA 15220
  - Or
  - (40.421224, -80.052655)



**NOTICE:**

When using an address, include complete address information. Incomplete information can result in an incorrect location.

If a Lat/Lng encoding does not exist for a given device, the MapAp will automatically use the Geocoding Service to generate a Lat/Lng encoding from a valid street address and append it to the end of the Location field.

If an address is incorrectly entered or is unrecognizable, the display on the map will default to the headend location defined in geomap\_headendLatLng= Default Location.

To map devices or alarms, select one or more devices from the Tree View, Network Inventory or Template Admin, Notifier, or POM and then select Map Location (“Map Alert” in Notifier/POM) from the right-click local context menu.

Within Tree Viewer, Network Inventory or Template Admin a Region, Headend, Hub or Group object can be selected to perform a “Map Branch” from the local context menu. This will map all devices within the targeted branch.



Fig. 13-7, Map Alert from Notifier – Menu Option

### 13.0 AlphaXD Utilities, continued

When the map is launched it will display each of the selected devices in their geographic locations, represented by an alarm icon colored with the highest alarm severity currently associated with the device. Hovering the mouse over the icon will bring up a popup box that contains the display name and IP address of the device. Clicking on the icon will display a popup box that contains the device type icon, display name, IP address, and street address.

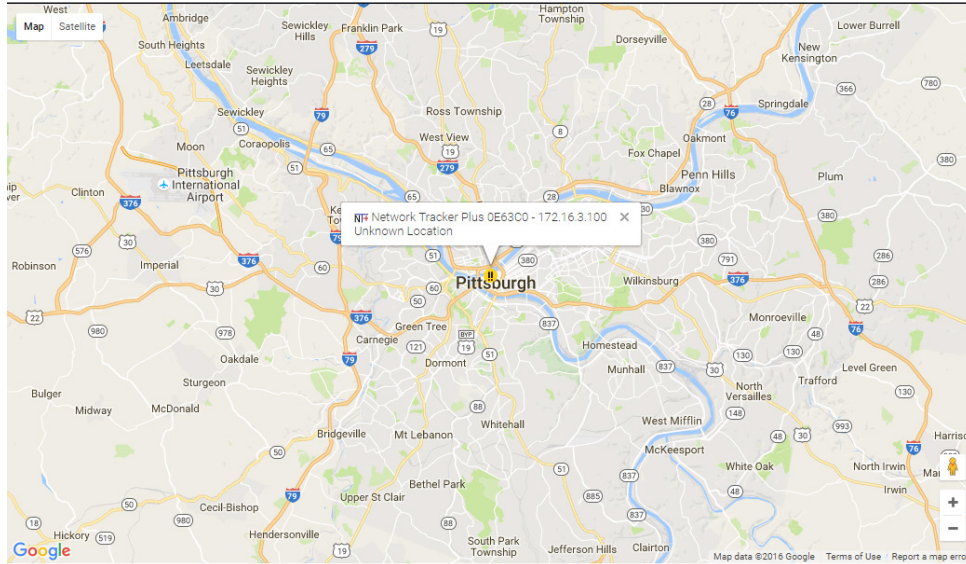


Fig. 13-8, Location Map

To the right of the map is a scrollable selection box that contains the display names of all the devices currently mapped. If the user selects one or more of the devices and clicks on “Quickest Route”, the page will show the quickest route from the default Headend Lat/Lng through all of the selected devices. “Clear Route” will clear the route and display the original map.

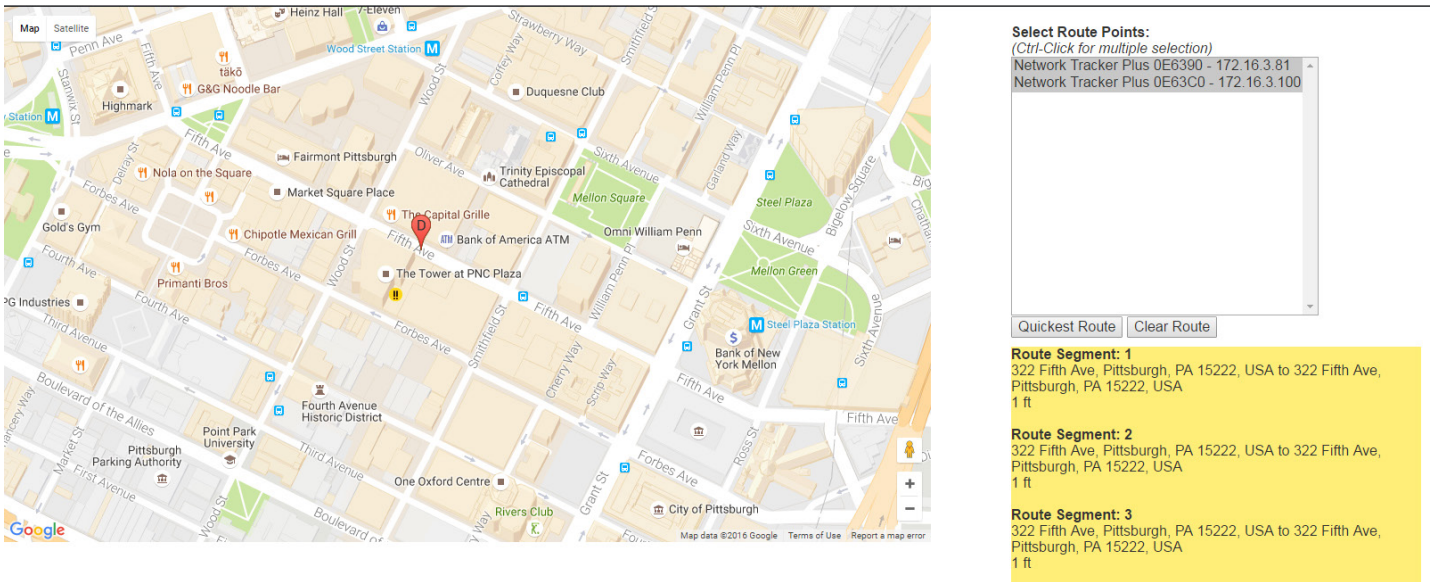


Fig. 13-9, Map with Routes



# 14.0 QAM Constellation Display

The QAM constellation display is useful in diagnosing line problems that might otherwise go undiagnosed. This chapter outlines how to access AlphaXD's QAM application and provides useful information on how to interpret the information presented in the QAM display.

**NOTICE:**

A DOCSIS 2.0 transponder will only display the constellation of the downstream QAM of the tuned DOCSIS downstream communications channel. The Network Tracker Plus can select from any downstream QAM channel defined in its channel plan.

## 14.1 The QAM Constellation Interface

The QAM Constellation Interface is a licensed application that consists of a panel of variables and settings on the left portion of the screen and the constellation map itself. The interface is accessed via the tree menu. At the device level, the QAM functionality is only supported by Alpha products that are based on the eCMM technology.

Access the QAM Interface:

1. Select a device from a tree view by highlighting the device.
2. Right-click on the device and select QAM Constellation from the menu. The menu option will display only if the application has been properly licensed for the AlphaXD system.

### QAM Constellation

Device Details

Name	Network Tracker Plus 0E6390
IP Address	172.16.3.81
MAC Address	00 26 97 0e 63 90

Configuration Settings

QAM Collection Interval	3 seconds
QAM Retention Count	10 samples
CER Refresh Interval	10 seconds
Zoom Level	1 point
Channel	Downstream
Suspend Collection	<input type="checkbox"/>

Downstream (256 QAM) **QAM locked**

Frequency	801.00 MHz (CMTS ch. 2)
Power	0.5 dBmV

Upstream

Frequency	32.00 MHz (CMTS ch. 3)
Power	37.8 dBmV

Downstream Signal Quality

Rx MER	40.3 dB / 39.2 dB
EVM	0.5 % / 0.7 %
Possible Impairments	Signal Quality Unknown

Codeword Error Rate **FEC locked**

	Pre-FEC	Post-FEC
Long Term	18.9E-6	12.2E-6
Short Term (Current)	0.000e+00	0.000e+00
Short Term (Previous)	0.000e+00	0.000e+00

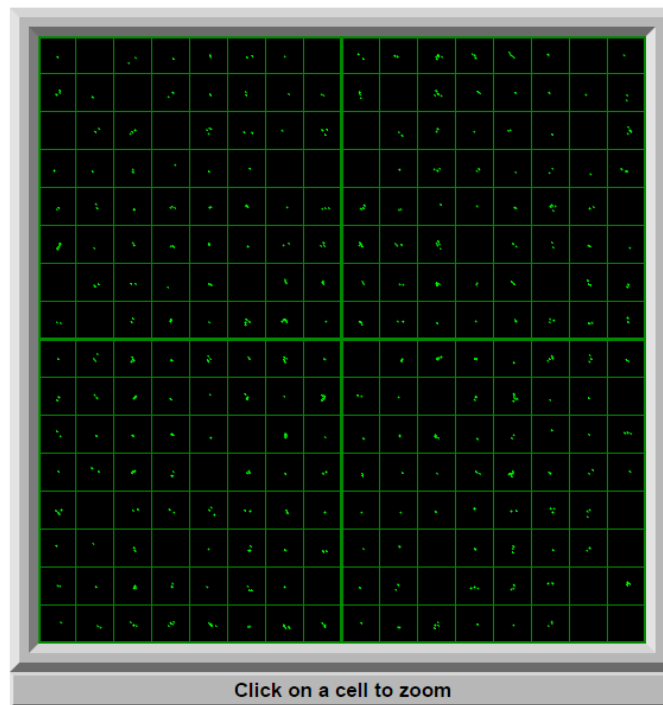


Fig. 14-1, QAM Constellation Interface

### 14.2 QAM Interface Variables and Parameters

#### Device Details

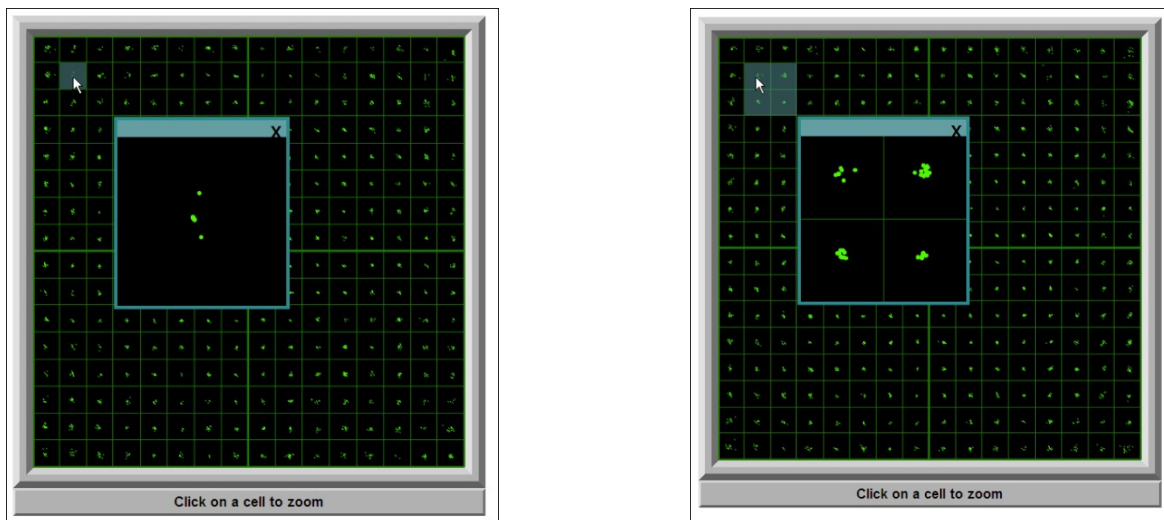
The device details supply the information necessary for identifying the device.

- Name – Device name.
- IP Address – IP address of the device performing the test.
- MAC Address – Media Access Control (MAC) address of the device performing the test.

#### Configuration Settings

The configuration settings are used to adjust certain aspects of the testing and data display.

- QAM Collection Interval – The interval at which the device will collect data. Select a value from the drop-down list, from 1 to 12 seconds.
- QAM Retention Count – Number of samples the map will retain before refreshing the data in the map. The user has the option of choosing 5, 10, 15, or 20 samples from the drop-down list.
- CER Refresh Interval – Enter the Codeword Error Rate (CER) refresh rate. This value (given in seconds) is used to provide signal quality data (long-term and short-term CER data) that is supplementary to the actual QAM data on the QAM Constellation page. Ideally, the CER refresh rate should be a whole multiple of the Constellation Refresh Rate, but is not required. The user has the option of choosing values of 10 to 60 seconds in 10 second intervals from the drop-down list.
- Zoom Level – Examine data more closely in the constellation map by clicking on individual quadrants in the map to magnify the data. This variable determines the extent to which the user can magnify the data. A zoom level of 1 allows the user to concentrate on a single quadrant, while a level of 4 will present the chosen quadrant and three adjacent quadrants. Please refer to the figures that follow.



**Fig. 14-2, Zoom Level of 1 (Left) and Zoom Level of 4 (Right)**

- Suspend Collection – Check this box to suspend sampling and uncheck to resume sampling.

## 14.0 QAM Constellation Map, continued

### Downstream (256 QAM) Frequency and Power

- Frequency – Downstream frequency in MHz.
- Power – Downstream power in dBmV.

### Upstream Frequency and Power

- Frequency – Upstream frequency MHz.
- Power – Upstream power dBmV.

### Downstream Signal Quality

- RxMER – Downstream signal quality. Modulation Error Ratio (SNR); hw/sw: ok 31-40; good 40 and higher. Also, the background color of this field reflects the range of the value. When the range is within acceptable values the field background is white; for marginal values the background is yellow; for an unacceptable value range the background is red.
- EVM – Downstream signal quality. Error Vector Magnitude (from hardware MER / software MER).

### Codeword Error Rate

- Long Term Pre-FEC – Downstream Signal Quality. Codeword error rate (CER) BEFORE forward error correction is applied.
- Long Term Post-FEC – Downstream Signal Quality. Codeword error rate (CER) AFTER forward error correction is applied. Should be  $< 9 \times 10^{-7}$ . Also, the background color of this field reflects the range of the value. When the range is within acceptable values the field background is white; for marginal values the background is yellow.
- Short Term (Current) Pre-FEC – Downstream Signal Quality. Codeword error rate (CER) BEFORE forward error correction is applied.
- Short Term (Current) Post-FEC – Downstream Signal Quality. Codeword error rate (CER) AFTER forward error correction is applied. Should be  $< 9 \times 10^{-7}$ . Also, the background color of this field reflects the range of the value. When the range is within acceptable values the field background is white; for marginal values the background is yellow.
- Short Term (Previous) Pre-FEC – Downstream Signal Quality. Codeword error rate (CER) BEFORE forward error correction is applied.
- Short Term (Previous) Post-FEC – Downstream Signal Quality. Codeword error rate (CER) AFTER forward error correction is applied. Should be  $< 9 \times 10^{-7}$ . Also, the background color of this field reflects the range of the value. When the range is within acceptable values the field background is white; for marginal values the background is yellow.



### 14.3 Interpreting QAM Constellation Map Data by Visual Inspection

The usefulness of the QAM constellation comes in the ability to recognize common shapes and responses within the display (individually by cell and the entire display as a whole). Examples of the data shown in the table below are illustrated in the figures that follow.






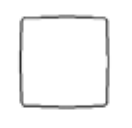


QAM Constellation Map Data			
Shape	Focus	Impairment	Description
	Individual cells and entire QAM constellation	Normal	Dots are centered in the individual QAM quadrants. The QAM constellation has a uniform square shape.
	Individual cells	Low CNR and/or Low MER	Individual cells of QAM constellation contain a fuzzy and diffused pattern.
	Individual cells	Coherent Interference	Individual cells of QAM constellation contain diffused hollow circles or “doughnuts”. This indicates an interfering carrier and shows the effect of not allowing the carrier to ever reach the proper point in the target range.
	Individual cells	Gaussian Noise	Individual cells contain a complete and fairly uniform smear up to all decision boundaries, and is usually caused by improper system setup, too many amplifiers in a cascade, damaged/ overheated hardware, and/or low power.
	Entire QAM constellation	Phase Noise	QAM constellation consists of smeared, concentric, circular patterns.
	Entire QAM constellation	Gain Compression	QAM constellation looks uniformly square, but the outside corners appear to be “smashed” toward center of grid (compression in the RF plant).
	Entire QAM constellation	I-Q Imbalance in the Modulator	Overall appearance of QAM constellation is rectangular rather than the desired square shape (square inequality).
	Entire QAM constellation	Quadrature Distortion	Overall appearance of QAM constellation has a twisted or skewed parallelogram shape.

Table 14-1, QAM Constellation Map Data

# 15.0 System Recommendations and Troubleshooting

## 15.1 New AlphaXD Installations

The details in this section are provided to help ensure a trouble-free new AlphaXD installation.

### Configuring AlphaXD to Discover DOCSIS-Based Elements

This section assumes that all of the DOCSIS-based devices in the system have been configured to forward their traps to the AlphaXD server and that all of the other configuration parameters have been set up correctly.

1. Using a client machine and a browser, log in to the AlphaXD machine. Perform the following actions:
  - Create groups
  - Apply scopes to the groups
  - Create users
  - Assign the users to the appropriate group(s) to grant them access to the various AlphaXD applications
2. From the AlphaXD Administration page, go to the Server Details menu and click on the Logs Configurator icon. This will enable Debug Logging for the following log files:
  - CTAuto-discovery
  - CTStatusPolling
  - Alert\_audit
  - CTTreeAPI
3. Autodiscovering devices: Alpha recommends discovering one device of each targeted device type and personality in the network, and set up the configuration thresholds for this device type based on the desired preferences. Discovery of a single device can be accomplished by configuring the seed file to discover just a single IP address or a narrow range of IP addresses.
4. Update the default templates and status poll interval parameters for the above discovered device type(s), based on preferences for limit thresholds.
5. When finished with the above configuration, run a manual backup of the system. Mark this as a baseline version and save this file.
6. Configure the seed file with the other desired IP addresses and/or network ranges for discovery, and (if desired) turn Auto-discovery ON in the seed file for sweep-based discoveries.

## 15.2 Fine-Tuning AlphaXD Parameters

Information on certain configuration files and parameters should be updated as the number and types of the devices managed by the AlphaXD system change over time. This will ensure optimal performance of the AlphaXD system.

### System Verification

- Periodically check the database backups. Verify that they have been set up and created correctly.
- Verify that the counts in the Network Inventory application match the number of devices deployed in the field and use the application to identify devices that are not provisioned or require downloads.
- Verify that the device counts are not reaching the licensed transponder counts to ensure newly deployed devices can still be discovered.
- Verify that the alert queue is staying clear by using the Fault Status link in the in the Administration tab.
- Run periodic reports such as the Alert Audit report, Provisioned transponder report, and Device Dead report. Save these reports for future comparisons.
- Create alert profiles that will serve as useful aids when performing bulk downloads to similar device types.
- Use tree views other than the native tree view, such as the HFC or custom tree views for everyday operation. The native view tree is typically very large and will require more time to search and refresh.
- Create custom trees and assign them to users, instead of granting users permission to access all of the trees in the AlphaXD system.
- Use the Fault Notifier's field selection, filtering, and layout capabilities to view preferred information.
- Periodically review and update the security permissions that have been assigned to various users and groups.

### Performance Tuning and Configuration

AlphaXD performs a background status poll on managed elements. A longer status poll interval implies a longer time to detect unit timeout and resynchronize any lost traps/alerts. On systems with a large number of devices, configuring the status poll interval with a small value (i.e., every 2 minutes) puts a heavy load on the CPU.

The following table displays the default status poll interval that is recommended, based on the number and type of the devices in the system. The table also recommends the optimal number of threads to configure. Apart from tuning the status poll interval parameter, there also exists the ability to define the number of threads (parallel processes).

STATUS POLL INTERVAL SETUP MATRIX (seconds)					
Number of Devices Polled	<1000	<3600	<7200	<10000	<15000
Thread Count*	3	6	7	8	8
Avg Dev / Thread	333	600	1028	1250	1875
Avg Dev polled/min	180	360	420	480	488
Avg Dev polled/min/thread	32	36	25	23	16
Minutes to complete Poll Cycle	6	10	18	21	31

**Table 15-1, Status Poll Interval Setup Matrix**

\* Thread count is set in AlphaXD\conf\threads.conf (STATUSPOLL)

\*\* Other changes may need to be made to NMSProcessBEconfiguration file variables based on device count, device type mix and network efficiency.

Use this information as a guideline. As the mix of device types in the system vary, the above parameters may need to be finely tuned to optimize the system. For additional information on updating the status poll interval on multiple devices simultaneously (i.e., in bulk), contact Alpha Technical Support.

## 15.3 AlphaXD Bandwidth Information

This information is meant to be used as a guideline as AlphaXD is implemented into a network.

### UI Load Up Time

UI Load Up Time		
Download Item	Size***	Download Time**
		Ethernet 100Mbps/sec
Login Screen [initial use]	250kb	2 sec
Notifier [initial use] (includes AdvenNet)	2.3MB (+1.9MB)	<.85 min
Notifier [subsequent use]	33KB	3 sec
Domain Options -> Open Native Tree- View	7.5KB	2 sec
Network Inventory	11KB	5 sec
Help Menu [initial use]	490KB	8 sec
Admin Menu [initial use]	53KB	2 sec
Add User Function	8KB	1 sec
System Setup Function [initial use]	16.1MB	<3 min

**Table 15-2, UI Load Up Time**

\*\* All numbers are approximate and subject to variances in network connection speed, other network traffic, and individual PC

\*\*\* Data size and transfer time measured using Net Limiter 2 Pro

\*\*\*\* Estimated

1. Trap-Based Traffic (for alarms):

- Each SNMP trap from the transponder to the AXD server is between 150 – 130 bytes. The total number of traps depends on the alarm limits and tolerances.
- If the limits are tight (narrow range) and the parameter values oscillate, one will get more alarms/clear traps compared to when the alarm limits are spread over a wider range. Proper use of dead band and alarm hysteresis can further reduce alarm chatter.
- Traps are one-way traffic events that flow from the transponder to the AXD server.

2. Synchronous Communication (Data Display & Scheduled Measurements):

- Data Display or Scheduled Measurements make an outgoing request from the AXD server to the transponder followed by a response from a transponder that is communicating.
- A request/response pair would consist of about 1496 bytes in each direction i.e. approximately 3000 bytes total (3k).

## 15.4 Supported Headend Optical Modules

Supported Headend Optical Modules				
Platform	Model Name	Product Description	AlphaXD Version Initial Support	Comments
GX2	GX2-CM100B*	GX2 Chassis Control Module	2.4	Integrated
GX2	GX2-PSAC10*	GX2 AC Power Supply	2.4	Integrated
GX2	GX2-PSDC10*	GX2 DC Power Supply	2.4	Integrated
GX2	GX2-LM1000B	GX2 1310 nm Transmitter	2.4	Integrated
GX2	GX2-LM1000E	GX2 1310 nm Transmitter – RoHS Version	2.4	Integrated
GX2	GX2-LC1000E	GX2 1310 nm eCWDM Transmitter	2.4	Integrated
GX2	GX2-RX200BX2	GX2 Dual Return Receiver	2.4	Integrated
GX2	GX2-RX200BX4	GX2 Quad Return Receiver	2.4	Integrated
GX2	GX2-EM870	GX2 1550 nm Broadcast Optical Transmitter	3.1	Integrated
GX2	GX2-EM1000	GX2 1550 nm Broadcast Optical Transmitter	3.1	Integrated
GX2	GX2-RX1000B	GX2 Forward Path Receiver	3.1	Integrated
GX2	GX2-OA100B13, 16, 18	GX2 EDFA Optical Amplifiers (Optical powers 13 dBm, 16 dBm, and 18 dBm)	3.1	Integrated
GX2	GX2-OA100B20, 22, 21X2	GX2 EDFA Optical Amplifiers (Optical powers 20 dBm, 22 dBm, and 21x2 dBm)	3.1	Integrated
GX2	GX2-RSW1000B	GX2 Forward Path RF Switch	3.1	Integrated
GX2	GX2-RSW200B	GX2 Return Path RF Switch	3.1	Integrated
GX2	GX2-DM870	GX2 Forward Path Narrowcast Transmitter	3.1	Integrated
GX2	GX2-DM200	GX2 Return Path Transmitter	3.1	Integrated
GX2	GX2-DM1000	GX2 Forward Path Narrowcast Transmitter	3.1	Integrated
GX2	GX2-OSW10B	GX2 Optical Switch	3.1	Integrated
GX2	N2U-OA300	2RU Erbium Doped Fiber Amplifier for PON (non-GX2)	3.1	Integrated
GX2	GX2-DRR-2X	GX2 2X Digital Return Path Receiver	3.2	Integrated
GX2	GX2-DRR-3X	GX2 3X Digital Return Path Receiver	3.1	Integrated
GX2	GX2-DRT-2X	GX2 2X Digital Return Path Transmitter	3.2	Integrated
GX2	GX2-DRR-4X	GX2 4X Digital Return Path Transmitter	3.2	Integrated
GX2	GX2-DRT-4X	GX2 4X Digital Return Path Transmitter	3.2	Integrated
GX2	GX2-DM2000	GX2 Direct Modulation Transmitter	4.1	Integrated
GX2	GX2-OA508B21	GX2 EDFA Optical Amplifier	4.1	Integrated
GX2	GX2-RX085BX4	GX2 High Sensitivity Receiver - 85 MHz	4.1	Integrated
GX2	GX2-EA1000B	GX2 Electro Absorption Transmitter - Analog - Rev B	4.1	Integrated
GX2	GX2-EA1000C	GX2 Electro Absorption Transmitter - Analog - Rev C	5.0	Integrated
GX2	GX2-GS1000	GX2 Electro Absorption Transmitter - Digital	5.0	Integrated
GX2	GX2-EML1000	GX2 External Modulation Light Transmitter	5.0	Integrated
GX2	GX2-DRR-2X-85	GX2 2x85 MHz Digital Return Receiver	5.0	Integrated

Table 15-3, Supported Headend Optical Modules

## 15.0 System Recommendations and Troubleshooting, continued

Supported Headend Optical Modules				
Platform	Model Name	Product Description	AlphaXD Version Initial Support	Comments
GX2-LITE	GX2-HSG-LITE	GX2 2RU Chassis (supports 3 single wide GX2 modules)	3.1	Integrated
Rack Mount Optics	N1U-OA500	1RU Erbium Doped Fiber Amplifier (non-GX2)	3.2	Integrated
Rack Mount Optics	N2U-OA300	2RU PON Erbium Doped Fiber Amplifier (non-GX2)	3.2	Integrated
GX2	GX2-EA1000	GX2 Electro Absorption Transmitter - Analog	3.2	Integrated
GX2	GX2-DUALDRR-2X	GX2 2X Digital Return Path Receiver	3.2	Integrated
GX2	GX2-LM1000S	GX2 1310 nm Transmitter	3.2	Integrated
GX2	N2U-OA200	2RU Fiber Amplifier (non-GX2)	3.2	Integrated
GX2	GX2-RX1000	GX2 1310 Laser Receiver	3.2	Integrated
GX2	GX2-RFA1000	GX2 Forward Path RF Amplifier	3.2	Integrated
GX2	GX2-RFA1000B	GX2 Forward Path RF Amplifier	3.1	Not Verified
Prisma	Prisma II XD Chassis	Chassis	5.3	Integrated
Prisma	Prisma II P2-HD-LN-RXR	Reverse Receiver	5.3	Integrated
Prisma	Prisma II P2-HD-RXR	Reverse Receiver	5.3	Integrated
Prisma	Prisma II HDTx	Laser Transmitter	5.3	Integrated
Prisma	Prisma II P2-HD-EDR-PRX85	Laser Receiver	6.0	Integrated
Prisma	Prisma II P2-HD-RXF	Laser Receiver	6.0	Integrated
Prisma	Prisma II 1550Tx	Laser Transmitter	6.0	Integrated
Prisma	Prisma II P2-HD-EDFA-GF	Optical Amplifier	6.0	Not Verified
Prisma	Prisma II P2-HD-13TxM-10-SA-F	Laser Transmitter	6.1	Integrated
Prisma	Prisma II P2-HD-EDFA-GF-20L-SA	Optical Amplifier	6.1	Integrated
Prisma	Prisma II P2HD1.215TXM - 12dBm ITU 44	Laser Transmitter	6.1	Integrated
Prisma	HDTxQ 10dBm ITU 29 (1024)	Laser Transmitter	6.5	Not Verified
Prisma	HDTxSQ-FS 10dBm ITU 35 (1024)	Laser Transmitter	6.5	Not Verified
Prisma	P2HD1.215TXQP 12dBm ITU 39 (1062)	Laser Transmitter	6.5	Not Verified
Prisma	P2HD1.2G15TX 10dBm ITU 24 (1065)	Laser Transmitter	6.5	Not Verified
Prisma	P2HD1.2G15TX 10dBm ITU 26 (1069)	Laser Transmitter	6.5	Not Verified
Prisma	P2-HD-RXR-HG (2011)	Laser Receiver	6.5	Not Verified
Prisma	P2-HD-RXR (2014)	Laser Receiver	6.5	Not Verified
Prisma	P2-HD-RXR (2019)	Laser Receiver	6.5	Not Verified
Prisma	P2-EDR-RX (2026)	Laser Receiver	6.5	Not Verified
Prisma	P2-HD-RXR-STD-300M (2032)	Laser Receiver	6.5	Not Verified
Prisma	HD EDFA BCST 20.0 (3022)	Optical Amplifier	6.5	Not Verified
Prisma	P2-HD-EDFA-VGF-1x21-SA 21.0 (3027)	Optical Amplifier	6.5	Not Verified
Prisma	1550nm Optical Transmitter XL 10GHZ PBG89 SA ITU 39 (1002)	Laser Transmitter	6.5	Not Verified
Prisma	1550nm Optical Amplifier 20dBm (3014)	Optical Amplifier	6.5	Not Verified
Prisma	1550nm Optical Amplifier 1x17.00 (3024)	Optical Amplifier	6.5	Not Verified

**Table 15-3, Supported Headend Optical Modules, Continued**

## 15.5 Supported HMTS Devices

Supported HMTS Devices				
Platform	Model Name	Product Description	AlphaXD Version Initial Support	Comments
HMS Transponder	LL-HMS-SG4	HMS SG4 Transponder via LL-HMTS	3.1	Integrated
HMS Transponder	LL-HMS-SG2	HMS SG2 Transponder via LL-HMTS	3.1	Integrated
HMS Transponder	LL-HMS-SG1	HMS SG1 Transponder via LL-HMTS	3.1	Integrated
Headend Controller	LL-HMTS	HMTS Headend Controller	3.1	Integrated

Table 15-4, Supported HMTS Devices

## 15.6 Troubleshooting

### AlphaXD Startup Issues

#### AlphaXD Startup Fails After Server Reboot

In some Windows 2008/2012 Server configurations, Oracle 12c database services do not completely start up after a system reboot resulting in a failure during AlphaXD start up. The console window may display these errors.

```

C:\Windows\System32\cmd.exe
SQLException while getting database connection. Check if database daemon is running
java.sql.SQLException: Io exception: Connection refused(DESCRIPTION=(TMP=)<USNNU
M=168821248><ERR=12528><ERROR_STACK=(ERROR=(CODE=12528><EMFI=4)))
  at oracle.jdbc.dbaccess.DBError.throwSQLException(DBError.java:134)
  at oracle.jdbc.dbaccess.DBError.throwSQLException(DBError.java:179)
  at oracle.jdbc.dbaccess.DBError.throwSQLException(DBError.java:333)
  at oracle.jdbc.driver.OracleConnection.<init>(OracleConnection.java:404)
  at oracle.jdbc.driver.OracleDriver.getConnectionInstance(OracleDriver.java:468)
  at oracle.jdbc.driver.OracleDriver.connect(OracleDriver.java:314)
  at java.sql.DriverManager.getConnection(Unknown Source)
  at java.sql.DriverManager.getConnection(Unknown Source)
  at jdbc.CreateSchema.instantiateConnection(CreateSchema.java:146)
  at jdbc.CreateSchema.init(CreateSchema.java:84)
  at com.adventnet.nms.startnms.NmsMainBE.main(NmsMainBE.java:341)
Exiting Web NMS
Press any key to continue . . .
    
```

Fig. 15-1, Oracle Database Errors

This is an Oracle issue and Alpha recommends two approaches to resolving it.

- Edit the listener.ora file (which may resolve the problem on some system configurations).
- Start the Oracle 12cR1 database service manually after server reboot, if editing the listener.ora file does not resolve the problem.

## 15.0 System Recommendations and Troubleshooting, continued

### Edit the listener.ora File

To edit the listener.ora file:

1. Open the file oracle\oracxd\NETWORK\ADMIN\listener.ora as an administrator in a text editor.

```
# listener.ora Network Configuration File:
```

```
D:\oracle\oracxd\network\admin\listener.ora
```

```
# Generated by Oracle configuration tools. SID_LIST_LISTENER =
```

```
(SID_LIST = (SID_DESC =
```

```
(SID_NAME = PLSExtProc)
```

```
(ORACLE_HOME = D:\oracle\oracxd)
```

```
(PROGRAM = extproc)
```

```
)
```

```
)
```

```
# listener.ora Network Configuration File:
```

```
D:\oracle\oracxd\network\admin\listener.ora
```

```
# Generated by Oracle configuration tools. SID_LIST_LISTENER =
```

```
(SID_LIST = (SID_DESC =
```

```
(GLOBAL_DBNAME = webnmsdb) (ORACLE_HOME = D:\oracle\oracxd) (SID_NAME
```

```
= webnmsdb)
```

```
)
```

```
(SID_DESC =
```

```
(SID_NAME = PLSExtProc) (ORACLE_HOME = D:\oracle\oracxd) (PROGRAM = extproc)
```

```
)
```

```
)
```



## 15.0 System Recommendations and Troubleshooting, continued

1. Edit the file according to the before and after examples, below. The lines to add and change are bolded in the “File after edit” as shown below.

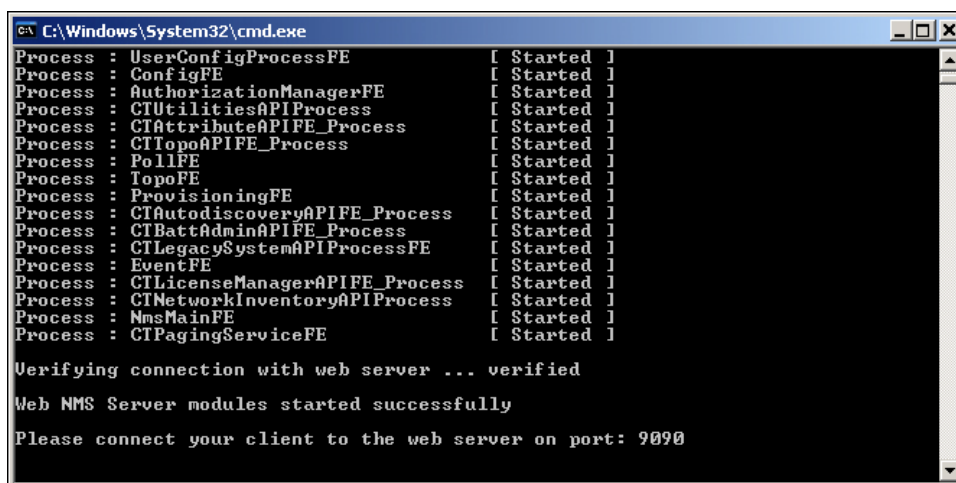
File before edit.

File after edit

### Starting the Oracle 12cR1 Database Service Manually

If editing the listener.ora file does not resolve the problem, the Oracle 12cR1 database service must be restarted manually after every server reboot.

1. From the Start menu, select Start > Run.
2. In the Run window, type cmd.
3. Click OK. The DOS command window displays.
4. In the DOS command window, type: net stop OracleServiceWEBNMSDB.



```
C:\Windows\System32\cmd.exe
Process : UserConfigProcessFE [ Started ]
Process : ConfigFE [ Started ]
Process : AuthorizationManagerFE [ Started ]
Process : CTUtilitiesAPIProcess [ Started ]
Process : CTAttributeAPIFE_Process [ Started ]
Process : CTTopoAPIFE_Process [ Started ]
Process : PollFE [ Started ]
Process : TopoFE [ Started ]
Process : ProvisioningFE [ Started ]
Process : CTAutodiscoveryAPIFE_Process [ Started ]
Process : CTBattAdminAPIFE_Process [ Started ]
Process : CTLegacySystemAPIProcessFE [ Started ]
Process : EventFE [ Started ]
Process : CTLicenseManagerAPIFE_Process [ Started ]
Process : CTNetworkInventoryAPIProcess [ Started ]
Process : NmsMainFE [ Started ]
Process : CTPagingServiceFE [ Started ]

Verifying connection with web server ... verified
Web NMS Server modules started successfully
Please connect your client to the web server on port: 9090
```

Fig. 15-2, Successful AlphaXD Restart

5. Press Enter. The following message displays: “The OracleServiceWEBNMSDB service was stopped successfully”.
6. Type net start OracleServiceWEBNMSDB.
7. Press Enter. The following message displays: “The OracleServiceWEBNMSDB service was started successfully”.
8. Restart the AlphaXD server application. Figure 13-2 shows a successful AlphaXD server restart.

## Errors Running Reports

When running AlphaXD on a “headless” Solaris server (a server that does not include graphics capability), graphics drivers for report generation are not loaded during installation. Running a report may result in an error. Restart AlphaXD to resolve this problem.

## Database Backup Failures

If the Automated or Manual Backups fail to properly backup the database information navigate to the AlphaXD/logs directory. Each backup attempt is logged to the most recent CTBackup.txt log file. Within the CTBackup.txt file, a second file will be identified which will show the root cause error. Confirm that the file is shared or has the correct security access to allow AlphaXD to write to the destination drive and directory.





---

Worldwide Corporate Offices

**North America**

Tel: +1 360 647 2360  
Fax: +1 360 671 4936

**Europe**

Tel: +49 9122 79889 0  
Fax: +49 9122 79889 21

**Latin America**

Tel: +561 792.9651  
Fax: +561 792.7157

**Asia Pacific**

Tel: +852 2736.8663  
Fax: +852 2199.7988